MULTI-LATERAL SECURITY OF INFORMATION SYSTEMS – ONE OF CONDITIONS FOR JOINING THE EUROPEAN INTEGRATIONS

Prof.dr.sc. Željko Hutinski
Fakultet organizacije i informatike
Pavlinska 2. 42000 Varaždin, Croatia
e-mail: zhutinsk@foi.hr

Tedo Vrbanec, dipl. inf.
Teacher training college Čakovec
Dr. Ante Starčevića 55, 40000 Čakovec, Croatia
e-mail: tedo.vrbanec@ck.tel.hr

European integrations implicate cooperation between countries related to many spheres of interest, on many different levels. The most common spheres of interest for cooperation are culture, education, enterprise, and also there is the possibility for cooperation of the bodies of state administration. The cooperation can be realized only if there is a possibility of information exchange in such relationship. Different treatment of the data content security can be an obstacle and a limitation for realization of such cooperation.

At the end of the year of 2000, Europe declared the norm ISO/IEC 17799 – 2000, whose implementation creates preconditions for unique methodological basis for development of the system of security for business subjects. The norm is not based upon the legislations of individual countries; it opens the possibility of development of the security system for every participant in this process, based upon individual interest and estimation of need. Coordination of different approaches and interest could be realized through multi-lateral process of development of data content security, which is a precondition for the realization of desired relationships.

Development of the security system based on the standard ISO/IEC 17799-2000 is a part of development of quality system, and it is being conducted through several phases, through implementation of methodological procedures required for the development and evaluation of the security system.

1. INTRODUCTION

Globalization tendencies in the world, including the European countries, are increasingly more present and inevitable. In the field of business systems activity, globalization tendencies are manifesting themselves through the coordinated common activity according to the rules and conditions for business that were agreed upon and adopted. Such rules must be followed by all countries-members of the European Union, joined members, but also other countries that have pretensions for entering the Union. The possibility of common action is enabled by unified methodological procedures, and developed information systems that are used for follow up and description of the business activity of the organizational system. Data exchange, as a way of coordination and synchronization of the common activity, is the precondition success of business activities. In communication, the contents that should not be accessible to the non-authorized users are often in use. As the communication channels, open commuted systems of fixed or mobile telephone network are used. In such conditions, a system of measures for data content security within every individual information system, but also the communication transmission, should be developed.

Many business subjects are already developing security measures for the protection of data integrity and information systems. Measures and procedures used for that purpose differ from system to system, with different effects of protection.

This is the reason why the coordination of methodology for the construction of security systems is needed. Through such coordination, a balanced level of content security will be achieved, with the use of the same protection measures, as well as the security of business subjects and protection of business information that are in the care of other business partners. With that purpose did European

Union declare the norm ISO/IEC 17799-2000; the implementation of this norm in the development of information system security ensures methodic construction and compatibility of the solutions.

2. THE DEVELOPMENT OF THE NORM ISO/IEC 17799-2000

BSI (the British Standard Institute) is the first organization that started with systematic standardization of what we today call *security.* This organization created the norm BS7799, which was (or, more precisely, its first part) later accepted by ISO, after a comprehensive revision under the code ISO/IEC 17799-2000.

ISO (the International Organization for Standardization) is the world federation of national institutions for standardization**,** i.e. ISO members[1]. It cooperates closely with IEC (the International Electro-technical Commission) regarding the issue of standardization in electro-technical field, and together they constitute a specialized system of world standardization**.** National bodies that are members of ISO or IEC are participating in the development of international standards through technical committees, founded by one of the organizations, with purpose to cover certain fields of common interest. At this moment, there are 207 such committees. Every ISO member that is interested in field of work of a specific committee can have a representative in that committee. This work is also joined by international governmental and non-governmental organizations that are connected to ISO.

International norms are developed in accordance with the rules declared in *ISO/IEC Directives, Part 3*. The blueprints of international norms that were adopted by technical committees are submitted to all ISO members for voting, before they are accepted. For the blueprints to achieve the status of norms, 75% of members need to accept them. The chronology of the development of the mentioned norm is as follows:

- First version was created as *DTI Code of Practice* in Great Britain;
- After various changes, in February 1995 it was published as the first version BS7799
    - That version was not widely accepted out of more reasons, for example:
        - Insufficient flexibility
        - Simplified approach to the issue of keys
        - Existence of non-defined fields of security
- The significantly altered second version BS7799 was published in May 1999;
- The same year the standard was formally confirmed;
- Very soon, supporting tools appeared;
- BS7799 was adopted and confirmed in quick procedure as ISO/IEC 17799-2000 standard in the December 2000

Basically, security measures are based upon the firm definition of the following processes:

- Identification and authentication (Who are you in the network communication? Can you prove it?)
- Data secrecy and integrity (Who is allowed to read this? Is the message content altered?)
- Access rights (Who is allowed to read, change, delete, copy the data?)
- Administration and access control (Who did what, and when?)

The examples that also regulate individual fields of information system security:

- ISO:
    - ISO 15504 (Common Criteria)
    - X.800 (former ISO 7498-2)
    - ISO/IEC TR 13335-1:1996 (Concepts and models for IT Security)
    - ISO/IEC TR 13335-2:1997 (Managing and planning IT Security)
    - ISO/IEC TR 13335-3:1998 (Techniques for the management of IT Security)
    - ISO/IEC TR 13335-4:2000 (Selection of safeguards)
    - ISO/IEC TR 13335-5 (Management guidance on network security)
- ISO/BSI/IEC:
    - ISO 17799 (BS7799 Part 1)
- IT Governance Institute: CobiT
- U.S. Congress: HIPAA

[1] Source: Zdravko Krakar: Organization of development of the information systems – script, Varaždin, 1996, p.135

- NIST:
  - SP 800-12, Computer Security Handbook
  - SP 800-14, Generally Accepted (Security) Principles & Practices
  - SP 800-18, Guide for Developing Security Plans
  - SP 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
  - SP 800-26, Self-Assessment Guide for IT Systems

The (developed) world is going through a real explosion of activities whose final goal is implementation of the norm ISO 17799 in the development of the information system security, but also its change:

- Many organizations have shown interest and are preparing for implementation
- Some are already implementing the norm
- Some organizations are already certified through British standard BS 7799
- The norm is being adopted all over the international community
- The standard is facing revision because of requests from national ISO committees.

3. STRUCTURE OF NORM ISO/IEC 17799:2000

Norm ISO/IEC 17799:2000, except for introductory, has 10 chapters:

- security policy,
- organizational security,
- classification and control of equipment,
- human resource security,
- physical security and security of environment,
- communication and operation management,
- access control,
- system development and maintenance,
- management of business activity continuity,
- complaints.

Information security policy

Information security policy provides direction and support in managing of system security. Management should provide clear direction for policy and provide support to the IT security by creating and upholding information security policy. A document about security policy has to be approved by management, printed and made known to every employee. Management support with respect to the IT security should be communicated and create structure organizational approach towards managing of IT security. The following should be a minimum:

a. definition of information security, its goals and domain, as well as importance of security as a factor in sharing of information
b. management statement as support to goals and principles of information security within the organization
c. short explanation of security policy, principles standards and requests for coordination of high importance for the entire organization:
   1. coordination with legal and contract requirements
   2. request for security education
   3. prevention and detection of viruses and other malicious software
   4. managing of business continuity
   5. consequences of breach of security policy
d. definition of general and specific duties and responsibilities for managing of IT security including reporting
e. refer to documentation that serves as a support to policy and create more detailed definition of security politics and policies for IT systems and rules that users have to follow

Organizational security

It is necessary to define group of managers that will serve as core for initiation, control and implementation of IT security. It is necessary to create a body through which management can approve security policy, delegate security authorizations and clearances and coordinate implementation of security through the entire system. It is important to keep contact with security specialists outside of the company to keep up with trends, standards and risk appraisal methodology as well as to establish contact that will be able to provide support in case of an incident. It is important to encourage multidisciplinary approach to information security. For example it is advisable to encourage cooperation of managers, users, administrators, application designers, information security personnel and field experts.

Classification and control of equipment

All important IT equipment should be recorded. For all important IT equipment an owner needs to be designated. By making someone responsible for equipment during the period of use it is ensured that security measures will be applied. Every valuable peace of equipment must have an owner that has to be responsible for maintaining and applying control mechanisms. Responsibility for implementation of control can as well be delegated. Responsibility has to remain with owner of the equipment. The process of assembling an inventory list is an important aspect of risk management. An organization has to be able to identify its assets and relative importance and value of its assets. Based on the inventory information organization can determine different levels of protection with respect to importance and value of equipment. It is imperative to keep track of inventory in every IT system. Every peace of equipment has to be clearly defined with agreed and documented ownership and security classification, location (important for recovery after damage or loss). Examples of equipment ownership in IT systems:

- information – databases and files, system documentation, user guides training material, operations procedures, support procedures, continuity plans, information archiving, recovery agreements
- software – applications, system software, development and maintenance tools
- physical assets – hardware, communication equipment, magnetic storage media, other technical equipment, furniture, location.

Personnel security

When hiring new employees security issues should not be forgotten, they should be included into a contract and tracked during hiring process. Potential employees should be carefully checked especially in case of sensitive positions. All employees and third parties that use IT infrastructure should sign confidentiality agreement, that protects all the information as secret.

A check needs to performed for everybody once they apply for the job. In this procedure the following should be included:

- accessibility of professional and personal recommendations,
- check of candidate's CV for accuracy,
- confirmation of academic and professional qualifications (degrees etc.),
- independent identity check (passport or similar document)

Physical security and security of environment

Physical security should prevent unauthorized access, damage and breaking in into premises and information system. Critical and sensitive parts of computer equipment should be placed in secured places with proper controls and security measures. Necessary is physical protection from unauthorized access, damaging and scrambling or performing other actions that would prevent system from normal operation. Protection has to be in accordance with detected risks. In order to reduce risk of unauthorized access, damaging of documents, media, or hardware, clean desk and screen policy should be enforced.

Managing communications and execution

This policy has to ensure correct and secure execution of data processing. It is necessary to define responsibilities for managing and supervision of system functionality. This includes development of operational instructions and procedures for actions that have to be taken in case of an incident. It is also important to have separation of duties and responsibilities to decrease the risk of accidental or intentional wrongdoing.

Operational procedures identified in security policy have to be documented and updated. Operational procedures have to be treated as official documents, updating and changes have to be approved by management. Documents have to specify procedures, tasks and activities for every position, including:

a. processing and handling of information
b. requests for distribution (including interdependencies with other systems), earliest and latest time for starting and finishing of work time
c. guidelines for handling of errors and other exceptions, that might arise, including limitations for use of the system tools
d. contact person for support during unexpected operational and technical situations
e. special instructions for handling of processed data including procedures for secret or confidential data processing results, including procedures for secure deletion of unnecessary data
f. in case of the problem with the system, procedures for resetting the system

Access control

Access to information and business processes should be controlled by rules based on business requirements and security. Special attention should be paid to policy of distribution and authorization of information.

Business requirements for access control should be defined and documented. Rules of access control and rights for each user or group of users should be clearly outlined in the access policy. This policy should take into account the following:

a. security requirements of each business application
b. identification of all information linked to business application
c. rules for distribution and authorization of information
d. consistency of access control with policy of information classification in various systems and networks
e. relevant laws and legal obligations that regulate data access and services access
f. standardized profiles of access for regular or usual business categories
g. management of access in distributed and network environment, which recognizes all possible types of connection.

Development and maintenance of the system

This includes infrastructure, business applications and user developed applications. Design and implementation of business processes that provide support to applications or services might have key role in security. Security requirements have to be identified and validated before development of the system. All security requirements including requirements for resetting of the system should be identified in the phase of planning the project phases and requirements. The security requirements have to be justified, coordinated and documented as part of the entire business IT system specification.

Managing business continuity

It is important to prevent interruptions in business activities and to protect critical business processes from large failures or catastrophes. The process of business continuity management should be implemented to reduce interruptions caused by catastrophes and security breaches (which can be caused by catastrophes, accidents, equipment failures or purposely provoked) to an acceptable level. A combination of preventive and reactive control mechanisms should be used to reach desired levels of business continuity. Management of business process continuity has to include control mechanisms for identification and reduction of risks as well as for containing of incidents and finally mechanisms that will ensure fast reinstating of applications

Coordination

Coordination is important to prevent breaking of laws, regulations or contracted security obligations. Legal advisors as well as lawyers and internal rules and regulations guidelines have to be consulted to determine specific legal requirements. Legal requirements and obligations vary from country to country.

Experience has shown that the following are critical success factors for successful implementation of information system security:

a. security policy, goals and activities that reflect business objectives
b. information security implementation approach that is consistent with organizational culture
c. noticeable support and commitment of management
d. thorough understanding of security requirements, risk assessment and management
e. efficient motivation system for development among all managers and employees
f. distribution of guidelines about the information security policy to all employees and contractors
g. provision of adequate education and training
h. far reaching and balanced measurement system for evaluation of security management and for receiving feedback for improvement measures

4. INTRODUCING NORM TO THE BUSINESS SYSTEM

To develop the security system according to the norm ISO/IEC 17799-2000, all described steps and proscribed actions should be followed. This guarantees equal approach to the risk assessment in the business system, and the choice of measures that will reduce the risk. Main steps that should be followed in the analysis of the security situation in the business system according to BS 7799-2 are shown in figure 1.

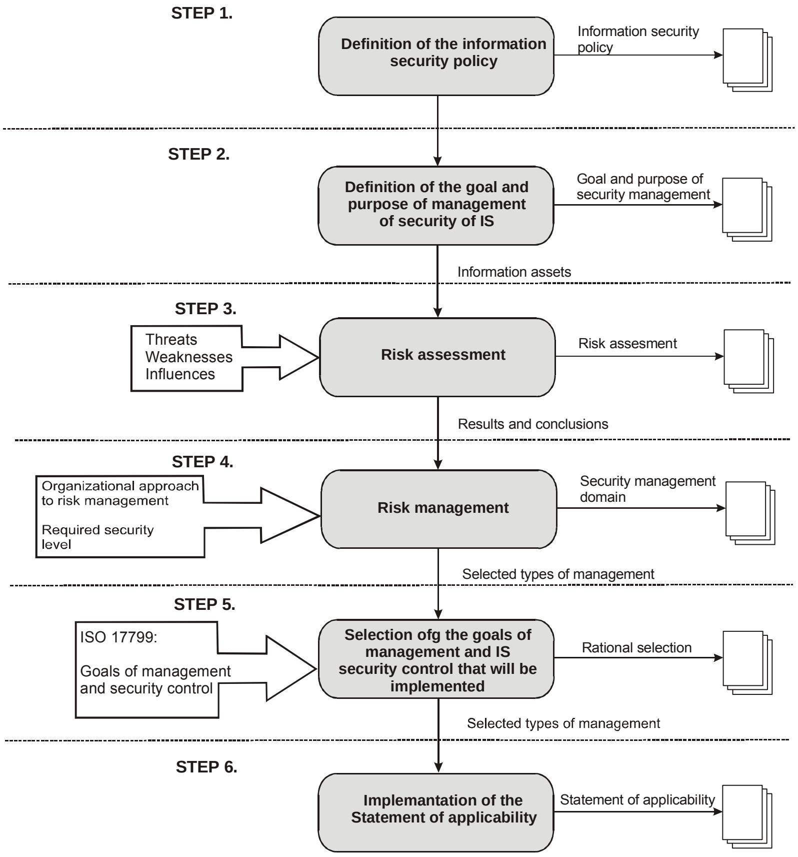
STEP 1.
Definition of the information security policy
Information security policy
STEP 2.
Definition of the goal and purpose of management of security of IS
Goal and purpose of security management
Information assets
STEP 3.
Threats
Weaknesses
Influences
Risk assessment
Risk assesment
Results and conclusions
STEP 4.
Organizational approach to risk management
Required security level
Risk management
Security management domain
Selected types of management
STEP 5.
ISO 17799:
Goals of management and security control
Selection ofg the goals of management and IS security control that will be implemented
Rational selection
Selected types of management
STEP 6.
Implemantation of the Statement of applicability
Statement of applicability

Figure 1. Main steps of analysis of the business system security

Information security policy

The first step consists of analysis and definition of all information assets important for an organization. After that, it is specified in detail in the document under the title *Information security policy*, along with the reasons of its importance. From the practical viewpoint, focus should be only on information assets with certain level of importance for an organization.

Definition of goal and purpose of information security

Exception of information with low level of importance enables us to define the purpose of information security. If the conclusion is that *the organization business as a whole* is important for the information security, the whole information system and its interface with the environment will have to be reviewed:

- IT
- Electronic forms of information exchange
- Data storage locations
- Telephone conversation
- Public relations etc

so we may stay within the purpose of information security. Alternately, we can focus on those systems that are in the direct contact with the clients/customers. The other extreme is the application of the norm BS 7799 only to the development, production and deliverance of the products that are of interest for the informational security.

Risk assessment

Now that we know which data are important to us and what values may they have, the next step is to find out how high is the risk of losing these data; it is necessary to take into account all aspects. The following should be reviewed:

- Complexity of the existing technologies
- Pressure of the technological progress
- Progress of the organization as a whole
- Real possibility of industrial espionage
- All other relevant risk aspects

Risk management

In this step, it is necessary to decide in which way to manage the risk. Some levers of the risk management may be the following:

- Technology
- Human resources
- Administrative procedures
- Physical protection
- Security etc.

If some type of protection cannot be implemented or it does not pay off, perhaps it is possible to detect the security incident while it is still in the beginning phase, and disable it before it caused real damage; or, at least, to diminish the damage that has already been done. It is also necessary to make an efficient plan for risk management.

Selection of the goals of security management and control

In this step, the forms of risk management that we chose are specified. BS 7799 contains various possibilities and forms of management of security of the information system, but the list is not final and it is possible to add measures and forms of protection that are adequate for us. That list is, in fact, ISO/IEC 17799-2000.

Applicability statement

As the final step of implementation of BS7799, the responsibility of the organization is identification of the security measures that will be implemented and the reasons for thier choice. It is also necessary to explain why some of the measures suggested in BS7799 are not relevant for the security system of the information system of that organization. It is completely in accord with the norm *not to choose any of the suggested security measures*, but to design a set of new measures. Still, it is necessary to justify all control mechanisms designed in such manner, for organization's benefit, as well as the benefit of others (revisers, law makers, clients...).

ISMS (The Information Security Management System)

The norm requires implementation of ISMS, the Information security management system. Still, it does not specify the manner in which it should be implemented. It is also one of the objections of some national ISO committees.

After the coordination of measures of security of the information system with the norm, it is necessary to conduct the procedure of certification as to verify the justification and appropriateness of specific security measures. Also, a certain level of data content security is guaranteed, so that all participants in the business transactions could be familiar with the measures, and rest assured that their data, which is being used in another information system, have adequate security treatment and protection.

There are several certification schemes present in the world today. For us, the most interesting one is the scheme of European accreditation (EA). This body originated by integration of two other bodies: EAC (European Accreditation of Certification) and EAL (European co-operation for Accreditation of Laboratories). These two were the roof organizations that have united the European national accreditation bodies, and now they are joined into one organization, EA, which deals with the assessment activities:

- Testing and measuring
- Inspection
- Certification of management systems
- Certification of the personnel
- Environment verification

In its document under the title EA7/03, EA declared guidelines for the national committees for accreditation[2] regarding the accreditation of the ***certification committees.*** The certification committees deal with the analysis of the coordination of ISMS – the Information security management systems with BS7799, and issue the certificates.

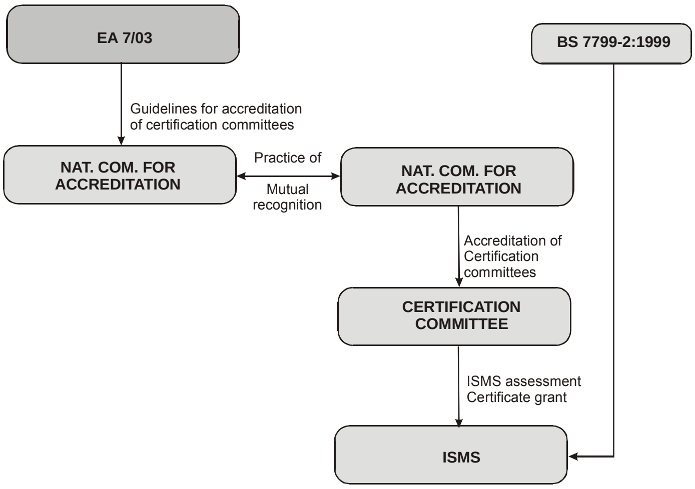
EA 7/03
BS 7799-2:1999
Guidelines for accreditation of certification committees
NAT. COM. FOR ACCREDITATION
Practice of
Mutual recognition
NAT. COM. FOR ACCREDITATION
Accreditation of Certification committees
CERTIFICATION COMMITTEE
ISMS assessment Certificate grant
ISMS

Figure 2: Relations between main participants in the certification process

The process of certification is conducted in the following manner:

- Preliminary actions/preconditions: creation of ISMS, consulting activities and coordination of ISMS with BS7799.
- Revision of the ISMS by BS7799 assessor who **must not** be a consultant, and who works for the certification committee.
- The certification committee issues certificate that will define the purpose of ISMS and other relevant details like *Applicability statement.* Only those certificate committees that have valid accreditation could issue the certificate.

5. CONCLUSION

Because of the development of local networks and linking with the Internet, the problems of information systems security are increasing. To enable undisturbed functioning of the information system, security and protection need to be carefully and properly planned, implemented and controlled, on both side of the communication channel, regardless to the special, economical or cultural distance. Only well-conceived and implemented protection on all levels, as well as the frequent control and supervision of the implementation of security measures can result in undisturbed work of the system, which is the precondition for joined business actions, and the reason for the integrations.

The assessment and formal implementation of the norm(s) of information security of IS are worth as much as the consciousness of the need for real implementation of security and control measures is strong. Perhaps the biggest single security challenge today is the consciousness of the personnel. Regarding the facts that security cracks are discovered every day, and that the virus are causing

[2] National committees for accreditation have a practice of mutual recognition, i.e. certificate in one country is valid in any other country

enormous damages, the education of the personnel ceases to be a matter of choice, and becomes inevitability

It is not enough to patch the security cracks with technology, for example to renew virus definitions or add anti-virus protection to the e-mail clients. It is necessary to educate people about the need to change their behavior and to respect the security policy. The most recent standard of information system security ISO/IEC 17799-2000 regards the consciousness of the personnel about the importance of information security to be the key precondition for security policy implementation.

The latest researches of *Information Week* magazine show that only 9% of the employees understands the security policy that they need to implement. This confirms the hypothesis that information security is not just a technological problem, but also an organizational problem. The organization policy should not be an obstacle in the normal work process; it should be a protection, for the organization as well as for every individual. On the other hand, it should also define penalties for breaking the rules. ISO/IEC 17799 – 2000 clearly indicates that the users of the information systems should be able to identify security incidents and to inform the management about them. It should be also made clear who is responsible for the reaction in case of security incidents.

The policy of information system security should establish a safe environment for the functioning of the information system. The security costs should be adequate to the data value, respecting the value the data may have for its owner, for its user and for potential intruder. The basic task of the information security policy is to initiate an organization and its human, organizational and technological resources to develop the necessary projects and analysis, and to implement the security measures and the related rules. In this process, observing the security norm(s) like ISO/IEC 17799-2000 is the guarantee that it is going in the right direction. In every organization that is aware of the meaning of security and the possibilities of the information technology, and that has a need for inter-organizational communication and/or entry into the global market through Internet, the introduction of such system of information security, which will be efficient and recognized by potential clients/customers and business partners, has become a necessity. Certification of the organizational system according to the norm ISO/IEC 17799-2000 (in this moment, it is still the norm BS7799) creates the strategic advantage and enables the real ascent of the business on the new, global market. We may only hope that the alternations of the norm ISO/IEC 17799-2000 will be made quickly, so the obstacles for certification and acceptance in all countries can be removed.

5. BIBLIOGRAPHY

1. *ISO/IEC 17799 – 2000* (*BS 7799 – 2000 Part 1*) – Međunarodna norma za izgradnju sigurnosti IS-a
2. Vladimir Anić, Ivo Goldstein: *Rječnik stranih riječi*, Novi Liber, Zagreb, 1999.
3. Zdravko Krakar: *Organizacija izgradnje informacijskih sustava* – skripta, Varaždin, 1996.
4. *Word Translator '97*, ver. 5.2e; www.tranexp.com
5. http://csrc.nist.gov/publications/secpubs/
6. http://healthnet.hnet.bc.ca/hds/proposed_standards/iso_17799_spid.html
7. www.active-information.co.uk/bs7799iso17799securityconsultant.htm
8. www.gammassl.co.uk/
9. www.iso-17799-security-world.co.uk/
10. www.iso17799software.com/
11. www.securityauditor.net/
12. www.vigilinx.com/pdf/50722_White_Paper-SAM.pdf
13. www.yourgateway.to/iso17799/
14. www.iso.com/ISO_AnnualreportE.p65
15. www.atsec.com/e/service_iso17799.php3
16. www.infoexpert.hr
17. www.in2.hr/hroug/glasnik3/security.htm
18. www.borea.hr
19. www.gammassl.co.uk/inforisk/
20. Goran Oparnica, *Sigurnost informacijskih sustava,* [www.in2.hr/hroug]
21. David Lineman: *Policies for the People!*; Info Security Magazine - Making Security a State of Mind, June 2001. [www.scmagazine.com/]
22. Miroslav Benak: *Bolje spriječiti nego liječiti*, PCchip, 14. 2. 2000. [www.pcchip.hr]
23. http://csrc.nist.gov/publications/nistpubs/