The Information Security Management System, Development and Audit

Traian SURCEL, Bucharest, Romania, tsurcel@ase.ro
Cristian AMANCEI, Bucharest, Romania, cristian.amancei@ie.ase.ro

Information security management system (ISMS) is that part of the overall management system, based on a business risk approach, that it is developed in order to establish, implement, operate, monitor, review, maintain and improve information security.

ISMS component of information system

Businesses have major goals (i.e. increasing profit, larger market share), none of these goals will be met by the business if they do not find out what users want, and also do not find ways of satisfying those users' needs. Information security should be an integral part of the organization's operating and business culture. Let's analyze the steps to be followed in establishing the ISMS in the organization.

The first step is to define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology. The scope needs to take account any interfaces with other systems, organizations, third party suppliers, and it also needs to take account any dependencies, e.g. security requirements that need to be satisfied by the ISMS.

The second step is to define the ISMS policy in terms of the characteristics of the business, the organizations, its location, assets and technology that includes a framework for setting its objectives and establishes an overall sense of the direction and principles for action with regard to information security. Also we have to take into account business and legal or regulatory requirements, and contractual security obligations in special with: third party suppliers, dial-up / internet access, shared processing with business partners.

We have to establish criteria against which risk will be evaluated and the structure of the risk assessment will be defined.

As the step three, at this moment, a systematic approach to risk assessment has to be defined. We can do this by identifying a method of risk assessment that is suited to the ISMS, and the identified business information security, legal and regulatory requirements. We have to set policies and objectives for the ISMS to reduce risks to acceptable levels and to determine criteria for accepting the risks and identify the acceptable levels of risk.

Step four is to identify the risks by: identify the assets within scope of the ISMS and the owners of these assets, identify the threats to those assets, identify the vulnerabilities that might be exploited by the threats, identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

Step five is to assess the risks, by assessing the business harm that might result from a security failure, taking into account the potential consequences of a lose of confidentiality, integrity or availability of the assets, and by assessing the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.

Step six is to identify and evaluate options for the treatment of risks. Actions the organization could consider: applying appropriate controls, knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance, avoiding risks, transferring the associated business risks to other parties (i.e. insurers, suppliers, third parties).

Step seven, select control objectives and controls for the treatment of risks. The selection of controls should be cost effective, i.e. the cost of their implementation should not exceed the financial impact of the risks they are intended to reduce. Some of the impacts will be non-financial, those impacts should be taken into account when they are related to safety, personal information, legal and regulatory obligations, image and reputation.

Step eight is to prepare a statement of applicabil-

ity. The control objectives, controls selected and the reasons for their selection shall be documented in the Statement of Applicability.

The last step is to obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

At this moment the ISMS project can move to next stages, implementation and operation of the ISMS, monitor and review of the ISMS, maintenance and improvement of the ISMS.

In order to be operable the ISMS documentation will include the following: documented statements of the security policy and control objectives; the scope of the ISMS, procedures and controls in support of the ISMS; risk assessment report; risk treatment plan; documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes; statement of applicability.

It's useful to take a look to some examples of control objective and controls for system development and maintenance and business continuity management.

a) System development and maintenance

1. Security requirements for operating systems and application systems, the control objective, is to ensure that security is built into information systems and can prevent loss, modification or misuse of user data. Controls that can be applied are:

- security requirements analysis and specification. Business requirements for new systems, or enhancements to existing system shall specify the requirements for controls;
- input data validation. Data input to application system shall be validated to ensure that it is correct and appropriate;
- control of internal processing. Validation checks shall be incorporated into systems to detect any corruption of the data processed. Reports with errors must be defined into the system to return missed matches that are found during processing;
- output data validation. Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances;

2. Ccryptographic controls, the control objective is to protect the confidentiality, authenticity or integrity of information. Controls that can be applied are:

- policies and management. A management system should be developed, based on an agreed set of standards, procedures and methods that shall be used to support the use of cryptographic techniques;
- encryption. Encryption shall be applied to protect the confidentiality of sensitive or critical information;
- non-repudiation services. Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action;

3. Security of system files, the control objective is to ensure that IT projects and support activities are conducted in a secure manner. Controls that can be applied are:

- control of operational software. Procedures shall be in place to the implementation of software on production systems.
- access control to program source library and database. Strict control shall be maintained over access to program source libraries and database or a third party provider can be used for development and maintenance of program source libraries.

4. Security in development and support processes, the control objective is to maintain the security of application system software and information. Controls that can be applied are:

- change control procedures. The implementation of changes shall be strictly controlled by the use of formal change control procedures and under strict observation.
- technical review of operating system changes. Application system shall be reviewed and tested when changes occur, before being applied on production servers.
- outsourced software development. Controls shall be applied to secure outsourced software development.

b) Business continuity management

For Business continuity management the control objective is to counteract interruptions to business activities and to protect critical business processes from the effects of

major failures or disasters. In practice the tolerance of the business to a system failure gives the importance of the business continuity management (for a business where system availability is very critical, tolerable disruption less than one day, the business continuity management will become very important). Controls that can be implemented are:

First control is the business continuity management process. The business should have a managed process in place for developing and maintaining business continuity throughout the organization.

Second control is the business continuity and impact analysis. In order to accomplish this, a strategy plan, based on appropriate risk assessment, will be developed for the overall approach to business continuity.

Third control is the business continuity planning framework. It has to be developed and maintained, a single framework of business continuity plans, in order to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

Fourth control is the testing, maintaining and re-assessing business continuity plans. Business continuity plans will be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.

ISMS – PDCA Model

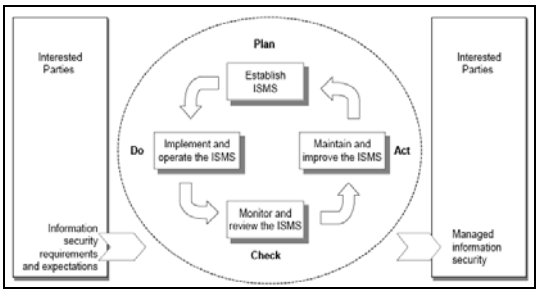
The ISMS process requirements address how an organization should establish and maintain their ISMS, based on the Plan-Do-Check-Act (PDCA) model.

Plan - establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with organization's mission and objectives.

Do - Implement and operate the ISMS policy, controls, processes and procedures, following the best practice approach.

Check - Assess and measure process performance (if applicable) against ISMS policy, objectives and practical experience and report the results to management for review.

Act - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.



PDCA model for ISMS

II. ISMS Audit

The ISMS audit can be analyzed also discussing shortly the stages necessary to accomplish this.

Stage 1, gain an understanding of the ISMS in the context of the organization's security policy and objectives, approach to risk management.

Stage 2 is more complex. We must obtain the confirmation that the organization is acting in accordance with its own policies, objectives and procedures and the ISMS is conform to all standard requirements. Next, assessment of information security related risks and the resulting design of its ISMS. It follows are some checking sub stages: checking objectives and targets derived from this process; checking performance monitoring, measuring, reporting and reviewing against the objectives and targets; checking management responsibility for the information security policy; confirmation that monitoring of the informatics systems is reviewed and a follow up is made for unusual actions; checking that the organization is aware of the IT environment importance; and checking the following issues to see how is the organization prepared:

- Does the organization ensure that the IT is part of the organization strategies?
- Is the IT department formally organized, and able to maintain the appropriate segregation of duties while also providing continuity of key IT functions?
- Is the organization able to keep their key employees?
- How is the organization able to continue their activity in the case of IT disruption or

lost of key employees?

Stage 3, review of the network diagram to see how is the organization prepared against external attacks (i.e. antivirus program, firewall) and review the IT organizational structure to see if appropriate segregation of duties is maintained.

Stage 4, refers to application. Review the process of implementing changes on the application. Review backups procedures, antivirus and other security systems used in the organization. Review the access on the network and on the application to see if an appropriate password policy is being implemented. Review the user access rights, according to their needs.

Stage 5, test of controls for the controls identified as being automated/semi-automated / manual.

III. Conclusion

The importance of ISMS continues to grow as the tolerable disruption for the IT systems tends to become very critical, in this environment the companies that are not conscious about the importance of the IT environment, that do not have an IT strategy developed and integrated with the company long term and short term strategy, can loose in the battle with the competition.

References

1. [GHS 04] Tim Grance, Joan Hash, Marc Stevens – *Security Considerations in the Information System Development Life Cycle*, NIST Gaithensburg, MD 20899-8930, USA, 2004;

2. [TRS 06] Traian Surcel, *Auditul şi managementul sistemelor informatice*, The Preceedings of The 2006 International Conference on Commerce, Bucureşti, 2006, ISBN 10-73-594-785-4;

3. [TSMS 05] Tr. Surcel , M.Stoica - *Reasearch Areas in Data Warehouse Systems Audit",* în Revista Economy Informatics vol V, nr. 1-4 / 2005, ISSN 1582-7941;

4. SR ISO/CEI 17799 *Tehnologia informaţiei Cod de practică pentru managementul securităţii informaţiei* , ASRO 2004 Indice de clasificare X 22