Pillars of IT Security[1]

Tamás SZÁDECZKY

ABSTRACT *The work gives a global overview of information technology's industrial security standards. These are widely used internationally, and include, for example, ISO/IEC 27001:2005 (the new international standard of the Information Security Management System) and ISO/IEC 27002 dealing with the practical rules for controlling information safety, the Control Objectives for Information and Related Technology (COBIT), Information Technology Security Evaluation Criteria (ITSEC), Common Criteria for IT Security Evaluation (CC), and the classic Trusted Computer Systems Evaluation Criteria (TCSEC).*

The article introduces forms of regulation in the field of IT security and their conceptual aims. It summarizes all computer security related law in Hungary in the business sector: data protection, electronic commerce, electronic communications, financial institutions and electronic signatures.

The author indicates the importance of using standards in order to strengthen computer security, and the work shows which standards are obligatory under Hungarian law and which standards are most commonly used by companies and other civil entities.

1. Foreword

In the '80s, it was thought that the huge advances of electronics and computer technology meant total priority for IT in society. In other words, when the Internet became popular and accessible for everyone, it was not only government organisations and scientists who thought that, in the '90s, everyone would shop via the Internet and that paper-based mail and data storage would be taken over by computers. Now, in the twenty-first century, we know that this was simply a dream. Why?

The intensive enhancement of technology, opportunities and purchasing power did not involve application development at the same speed and also the security of network-based activities did not reach a confidence-inspiring level. The enhancement and legal usability of public key cryptography and strong secret key algorithms made it possible for computer users to have secure communication, but it is still not enough. The security of a computer hardware element, computer system or network needs a comprehensive approach and so the security of the weakest link determines the security level of the total system.

The aim is to consolidate the security of IT elements, systems and networks at the same level in every respect. This consolidation can be generated by an evaluation of the existing systems or by designing new ones. Assessing security levels without standard requirements is possible, but not reliable. This work introduces those procedures which enable uniformity of the levels of IT security, the legal requirements in Hungary and current practice in using standards.

2. Standards

[1] Published in: Balogh, Zsolt György; Chronowski, Nóra; Hornyák, Szabolcs; Nemessányi, Zoltán; Pánovics, Attila; Peres, Zsuzsanna; Szőke, Gergely László (eds.) Essays of Faculty of Law University of Pécs: Yearbook of 2010. Pécs: University of Pécs Faculty of Law, 2010. 295 p. HU ISSN 2061-8824 pp. 247-268. (Series: Studia iuridica auctoritate Universitatis Pécs publicata; Vol. 147. HU ISSN 0324-5934)

IT security standards give a universal framework to achieve a solid level in computer systems and networks. These make assessment easier and give the possibility to use the results elsewhere - for example, as an element of quality management or of a financial audit. There are a number of standards, but all differ in their focus and approach. Some are quality standards with built-in result feedback.

According to Act XXVIII of 1995 on National Standardisation Section 6, the use of national standards should be voluntary. Legislation governing technical matters may cite the application of a national standard as being compliant with the relevant requirements laid down in legislation.

The applicability and usability of standards differ markedly[2] and the choice of a standard for a particular task needs knowledge both of standards and requirements.

2.1 TCSEC

Trusted Computer Systems Evaluation Criteria (TCSEC) was the first notable standard in the field of IT security. It was written by the Department of Defense of the United States of America in 1983, revised in 1985 and issued with ID DoD 5200.28-STD. TCSEC deals with the assessment of the level of a computer system's security. The data on the systems are the subject of state- or service secrecy, or, in other words, classified information. TCSEC, which was called the Orange Book (the colour of its cover) was a genuine military IT security standard written in the Cold War. TCSEC was created mainly for the U. S. Government and the armed forces. For the practical use of TCSEC the different services made their regulations to link their requirements to the specific situation. Army Regulation 380-19 can be an example for regulation of services. Although TCSEC is still used in U. S. government and military applications[3], it is now obsolete.

TCSEC highlighted the significance of security policies, which need to be well-defined and enforced by the system. The policy can be mandatory (with full access control) or discretionary. Accountability must be also assured, which means that all activities in the system have to be bound to a user (identification), the user's authorization resources have to be verified (authentication), the logs have to protected and authorized personnel can easily access and process them (auditing). These requirements are met by assurance mechanisms. These mechanisms can be operational, such as system architecture, integrity, trusted facility management and trusted recovery. They can be life-cycle assurances such as security testing, design specification and verification, configuration management and trusted distribution. All of these functions have to be continuously protected against unauthorised changes. All classes described later differ in terms of the documentation required, such as test and design documentation, trusted facility manual and the security features user's guide.

The categorisation of security levels in the TCSEC is divided into four divisions and several sub-classes. These categories are[4]:

- D: Minimal Protection
- Evaluated systems, that has failed to meet the requirements for a higher division.
- C: Discretionary Protection
  - C1: Discretionary Security Protection. In this level, the separation of users and data, i.e., Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis is required.

[2] Muha, Lajos: Szabványok és ajánlások az informatikai biztonság területén. In: VIII. Országos (Centenáriumi) Neumann Kongresszus kiadványa. 2003. p. 501.

[3] KÜRT Computer Rendszerház Rt.: Informatikai tanúsítás és audit megvalósítása Magyarországon. Kürt, Budapest, 2002. p. 16.

[4] Wikipedia: TCSEC. http://en.wikipedia.org/wiki/TCSEC [2008.10.11.]

    - C2: Controlled Access Protection. More finely grained DAC, individual accountability through log-in procedures, audit trails and resource isolation are required.
- B: Mandatory Protection
    - B1: Labelled Security Protection. Informal statement of the security policy model, data sensitivity labels, Mandatory Access Control (MAC) over select subjects and objects, label exportation capabilities are required. All discovered flaws must be removed or otherwise mitigated.
    - B2: Structured Protection. Requirements are: security policy model clearly defined and formally documented, DAC and MAC enforcement extended to all subjects and objects, covert storage channels are analyzed for occurrence and bandwidth, carefully structured into protection-critical and non-protection-critical elements, design and implementation enable more comprehensive testing and review, authentication mechanisms are strengthened, trusted facility management is provided with administrator and operator segregation, strict configuration management controls are imposed.
    - B3: Security Domains. Satisfies reference monitor requirements, structured to exclude codes not essential to security policy enforcement, significant system engineering directed toward minimizing complexity, security administrator is supported, audit security-relevant events, automated imminent intrusion detection, notification, and response, trusted system recovery procedures, covert timing channels are analyzed for occurrence and bandwidth.
- A: Verified Protection
    - A1: Verified Design. Functionally identical to B3, but requires formal design and verification techniques including a formal top-level specification, formal management and distribution procedures.
    - Beyond A1. System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB). Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications. Formal Specification and Verification is where the TCB is verified down to source code level, using formal verification methods where feasible. Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

2.2 ITSEC

As the European equivalent of TCSEC, Great Britain, France, the Netherlands and Germany created the Information Technology Security Evaluation Criteria (ITSEC). The ITSEC version 1.2 was experimentally published in 1991 for the European Communities. ITSEC is quite similar to TCSEC in its principles and requirements, but ITSEC defines specific requirements for IT system types. ITSEC has been largely replaced by Common Criteria, which provides evaluation levels defined similarly and implements the target of evaluation (TOE) concept and the Security Target (ST) document, providing sophisticated evaluation. ITSEC defines seven evaluation levels in respect of confidence in the correctness of a Target of Evaluation (TOE). E0 designates the lowest level and E6 the highest.

The seven evaluation levels can be characterised as follows[5]:

[5] Information Technology Security Evaluation Criteria (ITSEC) Version 1.2. Department of Trade and Industry, United Kingdom, London, June 1991. p. 46.

- Level E0. This level represents inadequate assurance.
- Level E1. At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.
- Level E2. In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.
- Level E3. In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
- Level E4. In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.
- Level E5. In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.
- Level E6. In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

There are ten Example Functionality Classes in ITSEC.[6] These are made to give system specific requirements. Example Functionality Classes F-C1, F-C2, F-B1, F-B2, F-B3 have been derived from the functionality requirements of TCSEC classes. Example Functionality Class F-IN is for TOEs with high integrity requirements for data and programs. It can be used for example in database systems. Example Functionality Class F-AV has high availability requirements, it is recommended for industrial controllers. In Example Functionality Class F-DI the highest priority is the data integrity during data exchange. Example Functionality Class F-DC is for TOEs and has to give maximal confidentiality during the data exchange, for example these can be cryptographic systems. Example Functionality Class F-DX is meant for networks with high demands on the confidentiality and integrity of the information to be exchanged. For example, this can be in case when sensitive information has to be exchanged via insecure networks.

2.3 Common Criteria

Aimed to make an international standard, the European Communities, the United States and Canada made the Common Criteria for Information Technology Security Evaluation, shortly called Common Criteria (CC). Its version 2.0 became an international standard ISO/IEC 15408 "Common Criteria for Information Technology security Evaluation, version 2.0". In Hungary the Inter-Departmental Committee for Informatics (ITB) issued the CC v2.0 as Recommendation 16. The actual version is CC v3.1. It is freely accessible at http://www.commoncriteriaportal.org/.

The Common Criteria has three parts:[7]

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements

[6] Ibid. pp. 121-150.

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 1, September 2006. p. 2.

The Common Criteria has eleven functionality classes in which the functional requirements are detailed. These are:[8]

- Class FAU: Security audit
- Class FCO: Communication
- Class FCS: Cryptographic support
- Class FDP: User data protection
- Class FIA: Identification and authentication
- Class FMT: Security management
- Class FPR: Privacy
- Class FPT: Protection of the TSF
- Class FRU: Resource utilisation
- Class FTA: TOE access
- Class FTP: Trusted path/channels

There are several families in each class and several components in each family which are indicated as, for example, FAU_ARP.1. All the components are expressions concerning the requirement.

The assurance classes are:[9]

- Class APE: Protection Profile evaluation
- Class ASE: Security Target evaluation
- Class ADV: Development
- Class AGD: Guidance documents
- Class ALC: Life cycle support
- Class ATE: Tests
- Class AVA: Vulnerability assessment
- Class ACO: Composition

The level of security is determined by the Evaluation Assurance Levels (EALs) like the Ex levels in the ITSEC. These are[10]:

- EAL1 - functionally tested
- EAL2 - structurally tested
- EAL3 - methodically tested and checked
- EAL4 - methodically designed, tested, and reviewed
- EAL5 – semi-formally designed and tested
- EAL6 – semi=formally verified design and tested
- EAL7 - formally verified design and tested

Common Criteria is supplemented with Common Methodology for Information Technology Security Evaluation (CEM). This evaluation methodology is also standardized as ISO/IEC 18045:2008.

2.4 ITIL

The IT Infrastructure Library (ITIL) was developed by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom for supporting high quality cost-effective IT services. Thus ITIL is not only an IT security standard, but the best practice collection in the field of IT services. ITIL framework is a source of good practice in service management. ITIL is used by organizations worldwide to establish and improve capabilities

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 2, September 2007. p. 4.

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 2, September 2007. p. 5.

[10] Ibid. pp. 5-6.

in service management. It follows the Plan-Do-Check-Act (PDCA) model. Security related matters are embedded in the standard as IT service continuity issues. The ITIL was developed in the 80s, and the current version is v3 (issued in 2007) although under constant development. Now it is maintained by United Kingdom's Office of Government Commerce (OGC). The ITIL Service Management became a British Standard BS 15000 and later an international standard ISO/IEC 20000.

The library contains five key ITIL books:[11]

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

2.5 ISO 27000 family

The United Kingdom Government's Department of Trade and Industry (DTI) was written IT security standard BS 7799. Its approach was different from the earlier standards, because it has up-down logic. All requirements are started from business needs. ‘The standard established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization. The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices and to help build confidence in inter-organizational activities’.[12]

The BS 7799, where the BS stands for British Standard, was issued by the British Standards Institute in 1995. This original part was called Part 1. It became an international standard, called ISO/IEC 17799:2000 "Information Technology - Code of practice for information security management".

The British Standards Institute attached a second part to BS 7799 in 1999, named BS 7799-2 or BS 7799 Part 2 "Information Security Management Systems - Specification with guidance for use." The International Organization for Standardization and the IEC adopted it to an international standard ISO/IEC 27001:2005. The standard determines the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) and specifies requirements for the management of the implementation of security controls. It follows the Plan-Do-Check-Act (PDCA) model. The ISO/IEC 27001 aligns with quality assurance standards like ISO 9001 or ISO 14001. It is recommended to use this standard together with ISO/IEC 17799:2005. ISO/IEC 27001 is applicable to all organisations. It has process approach.

Due to forming a new family of standards, ISO/IEC 17799:2005 was renumbered to ISO/IEC 27002:2005. New family member standards are ISO/IEC 27005 methodology independent ISO standard for information security risk management (evolved from ISO/IEC 13335-3 and ISO/IEC 13335-4) and ISO 27006 providing guidelines for the accreditation of organizations offering ISMS certification. Numerous new standards will be a part of 27000 family, like ISO/IEC 27003, intended to offer guidance for the implementation of an ISMS (IS Management System); ISO/IEC 27004 covering information security system management measurement and metrics.[13]

[11] ITIL Version 3 Service Strategy. Office of Government Commerce, p. 23.

[12] 27000.org directory: Introduction to ISO 27002. http://www.27000.org/iso-27002.htm [2008. 12. 03.]

[13] Dósa, Imre et al.: Az informatikai jog nagy kézikönyve. Complex, Budapest, 2009. p. 686.

The content sections of the ISO/IEC 27001:2005 standard are[14].

- Introduction
- Scope
- Normative references
- Terms and definitions
- Information security management system
- Management responsibility
- Internal ISMS audits
- Management review of the ISMS
- ISMS improvements
- Annex A - Control objectives and controls
- Annex B - OECD principles and this International Standard
- Annex C - Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard

The ISO/IEC 27002:2005 consists of the following chapters[15].

- Introduction
- Scope
- Terms and definitions
- Structure of this standard
- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

2.6 COBIT

In 1992 the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) issued the Control Objectives for Information and related Technology (COBIT), which is a framework for IT management. COBIT is a best practice collection based on business requirements. It has not become a standard and is also not intended to be that. The current version, COBIT 4.1 has 34 high-level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation. Although it is not designed to collaborate with other standards, a number of mappings were made to improve collaboration and bind requirements between other standards like ITIL, ISO 27002 and PMBOK[16].

[14] ISO/IEC 27001:2005 Information technology. Security techniques. Specification for an Information Security Management System. p. 16.

[15] ISO/IEC 27002:2005 Information technology. Security techniques. Code of Practice for Information Security Management. p. 10.

[16] Guide to the Project Management Body of Knowledge (PMBOK) by Project Management Institute

The controlled processes by the COBIT are the following[17].

- Plan and Organise
  - PO1 Define a strategic IT plan.
  - PO2 Define the information architecture.
  - PO3 Determine technological direction.
  - PO4 Define IT processes, organisation and relationships.
  - PO5 Manage IT investment.
  - PO6 Communicate management aims and direction.
  - PO7 Manage IT human resources.
  - PO8 Manage quality.
  - PO9 Assess and manage IT risks.
  - PO10 Manage projects.
- Acquire and Implement
  - AI1 Identify automated solutions.
  - AI2 Acquire and maintain application software.
  - AI3 Acquire and maintain technology infrastructure.
  - AI4 Enable operation and use.
  - AI5 Procure IT resources.
  - AI6 Manage changes.
  - AI7 Install and accredit solutions and changes.
- Deliver and Support
  - DS1 Define and manage service levels.
  - DS2 Manage third-party services.
  - DS3 Manage performance and capacity.
  - DS4 Ensure continuous service.
  - DS5 Ensure systems security.
  - DS6 Identify and allocate costs.
  - DS7 Educate and train users.
  - DS8 Manage service desk and incidents.
  - DS9 Manage the configuration.
  - DS10 Manage problems.
  - DS11 Manage data.
  - DS12 Manage the physical environment.
  - DS13 Manage operations.
- Monitor and Evaluate
  - ME1 Monitor and evaluate IT performance.
  - ME2 Monitor and evaluate internal control.
  - ME3 Ensure compliance with external requirements.
  - ME4 Provide IT governance.

3. Legal requirements

The first and most fundamental level of requirements and unification of security is the legal basis. Legal requirements for IT security are constituted by the legislator mostly to increase public confidence in business and government processes. This confidence is achieved by various sophisticated requirements in different sectors. In this part I will introduce only the act-level regulation of different business fields - due to limitations on space.

[17] COBIT 4.1. Framework, Control Objectives, Management Guidelines, Maturity Models. IT Governance Institute, Rolling Meadows, IL, USA, 2007.

3.1 Data protection

As a general obligation, all institutions managing and processing personal data, except private users, fall under Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest. Section 10 concerning Security of Processing:

(1) Data managers, and, within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

This is not detailed and explained; no controls are built into the law. The Parliamentary Commissioner for Data Protection and Freedom of Information can supervise those data management and data processing, but has no coercive power, and publicity is effective only in government cases. The Act IV of 1978 on the Criminal Code specifies Misuse of Personal Data in Section 177/A. statement of facts:

(1) Any person who, in violation of the statutory provisions governing the protection and processing of personal data:

a) is engaged in the unauthorized and inappropriate processing of personal data;

b) fails to notify the data subject as required by law;

c) fails to take measures to ensure the security of data;

and thereby imposes significant injury to the interests of another person or persons is guilty of a misdemeanour punishable by imprisonment for up to one year, community service, or a fine.

(2) The acts described under Subsection (1) shall be upgraded to felonies and punishable by imprisonment for up to three years if they are committed by a public official in the course of discharging a public duty or in the pursuit of unlawful financial gain or advantage.

(3) Any misuse of special personal data shall be treated as a felony punishable by imprisonment for up to three years.

3.2 Electronic commerce

Act CVIII of 2001 on Electronic Commerce and on Information Society Services Section 4, Information to be provided in connection with Information Society services:

(3) Service providers shall provide general information concerning the level of security employed in the applied systems of information technology, the risk factors to which users are exposed, and the precautions they are required to take.

In this case, no obligations are declared regarding security, but informing clients is obligatory. This form of regulation generates a need for individual discretion and later the improvement of service quality through client demand. This approach is similar to quality assurance. Real obligations and aims are formed by the customers.

3.3 Electronic Communication

Act C of 2003 on Electronic Communications Section 156:

(1) Service providers shall take appropriate technical and organizational measures - jointly with other service providers if necessary - in order to safeguard the security of their services.

The focal point of this paragraph is the intended cooperation between service providers for security reasons. This means mostly access control measures.

(2) The technical and organizational measures shall be sufficient - with regard to best practices and the costs of the proposed measures - to afford a level of security appropriate to the risk presented in connection with the services provided.

This requirement suggests risk assessment and appropriate security measures. Despite significance and sensitivity of ICT area, the regulation and detailed requirements are scanty, even in decree-level regulations.

3.4 FPial sector

Financial sector is regulated by Act CXII of 1996 on Credit Institutions and Financial Enterprises (Hpt.), Act LXXXII of 1997 on Private Pensions and Private Pension Funds (Mpt.), Act XCVI of 1993 on Voluntary Mutual Insurance Funds (Öpt.), Act CXX of 2001 on the Capital Market (Tpt.) and Act LX of 2003 on Insurance Companies and Insurance Activity (Bit.).

Before 2004 the regulation of this field was similar to data protection act. Hpt. section 13. about Personnel and Material Requirements was the only obligation of security:

(1) Financial service activities may be only commenced or performed if the requirements pertaining to

d) the technological, informatics, technical, and security background and the premises suitable for carrying out the activities,

f) information and control system for reducing operating risks, and a plan for handling extraordinary situations

More details and a more precise requirement list were introduced by Act XXII of 2004 on Amendment of Acts Related to Increased Defence of Investors and Depositors and Act CI of 2004 on Amendment of Acts Related to Taxes, Contributions and Other Budget Payments. These Acts embodied requirements similar to those of the Protection of Information Systems to Hpt. 13/B. §, Mpt. 77/A. §, Öpt. 40/C. § and Tpt. 101/A. §.[18] Bit. was not amended, but the same controls are recommended by the Hungarian Financial Supervisory Authority[19].

(1) Financial institutions are required to set up a regulatory regime concerning the security of their information systems used for providing financial services and financial mediation, and to provide adequate protection for the information system consistent with existing security risks. The regulatory regime shall contain provisions concerning requirements of information technology, the assessment and handling of security risks in the fields of planning, purchasing, operations and control.

The regulatory regime refers to the system of regulations such as IT security policy, IT security laws, IT operational regulations. These regulations should be made and regularly (for example yearly) updated by the management. All users must know the relevant regulations.

(2) Financial institutions shall review and update the security risk assessment profile of the information system whenever necessary, or at least every other year.

[18] Currently the requirements changed and moved to Government Decree No. 283/2001. (XII. 26.) of the Cabinet.

[19] PSZÁF: A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről. p. 3.

The organisation must implement a risk assessment procedure and regular assessments. In case of usage of outsourced services, the organisation must include the outsourced areas to the assessment, also.

(3) The organizational and operating rules shall be drawn up in the light of the security risks inherent in the use of information technology, as well as the rules governing responsibilities, records and the disclosure of information, and the control procedures and regulations integrated into the system.

Roles, tasks and responsibilities have to be clearly defined without any incongruity. Scope of authority of workers has to be adequate to the role and responsibility. A Chief Information Officer (CIO) position should be formed to be responsible for IT.

(4) Financial institutions shall install an information technology control system to monitor the information system for security considerations, and shall keep this system operational at all times.

This requirement does not refer to a computer system or application, but to a set of controls and effective internal audit system. This control system has to be regularly revised, and activity and effectiveness should be measured.

(5) Based on the findings of the security risk analysis, the following utilities shall be implemented as consistent with the existing security risks:

Risk assessment in paragraph (2) is the starting point of the following.

a) clear identification of major system constituents (tools, processes, persons) and keeping logs and records accordingly;

The organisation has to make an inventory of configuration. The actual state and all previous states have to be accessible and at all times up-to-date

b) self-protection function of the information technology security system, checks and procedures to ensure the closure and complexity of the protection of critical components;

At this point, the most important is the conformity of security measures with business and organisational requirements. This conformity demands proportionate defensive measures.

c) frequently monitored user administration system operating in a regulated, managed environment (access levels, special entitlements and authorizations, powers and responsibilities, entry log, extraordinary events);

Identity- and access management procedures and rules have to be created, with rules responsible for databases. Changes in position or responsibility have to appear immediately in access levels.

d) a security platform designed to keep logs of processes which are deemed critical for the operation of the information system and that is capable of processing and evaluating these log entries regularly (and automatically if possible), or is capable of managing irregular events;

Application of log analysers used widely in the industry should be used. If not, log saving, secure archiving and manual analysis is the minimum.

e) modules to ensure the confidentiality, integrity and authenticity of data transfer;

Secure channels or protocols have to be used for communication, such as HTTPS, SSL, SSH, SFTP.

f) modules for handling data carriers in a regulated and safe environment;

Data storage media, such as DVDs, magnetic tapes have to be stored securely. It is necessary to protect them against losses and incidents due to deficiencies of technical requirements, electromagnetic disturbances, technical reliability problems, and to protect them against intentional damage and access management.

g) virus protection consistent with the security risks inherent in the system.

Protection against malicious programs is necessary in servers, desktops and mobile devices.

(6) Based on their security risk assessment profile financial institutions shall implement protection measures to best accommodate their activities and to keep their records safe and current, and shall have adopted the following:

Requirements declared in this point are minimum requirements, all are obligatory.

a) instructions and specifications for using their information system, and plans for future improvements;

Every system and application has to be documented. All services must have Service Level Agreements (SLA).

b) all such documents which enable the users to operate the information system designed to support business operations, whether directly or indirectly, independent of the status of the supplier or developer of the system (whether existing or defunct);

Within the scope of availability plan, all of these acts are included.

c) an information system that is necessary to provide services and equipment kept in reserve to ensure that services can be provided without interruption, or in the absence of such equipment, solutions used in their stead to ensure the continuity of activities and/or services;

Disaster Management Plan and Business Continuity Plan are eligible for this.

d) an information system that allows running applications to be safely separated from the environment used for development and testing, as well as proper management and monitoring of upgrades and changes;

Separation of working and test environments is an industrial common necessity. Also, the personnel of these systems should be different.

e) the software modules of the information system (applications, data, operating system and their environment) with backup and save features (types of backup, saving mode, reload and restore tests, procedure), to allow the system to be restored within the restoration time limit deemed critical in terms of the services provided. These backup files must be stored in a fireproof location separately according to risk factors, and the protection of access in the same levels as the source files must be provided for;

System backup operations also should be regularly tested.

f) a data storage system capable of frequent retrieval of records specified by law to provide sufficient facilities to ensure that archived materials are stored as defined by legal regulation, or for at least five years, and able to be retrieved and restored at any time;

Data retrieval is necessary in many cases, for example, tax revenue, anti-terrorism, data protection. A complex solution for all must be implemented, such as a high-security magnetic tape data storage system.

g) an emergency response plan for extraordinary events capable of causing any interruption in services.

Disaster Management Plan and Business Continuity Plan mentioned in paragraph c) are eligible for this function.

(7) Financial institutions shall have available at all times:

Available at all times means before financial services are authorised, and thereafter on a 24/7 basis;.

a) operating instructions and models for inspecting the structure and operation of the information system developed by themselves or developed by others on a contract basis;

All software documentations must be present and up to date.

b) the syntactical rules and storage structure of data in the information system they have developed themselves or developed by others on a contract basis;

Software documentations, especially database documentation, must contain data definition.

c) the scheme of classification of information system components into categories defined by the financial institution;

The computers, systems and networks have to be classified as to sensitivity. These rules have to be documented.

d) a description of the order of access to data;

Written rules of access control must be present.

e) the documents for designating the data manager and the system administrator;

These documents have to be present in order to ascertain personal responsibilities.

f) proof of purchase of the software used;

Also as a tax revenue requirement, all software licences and invoices must be present. A software inventory is also necessary.

g) complex and updated records of administration and business software tools comprising the information system.

A software inventory satisfies this requirement.

(8) All software shall comprise an integrated system:

This paragraph defines software minimum requirements.

a) that is capable of keeping records of the data and information required for regular operations and as prescribed by law;

As mentioned above, long-term preservation is required in more fields. The software also has to facilitate this.

b) that is capable of keeping reliable records of money and securities;

Since money is nowadays mostly account money (i.e., with no physical form), reliable records are essential for trust in the financial system.

c) that has facilities to connect, directly or indirectly, to national information systems appropriate for the activities of the financial institution;

Most administrative data is changed via computer systems, such as tax revenue, statistical information. Implementation and maintaining interfaces to them is the responsibility of the organisation.

d) that is designed for the use of checking stored data and information;

Embedded controls for data self correction and correction is imperative in such large databases.

e) that has facilities for logic protection consistent with security risks and for preventing tampering.

Value and sensitivity of stored data need endeavour on hardening logical security.

(9) The internal regulations of the financial institution shall contain provisions concerning the knowledge required in the field of information technology for filling certain positions.

In other fields job descriptions contains required IT knowledge, but financial institutions have to determine them in regulations.

As the mass of requirements shows, financial sector has much more regulations than sectors above. Reason of this is the importance and significance of this field. Most citizens keep savings in those organisations. A defect in the financial institution drastically decreases trust in the sector and the financial system inducing significant losses.

3.5 Electronic signatures

Electronic signature services such as certificate issuing, time-stamping, electronic archiving are well regulated in accordance with Directive 1999/93/EC of the European Parliament and of the Council. Act XXXV of 2001 on Electronic Signatures Section 8/B. Voluntary Accreditation is the starting point of the regulation.

(1) Service providers may devise voluntary accreditation schemes to enhance the level of their services, and to attest their organizational structure and the products and networks they

use in the provision of services, information technology security requirements laid down in specific other legislation or any other criteria they choose to adhere to voluntarily.

Voluntary accreditation is a legal possibility, but all providers are accredited in another ways. Currently no voluntary accreditation system operates in Hungary, and in its place there is a strict surveillance.

Section 7. on notification

(1) The services referred to in Paragraphs a)-d) of Subsection (1) of Section 6 in connection with electronic signatures may be provided by natural persons whose permanent or habitual residence is located in Hungary or by legal persons and unincorporated organizations that are established or have business establishments in Hungary subject to notification of the Communications Authority within 30 days before commencing activities.

In contrast to electronic communication, in the case of electronic signature services the provider has to notify authorities in advance - is a stricter control.

(2) The following shall be attached with the notification:

a) service procedures,

b) general contract terms and conditions,

c) a certified copy of the document that proves the applicant and his employees have no prior criminal record as well as a copy of documents proving their qualifications,

d) proof of liability insurance coverage and access to other financial resources as specified in specific other legislation, and

e) the authentication system and time-stamping system drafted, respectively, by the certification-service-provider and time-stamping service provider.

Procedures, plans and other proofs have to be sent prior to the start of an electronic signature service. The National Communication Authority will review those documents before giving permission for the service. Section 9. on Certification Services defines the following.

(1) Prior to contracting, the service provider shall inform the recipient of the service concerning the manner of using the service, the level of security, and - where applicable - any attestation of their organizational structure and the products and networks they use in the provision of services, information technology security requirements laid down in specific other legislation, or any other criteria they chose to adhere to voluntarily that have been attested under a voluntary accreditation scheme, and the service procedures and the contract terms and conditions, in particular the limitations defined in Subsection (2). If the inspection referred to in Subsection (3) of Section 20 is not completed at the time of commencement of the provision of services, the service provider shall inform the recipient of the service accordingly.

By this self control mechanism, clients should be informed of security measures, and so security has become a business requirement. Despite the lack of Parliamentary Act-level regulations, more governmental and ministerial decrees define regulations. However, electronic signature services are less regulated, and even self-regulation works less effectively than in the financial sector.

4. Application and results

From the standards detailed above TCSEC, ITSEC and the Common Criteria could primarily be used for evaluating hardware and software elements, but not for complex IT systems. For such complex evaluation, the ITIL, the ISO/IEC 27002 and the COBIT can be used. ITIL is the most complicated standard; its main function is IT services management, and so security is only a subsidiary topic. COBIT was published in the United States by experts dealing with financial informatics and so can be used satisfactorily in the field of finance (e.g., in banking informatics). Due to its structure, approach, and detail, ISO/IEC 27002 together with ISO/IEC 27001 are the most appropriate for using as IT security standards for designing and implementing secure systems and networks for IT experts broadly.

The application of different standards depends on the specifics of the field, international practice and the practice of the authorities involved. In respect of general business activities (where data protection and electronic commerce regulation apply) standards are rarely used, mostly due to the high cost of implementation and maintenance. European Union projects (financial support) demand the application of Common Criteria for products and ISO/IEC 27002 for organisations[20]. Firms in the telecommunications sector use no standards or ISO/IEC 27001[21]. Due to the recommendations and practice of the Hungarian Financial Supervisory Authority, the financial sector mostly uses COBIT – albeit informally[22]. In the field of electronic signature services, current certification service providers use either no standards or ISO/IEC 27001[23].

This survey shows, we feel, that a relatively low interest is shown by business in the use of international IT security standards, despite their significance and the high risk obvious in some areas. No requirement is found in Hungarian Acts of Parliament for the use of standards in IT security. There are built-in self control procedures in most Acts, but, in practice, those procedures do not work well. Higher level and more technical regulation is recommended, and increasing business requirements might enhance the security level in business fields and, therefore, at the administrative level also.

[20] Council Resolution of [6] December 2001

[21] Homepage of Magyar Telekom Plc. http://www.telekom.hu/rolunk/iranyelveink/minoseg_garanciai [2008.12.03.]

[22] PSZÁF op. cit. p. 3.

[23] Homepage of Microsec Ltd. http://srv.e-szigno.hu/menu/index.php?lap=bizt_gar [2008.12.04.]