Information Security Specialist Training on the Basis of ISO/IEC 27002

Natalia Miloslavskaya, Alexander Tolstoy

Information Security Specialist Training on the Basis of ISO/IEC 27002

Natalia Miloslavskaya, Alexander Tolstoy

Moscow Engineering Physics Institute (State University), Russia, {milmur, ait}@mephi.edu

Abstract: Information Security (IS) specialists' training for all sectors of trade, industry and government has never been more important as intellectual property and other sensitive or business-critical information becomes the life-blood of many companies today. Analysis of the experience collected within training of IS specialists at the Moscow Engineering Physics Institute (State University) (the MEPhI) at the Information Security Faculty allows forming the basic requirements to the level of their preparation. To form such requirements it is expedient to take a look at the types and tasks of professional activity of the graduates and to formulate their qualification characteristics. This paper formulates these characteristics on the basis of ISO/IEC 27002 (former ISO/IEC 17799:2005).

Keywords: Information Security Education, Specialist Training, ISO/IEC 27002

1. ISO/IEC 27002

A family of Information Security Management System (ISMS) International Standards, being developed within Joint Technical Committee ISO/IEC JTC 1/SC 27, includes International Standards on ISMS requirements, risk management, metrics and measurement, and implementation guidance. The ISO/IEC 27002 Standard "Information Technology – Security Techniques – Code of Practice for Information Security Management" gives comprehensive guidance on best practice methods for implementing ISO/IEC 27001 "Information Security Management Systems Specification", which specifies requirements for establishing, implementing, maintaining, improving and documenting ISMS for both public and private sector organizations.

ISO/IEC 27001 is the de-facto international standard. It specifies requirements for establishing, implementing, maintaining, improving and documenting ISMS for both public and private sector organizations. It specifies security controls to be implemented by an organization following a risk assessment to identify the most appropriate control objectives and controls applicable to their own needs. This standard forms the basis of an assessment of the ISMS of the whole, or part of an organization and covers the eleven clauses of good IS practice: Security Policy; Organizing 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.

ISO/IEC 27002 [1] as a technology independent standard offers a framework to assist any organization to develop a true security minded corporate culture by instilling best practice and detailed guidance regarding all manner of security issues. The guiding principles cover three main aspects: strategic, operational and compliance. ISO/IEC 27002 concentrates on the IS management aspects, defining the controls in enough detail to make them applicable across many different applications, systems and technology platforms without losing any of the benefits provided by standardization. The main characteristics of ISO/IEC 27002 are the following: proven value; widely known and accepted; easy to understand; continuous value; market driven; flexible; adaptable; scalable and so on.

Thus ISO/IEC 27002 provides a stable and comprehensive base for formulating the qualification characteristics of IS specialists, being capable to design, implement and control IS at various types of business organizations. Alignment with the standard also offers a high level of standardization in training worldwide with skills and knowledge set founded upon a uniform, known and acceptable base.

2. IS Specialists' Training and International Standards

Comprehensive security requires secure technologies, organizational processes and people with the necessary background and skills. A large number of certifications are found in the field of IS.

(ISC)² offers the Systems Security Certified Practitioner (SSCP) and the Certified Information Systems Security Professional (CISSP) certifications. The Information Systems Audit and Control Association (ISACA) has a pair of vendor-neutral credentials: the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM). CompTIA Security+ certification exam covers communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organizational security. Software provider Check Point offers a range of security

and security management certifications that deal with both general skills and knowledge as well as the company's specific solutions: the Check Point Certified Security Principles Associate (CCSPA), the Check Point Certified Security Expert (CCSE), the Check Point Certified Managed Security Expert (CCMSE). In the Cisco qualified specialist category, there are a few certifications around specific areas of security, including the Cisco Firewall Specialist, the Cisco IDS Specialist and the Cisco Certified Security Professional (CCSP) and so on.

The Global Information Assurance Certification (GIAC) organization, being founded in 1999 by the SANS Institute to validate the real-world skills of IT security professionals, has the main purpose to provide assurance that a certified individual has practical awareness, knowledge and skills in key areas of computer and network and software security.

The SANS training and GIAC certifications address a range of skill sets and some advanced subject areas such as audit, intrusion detection, incident handling, firewalls and perimeter protection, forensics, hacker techniques, Windows and Unix operating system security.

GIAC currently offers certifications for over 20 job-specific responsibilities that reflect the current practice of IS. At present GIAC certifications cover four IT/IT Security job disciplines: Security Administration, Management, Audit, Software Security.

The SANS training course "SANS 17799/27001 Security & Audit Framework, Mgt-411" implements step by step pragmatic examples to move quickly into compliance with the standard and certification. This track is designed for IS officers or other management professionals who are looking for a how-to guide for implementing the standard effectively. "GIAC Certified ISO-17799 Specialist" (G7799) candidates must demonstrate understanding of the standard and the ability to put it into practice.

Summing up all these certifications it is possible to state that the international perspective of IS specialists' training should be focused on the following international standards: ISO/IEC 27002/27001, Common Criteria, ITSEC and IS bodies of knowledge recommended by professional computing organizations [2].

3. Initial Data for Formulating Qualification Characteristics

"IS specialist" term applies to many positions, responsible for finding and solving security problems in computer systems. What the IS specialist actually does depends on many factors ─ the type and size of the employer, information that needs protection and computers the organization uses.

The basic qualification characteristics of a specialist with higher education are formulated on the basis of his/her special (professional) competences [3] - abilities to solve definite problems and carry out specific work within his/her line. IS specialists must be able to do a number of tasks, to think logically, to pay attention to details and to make sure their work is exact.

Formulating the qualification characteristics is possible only when considering separate typical objects where IS tasks are being carried out. ISO/IEC 27002 analysis shows that there is enough information to formulate the qualification requirements for specialists, ensuring functioning of IS systems of any organization.

The Russian universities allow up to 1 year for practicing and preparing of the graduate qualification paper (diploma project) (for example, the MEPhI students have 10th and 11th semesters). During this period graduates' activities within a specific organization can be divided into three main streams.

1. Forming the goals of ensuring organization's IS (is based upon defining assets to be protected, all types of vulnerabilities, IS paradigm and basic principles, threats' and IS violators' models, implementing risk assessment and forming IS policies).

2. Implementation of these goals (via services/systems/personal).

3. Control of progress in reaching IS goals based upon checks and evaluation of organization's IS (IS monitoring and audit) and defining maturity of organization's IS management processes.

These graduates act as the assistants for organization staff:

- *privacy officers* (develop/implement IS policies and procedures);
- *IS architects* (direct organization-wide security technology);
- *IS analysts* (conduct IS assessments for an organizations);
- *virus technicians* (analyze newly discovered computer viruses and devise ways to defend against them);
- *"red team" testers* (plan/carry attacks on the computer systems);
- *cryptographers* (keep information secure by encrypting it);
- *cryptanalysts* (analyze hidden information);
- *security administrators* (develop/implement protection systems that detect, prevent, contain and deter security risks; update security procedures and establish and maintain access rules);
- *IS incident response team members* (work together to prepare for and provide rapid response to security threats);
- *disaster recovery specialists* (design and implement programs to recover data lost in a disaster);
- *computer crime specialists/computer forensic investigators* (preserve, identify, extract and document evidence if IS incident);
- *IS auditors* (evaluate IS adequacy, effectiveness and efficiency);
- *chief IS officers* (supervise the entire IS department and staff).

Our experience collected since 1995 and ISO/IEC 27002 content analysis allow grouping practice and diploma project topics, incorporating technical, organizational and management aspects (with deeper specification than three main streams), as follows:

- risk management (including development of IS threats' and violators' models, asset management, vulnerabilities assessment);
- IS policies and procedures development;

- business continuity planning and management;
- ISMS design;
- design/development of information protection technologies, tools, means, system/subsystem;
- IS tools and services support and administering;
- physical and environmental security;
- human resources security;
- IS incident management;
- computer forensics;
- IS monitoring and auditing (external, internal, self-assessment against policies, procedures, standards).

To define functions of IS specialists working within concrete objects it is necessary to define IS role for those objects and line of IS specialist activity. Such information could be obtained upon analysis of ISO/IEC 27002.

4. IS Role at Protected Objects

ISO/IEC 27002 defines IS role for any organization as *"…the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. IS is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met."* [1]. Thus when training IS specialists, peculiarities of protected objects should be taken into consideration and they should be reflected in their qualification characteristics.

But it is also important to define subjects that could interact with each other in situations when IS risks could appear. The standard defines the following subjects: *owner of organization's assets and violator trying to influence those assets*. IS role is defined by the tasks being carried out within the conditions of opposition of an owner and a violator for the control over the assets.

While indentifying its security requirements an organization should consider three main sources. The first one *"…is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated." The second "…is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment." And the third "…is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations."* [1].

IS risks, whose essence is natural vagueness of the future, are an objective reality and they could be lowered only to the level of vagueness of subjects characterizing the nature of business. The remaining part of IS risk defined by the factors of the environment of organization's functioning, for which organization cannot influence at all, should be accepted. In that case ensuring IS at an object should lower risks to a certain level.

After that phase an organization should implement the IS goals ─ *"appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level… The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations."* [1]. The controls can be considered as guiding principles for IS management and applicable for most organizations.

Ensuring IS for an organization is the process that should be efficiently managed. The main IS role is defined by the organization's IS strategy which lies in ISMS deployment, exploitation, check and improve. Along with that IS management is a part of the overall corporate organization's management which is oriented for reaching organization's goals through ensuring protection of its assets. An organization's ISMS is a part of the overall management system based on the business risk approach whose goal is to create, implement, operate, monitor, analyze, support and rise IS of an organization (ISO/IEC IS 27001).

5. IS Specialist Line of Activity

It is possible to formulate the main lines of activity of IS specialist on the basis of the section 0.7 of the ISO/IEC 27002 standard:

"a) IS policy, objectives, and activities that reflect business objectives;

b) an approach and framework to implementing, maintaining, monitoring, and improving IS that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

d) a good understanding of the IS requirements, risk assessment, and risk management;

e) effective marketing of IS to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on IS policy and standards to all managers, employees and other parties;

g) provision to fund IS management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective IS incident management process;

j) implementation of a measurement system that is used to evaluate performance in IS management and feedback suggestions for improvement."

6. Conclusion

Analysis of the experience collected within training of IS specialists with higher education at the MEPhI and of ISO/IEC 27002 allows one to define two types of IS specialist professional activity: technological (ensuring functioning of the main IS technologies) and organizational and technological (ensuring functioning of ISMS).

Qualification requirements are defined by the types of tasks being carried out by the specialists and requirements to the level of knowledge and skills. Three main streams (listed in section 3) define three tasks solved (special competence). The level of knowledge and skills is associated with staff functions (section 3).

IS specialists should –

know:

- normative base, related to ensuring IS;
- the impact which interruptions caused by IS incidents are likely to have on the business;
- principles of ensuring IS;
- methods of IS risk assessment and management;
- IS architectures and infrastructures;
- basic methods of IS management;
- IS effectiveness evaluation methods;
- methods of system IS monitoring and auditing;
- basic methods of IS incident management process;
- business continuity planning and management;
- fundamentals of computer forensics;

be able:

- identifying all the assets involved in critical business processes;
- define models of IS threats and violators;
- develop, review, implement and improve IS policies and procedures;
- conduct IS risk assessment and management at the object (including reducing and avoiding risks);
- develop, deploy, check (and test), improve ISMS;
- administer IS tools (hardware/software) and subsystems of certain information technologies and automated systems;
- review the effectiveness of IS policy and procedures implementation;
- collect evidence for IS incident handling;
- providing appropriate IS awareness, training and education;

have an idea of:

- methods of building object management systems;
- peculiarities of psychology and ethics of team relations;
- defining the resources (financial, organizational, technical and environmental) needed for IS.

These requirements have universality and do not depend upon national and other peculiarities of systems being secured. To conclude, future work should be on the basis of formulated qualification requirements and details of educational course content specified in IS curricula.

References

1. International Standard ISO/IEC 17799. Second edition. 2005-06-15. “Information technology — Security techniques — Code of practice for information security management”. Available: http://www.iso.org.
2. Armstrong Colin J. And Armstrong Helen L. Mapping information security curricula to professional accreditation standards // Proceedings of the 2007 IEEE Workshop on Information Assurance. US Military Academy, West Point, NY 20-22 June 2007.
3. Kurilo Andrey P., Miloslavskaya Natalia G., Tolstoy Alexander I. Information Security Specialist Training for the Banking Sphere // Proceedings of the 5th World Conference on Information Security Education WISE5. US Military Academy, West Point, NY 19-21 June 2007.