



PÉNZÜGYI SZERVEZETEK  
ÁLLAMI FELÜGYELETE  
HUNGARIAN FINANCIAL  
SUPERVISORY AUTHORITY

Guide 1/2007 of the Hungarian Financial Supervisory Authority  
on the protection of the information technology systems  
of financial institutions

Budapest, October, 2007.

## **TABLE OF CONTENTS**

1. THE OBJECTIVE OF ISSUING THIS GUIDE .....	3
2. THE INTENDED USERS OF THIS GUIDE.....	3
3. RELATED REGULATIONS .....	3
4. EFFECTIVE DATES.....	4
5. APPLICATION.....	4
6. THE CONNECTION BETWEEN IT SECURITY AND IT GOVERNANCE .....	5
7. The COBIT (Control Objectives for Information and Related Technology) OPEN STANDARD ....	5
7.1 THE HISTORY OF COBIT.....	5
7.2 AN OVERVIEW OF THE COBIT MANUALS .....	6
8. The interpretation of legal requirements and the associated supervisory expectations .....	7
ANNEX I: LEGAL REQUIREMENTS AND THE CORRESPONDING CHAPTERS IN COBIT .....	26
ANNEX II: LIST OF COBIT MANUALS BY GROUP, AVAILABILITY .....	30
11.1. IT GOVERNANCE .....	30
11.2. SIMPLIFIED COBIT FOR BEGINNERS .....	30
11.3. BASIC COBIT BOOKS.....	30
11.4. REALIZING THE OBJECTIVES OF COBIT.....	31
11.5. COBIT ON THE INTERNET (INCLUDING CONTROL PRACTICES) .....	31
11.6. OTHER COBIT PUBLICATIONS .....	31
ANNEX III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS.....	32
ANNEX IV: INCOMPATIBLE DUTIES AND RESPONSIBILITIES IN COBIT .....	50

## **1. THE OBJECTIVE OF ISSUING THIS GUIDE**

By issuing this guide the Hungarian Financial Supervisory Authority wishes to help reinforce the protection of the information technology systems of financial institutions governed by the regulations of the industry (Cife., Cma., Ifcd., Pfa., Vfa., Insa.). More specifically this manual helps

- financial institutions better comply with legal requirements and
- create a consistent interpretation and approach among the financial institutions and the Supervisory Authority

by

- pointing out the close link between IT security and the quality of IT governance, and by
- promoting the more widespread use of the COBIT (Control Objectives for Information and Related Technology) information governance tool in Hungary.

In this Guide the references to „CobiT” apply to version 4.1 of CobiT, that is the latest version. Fulfilling the requirements specified in this guide serves the core interests of the financial institutions and their customers therefore during its audits the Supervisory Authority examines the compliance with these requirements and takes significant discrepancies into account in the evaluation of the organization.

## **2. THE INTENDED USERS OF THIS GUIDE**

In the financial institutions

- executives responsible for any IT area,
- professionals dealing with IT security,
- professionals analyzing operating risks,
- IT auditors,
- IT professionals,
- the users of the IT systems.

## **3. RELATED REGULATIONS**

After the amendments of 2004

- Act CXII of 1996 on Credit Institutions and Financial Enterprises (Cife.),
- Act LXXXII of 1997 on Private Pensions and Private Pension Funds (Pfa.),
- Act XCVI of 1993 on Voluntary Mutual Insurance Funds (Vfa.) and
- Act CXX of 2001 on the Capital Market (Cma.) that was annulated and incorporated by the
- Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities (Ifcd.)

(hereinafter collectively referred to as sectoral acts)

set essentially identical requirements<sup>1</sup> regarding the protection of the information technology systems of financial institutions. Act LX of 2003 on Insurance Institutions and the Insurance Business (Insa.) does not yet specify similar requirements for the insurance sector, but the Hungarian Financial Supervisory Authority has already initiated the codification and believes it to be useful to follow the instructions of this manual.

Institutions falling within the jurisdiction of Government Decree No. 283/2001. (XII. 26.) on the necessary personnel, equipment, technical and security facilities required for the provision of investment and commodity exchange services, securities safe-keeping and securities custody

---

<sup>1</sup> There are some minor differences, but those do not concern this guide.

services, and clearing services must comply with the requirements of the Decree even after the legislative amendments of 2004.

#### **4. EFFECTIVE DATES**

The following table lists the dates from which the legal requirements introduced by the amendments of the acts in 2004 apply.

<b>Act</b>	<b>Section regarding the protection of the IT system</b>	<b>Date when the legal requirement becomes effective</b>
Act CXII of 1996 (Cife.)	Section 13 (C), introduced by act XXII of 2004	Applicable to <b>financial institutions that did not fall within the jurisdiction of Government Decree No. 283/2001. (XII. 26.)</b> on the necessary personnel, equipment, technical and security facilities required for the provision of investment and commodity exchange services, securities safe-keeping and securities custody services, and clearing services; but were already operating when this Act entered into force or had submitted a request for foundation license before the Act entered into force <b>from November 1, 2005. Financial institutions that</b> were operating on 05.06.2004 and <b>fall within the jurisdiction of Government Decree No. 283/2001. (XII. 26.)</b> on the necessary personnel, equipment, technical and security facilities required for the provision of investment and commodity exchange services, securities safe-keeping and securities custody services, and clearing services <b>must comply</b> with the provisions of section 13 (C) of the Cife. <b>from January 1, 2005.</b>
Act LXXXII of 1997 (Pfa.)	Section 77 (A) introduced by Act CI of 2004	01.01.2006.
Act XCVI of 1993 (Vfa.)	Section 40 (C) introduced by Act CI of 2004	01.01.2006.
Act CXX of 2001 (Cma.)	Section 101/A introduced by act XXII of 2004 The pertinent section has been annulated by Ifcd. and has been incorporated it into Section 12	<b>Service providers</b> and clearing organizations <b>that</b> were operating on 05.06.2004 and <b>fall within the jurisdiction of Government Decree No. 283/2001. (XII. 26.)</b> on the necessary personnel, equipment, technical and security facilities required for the provision of investment and commodity exchange services, securities safe-keeping and securities custody services, and clearing services must comply with the provisions of section 13 (C) of the Cife. <b>from January 1, 2005</b> , that was annulated by Ifcd..
Act CXXXVIII of 2007 (Ifcd.)	Section 12 introduced by Act CIII of 2008	Information security requirements prescribed in Ifcd. must be met from the date defined in Cma..

It is recommended to comply with the provisions of this guide from the day after the guide is published.

## **5. APPLICATIONS**

This manual applies to the IT systems operated by financial institutions falling within the jurisdiction of the Cife., the Cma., the Ifcd., the Pfa. and the Vfa. This guide supersedes guide 3/2005.

According to section 65 (b) of the Insa.: “The requirements of authorizing and conducting insurance activities include: b) the establishment of a continuous record-keeping, data processing and reporting system, an information and auditing system for reducing operating risks, and a contingency plan”. Additionally, according to section 66 (1) (a) the insurer must be able to “provide the personnel and equipment required to begin the operation”. Even though the Insa. does not provide detailed instructions regarding the fulfillment of the above requirements, we make the following recommendations in order to help comply with the requirements.

Even though there are no mandatory requirements applicable to the insurance sector, the Supervisory Authority recommends that institutions falling within the jurisdiction of the Insa. also follow the instructions of this guide regarding the protection of their IT systems.

## **6. THE CONNECTION BETWEEN IT SECURITY AND IT GOVERNANCE**

In today’s globalized world the new possibilities offered by information technology are offset by the appearance of previously unknown operating risks threatening IT security. Trying to ensure IT security only by introducing *security* measures or *security* standards will not be effective. Economic information security serving business objectives may more easily be achieved using internationally renowned *IT governance* practices that focus on the orderly, controlled and secure development, maintenance and operation of the IT systems.

CobiT 4.1 has been added another chapter (IT Governance - ME4) that supports IT governance demonstrated by the following figure by providing a framework that ensures that:

- information technology should be in line with business processes,
- information technology enables attaining business objectives and maximize benefits,
- IT resources should be use responsibly,
- IT risks should be managed adequately.



- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

• **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.<sup>2</sup>

## **7.7. The COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY) OPEN STANDARD**

COBIT is the open standard and an increasingly widely renowned *tool* of IT *governance* worldwide, which integrates information, information technology and the practices for controlling the associated risks into a single system. It builds on the previous achievements of IT governance as well as the methodology of modern corporate governance. It emphasizes that information technology must serve the business objectives. By using COBIT, business executives, professionals managing operating risks, IT specialists and auditors can cooperate efficiently through using the same approach and terminology. These qualities make COBIT especially well suited to be used in financial institutions. The legal requirements regarding the protection of the IT systems of financial institutions and the corresponding parts of COBIT are listed in Annex I. Due to the different origin, creators, purpose, users etc. of the two resources the matching is not exact or indisputable, but aims to adapt and extend the regulations to fully cover the COBIT standard created and maintained based on international practices. Due to the inexact matching certain parts of COBIT appear in more than one place in the regulations.

### **7.1 THE HISTORY OF COBIT**

The backbone of the research behind the standards is the Information Systems Audit and Control Association (ISACA), which has approximately 35,000 members. COBIT is published by ISACA's peer organization, the IT Governance Institute (USA), established in 1998. So far there have been published four editions of COBIT: the first in 1996, the second in 1998, the third in 2000 and the fourth in 2007, they also published a simplified version as an introduction. COBIT is under continuous development. In 2003 the internet edition was published, along with a simplified introductory version. COBIT's elaborate auditing methodology significantly contributes to its increasing international recognition. The Supervisory Authority's IT supervisors are

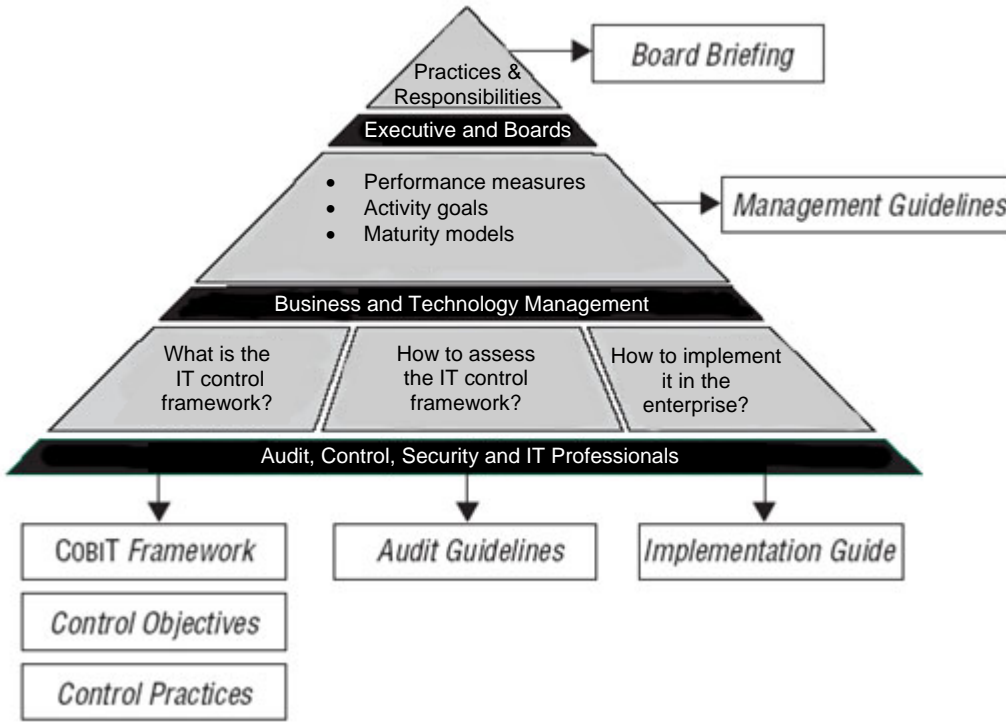
---

<sup>2</sup> CobiT 4.1 © 2007 IT Governance Institute. (p.6)

members of the ISACA and have been reviewing the IT systems of financial institutions using COBIT approach. Their current investigation methodology is also based on COBIT.

## **7.2 AN OVERVIEW OF THE COBIT MANUALS**

Today IT governance, and its tool, COBIT are documented in several technical books. The following diagram helps understanding the structure of the basic books.



For a listing of COBIT manuals by thematic groups and availability information see Annex II.

## **8. THE INTERPRETATION OF LEGAL REQUIREMENTS AND THE ASSOCIATED SUPERVISORY EXPECTATIONS**

Below we provide additional notes to the interpretation of certain legal requirements, but we emphasize that **our main objective is to facilitate the usage of the CobiT system, which uses proven procedures and methods used in the practice of IT governance**. Parts of the CobiT literature are also available in Hungarian (e.g. <http://www.isaca.hu>). We have focused the explanation of some of the selected legal requirements on answering previous questions. The explanations of the abbreviations used in the regulations can be found in Annex III.

The protection of the IT system is always the responsibility of the management of the financial institution. This responsibility may not be shifted to others (but can be delegated under the right circumstances). The financial institution can also commission external organizations (e.g. via outsourcing) to create and operate the protection system and to supervise the operation, but even then ensuring the compliance of the control environment remains the responsibility of the management.

1. **Pfa. section 77 (A) (1), Vfa. section 40 (C) (1), Ifcd. section 12 (1) – (2), Cife. section 13 (C) (1)**

***The financial institution must create a regulation system for the IT system used in its operations and must provide protection for the IT system in proportion to the risks. The regulation system must specify the information technology requirements as well as the assessment and management of security risks in planning, procurement, operation and auditing.***

With regards to the “regulating system” the Supervisory Authority recommends that the financial institutions create and continuously update the major IT regulations. The Supervisory Authority also recommends that the financial institutions design the hierarchy of the regulation system using the “directives – policies – procedure systems” structure. There are no requirements regarding the quantity or format of the regulations, but they must correspond to the organization’s daily operations. The regulation system must specify the effective date of the regulations (when a modified policy will enter into force), their level of actualization, scope, and degree of familiarity. The regulation system must include at least the IT security policy, the IT security regulation, the operational rules of the IT system, the management of accessibility and permissions, the anti-virus protection regulation, the rules of backup and archival, the methods of analyzing and managing risks (documented methodology used to analyze the risks), change management, the process and technical requirements of formulating and issuing regulations, and the requirements of availability and awareness among employees.

The management of the financial institution must review the “directives, policies and procedure systems” regularly (at least once a year) – or when there are significant changes in the operating environment – and modify them as necessary. The management must also examine if the directives in use are up to date, and must create an appropriate system and procedure for periodically reviewing and approving standards, principles, objectives, directives, and procedures.

IT users must be familiarized with the security rules applicable to them. It must be made sure that the every user fully understands the importance of the security rules. Education must convey the message that IT security is in the interest of the entire financial institution – and thus every employee – and everybody is responsible for it.

With regards to „information technology requirements” the Supervisory Authority recommends consulting the CobiT manuals mentioned in the introduction as well as this guide. In order to manage its IT systems the financial institution needs to create a control environment covering the major areas specified by law and used by CobiT as the foundations of the system.

In case of outsourcing the policies are created and amended in accordance with the contract

(either by the financial institution or the service provider), but both parties must ensure that the relevant policies are enforced in their organization and that their users are properly informed.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement of the law: “PO6 – Communicate Management Aims and Direction”, “ME3 – Ensure regulatory compliance”, and “A11 – Identify Automated Solutions”.*

**2. Pfa. section 77 (A) (2), Vfa. section 40 (C) (2), Ifcd. section 12 (3), Cife. section 13 (C) (2)**

***The financial institution must review and update the security risk analysis of the IT system as necessary, but at least once every two years.***

In order to manage the risks of IT security it is recommended to select a method of risk analysis that allows for a systematic assessment and management of IT security risks. The assessment, analysis and management of the risks must be adapted to the most critical business processes of the financial institution and must cover planning, development, procurement, operation, outsourcing and auditing. The creation of work documents and the presentation of the protective measures against each managed risk are important for assessing the risks and evaluating the adequacy of the risk analysis. In case of outsourcing the risk analysis must cover all the system components of the outsourcing partner associated with the provided service, otherwise the compliance of the service cannot be ensured.

The financial institution must lay down the requirements of regular risk analysis in its internal policy and comply with the requirements (the methodology must be described in the internal policy to provide information, allow verification, and enable repeated performance). The assessment and analysis of the risks must be performed after new systems are installed, with regards to changes in the environment, and with predefined regularity (annually, if possible). The risk analysis must cover every system (both software and hardware).

*The Supervisory Authority recommends consulting the following chapter of CobiT to help interpret this requirement of the law: “PO9 – Assess Risks”.*

**3. Pfa. section 77 (A) (3), Vfa. section 40 (C) (3), Ifcd. section 12 (4), Cife. section 13 (C) (3)**

***The organizational and operational rules; the policies on responsibility, recordkeeping, and providing information; and the rules and requirements of verification built into the process must be specified with regards to the security risks arising from the use of information technology.***

With regards to the “organizational and operating rules” and “the policies on responsibility, recordkeeping, and providing information” the Supervisory Authority recommends that the financial institutions define, document, and continuously maintain the structure and relationships of their IT department (organizational and operational guidelines / charter, organizational charts, job descriptions etc.). The duties and responsibilities must be clearly defined, while avoiding conflicts of interest (incompatibility – see Annex IV). Duties and responsibilities must be separated so that no single person is responsible for the governance, execution and control of all the critical procedures, as this would enable malfeasance. The most important conflict of interest is properly separating the duties of the system administrator, developer, and operator; and creating the control function of the software librarian in the IT organization. The management must ensure that every employee of the organization understands his/her duties and responsibilities regarding the information systems. All the employees must have the authority to perform their duties, and must be informed about the extent of their responsibility for control and security.

The management must appoint an “IT security manager” who is responsible for the physical and logical safety of the organization’s IT assets, and reports directly to the senior executive of the organization. The management must create a procedure to officially appoint the owners and managers of the data, and must make sure that every IT asset (data and system) has an appointed owner who makes decisions about classification and access levels. In case of records systems the data owner is usually not an IT specialist, but the head of the functional area involved (accounting, book-keeping etc.). The data owner of the IT service applications is an IT specialist (Windows domain system, Active Directory, data transfer network control application, log collecting and analyzing application etc.).

The necessary number of employees must be reviewed periodically, so that there are a sufficient number of properly qualified employees in the IT department even in case of substitution. The management must specify and regularly update the job descriptions of IT employees. The job descriptions need to clearly define authorities and responsibilities, including the qualifications and experience required for the job. In case of financial institutions the IT qualifications and experience required for each job must be specified in the internal policy, not in the job description.

In case of outsourcing the service provider (outsourcing partner) must also meet the legal requirements applicable to the financial institution in the area affected by the outsourcing.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help interpret this requirement of the law: “PO4 – Define the IT Organization and Relationships” and “PO7 – Manage Human Resources”.*

**4. Pfa. section 77 (A) (4), Vfa. section 40 (C) (4), Ifcd. section 12 (5), Cife. section 13 (C) (4)**

***The financial institution must establish and operate an IT control system monitoring the secure operation of the IT system.***

The IT control system does not refer to a single application, but rather the establishment and operation of a control environment monitoring IT governance activities, which includes all the directives, processes, procedures, practices, daily routines, devices, human resources and organizational structures that make it possible.

The management must evaluate (based on the performance indicators and key success criteria specified in the internal and external service level agreements) the services provided by the IT department in key applications, and compare them to the planned service levels. The performance of the IT department must be evaluated regularly. The management must periodically examine how much the users are satisfied with the services provided by the IT department. Reports need to be submitted to the management on the progress made towards realizing the objectives of the organization and the steps taken to reduce risks. The management must also evaluate the effectiveness of internal auditing procedures integrated into the organization's regular procedure system. The management must then take the necessary steps based on the findings of these reviews.

The internal auditing procedures are effective if the preventive controls quickly discover and correct the errors and contradictions before they could influence the normal operation of the system or the provision of services.

Operating security and internal auditing must be reviewed regularly. It must be examined – via self evaluation or independent auditing – whether the security and internal auditing procedures comply with the applicable security and internal auditing requirements. As part of its supervisory duties the management must discover the vulnerable points and the security problems.

Prior to introducing critical new IT services the management must get an expert certification / attestation / evaluation of the security and internal auditing procedures of the systems involved. Following the introduction of the new service the previously acquired expert certification / attestation / evaluation will need to be renewed periodically. Prior to using the services of an external service provider (outsourcing) the management must get an expert certification / attestation / evaluation of the security and internal auditing procedures used by the service provider. Following the introduction of the new service the previously acquired expert certification / attestation / evaluation will need to be renewed periodically (after any significant changes of the IT architecture). The independent expert can be the internal auditor of the financial institution, is he/she has the professional and technical knowledge, abilities and experience necessary to effectively and efficiently perform such tasks.

The management must design an auditing policy in which it describes the duties, authority, reporting obligations and accountability of the auditors. This policy must be reviewed periodically. The auditor must be independent from the department it audits (actual and perceived independence) to be able to give an objective analysis.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help interpret this requirement of the law: "ME1 – Monitor and Evaluate IT Performance", "ME3 – Ensure Regulatory Compliance", "ME2 – Monitor and Evaluate Internal Control" and "ME4 – Provide IT Governance".*

**5. Pfa. section 77 (A) (5), Vfa. section 40 (C) (5), Ifcd. section 12 (6), Cife. section 13 (C) (5)**

*The measures described in paragraphs a)-g) must be introduced based on the results of the security risk analysis and depending on the significance of the security risks.*

The requirements listed in this section must be fulfilled based on the results of the risk analysis mentioned in paragraph (2) of the sectoral acts.

**6. Pfa. section 77 (A) (5) (a), Vfa. section 40 (C) (5) (a), Ifcd. section 12 (6) (a), Cife. section 13 (C) (5) (a)**

***Based on the results of the security risk analysis and depending on the significance of the security risks the most important components of the system (devices, processes, persons) must be clearly identified and logged.***

A comprehensive and up to date record of the IT devices and systems (hardware and software, applications installed on servers and workstations, technological system diagrams and data link diagrams etc.) must be available (this is the basis of the previously mentioned risk analysis). The management of the IT department must ensure that the configuration records contain the current status of each item, along with any previous changes. The changes of the configuration components must also be tracked in accordance with the change management policy (e.g. new components, “under development”, etc.). The proper procedures must ensure that only authorized and identifiable configuration components can be added to the (configuration) inventory upon procurement and removed from the inventory upon disposal (sale). The configuration maintained by the IT department records and the consistency of its entries must be checked regularly. Software must be recorded and used with the appropriate license.

In case of outsourcing the record must also include all the assets at the service provider (outsourcing partner) that is in any way involved in providing the service to the financial institution.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help interpret this requirement of the law: “DS9 – Manage the Configuration”.*

**7. Pfa. section 77 (A) (5) (b), Vfa. section 40 (C) (5) (b), Ifcd. section 12 (6) (b), Cife. section 13 (C) (5) (b)**

***Based on the results of the security risk analysis and depending on the significance of the security risks the self-defense of the IT security system, and the inspections and procedures ensuring that the system’s critical components are fully and securely protected must be implemented.***

It must be ensured that the security measures of the IT systems are in line with the business / organizational requirements. This includes IT risk analysis; creating and implementing an IT security plan, and updating it in accordance with the changes of the IT configuration; evaluating the effects of requested changes on IT security; supervising the implementation of the IT security plan; and adapting the IT security procedures to other policies and procedures.

The usage of and access to IT resources must be limited using procedures that check identification, authentication and authorizations (even within the IT department). Unauthorized user access must be prevented. The management must create procedures that verify – in accordance with the IT security policy – the authenticity of the other party forwarding the transactions, and which can be used to verify the authenticity of the transactions and the identity of the users logging into the system. Where necessary it must be ensured that neither party is able to deny the transactions (nonrepudiation). Verification procedures must ensure that the parties cannot deny initiating, accepting, starting and completing transactions. It must be ensured that the data of confidential transactions is exchanged through trusted channels. Confidential information includes information about security procedures, the information of confidential transactions, passwords and cryptographic keys. All hardware and software associated with security procedures must be protected from unauthorized access in order to safeguard their integrity and their secret codes. Additionally, the organization must keep the structure of the security system confidential. It cannot build its security on the confidentiality of the security system’s plan.

The management must ensure the integrity of the cards and other physical devices used to authenticate and store financial and other confidential information, taking into account the associated devices, equipment, employees and validity checking methods.

Appropriate measures must be introduced to provide physical protection for the IT assets and control the access to the assets, including the use of IT assets outside the premises. The physical protection and access control must be extended to the cables connecting the components of the system, the supporting services (e.g. sources of electricity), the storage media used for backups, all other components required for the operation of the system. Only authorized personnel may be granted access privileges. The appropriate procedures must be used to ensure that third parties, i.e. persons not in the group operating the IT department can only enter key premises (server room, communication switching units etc.) accompanied by a member of the group. Visits must be logged and the log needs to be checked periodically. The management of the IT department must ensure that appropriate protective procedures are in place against environmental hazards (e.g. fire, dust, electricity, high temperature or humidity etc.). The management must periodically assess the need for uninterrupted power supplies and generators to ensure the safe operation of critical applications.

In case of outsourcing the service provider (outsourcing partner) must meet the above requirements.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement of the law: “DS5 – Ensure Systems Security”, “DS12 – Manage Facilities” and “ME2 – Ensure Regulatory Compliance”.*

**8. Pfa. section 77 (A) (5) (c), Vfa. section 40 (C) (5) (c), Ifcd. section 12 (6) (c), Cife. section 13 (C) (5) (c)**

***Based on the results of the security risk analysis and depending on the significance of the security risks the system’s user administration (access levels, unique authorizations, approvals, responsibilities, access logging, extraordinary events) must be regulated, verifiable and regularly checked.***

The management must create procedures that ensure that the appropriate action is taken in time regarding the requests, recording, issuing, suspension, and cancellation of user authorizations (policy). An official authorization procedure must be introduced, in which the owner of the data and the system authorizes the access (access levels). The security of third party access must also be specified in a contract, along with the requirements of administration and confidentiality. In case of outsourcing the contract established between the parties must include provisions regarding the risks and the security procedures and checks associated with the information systems and networks. Access privileges must be reviewed and confirmed periodically (recommended at least quarterly, or after any significant changes in the application, organizational or operating structure).

The IT security manager mentioned in paragraph 3 above must ensure that security related events are logged, that all the system immediately notifies all the concerned internal and external parties of any *signs of security violation*, and that necessary steps are taken in response to such signs. The IT security manager must make sure that events concerning the operation of the security system and the violations of the security requirements are recorded, reported and examined in order to detect and identify unauthorized access and access attempts.

The management must create procedures that require the owners of the data to formally classify the information by level of confidentiality, in accordance with the requirements of the data classification system (access levels based on user functions).

If possible, the identification and authorizations of users and the identification of systems and data owners should be managed by a single central system to make comprehensive authorization checks unified and efficient.

The administration of user privileges must specify the rights assignable to different functional

user groups (accountant, account manager, cashier etc.) in each system, and – if possible – users should only be granted these group privileges. The authorization permits must carry the signature of the person granting the authorization or – in case of electronic authorization – the secure (certifiable) permission issued by the system. The authorization forms (electronic or printed) should be designed so that they clearly specify the granted privileges. The granted privileges must be recorded (authorization registry). This registry should keep a history of privileges, and be able to list all the privileges of a user that have been recorded in the IT system. The user privileges stored in the systems must match those of the issued permits and the authorization registry. The policy and the registry must take into account the users with special privileges (system administrators, technical staff) and the diversity of the system components (operating system, database management application etc.). The administration must cover all of these elements. The logging of authorization changes must be activated in the systems and a procedure needs to be created that monitors the changes / modifications of user privileges.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “DS5 – Ensure Systems Security”, “DS7 – Educate and Train Users” and “DS8 – Manage Service Desk and Incidents”.*

**9. Pfa. section 77 (A) (5) (d), Vfa. section 40 (C) (5) (d), Ifcd. section 12 (5) (d), Cife. section 13 (C) (5) (d)**

***Based on the results of the security risk analysis and depending on the significance of the security risks a security environment must be created, which logs the events of the processes critical to the operation of the IT system, and is capable of regularly (or automatically) evaluating the logs and handling irregular events.***

The requirements of the appropriate “security environment” and the results of the preliminary risk analysis must be considered when purchasing IT products. The proper procedures must be introduced to ensure that chronological information is recorded in the operational logs, making it possible to reconstruct, review and analyze the chronology of data processing events and associated / supporting activities. The events of critical systems must also be logged, and the logs need to be checked and saved to backup regularly.

The procedures and methods performing the necessary logging need to be specified in the development life cycle policy (change management) when the specifications of the new IT system development projects are worked out. The management must make sure that the requirements applicable to developing new systems also apply to any major modification of the existing systems.

The security and internal auditing aspects of the systems undergoing development or modification need to be specified during conceptual planning, so that the security aspects can be integrated in the design at the earliest possible stage of planning.

The financial institution must create procedures that ensure that the applications – where necessary – have functions that routinely check the operations performed by the software in order to ensure the integrity of the data. The procedures must also be able to restore the integrity of the data either by rolling back transactions or by other means.

Configuring and updating the parameters of the system software should be given proper attention.

System logs need to be analyzed for security purposes continuously, and the analysis needs to be documented. In case of multiple systems and major organizations the proper IT support for log analysis is almost essential for cost effective quality work.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “AI2 – Acquire and Maintain Application Software”, “AI3 – Acquire and Maintain Technology Infrastructure”, “AI4 – Develop and Maintain IT Procedures” and “DS13*

– *Manage Operations*”.

**10. Pfa. section 77 (A) (5) (e), Vfa. section 40 (C) (5) (e), Ifcd. section 12 (6) (e), Cife. section 13 (C) (5) (e)**

***The confidentiality, integrity and authenticity of data transfers need to be ensured based on the results of the security risk analysis and depending on the significance of the security risks.***

The management must ensure the protection of confidential information is protected during data transfer and transport, and prevent unauthorized access, modification, misdelivery. The management must also develop procedures, rules and computer and network protocols to preserve the integrity, confidentiality and nonrepudiation of confidential messages transferred over the Internet or other public networks. The authenticity and integrity of information received from outside the organization needs to be properly verified before taking any critical action. Proper encryption and secure protocols (HTTPS, SSL, SSH etc.) must be used when transferring information.

Considering that traditional geographic and temporal limitations are becoming less and less important, the management needs to create procedures and rules to ensure the authenticity and integrity of critical electronic transactions. Every flow of information to and from external networks needs to be kept under control in both directions. Connections to the Internet and other public networks must be provided with adequate protection (e.g. firewalls, intrusion prevention systems etc.) to prevent unauthorized access to internal resources and attacks intended to render the services unusable (e.g. Denial of Service attacks).

*The Supervisory Authority recommends consulting the following chapters of CobiT to help interpret this requirement of the law: “DS5 - Ensure Systems Security” and “DS11 – Manage Data”.*

**11. Pfa. section 77 (A) (5) (f), Vfa. section 40 (C) (5) (f), Ifcd. section 12 (6) (f), Cife. section 13 (C) (5) (f)**

***Based on the results of the security risk analysis and depending on the significance of the security risks the handling of storage media needs to be regulated and secure.***

Based on the results of the risk analysis rules need to be set for the regulated and secure handling of storage media, with regards to traceability requirements, cost-effectiveness and security principles. Storage time and parameters need to be specified for documents, data, programs, reports, and messages (incoming and outgoing), as well as the information (keys, certificates) used to encrypt and authenticate them. The management must make sure that there is a systematic inventory of the storage media, and that any discrepancies detected while taking inventory are handled in time. The management must also introduce the necessary measures to ensure the integrity of the storage media. The management needs to make sure that there is a proper policy and system of procedures to protect the storage media. Separate rules and requirements need to be defined regarding the identification labels of backup media, the storage of the media and the tracking of its physical movements, so that the storage media can always be accounted for. Persons responsible for the storage media library (magnetic tapes, removable tape cartridges and other removable storage media, discs, CDs, DVDs) need to be appointed.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: “DS11 – Manage Data”.*

**12. Pfa. section 77 (A) (5) (g), Vfa. section 40 (C) (5) (g), Ifcd. section 12 (6) (g), Cife. section 13 (C) (5) (g)**

***Virus protection needs to be provided based on the results of the security risk analysis and depending on the significance of the security risks.***

The management must develop proper preventive, detective and corrective measures, responses and reporting procedures against malicious software such as viruses and “trojan” programs. The management must make sure that adequate procedures are introduced in the entire organization to protect against computer viruses. These procedures must include virus protection, virus detection, the appropriate response, and reporting obligations. Rules need to be created and implemented to limit personal use of IT resources and the use of unauthorized software. The organization must run anti-virus software on all the workstations and servers capable of running viruses. The management of the IT department must periodically verify that no unauthorized programs have been installed on the organization’s personal computers.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “DS5 – Ensure Systems Security” and “DS9 – Manage the Configuration”.*

**13. Pfa. section 77 (A) (6), Vfa. section 40 (C) (6), Ifcd. section 12 (7), Cife. section 13 (C) (6)**

***In order to perform its duties and keep secure and up to date records the financial organization must introduce the justified protective measures based on the security risk analysis, and must possess at least the items specified in paragraphs a)-g).***

Protective measures should be introduced based on the results of the risk analysis mentioned in paragraph (1) of the sectoral acts, but the phrase “must possess at least” means that the items listed in section (6) are the minimum requirements.

**14. Pfa. section 77 (A) (6) (a), Vfa. section 40 (C) (6) (a), Ifcd. section 12 (7) (a), Cife. section 13 (C) (6) (a)**

***The financial organization must have development plans and instructions and specifications for operating the IT system.***

The IT department must create standardized procedures for operating the IT system (including network operation), and properly document these procedures. All the IT solutions and platforms used by the organization must be operated according to these procedures. The efficiency and proper use of the regulations needs to be verified periodically. The management of the IT department must make sure that the operating staff has the necessary knowledge and experience to document, regularly test, and – if necessary – modify the launch procedure and the other operating duties. The management of the IT department must also make sure that processes, procedures and tasks are planned with maximum efficiency, throughput and utilization in order to ensure reaching the objectives specified in the service level agreements (SLAs). The proper procedures need to be used to identify, examine and approve any deviation from the specified sequence of work processes. The proper procedures must also be used to ensure that processing in continuous even during shift changes among operators. The rules of transferring jobs, updating status reports and reporting on responsibilities for tasks need to be specified accordingly. The proper procedures must be introduced to ensure that chronological information is recorded in the operational logs, making it possible to reconstruct, review and analyze the chronology of data processing events and associated / supporting activities. The management must provide adequate physical protection for the special forms and confidential output devices. In case of remote operation separate procedures need to be created for specifying and performing connection to and disconnection from the remotely operated workstation. Every application must have operating instructions.

The management is responsible for drawing up and implementing long term and short term plans that that correspond to the financial institution's long term and short term objectives. The IT planning must take into account the results of the risk analyses, the environmental, technological and human resources risks, and the introduction of timely and necessary changes.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO1 – Define a Strategic IT Plan”, “PO2 – Define the Information Architecture”, “PO3 – Determine Technological Direction”, “PO5 – Manage the IT Investment”, “P10 – Manage Projects”, “DS6 – Identify and Allocate Costs” and “DS13 – Manage Operations”.*

**15. Pfa. section 77 (A) (6) (b), Vfa. section 40 (C) (6) (b), Ifcd. section 12 (7) (b), Cife. section 13 (C) (6) (b)**

***The financial organization must have all the necessary documentation to ensure the continuous and secure operation of the IT systems directly or indirectly supporting its business operations – even after the supplier or the system developer has discontinued its operations.***

The management must make sure that the business requirements of the IT system's availability and performance are defined, and the specifications and requirements of availability are specified accordingly. The management must make sure that an availability plan is drawn up, which ensures, monitors and verifies the availability of the IT services. The management must also make sure that extraordinary events are reported in time, with sufficient details.

The financial institution's system development methodology must specify the rules of software documentation, the testing requirements of programs developed as part of the development or modification of the IT system, and the standards of supervising, documenting and sustaining the testing. The financial institution's system development life cycle methodology must specify when the old and new systems need to be run alongside one another, and require that documented test results to be preserved from all IT system development, implementation and modification projects.

The management must make sure that the services provided by third-party service providers are accurately defined, and that the technical and organizational connections to suppliers are properly documented. The management must implement proper procedures to ensure that the relationships with third-party service providers are regulated by official written contracts established before work began. This requirement may only be disregarded under extraordinary circumstances, as described in the applicable policy! The management must make sure that the security agreements made with the third-party service providers (e.g. confidentiality agreements) comply with general business standards, and legal and regulatory requirements, including the provisions regarding financial responsibility. The management must make sure that the services provided by third-party service providers are continuously monitored in order to verify the fulfillment of the contract.

The management must create the proper procedures to ensure that the third-party system developers can be contacted to discuss delivery/acceptance criteria, change management, solving problems that arise during development, user roles, technical equipment, technical environment, development tools, software, standards and procedures.

If a third-party developer is used, the contract must require that the information needed to reproduce the developed software (source code, database definition etc.) is placed in custody, so that the financial institution can access it in order to ensure the continuous operation of its IT system if the developer discontinues its operations.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: "AI5 – Procure IT Resources", "DS2 – Manage Third-party Services", "DS3 – Manage Performance and Capacity" and "PO8 - Manage Quality".*

**16. Pfa. section 77 (A) (6) (c), Vfa. section 40 (C) (6) (c), Ifcd. section 12 (7) (c), Cife. section 13 (C) (6) (c)**

***The financial organization must have the IT system necessary to provide its services, backup equipment to ensure the continuity of the services or – in the absence of such equipment – other solutions that ensure the continuity of its operations and services.***

The management of the IT department must develop an IT continuity framework based on the business continuity plan, which specifies the duties and responsibilities, the risk based approach to

be used, and the rules and structures for documenting and approving the IT continuity plan. The management must make sure that the IT continuity plan is consistent with the business continuity plan. The management of the IT department must create proper change management procedures to ensure that the continuity plan is always up to date and adapted to the business / organizational requirements. The management must evaluate the adequacy of the plan periodically – or when there has been a significant change in the organization, in the business operation, or in the IT infrastructure – in order to maintain the effectiveness of the continuity plan. The disaster recovery policy must ensure that all concerned parties receive regular training about the rules of procedure in case of a disaster or extraordinary event. The disaster recovery policy must also ensure that the users can create adequate alternative processing procedures that can be used until the IT department fully restores the system after the shutdown or disaster. The continuity plan must specify the critical applications, third-party service providers, operating systems, employees, inventory and data files required for the recovery, as well as the time needed to perform the recovery. The management must make sure that the continuity plan requires backup sites and hardware specifications to be specified, and a final alternative to be selected. If necessary, these services need to be regulated by a contract. The disaster recovery and business continuity plans must consider storing critical backup media, documentations and other IT resources in an external location. The managers responsible for business processes and the employees of the IT department need to be involved in deciding which backup resources are to be stored in an external location.

The management must create a framework for the services that helps design formal service level agreements and specifies the minimal contents thereof (availability, reliability, performance, capacity, service fees, change management etc.). The users and the IT department need to establish a written agreement that specifies the service level both in terms of quantity and quality. The proper procedures must be used to ensure that the manner and responsibility of fulfilling the obligations arising from the relationships between the concerned parties is properly defined, coordinated, and sent to all the concerned departments. The management of the IT department must appoint a service level manager who monitors the fulfillment of specific service criteria. The management must periodically review the service level agreements and renew the contracts with the third-party service providers.

The management of the IT department needs to create a problem solving system that records, analyzes, and at the right time resolves the abnormal events (extraordinary events, problems, errors) that occur during operation. Any changes in emergency program procedures need to be immediately tested, approved and reported. In case of a major problem an “extraordinary event report” needs to be created. The management create proper problem escalation / forwarding procedures (towards the appropriate persons) in order to resolve the detected problems as quickly and efficiently as possible. The procedures must specify the associated priorities. The procedures must also document the decision preparing procedure for implementing the IT continuity plan. The problem solving system must have proper control logs that allow the staff to discover the underlying reasons of the problems by tracing back the extraordinary event to its roots.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO1 – Define a Strategic IT Plan”, “PO2 – Define the Information Architecture”, “Manage the IT INvestment”, “DS1 – Define and Manage Service Levels”, “DS3 – Manage Performance and Capacity”, “DS4 – Ensure Continuous Service” and “DS10 – Manage Problems and Incidents”.*

**17. Pfa. section 77 (A) (6) (d), Vfa. section 40 (C) (6) (d), Ifcd. section 12 (7) (d), Cife. section 13 (C) (6) (d)**

***The financial organization must have an IT system that allows the application environment to be securely separated from the development and testing environment, and ensures adequate change monitoring and change management.***

A procedure needs to be created – as part of the system development methodology – to scale and optimize user applications and forecast the resources required by new and significantly modified software. An implementation plan needs to be drawn up and approved by the concerned parties to measure the achieved progress. The implementation plan must have instructions for the following: preparing the premises, procuring and installing the devices, installing modifications for the operating system, introducing operating procedures and migration. The system development methodology must make sure that the necessary components of the old system are migrated to the new system – in accordance with previously drawn up plans – in every IT system development, implementation and modification project.

In case of migration and data conversion the management must require data transformation plans to be drawn up, which specify methods used to collect and verify the data to be converted, as well as detect and resolve the problems found during transformation (data transformation and conversion).

The system administration and the management of the IT department need to develop strategies and plans for testing. The employees of the affected departments and the operating group of the IT department needs to be trained as required by the training plan. The management must make sure that – prior to deployment in the real environment – changes are tested in a separate environment by an independent testing group (independent from the creators of the system) in accordance with the impact and capacity analyses. Testing upon delivery needs to be performed in an environment similar to the future operating environment.

In case of software changes the management of the IT department and the other affected departments need to formally approve the test results as part of the final delivery/acceptance and quality assurance testing procedure. The management must stipulate that the heads of the operating division and the user classes have to formally accept the test results and the security level of the systems along with the accepted level of risk. The management must create and implement formal procedures to regulate the introduction of the new system from system development to testing to deployment. The management must stipulate that the new system may only be deployed after successful testing, with the permission of the system's owner. The different (development, testing, operating) environments of the applications need to be separated and adequately protected.

The regulatory system of the financial institution must specify that the operating requirements of the IT system (capacity, throughput etc.) need to be analyzed after implementation to decide whether the system meets the user requirements.

Changes occurring in the financial institution need to be managed. Formal rules and official procedures need to be defined to manage the changes (of data, hardware, software, infrastructure, technology, human resources etc.). It is recommended to appoint change managers to handle change management tasks. The managements must stipulate that requests for changes, system maintenance and maintenance by suppliers are submitted in a pre-defined format, and such tasks are performed according to the requests. Requests for changes need to be categorized and assigned priority. A separate policy needs to be developed for urgent cases. The persons requesting the changes need to be notified of the status of their requests.

A procedure needs to be created to make sure that requests for changes are evaluated methodically, and that the system currently in use is taken into consideration, as well as all the possible consequences – considered in the risk analysis – that could affect the system’s functionality. The management must ensure that the change management, software management and software distribution correspond to the overall configuration management system. The system monitoring the changes made in the application system need to be automated in order to record the complex major changes of the IT systems.

The IT management must specify the parameters of urgent (emergency) changes and the method of regulating such changes, if they are outside the procedure of regular technical, operational and executive evaluation prior to introduction. Urgent changes need to be recorded and approved in advance by the IT management.

The rules of change procedures needs to stipulate that if a system change is implemented, then the associated documentation and procedures must also be updated. The management must specify the tasks performed by the maintenance staff and make sure that the maintenance is properly supervised. Access privileges must also be regulated in order to prevent unauthorized access to the automated systems.

The management must specify and implement rules for introducing new software versions, covering approval and acceptance, assembling and testing the software package, delivering the new software etc. Proper internal auditing measures need to be introduced to ensure that the new software components are installed in the right place, at the right time, allowing verification (e.g. by means of the audit log).

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “AI7 – Install and Accredite Solutions and Changes” and “AI6 – Manage Changes”.*

**18. Pfa. section 77 (A) (6) (e), Vfa. section 40 (C) (6) (e), Ifcd. section 12 (7) (e), Cife. section 13 (C) (6) (e)**

***The financial organization must have backups of the software components of the IT system (applications, data, operating systems and their environments) and backup systems (specifying backup types, methods, restoration and recovery tests, procedure system) that make it possible to restore the system within the critical recovery time of the service provided by the system. These backups need to be stored separately (in terms of environmental risks) and protected. The backups must be protected against unauthorized access the same as their source systems.***

The management must develop a suitable strategy for data backup and recovery including an overview of business requirements, as well as the creation, implementation, testing and documentation of the recovery plan. Proper procedures must be introduced to ensure that the backups meet these requirements. Proper procedures must be introduced to ensure that the backups are created in accordance with the backup strategy. The usability of the backups needs to be checked periodically. The backup requirements specified for IT storage media need to ensure that the data, software and related documents are stored properly both in and outside the premises. The backups need to be stored in a secure location. The physical accessibility of the storage facility and the security of the data files and other backup items need to be checked periodically. It must be ensured that the data and system backups can be restored even if the software and hardware environment changes.

The data owners need to specify the classification and sharing parameters of their data, and when (if ever) the programs and files should be archived and deleted.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: “DS4 – Ensure Continuous Service” and “DS11 – Manage Data”.*

**19. Pfa. section 77 (A) (6) (f), Vfa. section 40 (C) (6) (f), Ifcd. section 12 (7) (f), Cife. section 13 (C) (6) (f)**

*The financial organization must have a data storage system capable of repeatedly accessing the records specified by law, which ensures that the archived data can be restored and accessed any time for the period of time specified by law, but for at least 5 years (5 years after the termination of a customer’s membership in case of funds).*

The management must create rules and procedures to ensure that the data is archived in accordance with legal and business requirements, and that archived data is protected and kept record of same as the original.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: “DS4 – Ensure Continuous Service” and “DS11 – Manage Data”.*

**20. Pfa. section 77 (A) (6) (g), Vfa. section 40 (C) (6) (g), Ifcd. section 12 (7) (g), Cife. section 13 (C) (6) (g)**

*The financial organization must have a plan to manage extraordinary events that impede the continuous provision of services.*

The requirements of this paragraph are the same as those listed under paragraph (6) (c) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “DS1 – Define and Manage Service Levels”, “DS4 – Ensure Continuous Service” and “DS10 – Manage Problems and Incidents”.*

**21. Pfa. section 77 (A) (7), Vfa. section 40 (C) (7), Ifcd. section 12 (9), Cife. section 13 (C) (7)**

*The items specified in paragraphs a)-g) must be available to the financial organization at all times.*

In the Supervisory Authority’s interpretation “available at all times” means that the financial organization must meet the listed minimum requirements from the time of requesting its permit and continuously during its business operation.

**22. Pfa. section 77 (A) (7) (a), Vfa. section 40 (C) (7) (a), Ifcd. section 12 (9) (a), Cife. section 13 (C) (7) (a)**

*The system manuals and models necessary to check the structure and operation of the systems developed for and ordered by the organization must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (5) (a) and paragraph (6) (a)-(b) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “A11 – Identify Automated Solutions”, “A12 – Acquire and Maintain Application Software”, “A14 – Develop and Maintain IT Procedures”, “PO2 – Define the Information Architecture” and “PO8 – Manage Quality”.*

**23. Pfa. section 77 (A) (7) (b), Vfa. section 40 (C) (7) (b), Ifcd. section 12 (9) (b), Cife. section 13 (C) (7) (b)**

*The syntactic rules and data storage structure of the IT system developed by or for the organization must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (6) (a)-(b) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “A12 – Acquire and Maintain Application Software”, “PO2 – Define the Information Architecture” and “A11 – Identify Automated Solutions”.*

**24. Pfa. section 77 (A) (7) (c), Vfa. section 40 (C) (7) (c), Ifcd. section 12 (9) (c), Cife. section 13 (C) (7) (c)**

*The security classification system of the IT system components created by the organization must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (5) (c) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO2 – Define the Information Architecture” and “DS5 – Ensure Systems Security”.*

**25. Pfa. section 77 (A) (7) (d), Vfa. section 40 (C) (7) (d), Ifcd. section 12 (9) (d), Cife. section 13 (C) (7) (d)**

*The rules of data access must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (5) (a) and (c) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO2 – Define the Information Architecture”, “PO4 – Define the IT Organization and Relationships” and “DS5 – Ensure Systems Security”.*

**26. Pfa. section 77 (A) (7) (e), Vfa. section 40 (C) (7) (e), Cma. section 101 (A) (7) (e), Ifcd. section 12 (9) (e), Cife. section 13 (C) (7) (e)**

*The document appointing the data owner and the system administrator must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (3) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO4 – Define the IT Organization and Relationships” and “PO7 – Manage Human Resources”.*

**27. Pfa. section 77 (A) (7) (f), Vfa. section 40 (C) (7) (f), Ifcd. section 12 (9) (f), Cife. section 13 (C) (7) (f)**

*The contracts certifying the proper licensing of the software in use must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (1) and (5) (a) - (b) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO6 – Communicate Management Aims and Direction” and “DS9 – Manage the Configuration”.*

**28. Pfa. section 77 (A) (7) (g), Vfa. section 40 (C) (7) (g), Ifcd. section 12 (9) (g), Cife. section 13 (C) (7) (g)**

*A comprehensive and up to date record of the business and management software used in the IT system must be available to the financial organization at all times.*

The requirements of this paragraph are the same as those listed under paragraph (5) (a) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: “DS9 – Manage the Configuration”.*

**29. Pfa. section 77 (A) (8), Vfa. section 40 (C) (8), Ifcd. section 12 (10), Cife. section 13 (C) (8)**

***The software used in the financial organization must collectively be capable of performing the tasks specified in this paragraph.***

The requirements listed in this paragraph are minimum software requirements.

**30. Pfa. section 77 (A) (8) (a), Vfa. section 40 (C) (8) (a), Ifcd. section 12 (10) (a), Cife. section 13 (C) (8) (a)**

***The software used in the financial organization must collectively be capable of keeping records of the information required for operation and specified by law.***

The requirements of this paragraph are the same as those listed under paragraph (1) and (6) (c)-(d) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “PO1 – Define a Strategic IT Plan”, “ME3 – Ensure Regulatory Compliance”, “PO8– Manage Quality”, “AI7 – Install and Accredite Solutions and Changes” and “DS1 – Define and Manage Service Levels”.*

**31. Pfa. section 77 (A) (8) (b), Vfa. section 40 (C) (8) (b), Ifcd. section 12 (10) (e), Cife. section 13 (C) (8) (d)**

***The software used in the financial organization must collectively be capable of using the stored information to perform audits.***

The requirements of this paragraph are the same as those listed under paragraph (5) (f) and (6) (e)-(f) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: “DS11 – Manage Data”.*

**32. Pfa. section 77 (A) (8) (c), Vfa. section 40 (C) (8) (c), Ifcd. section 12 (10) (f), Cife. section 13 (C) (8) (e)**

***The software used in the financial organization must collectively be capable of providing logical protection and safeguarding data integrity in proportion to the security risk.***

The requirements of this paragraph are the same as those listed under paragraph (5) (b)-(d) of the sectoral acts.

*The Supervisory Authority recommends consulting the following chapters of CobiT to help fulfill this requirement: “AI2 – Acquire and Maintain Application Software”, “DS5 – Ensure Systems Security” and “DS11 – Manage Data”.*

**33. Ifcd. section 12 (10) (b)-(c)-(d), Cife. section 13 (C) (8) (b)-(c)**

*The software used in the financial organization must collectively be capable of keeping secure records of the money and the securities, keeping separate and up to date records of investment and commodity exchange services, and connecting to the national IT system directly or indirectly.*

The requirements of this paragraph are the same as those listed under paragraph (5) and (6) of the sectoral acts.

**34. Pfa. section 77 (A) (9), Vfa. section 40 (C) (9), Ifcd. section 12 (11), Cife. section 13 (C) (9)**

*The internal policies of the financial organization must specify the IT knowledge required for each job.*

The IT knowledge and experience required for each job needs to be specified in the financial institution's internal policies as well as the job descriptions. Every employee must participate in regular trainings describing the principles of IT security. These trainings focus on familiarizing employees with security issues and handling extraordinary events. The requirements of this paragraph are related to those listed under paragraph (3).

*The Supervisory Authority recommends consulting the following chapter of CobiT to help fulfill this requirement: "PO7 – Manage Human Resources".*

**The opinions stated in this guide are not legally binding or mandatory. The expectations are based on international recommendations and best practice.**

## Annex I: Legal requirements and the corresponding chapters in CobiT

### ANNEX I: LEGAL REQUIREMENTS AND THE CORRESPONDING CHAPTERS IN COBIT

Summary of legal requirements regarding the protection of the IT system <sup>3</sup>	Name of the corresponding area and process in COBIT
(1) The financial institution must create a regulation system for the IT system used in its operations and must provide protection for the IT system in proportion to the risks. The regulation system must specify the information technology requirements as well as the assessment and management of security risks in planning, procurement, operation and auditing.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO6 – COMMUNICATE MANAGEMENT AIMS AND DIRECTION</p> <p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> <p>AI1 – IDENTIFY AUTOMATED SOLUTIONS</p> <p style="text-align: center;"><b>ME – MONITOR AND EVALUATE</b></p> <p>ME3 – ENSURE REGULATORY COMPLIANCE</p>
(2) The financial institution must review and update the security risk analysis of the IT system as necessary, but at least once every two years.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO9 – ASSESS RISKS</p>
(3) The organizational and operational rules; the policies on responsibility, recordkeeping, and providing information; and the rules and requirements of verification built into the process must be specified with regards to the security risks arising from the use of information technology.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO4 – DEFINE THE IT ORGANIZATION AND RELATIONSHIPS PO7 – MANAGE HUMAN RESOURCES</p>
(4) The financial institution must establish and operate an IT control system monitoring the secure operation of the IT system.	<p style="text-align: center;"><b>ME – MONITOR AND EVALUATE</b></p> <p>ME1 – MONITOR AND EVALUATE IT PERFORMANCE ME2 – MONITOR AND EVALUATE INTERNAL CONTROL ME3 – ENSURE REGULATORY COMPLIANCE ME4 – PROVIDE IT GOVERNANCE</p>
(5) The following measures must be introduced based on the results of the security risk analysis and depending on the significance of the security risks:	
a) the most important components of the system (devices, processes, persons) must be clearly identified and logged,	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS9 – MANAGE THE CONFIGURATION</p>
b) the self-defense of the IT security system, and the inspections and procedures ensuring that the system's critical components are fully and securely protected must be implemented.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS12 – MANAGE FACILITIES</p> <p style="text-align: center;"><b>ME – MONITOR AND EVALUATE</b></p> <p>ME2 – MONITOR AND EVALUATE INTERNAL CONTROL</p>
c) the system's user administration (access levels, unique authorizations, approvals, responsibilities, access logging, extraordinary events) must be regulated, verifiable and regularly checked.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS7 – EDUCATE AND TRAIN USERS DS8 – MANAGE SERVICE DESK AND INCIDENTS</p>

<p>d) a security environment must be created, which logs the events of the processes critical to the operation of the IT system, and is capable of regularly (or automatically) evaluating the logs and handling irregular events.</p>	<p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b>  AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE  AI3 – ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE  AI4 – DEVELOP AND MAINTAIN IT PROCEDURES</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b>  DS13 – MANAGE OPERATIONS</p>
--	--

---

<sup>3</sup> References to the provisions of Cife., Ifcd., Pfa. and Vfa., being aware of and complying with which can also be useful for insurance companies.

## Annex I: Legal requirements and the corresponding chapters in CobiT

e) the confidentiality, integrity and authenticity of data transfers need to be ensured.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS11 – MANAGE DATA</p>
f) the handling of storage media needs to be regulated and secure.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS11 – MANAGE DATA</p>
g) virus protection needs to be provided in proportion to the security risk of the system.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS9 – MANAGE THE CONFIGURATION</p>
(6) In order to perform its duties and keep secure and up to date records the financial organization must introduce the justified protective measures based on the security risk analysis, and must have at least the following items:	
a) development plans and instructions and specifications for operating the IT system.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO1- DEFINE A STRATEGIC IT PLAN PO2- DEFINE THE INFORMATION ARCHITECTURE PO3 – DETERMINE TECHNOLOGICAL DIRECTION PO5- MANAGE THE IT INVESTMENT PO10 – MANAGE PROJECTS</p>
b) all the necessary documentation to ensure the continuous and secure operation of the IT systems directly or indirectly supporting its business operations - even after the supplier or the system developer has discontinued its operations.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO8 – MANAGE QUALITY</p> <p style="text-align: center;"><b>AI - ACQUISITION AND IMPLEMENTATION</b></p> <p>AI5- PROCURE IT RESOURCES</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS2 – MANAGE THIRD-PARTY SERVICES DS3 – MANAGE PERFORMANCE AND CAPACITY</p>
c) the IT system necessary to provide its services, backup equipment to ensure the continuity of the services or - in the absence of such equipment - other solutions that ensure the continuity of its operations and services.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO1 – DEFINE A STRATEGIC IT PLAN PO2 – DEFINE THE INFORMATION ARCHITECTURE PO5 – MANAGE THE IT INVESTMENT</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS1 – DEFINE AND MANAGE SERVICE LEVELS DS3 – MANAGE PERFORMANCE AND CAPACITY DS4 – ENSURE CONTINUOUS SERVICE DS10 – MANAGE PROBLEMS AND INCIDENTS</p>
d) an IT system that allows the application environment to be securely separated from the development and testing environment, and ensures adequate change monitoring and change management.	<p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> <p>AI7 – INSTALL AND ACCREDIT SOLUTIONS AND CHANGES AI6 – MANAGE CHANGES</p>
e) backups of the software components of the IT system (applications, data, operating systems and their environments) and backup systems (specifying backup types, methods, restoration and recovery tests, procedure system) that make it possible to restore the system within the critical recovery time of the service provided by the system. These backups need to be stored separately (in terms of environmental risks) and protected. The backups must be protected against unauthorized access the same as their source systems.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS4 – ENSURE CONTINUOUS SERVICE DS11 – MANAGE DATA</p>
f) a data storage system capable of repeatedly accessing the records specified by law, which ensures that the archived data can be restored and accessed any time for the period of time specified by law, but for at least 5 years.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS4 – ENSURE CONTINUOUS SERVICE DS11 – MANAGE DATA</p>

g) a plan to manage extraordinary events that impede the continuous provision of services.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS1-DEFINE AND MANAGE SERVICE LEVELS DS4 – ENSURE CONTINUOUS SERVICE DS8 – MANAGE SERVICE DESK AND INCIDENTS DS10 – MANAGE PROBLEMS
--	--

**Annex I: Legal requirements and the corresponding chapters in CobiT**

(7) The following items must be available to the financial organization at all times:	
a) the system manuals and models necessary to check the structure and operation of the systems developed for and ordered by the organization.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO2 – DEFINE THE INFORMATION ARCHITECTURE PO8 – MANAGE QUALITY <p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> AI1 – IDENTIFY AUTOMATED SOLUTIONS AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE AI4 – DEVELOP AND MAINTAIN IT PROCEDURES
b) the syntactic rules and data storage structure of the IT system developed by or for the organization.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO2 – DEFINE THE INFORMATION ARCHITECTURE <p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> AI1 – IDENTIFY AUTOMATED SOLUTIONS AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE
c) the security classification system of the IT system components created by the organization.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO2 – DEFINE THE INFORMATION ARCHITECTURE <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS5 – ENSURE SYSTEMS SECURITY
d) the rules of data access.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO2 – DEFINE THE INFORMATION ARCHITECTURE PO4 – DEFINE THE IT ORGANIZATION AND RELATIONSHIPS <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS5 – ENSURE SYSTEMS SECURITY
e) the document appointing the data owner and the system administrator.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO4 – DEFINE THE IT ORGANIZATION AND RELATIONSHIPS PO7 – MANAGE IT HUMAN RESOURCES
f) the contracts certifying the proper licensing of the software in use.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO6 – COMMUNICATE MANAGEMENT AIMS AND DIRECTION <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS9 – MANAGE THE CONFIGURATION
g) a comprehensive and up to date record of the business and management software used in the IT system.	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS9 – MANAGE THE CONFIGURATION
(8) The software used in the financial organization must collectively be capable of the following::	
a) keeping records of the information required for operation and specified by law.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> PO1 – DEFINE A STRATEGIC IT PLAN PO8 –MANAGE QUALITY <p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> AI7 – INSTALL AND ACCREDIT SOLUTIONS AND CHANGES <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS1 – DEFINE AND MANAGE SERVICE LEVELS <p style="text-align: center;"><b>ME – MONITOR AND EVALUATE</b></p> ME3 – ENSURE REGULATORY COMPLIANCE
b) keeping secure records of the money and the securities,	<p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> DS11 – MANAGE DATA

c) directly or indirectly connecting to the national IT systems associated with the financial institution's activity.	<p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> <p>AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS11 – MANAGE DATA</p>
d) using the stored information to perform audits.	<p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> <p>AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS11 – MANAGE DATA</p>
e) providing logical protection and safeguarding data integrity in proportion to the security risk.	<p style="text-align: center;"><b>AI – ACQUISITION AND IMPLEMENTATION</b></p> <p>AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE</p> <p style="text-align: center;"><b>DS – DELIVERY AND SUPPORT</b></p> <p>DS5 – ENSURE SYSTEMS SECURITY DS11 – MANAGE DATA</p>
(9) The internal policies of the financial organization must specify the IT knowledge required for each job.	<p style="text-align: center;"><b>PO – PLANNING AND ORGANIZATION</b></p> <p>PO7 – MANAGE HUMAN RESOURCES</p>

## Annex II: List of CobiT manuals by group, availability

### ANNEX II: LIST OF COBIT MANUALS BY GROUP, AVAILABILITY

#### II.1. IT GOVERNANCE

Title	Free download from the Internet (without ISACA web profile)	Available for purchase at the following address
Board Briefing on IT Governance	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>
IT Governance Executive Summary	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	
Information Security Governance: Guidance for Boards of Directors and Executive Management	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>
IT Governance Implementation Guide	not available	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>

#### II.2. SIMPLIFIED COBIT FOR BEGINNERS

Manual and assessment program	Free download from the Internet (with ISACA web profile)	Available for purchase at the following address
COBIT Quickstart	not available	<a href="http://www.isaca.org/quickstart">http://www.isaca.org/quickstart</a>

#### II.3. BASIC COBIT BOOKS

Title	Free download from the Internet (with ISACA web profile)	Available for purchase at the following address
COBIT And Related Products Brochure	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT	
COBIT Executive Summary  In Hungarian: COBIT Összefoglaló áttekintés	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT <a href="http://www.pszaf.hu/">http://www.pszaf.hu/</a>	<a href="http://www.isaca.hu/">http://www.isaca.hu/</a>
COBIT Framework  In Hungarian: COBIT Keretrendszer	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT <a href="http://www.pszaf.hu/">http://www.pszaf.hu/</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>  <a href="http://www.isaca.hu/">http://www.isaca.hu/</a>
COBIT Control Objectives  In Hungarian: COBIT Kontroll célkitűzések	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT <a href="http://www.pszaf.hu/">http://www.pszaf.hu/</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>  <a href="http://www.isaca.hu/">http://www.isaca.hu/</a>
COBIT Management Guidelines	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>
COBIT Audit Guidelines	Only for ISACA members: <a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>

## Annex II: List of CobiT manuals by group, availability

COBIT Implementation Tool Set  In Hungarian: COBIT Alkalmazási módszerek	<a href="http://www.isaca.org/">http://www.isaca.org/</a> Navigation: Governance / COBIT / Obtain COBIT <a href="http://www.pszaf.hu/">http://www.pszaf.hu/</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>  <a href="http://www.isaca.hu/">http://www.isaca.hu/</a>
---	--	--

### **II.4. REALIZING THE OBJECTIVES OF CobiT**

Title	Free download from the Internet (with ISACA web profile)	Available for purchase at the following address
COBIT Control Practices	not available	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>

### **II.5. CobiT ON THE INTERNET (INCLUDING CONTROL PRACTICES)**

Title	Free download from the Internet (with ISACA web profile)	Available by annual subscription at the following address
COBIT Online	not available	<a href="http://www.isaca.org/cobitonline">http://www.isaca.org/cobitonline</a>

### **II.6. OTHER CobiT PUBLICATIONS**

Title	Free download from the Internet (with ISACA web profile)	Available for purchase at the following address
COBIT Security Baseline	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>
	Free download from the Internet (without ISACA web profile)	
COBIT Mapping: Overview of International IT Governance	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	
IT Control Objectives for Sarbanes- Oxley	<a href="http://www.isaca.org/downloads">http://www.isaca.org/downloads</a>	<a href="http://www.isaca.org/bookstore">http://www.isaca.org/bookstore</a>

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **ANNEX III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

#### **Data**

The manifestation of information, i.e. a non-interpreted but interpretable form of conveying facts and concepts.

#### **Data file**

A physical or logical combination of data in an IT system stored under a single name. The data can be accessed by this name.

#### **Data owner**

A person who rates and classifies data by the financial institution's authorization. The data owner is responsible for the handling of the data he/she rated.

#### **Database**

A body of information stored electronically, in digital format.

#### **Data security**

A system of technical and organization measures and procedures used to prevent the unauthorized access, modification and destruction of data.

#### **Data processing**

The performance of data management operations and technical task regardless of the location or the methods and tools used to perform the operations.

#### **Data processor**

A natural person, legal entity, or company without legal entity commissioned to process data by the data manager.

#### **Data management**

The collection, recording, storage, usage (including forwarding and disclosure) and deletion of data regardless of the procedure used. Data management also includes the modification of the data and the prevention of its further use.

#### **Data manager**

The natural person, legal entity, or company without legal entity that specified the objective of managing the data, makes and carries out decisions regarding the management of the data, or commissions a data processor to carry out its decisions.

#### **Data forwarding**

When the data is made accessible to a specific third party or application.

#### **Data deletion**

Rendering the data unrecognizable in way the makes recovery impossible.

#### **Data protection (privacy)**

The legal regulation of data management regarding the legal protection of the parties concerned by the management of a specific cluster of data on a certain level, and regarding the legality of the procedures used to manage the data.

#### **Administrative protection**

Protection by organizational and regulatory means.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Basic threats**

A universal grouping of threats. Includes the violation and loss of privacy, authenticity, integrity, nonrepudiation, availability and functionality.

### **Application**

A combination of hardware, software and communication resources joined under the same name to help realize a business objective of the financial institution. Applications are characterized by human-computer interaction. The technology (know-how) created based on the entire IT system of the financial organization in order to achieve specific business, banking, organizational and other objectives in support of the organization's operations is considered related to the application, just like the built-in theoretical model and the documentation of application.

### **Application program (application software)**

A program introduced by the user for its own purposes, which uses the functions of the hardware and the operating system.

### **Application (real) (system) environment**

The sum of all the components of the financial institution's IT system that the application uses in its normal operation to generate valid results / transactions. The main difference between the real environment and all the other environments (development, testing) is the validity of the operating results generated in the real environment.

### **Application user**

The financial institution that uses the application –with the possible contribution of a supplier or service provider – to realize its own business objectives.

### **Application supplier**

The developer / maker / distributor / licensor of the application that creates new versions of the system to fix the problems in the application or to fulfill new requirements.

### **Application service provider**

The unit of the organization (or contracting partner) making the IT resources of the application available to the financial institution as an IT application, in accordance with the financial institution's requirements. The service provider is responsible for installing the new versions of the applications provided by the supplier by the user's authorization (version changes). The user, the supplier and the service provider of the application can be the same company.

### **Average recovery time**

The average shutdown time required to find and solve problems.

### **Archiving**

Creating a special backup of a certain application (or – in the broader sense – IT system) environment (i.e. not only the data content). It's a special backup because both the archived and the remaining system must remain logically intact and restorable. Archiving – unlike creating backups – is usually done primarily to increase efficiency rather than security (most often to increase the speed of the remaining environment / system).

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Backup system**

A system storing backup copies in order to ensure the accessibility of data for IT security purposes. The term can also mean an IT system with minimal reserve capacity.

### **BCP**

See Business Continuity Planning.

### **Confidentiality**

(a quality of the organization) A quality of the financial institution which ensures that only the parties authorized by the organization can access the data.

(an attribute of data) An attribute assigned to the data by the managing system that indicates / represents the enforcement of protective measures corresponding to the classification of the data. An attribute of the data, which means that only the authorized parties can access the data and make decisions regarding usage.

### **Security**

The condition of the organization in which it faces the least danger; it is able to provide its services under the accepted / required terms and conditions and without limitation; it does not suffer any losses that would significantly affect the performance of its duties and functions; the risk calculated based on the probability of a harmful event and the amount of the potential loss is acceptably low; and the residual risk of the risk management procedures is tolerable for the organization. A satisfactory condition of the protected IT system that provides full, secure and continuous protection in proportion to the risks. In the IT systems security means compliance with requirements and standards that enhance the functionality of the system and the availability, integrity and authenticity of the information.

### **Security audit**

An independent analysis of the records and activities related to the IT system, an analysis of the adequacy of the system checks, means to ensure the adequacy of the policies and operating procedures, identification of the weak points in security in order to implement the security changes recommended by the audit, the policies and the procedures.

### **Security event**

An unfavorable change in the security of the IT system, which may lead to a violation of the privacy, integrity, authenticity, functionality or availability of the data managed in the IT system.

### **Security demand**

An expectation or objective created when one or more risks are unacceptably high and therefore something needs to be done in order to protect the IT system.

### **Security risk (IT risk)**

A measurement of probability calculated based on to probability of an event jeopardizing the operation of the IT system and the magnitude of the potential damage. It can be expressed in necessary labor hours, time, money, or a combination thereof.

### **Security environment**

The laws, the internal rules and expectations of the business organization, the customs, the competency and the knowledge define the environment in which the institution will use its resources.

### **Security requirements**

The measures necessary to counter the threat factors representing unacceptably high risk, as identified in the risk analysis.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Security mechanism**

A procedure, method or solution plan – possibly regarding computer technology – that fulfills one or more security requirements.

### **Security classification**

An attribute of the data defining the level of protection (handling methods and conditions, protective measures) to be used when managing the data.

### **Security gap**

Measures need to be introduced in several different areas in order to protect the IT system. The preventive, precautionary measures can affect architectural, technical, organizational and personnel matters. These measures must be coordinated and combined in an IT security regulation system. It is important to know that no IT system can be 100% secure. There is no perfect solution. The residual risks must be known and taken into consideration. The purpose for creating the regulation system is to reduce these residual risks to a tolerable level. The need for protection depends on the characteristics of the IT system and the on the environment in which it will be introduced.

### **CA**

See Certification Authority.

### **Cracker**

A person breaking into an IT system using IT devices with the intent of causing destruction.

### **CRAMM**

CCTA Risk Analysis and Management Method – a risk analysis and risk management methodology developed by the Central Computer and Telecommunication Agency in the United Kingdom.

### **Demo software**

Many companies making licensed software also publish trial or demonstration (demo) versions of their programs for free or at a low price. These versions are intended for presentation, testing and trial, therefore they often don't provide full functionality and can only be used for a limited time. These software versions may not be used commercially.

### **Distributive backup**

A backup solution in which the users in the same group create local backups of their own databases on their on computers.

### **DRP**

See Disaster Recovery Planning.

### **Digital signature**

See Electronic signature.

### **Homogeneity**

The security covers the institution's entire operation and is equally strong at every point.

### **Single repair time**

The time between detecting a problem in the IT system and returning to normal operation (after resolving the problem).

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Electronic signature**

An encrypted data sequence assigned to the data managed in the IT system that can be used to certify the authenticity and integrity of the data.

### **Availability**

A state in which all the services of an IT application can be used to process information in a certain place at a specific time.

### **Audit trail**

A log of IT activities which can be used to detect and report illegal and improper activities.

### **Obsolescence period**

The last phase of the IT product's life cycle during which the breakdown factor increases and the quality of the system components deteriorates due to irreversible changes.

### **Value**

The value of the information and information processing depends on their importance in fulfilling user requirements. The value of an IT system component can be derived from the value of the information and information processing involved in the procedures using the system component in question.

### **Development (system) environment**

The sum of all the components in the IT system of the application supplier / developer used to create an application for financial use. A development environment cannot generate valid results / transactions.

### **Separation of duties**

A separation of critical security tasks associated with the use and operation of the IT system.

### **Accountability**

An attribute that allows the activities of a procedure to be definitely traced back to a specific process.

### **User**

The person, organization or group that uses one or more IT systems to perform its duties.

### **User authentication**

Verification of the user's authenticity (every user verified at login) and the use of various identification devices (e.g. password, smart card, biometric identification etc.).

### **User application (user software)**

See Application program.

### **Threat**

The possibility of a security breach.

### **Threatened**

A state, in which resources may be exposed, altered or destroyed.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Threat analysis**

The determination of a significant It threat factor.

### **Threat factor**

A circumstance or event that threatens availability, integrity, confidentiality or authenticity of data or information being processed in the IT system, or the operability of the IT system or any of its components. Threat factors include not only attacks by individuals against the IT system but all threats in the broader sense such as ransom events, the impacts of external events, and circumstances that arise from nature of information technology itself. (Examples: fire, power outage, data entry error, improper handling, hardware breakdown, computer viruses, program malfunctions.)

### **Worm program**

A malicious program spreading from one IT system to another through the IT network.

### **Physical security**

Measures taken to physically protect resources against intentional and inadvertent threats and protection created in physical space against intentional and inadvertent attacks.

### **Physical protection**

See Physical security.

### **Continuity**

Uninterrupted availability of business activities.

### **Continuous protection**

A protective solution that remains uninterrupted despite changing circumstances and conditions.

### **Freeware software**

Free software that can be used without a license because its creators do not enforce copyright.

### **Functionality**

An attribute of the IT system component which means that the component is serving its purpose and is usable.

### **Weak point**

The part or quality of the IT system component that exposes it to threat factors.

### **Hacker**

A person breaking into an IT system using IT devices without the explicit intent of causing harm.

### **Network**

The connection of computers (or – more generally – IT systems) and the logical and physical devices conducting the data exchange between the different components of the connected systems.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Network cooperation**

A cooperation of devices using identical communication standards.

### **Hash function**

A transformation that creates a unique, fixed-size digital string from a text of arbitrary length.

### **Useful life**

The consistent middle phase of an IT product's life cycle during which the breakdown factor is more or less constant.

### **Three-generation principle**

A solution for implementing the IT system and ensuring the availability of data that restores the functionality of the IT system using the last three backups.

### **Restoration (recovery)**

Returning the resources damaged in a disaster to their original condition in their original place.

### **The probability of error-free operation**

The probability of no errors being encountered in a certain period of time, under specific operating and environmental conditions.

### **Certification Authority (CA)**

A trusted specialized organization trusted by everyone that is authorized to issue certificates to clients and servers.

### **Authenticity**

A piece of data is authentic if it can be positively determined who it was created by and that it has not been altered since its creation. Authenticity is an attribute of the data (and the storage media) which certifies that the data can be or is proven to originate from the required source.

### **Access**

A procedure that makes the resources of the IT system and the information stored therein available to the user of the IT system for a specific purpose, in a specific place and time, based on the users authorization. The procedure may be called for example by entering a username to be allowed to read, write or delete some data.

### **Access control**

The prevention of unauthorized access to IT resources, including the prevention of unauthorized use.

### **Access control list**

A register of the entities authorized to access the IT resources and their access privileges.

### **Human security**

Protection against possible intentional and inadvertent human attacks against the confidentiality and/or integrity and/or availability of IT resources by the employees or contracted third parties.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Illegal software**

A software product protected by copyright that is used without all the documents necessary to certify legality (license, invoice, bill of delivery, contract of donation) being available, as well as software not used in accordance with the provisions of the license agreement.

### **Unauthorized person**

A person not authorized to access the data.

### **Informatics (IT)**

The science of computer information systems that provides theory, approach and methodology for planning, developing, organizing and operating computer information systems.

### **IT security**

A satisfactory state of the financial institution's IT system in which the confidentiality, authenticity, integrity and availability of the data managed by the IT systems and the availability and functionality of the IT systems is fully, securely and continuously protected in proportion to the risks.

### **IT security manager**

The person responsible for establishing IT security in the financial institution. The IT security manager takes part in designing, teaching and updating the IT security policy and regulations and is responsible for supervising and enforcing them.

### **IT security plan**

Hardware, software, training, regulatory and other documents related to IT security pertaining to budget and other resources that are part of the annual IT plan.

### **IT system**

A combination of hardware, software and communication devices and the organizations managing / serving them that the financial institution uses in accordance with its business policy to realize its objectives.

### **IT disaster**

An undesired event that causes loss of data transmission, storage and processing abilities for an extended period of time.

### **IT disaster situation**

A situation in which the last operational state of the system cannot be restored within the specified recovery time.

### **IT disaster recovery plan**

A series of procedures or step to ensure that the organization's critical information processing capabilities can be restored – along with the necessary current data – in an acceptably short period of time.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **IT system**

Electronic data processing devices and procedures supporting information, management or business processes or services, plus the human resources and related processes serving the above.

### **IT system component**

A separate unit in the IT system required to introduce / create the system and affected by threat factors.

### **IT system analysis**

An analysis conducted before purchasing and introducing an IT system in order to determine the requirements of the system. It is based on the objective of introducing the IT system and on the environment in which the system is to be introduced.

### **IT emergency**

An undesired situation that can be resolved within a certain period of time using specific resources and adhering to the rules of the IT security system.

### **Information**

Accessible observation, experience or knowledge about certain facts, objects or phenomena that changes or fundamentally influences somebody's understanding, knowledge set or knowledge structure by reducing or negating uncertainty. In general information is enlightenment about the processes and material relationships of reality.

### **Information system**

A system capable of methodically collecting, storing, processing (entering, modifying, systemizing, aggregating), forwarding, receiving, displaying, destroying etc. information for a specific purpose. If the system is supported by computer technology then it's a computer information system.

### **Information protection**

Protection of the confidentiality, authenticity, and integrity of the data managed by the IT systems.

### **Directives**

General rules accepted, followed and communicated by the management of the organization. The highest level of the regulatory structure. The details of its implementation can be found in the other elements of the regulatory structure (instructions, circular mail, regulations, procedure systems, manuals etc.).

### **Authorization**

Permission granted to perform operations in the IT system.

### **Authorized user**

A user that has authorization to perform an operation.

### **Damage / loss**

Decrease of an item's value in the IT system due to the effect of a threat factor.

### **Disaster**

Interruption of the regular and continuous operation of the IT system.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Disaster Recovery Planning (DRP)**

Plans for restoring the IT system after the interruption or significant reduction of the system's availability.

### **Initial period**

The first phase of the IT product's life cycle during which the breakdown factor gradually decreases.

### **Client category**

A system of categories regulating the configuration of the institution's client computers that helps ensure that the software required for optimal operation (and nothing else) is installed on the users' computers.

### **Client consolidation**

A process based on the client categories that unifies all the client computers in the institution in order to simplify recordkeeping and make software asset management more efficient.

### **Risk**

The degree of IT threat resulting from a threat factor that is revealed during risk analysis, through the assessment of the risk factors. The risk is made up of two components: the magnitude of the potential damage / loss and the probability (frequency) of the harmful event.

### **Risk analysis**

An analytical and assessing expert examination that determines the value of the potential damage / loss and the probability (frequency) of the harmful events by evaluating the data and applications in the IT systems and analyzing their weak points and threats.

### **Risk management**

Designing, analyzing and introducing protective measures that reduce residual risks to a tolerable level.

### **Risk handling**

See Risk management.

### **Protection in proportion the risks**

Protection that derives risks from the probability of relevant threats and the extent of damage / loss they can cause. The resources spent on protection are consistent with the value of the protected assets and risk reduction.

### **Environmental security**

The protection of the availability and integrity of the IT system's resources against natural disasters.

### **Mandatory access protection**

An indicator (label) is assigned to each subject and object according to their secret protection classification. Access can be granted if the subject's secret protection classification is higher than that of the object.

### **Data of public interest**

Non-personal information managed by an individual or organization performing state, municipality or other public duties specified by law.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Central backup**

A backup procedure in which the data scattered in the network or found in different nodes of the network is saved or moved to a designated central computer where the backup is created.

### **Cryptoanalysis (cryptographic examination)**

Attempt by an unauthorized party to restore the original message without the knowledge, or only with partial knowledge of the decoding procedure.

### **Cryptography**

The research and application of mathematical procedures, algorithms and security regulations that serve primarily to conceal information from unauthorized parties.

### **Cryptology**

The theory and practice of cryptoanalysis and cryptography.

### **Critical recovery time**

The period of time for which the institution may stop providing services (for any reason) without suffering significant pecuniary or moral losses. The maximum amount of time that an application (or – more broadly – the entire IT system) can be out of service without the financial institution incurring material or non material losses beyond the tolerable level (considering the duties and obligations of the institution).

### **Special data**

Personal information about race, nationality, ethnic origin, political affiliation, religious and other beliefs, health status, addictions, sexuality and criminal record.

### **Legal software**

A software product protected by copyright that is used in accordance with the provisions of the license agreement, with all the documents necessary to certify legality (license, invoice, bill of delivery, contract of donation) being available.

### **Logic bomb**

A part or structure of a virus that is activated by time, the occurrence of an event, or a certain value of a logical variable.

### **Logical protection**

Protection in the IT system provided by means of IT devices.

### **Backup, backup scheme**

Copying a certain application (or – in the broader sense – IT system) environment (i.e. not only the data content) to a suitable storage medium without disrupting the environment.

Backups are usually created for the purpose of restoring the saved environment. The backup scheme consists of the specification of the components of the saved environment and the circumstances of creating the backup, such as the condition of the saved environment, the time or period of making the backup, periodicity, provisions regarding handling / guarding / storage, storage requirements, markings / records to be used, rules of updating etc. The purpose of the backup order is to guarantee the success of future use / restoration.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Residual risk**

Consciously accepted risk remaining despite the successful introduction of measures to counter the threat factors.

### **Reliable operation**

Protection of the availability and functionality of the IT systems and the data they manage.

### **Reliability**

In the technical sense reliability is an attribute of the IT system or an IT system component that defines to what extent the system / component can be expected to operate properly, error-free if the operating conditions are maintained.

In the mathematical sense reliability is a statistical term representing the probability of a parameter of the system or a system component falling between certain limits.

### **Breakdown factor**

An indicator of the reliability of the IT system (or a system component) that determines the probability of the system / component failing within a short period of a certain time provided that it has not failed before that time.

### **Average operating time between breakdowns**

A quantitative indicator frequently used to describe the reliability of the IT systems: the average length of error-free operation between two successive breakdowns.

### **Non-circumventability**

Ensuring that a protective measure cannot be evaded.

### **Deciphering (decryption)**

The restoration of the original message by the addressee using the proper decoding procedure.

### **Personification**

An entity (person, program, process) making itself appear to be a different entity.

### **Backup creation (saving)**

An IT procedure that copies the important, digitally stored data in the IT system to a special storage medium (backup medium), using a special device.

### **Backup medium**

The storage medium (usually magnetic tape) containing the duplicate data of the backups.

### **Backup device**

An IT device that can be used to create electronic copies of the databases stored in the IT system.

### **Backup software**

The software creating the connection between the operating system and the backup device. This software needs to make sure that the databases can be copied to the backup medium even under special circumstances.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Rating (classification)**

The decision made by the authorized person determining that a data should be kept confidential due to its nature.

### **Operability**

The system and its components remaining in the expected and required operating condition. Operability often means the same as operational reliability. The system administrator performs the basic tasks of preserving this state.

### **Defective operation, extraordinary event**

An anomaly / irregularity in the operation of the IT system. A deviation from proper operation.

### **Logging**

A function recording and documenting user authorizations and ensuring accountability in access protection.

### **Four eyes principle**

A task that may only be performed by two persons supervising each other's activities.

### **Public key infrastructure**

The infrastructure that extends the encryption methods of the Certification Authority (complying with international requirements and standards) to personnel and the physical and IT environment.

### **Public key system**

A cryptographic system whose members use a common algorithm to encrypt and decrypt data. The encryption algorithm has two keys (per user). One (the public key) is disclosed along with the user's name, while the other one is kept secret (secret key). One of the keys is used to encrypt, the other is used to decrypt.

### **Disclosure**

Making the data accessible to everybody.

### **Paper-based information**

Information concerning the usage and operation of the IT system that is available on paper.

### **Passive threat**

The danger of unauthorized disclosure of information without a change in the state of the IT system.

### **PKI**

See Public key infrastructure.

### **Problem**

A unique, highly disruptive event that significantly reduces the quality of the service provided to the users.

### **Program**

A procedure that can be executed by an IT system directly, or after transformation.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Trial version**

See Demo software.

### **Public Key Cryptosystem**

See Public key system.

### **Encryption**

Encoding a message using a cryptographic procedure, tool or method. The result is the encrypted message.

### **Availability**

A state of the IT system in which the services are constantly accessible over a period of time and the operability of the system is not obstructed even temporarily.

### **System**

A combination of items with a definable connection to one another.

### **System components**

The components of the IT system “surrounding” the data.

### **System program (system software)**

Basic software required for using the hardware and application software of the IT system. (The largest part of the system programs are the operating systems.)

### **System organization**

Organizing the management and control of the institution’s processes.

### **System administrator**

The person or unit of the organization responsible for operating a system according to business requirements.

### **System manual**

A practical but not accurate collective term for the documentation of financial applications (the IT system) and the related system components. The accurate term would be the standardized specification, system / module plan, development document, test protocol, operating instructions, user instructions etc. described in the financial internal auditing system of the financial institution (or the application service provider or the application supplier).

### **System model**

An abstract concept consisting of the description of the financial application’s processes and operations, the definition of the data model serving these processes and operations, the control scheme of related organization, human and machine operations, the data flow system and its control / operating criteria – including the technological description of the interfaces of the connected systems and the system presumed to be operational.

### **Vulnerability**

The possibility of resources being damaged in case the source of danger carries out an attack.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Window of vulnerability**

The period of time following the interruption of the IT service that the institution can endure without breaking the continuity of its normal operation.

### **Integrity**

As an attribute of the data it represents that the data is physically and logically complete, intact and unaltered. As an attribute of the IT system it means that the only the authorized parties can modify the data managed by the system and the other system components. All other alterations (both inadvertent and intentional) are impossible therefore the data and the processing are accurate and intact.

### **Shareware software**

Software that can be used free of charge for a certain period of time. It usually has limited functionality and needs to be registered and paid for eventually.

### **Rule based security policy**

An IT security policy based on general rules that apply to every user. These rules are usually based on the comparative sensitivity of accessible resources and the characteristics of the entities acting on behalf of the users or user groups.

### **Cyber-crime**

Acts committed against the confidentiality, authenticity, integrity and availability of the data managed by the IT systems or against the availability and functionality of the system components using IT devices, for financial gain or with the intent of causing damage.

### **Accountability**

Ensuring that the operations performed in the IT system are recorded for future verification.

### **Personal data**

Data pertaining to a natural person and the conclusions that can be drawn from said data.

### **Software**

A logical component of an IT system required for controlling its operation.

### **Software asset management principles**

The basic rules of purchasing and distributing software, such as (1) Only legal (properly licensed) software can be used; (2) Only the software absolutely necessary for work can be installed on the computer; (3) All employees need to have the software environment required to do their work effectively and efficiently; (4) Uniformity, easy to manage configurations.

### **Software librarian**

The person responsible for protecting and maintaining all the programs and data files. An important element of change management that ensures the separation of development and operating functions.

### **Software inventory**

A documented description of all the software installed on the computers (and other devices capable of running programs) in the organization's IT system.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Software system**

All the software used in the institution's IT system.

### **Necessary knowledge principle**

The owner of sensitive information specifying the authorizations necessary to access, possess, or use the information for a user considering the user's obligations.

### **Testing (system) environment**

The sum of all the components of the company's / organization's IT system put together to check the operation of a certain financial application. A testing environment cannot generate valid results / transactions.

### **Attack**

A person's act with the intent of endangering or harming an IT system.

### **Attack potential**

The chance of the attack being successful.

### **Comprehensive protection**

The protection of the IT system is considered comprehensive if it covers all the components of the IT system.

### **Optional access protection**

A subject may transfer its access privileges to another subject.

### **Secret protection**

Creating the conditions for protecting the confidentiality of secret information and other resources.

### **Secret personal information**

All the facts, information and data available to the institution regarding the identity, details, financial and economic status, business activity, management, ownership and/or business relations of a customer, as well as information on the customer's relationship with the institution.

### **Trojan program**

A malicious program built into another program by its designer that performs illegal operations (e.g. deletes data, performs illegal disk operations, destroys programs etc.) without the user's intention or knowledge.

### **Firewall**

A computer device that physically and logically separates one network from another.

### **Operational readiness factor (availability)**

The probability of a specific IT system component being operational at a certain time.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Operational software**

Software used to supervise and control the operation of the IT system.

### **Trade secret**

All the facts, information and data pertaining to operation and business activity that the concerned party – in its own equitable interest – has taken the necessary measures to keep confidential.

### **Business Continuity Planning (BCP)**

Maintaining the availability of the IT system on a level which ensures that the losses due to any failure are tolerable for the organization.

### **Property security**

A state of the institution in which there is minimal threat against the availability, confidentiality and integrity of the resources of the value system.

### **Source of danger**

All the things that would have an undesirable effect on the operation of the system or impair the security of the resources in case of an attack.

### **Protective measure**

Steps taken using technical devices to reduce the probability of a threat being realized, and/or the damage sustained if the threat is realized.

### **Protective mechanisms**

Protective measures specified in IT security standards that the hardware and software makers build into their products and provide to the users.

### **Restoration**

The process of re-establishing the data structure most similar to the last intact state of the damaged data from the storage media containing the backup, using a backup device.

### **Virus**

A malicious program created illegally, as part of a user application. When the application is used, the virus may “infect” other system programs or user programs in the IT system, duplicating (or mutating) itself. It may create a Trojan horse effect when a logic bomb condition is fulfilled (e.g. at a specific time, when the available disk space reaches a certain value etc.).

### **Virus protection system**

The virus protection system and the associated protective mechanisms are responsible for detecting the viruses threatening the IT system, actively or passively preventing the viruses from causing harm, and – if possible – destroying them.

### **Full protection**

The protection is full if it takes into account all the relevant risks.

### **Comprehensive protection**

The protection is comprehensive if it covers all the components of the IT system.

## **Annex III: THE DEFINITIONS OF TERMS USED IN THE REGULATIONS**

### **Version**

A specific (well defined) state of the IT system which carries the same meaning for the supplier, the service provider and the user (within the limits of their cooperation).

### **Version number**

A text code used to identify a specific version of the application. Most often it's a combination of numbers and punctuation marks. Version numbers are usually assigned by the supplier of the system. Normally the name of the IT system mentioned without the version number refers to the product in general (all versions), while the name used with the version number refers to a specific stage of the product.

### **Version change**

The process of creating and introducing a new / modified version of the IT system for internal or external reasons, from the initiation to being in everyday use. The unique feature of the version change is that the source code is modified – as opposed to system modifications where only parameters are changed. (See also: Change management).

### **Change management**

The regulated recording, managing and verification of the changes of IT resources (data, infrastructure, technology, hardware, software, personnel, rules etc.) The change manager is responsible for performing change management tasks.

### **Disruptive events**

Unexpected phenomena that have detrimental effects on IT services.

### **Full protection**

The protection of the IT system is considered full if it takes into account all the relevant risks.

**Annex IV: INCOMPATIBLE DUTIES AND RESPONSIBILITIES IN COBIT**

**ANNEX IV: INCOMPATIBLE DUTIES AND RESPONSIBILITIES IN COBIT**

<b>Incompatible duties and responsibilities (in CobiT)</b>										
	User	IT auditor	Developer	Software librarian	Dev. supporter	System admin.	Network admin	Database admin.	Operator	IT security manager
User			X	X	X		X	X	X	
IT auditor			X	X	X	X	X	X	X	
Developer	X	X		X	X	X	X	X	X	X
Software librarian	X	X	X		X	X	X			X
Devel. supporter	X	X	X	X		X	X	X		X
System admin.		X	X	X	X			X	X	
Network admin	X	X	X	X	X			X	X	
Database admin.	X	X	X		X	X	X			
Operator	X	X	X			X	X	X		X
IT security manager			X	X	X				X	

The Xs indicate incompatible duties and responsibilities  
 Blue background: parts of operation