13th International Research/Expert Conference
"Trends in the Development of Machinery and Associated Technology"
TMT 2009, Hammamet, Tunisia, 16-21 October 2009

ADAPTATING INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION TO ORGANISATION DEMANDS

Enver Delić, IPI Instut za Privredni Inženjering, Saradnik za sisteme upravljanja, ISO 27001 Lead Auditor, enver.d@ipi.ba
Elvis Pivić, a|NET, Saradnik za ekonomsko-pravne poslove, ISO 9001 Internal Auditor, elvis@anet.ba
Zenica, Bosnia and Herzegovina

ABSTRACT
The proliferation of increasingly complex, sophisticated and global threats to information security, in combination with the compliance requirements of a flood of computer and privacy-related regulation around the world, is driving organizations to take a more strategic view of information security. This document describes process of preparing the organization for adopting best practices in information system management based on clauses of ISO/IEC 27001:2005. Special attention is given to the processes of information classification and access control, business continuity, education and training of employees as well as management of system maintenance.
Key words: ISMS, information security, ISO 27001, management systems

1. INTRODUCTION
In 2009 "IPI Institut za privredni inženjering Zenica" has successfully passed certification of the information system for gathering, processing and distributing data from vehicle testing stations named "a|TEST", according to ISO/IEC 27001:2005.
During the implementation process we gathered valuable experience that we think other organizations that want to implement this standard might find usable. In this document we will explain necessary procedures and protection methods for the effective protection of confidential information in different surroundings.

2. INFORMATION SECURITY MANAGEMENT SYSTEM
Efficient implementation and maintenance of secure organization surroundings for information, transactions and predefined set of important processes is managed through information security management system (ISMS), in which we can separate several phases:

1. Organization of security with definitions of rules and responsibilities of all involved employees
2. Documenting:
   - Risk analyses
   - Policies, rules, guides and manuals
   - Raising awareness on information security through education, process redesign and technology use
3. Supervision and audit
4. Business continuity and disaster recovery plans

2.1. Management support
Management's responsibility goes beyond the basics of support. They must set the tone for the entire program. It is not enough just to bless the program. Management must own up to the program by

becoming a part of the process. Management is responsible for overseeing the development, implementation, and maintenance of ISMS. This includes defining the information security objectives of the organization, allocating an amount of money to be invested in information security, and ensuring the compliancy and enforcement of implementation.
It is the responsibility of management to form Information Security Management Committee that will be responsible for reviewing changes in the business and determining how ISMS implementation should support those changes.

2.2. Security policy
The purpose of the policy is to protect the organization's information assets from all threats, whether internal or external, deliberate or accidental. It has to be approved by top management. Policy should include requirements for integrity, availability and congeniality of the information covered by ISMS. Policy also helps us delegate responsibilities of employees, define processes and audit effectiveness of ISMS implementation.
ISMS policy at IPI Institut za Privredni Inženjering covered these topics:

- Company environment
- Main processes
- Data classification
- Manuals
- Support processes

Security policy is changing continuously and adapting to organization needs.

2.3. Data classification
A formal assessment needs to be undertaken of the risk of inappropriate exposure of information under the control of the organization. For new information systems, risk assessment is to be done during the business case development so that costs can be identified and risks registered. Once the business sponsor has made a decision as to the classification of the information, the decision should be noted in the department's "Asset Register". This classification should be reviewed by the business owner at least annually.

2.4. Processes
An organization must identify and manage a number of its activities to effectively operate its ISMS. ISO/IEC 27001 recommends that an organization should adopt a process approach when it establishes, implements, operates, monitors, reviews, maintains and improves the organization's ISMS.
In the process approach, what are referred to as processes are any activities that are managed using management resources in order to transform inputs into outputs. A process approach means identifying the processes within an organization, grasping their interaction, and applying and managing a series of those processes as a system.
The adoption of this process approach provides organizations with the benefit of being able to effectively operate their ISMS, through managing combinations of and interaction among processes together with links of individual processes.
Among the most important identified processes at IPI Institut za Privredni Inženjering are:

- "Access Control" with descriptions of methods for assigning, revoking, supervision and revision of access rights for different user groups. Rights and responsibilities have to be separated among different groups, and we can recommend revoking of "*superuser"* account because of supervision difficulties.
- "Business Continuity" contains plan for restoring the basic organization process in case of system breakdown at secondary location and set of measures for troubleshooting. Plan also includes set of procedures which define incident management responsibilities and notifications scheme.
- "Resource Management" has to be connected with access control to improve efficiency. All resources must be listed, evaluated for importance based on confidentiality, availability and integrity requirements, and have dedicated owner.
- "Employee Education" has to be management's strategic decision, well planed and adapted to organization needs and employee interests. If we know that most of the

information security threats come from people and that most of the standard clauses are related to people, than this segment is of the most importance.

- "System Maintenance" is the most vulnerable process that we have to consider. Large number of threats that have to be controlled complicates the implementation of threat management controls.
- "Document Management" is almost identical to demands of ISO 9001 standard, and organizations that have this standard implemented will have easier job implementing ISO 27001.

2.5. System implementation procedure

During system implementation it is necessary to define major business processes, analyze them and put them in context of organizations major business activities. After that we identify all resources required for operation basic system functions, their importance, known threats and vulnerabilities and consequences of undesired situation. Based on these factors we create business continuity plan.

Since the humans are the most critical part of system security we have to raise information security awareness with appropriate propaganda material and continuous education. IT administrators and other technical stuff should attend specialized courses in security technology (Intrusion detection and prevention systems, Firewalls, Virtual Private Networks, Encryption methods, etc). Thanks to the WEB apps we can distribute education material easily, as well as running continuous knowledge assessment.

Penetration testing (aka *Ethical hacking*) is a ¸information system security assessment method that represents real hacker attacks. Penetration testing should be carried out carefully, as it could lead to a system compromise. In practice, penetration testing should not be scheduled until the organization considers that it has implemented the controls identified by its risk assessment and statement of applicability (SoA), and planning for the tests should include ensuring that suitable back-up and business continuity arrangements are in place beforehand.

Regarding internal audit, no audit can take place until sufficient time has passed for the organization to demonstrate compliance with the full PDCA cycle, legal requirements and with clause 7, the requirement for continual improvement. In other words, auditors will be looking for evidence that the ISMS is continuing to improve, not merely that it has been implemented. This means that a period of time will have to elapse between completion of the implementation and commencement of audit. How long will depend on the complexity of the organization and its ISMS, but one should assume that there will need to be at least one cycle of internal audits for all of the key processes and arrangements. During internal audit at IPI Institut za Privredni Inženjering we used services of two certified 27001 and 9001 auditors.

During implementation period we developed set of strategies and methods that can be used to achieve preparedness for certification in a more efficient and effective manner, and we will use them to set up ISMS in their organizations after which they can opt for certification against ISO/IEC 27001.

3. CONCLUSION

ISO/IEC 27001 is in information security what ISO 9001 is in business excellence and quality – standard written by worlds leading experts in the field of information security management with purpose of setting up a methodology for proper deployment of ISMS at any organization. The path to the successful ISMS implementation is determined by careful choice of experienced experts with outstanding knowledge of standard clauses and Plan-Do-Check-Act model.

It should be noted that ISO 27001 is a service assurance scheme, not a product badge or cast-iron guarantee. Achieving ISO27001 certification does not of itself prove that the organization has a completely secure information system; it is merely an indicator, particularly to third parties, that the objective of achieving complete security is being effectively pursued. Information security is, in the terms of the cliché, a journey, not a destination.

4. REFERENCES

[1] Sandra Senft, Frederick Gallegos: Information Technology Control and Audit, Auerbach Publications, 2008.

[2] Mr.Sc. Leon Maglić: Istraživanje efektivnosti sustava upravljanja kvalitetom, Doktorski rad, Sveučilište u Zagrebu, Fakultet strojarstva i brodogradnje, 2008.

[3] Enver Delić, Elvis Pivić, Adnan Strojil: Nadzor ISMS-a i ISO/IEC 27001:2005, 6. Naučno-stručni skup sa sa međunarodnim učešćem "KVALITET 2009", Neum

[4] Andreas Mitrakas: Information Security and Law in Europe: Risks Checked? European Network and Information Security Agency (ENISA), 2006.

[5] Enver Delić, Dragana Agić: Implementacija ISO 27001, 6. Naučno-stručni skup sa sa međunarodnim učešćem "KVALITET 2009", Neum 2009.

[6] Mario Apostolov: Using International Standards, Norms and Tools for e-Business, SEE Ministerial Conference on Information Society Development Sarajevo, 2007