Uchwała Senatu Nr XXVII/188/07/08 z dnia 28 stycznia 2008 r. w sprawie wprowadzenia na Politechnice Śląskiej Systemu Zapewnienia Jakości Kształcenia.

Waks, S., Frank, M., 1999, *Application of the Total Quality Management Approach Principles and the ISO 9000 Standards in Engineering Education*, European Journal of Engineering Education, vol. 24, no. 3, pp. 249–258.

ROLA AUDYTU W SYSTEMIE ZAPEWNIENIA JAKOŚCI KSZTAŁCENIA

Streszczenie: Podstawowym celem artykułu jest zdefiniowanie roli audytu w systemie zapewnienia jakości kształcenia. Przedstawiono w nim wybrane zagadnienia dotyczące audytu systemu zapewnienia jakości kształcenia na wielowydziałowej wyższej uczelni. Opierając się na doświadczeniach autora pełniącego funkcję pełnomocnika rektora ds. systemu zapewnienia jakości kształcenia, przeprowadzono dyskusję czynników i uwarunkowań wpływających na proces audytu. Zaprezentowano podstawowe informacje o audycie w systemie zapewnienia jakości kształcenia funkcjonującym na Politechnice Śląskiej. Zwrócono uwagę na określenie celów audytu, jednoznaczne zdefiniowanie jego wymagań oraz właściwy dobór i przygotowanie zespołu ludzkiego odpowiedzialnego za proces audytu. Zaprezentowano podstawowe zadania, jakie stoją przed audytem. Określono warunki, jakie powinny być spełnione, aby proces audytu przebiegał właściwie. W podsumowaniu odniesiono się do zadań audytu i jego roli w kształtowaniu jakości w edukacji.

Jacek Łuczak[1], Małgorzata Miśniakiewicz[2]
[1] Poznań University of Economics, Poland
[2] Cracow University of Economics, Poland

RISK MANAGEMENT AS BASIC OF MANAGEMENT SYSTEM ON POLISH GOVERNMENT OFFICES EXAMPLE

Abstract: The paper discusses the issue risk management from the perspective of an Information Security Management System and general Management System. It is also a review which attempts to thoroughly present how complex the issues related to information security in organisations and procedures implemented in them are. The primary aim of this paper is to review a number of methods and concepts utilised as a part of a systematic approach to information security management according to the most widespread standard. The concepts and methods are also based on information security risk assessment.

The paper focuses on the process of risk assessment in Polish government offices which can be regarded the cornerstone of management the organization. A wide range of theoretical concepts, practical methods and approaches to information security and risk assessment is to be presented in it. It also presents a number of methods which can be used in the risk assessment process.

Keywords: risk management, Information Security Management System, information security, risk assessment.

Information security risk management

Risk management is the process of risk assessment aimed at mitigating the risk to an acceptable level. It should consist of the following phases: planning, acquiring, developing, testing and properly structuring the IT systems [Molski & Łachota 2007, p. 90].

M.E. Whitman points out to the co-relation between risk assessment and risk mitigation. This co-relation constitutes the essence of risk management [Whitman & Mattord 2006, p. 50] (Figure 1).

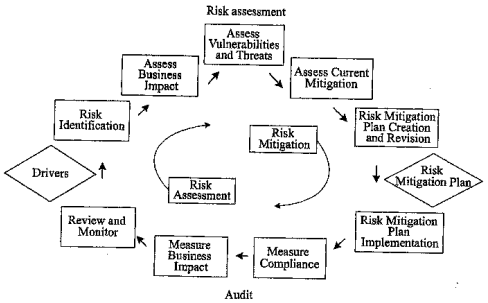

Figure 1. General structure of the risk management in Information Security Management System (ISMS)

Source: Inter alia Whitman & Mattord 2006, p. 50

M.E. Whitman and H.J. Mattord [2006, p. 53] determine the following stages of risk management:
- identifying the risk,
- assessing the impact on the activity,
- assessing vulnerabilities and threats,
- assessing existing measures to mitigate the risk,
- compiling and reviewing a Risk Mitigation Plan,
- implementing the Risk Mitigation Plan,
- measuring conformance,
- measuring the impact on the activity,
- review and monitoring.

According to PN-I-13335-1:1999 standard[1] risk management is the complete process of identifying, controlling, eliminating or mitigating the probability of the occurrence of uncertain events which can influence the assets of an IT system [PN-I-13335-1, 1999, p. 9].

This approach is also followed by Ch. Alberts and A. Dorofee who make use of the modified quality circle model (PDCA) – Figure 2.

[1] PN-I-13335-1:1999 is the Polish translation of a standard issued by the International Standard Organization and International Electrotechnical Commission under the name ISO/IEC TR 13335-1.

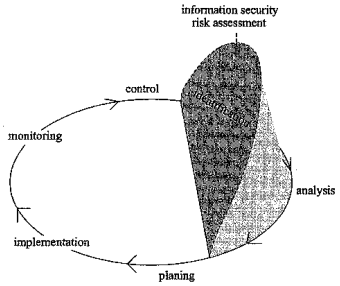

Figure 2. Risk assessment in the process of information security risk management

Source: Alberts & Dorofee 2003, p. 11

According to the model, the main aim of the process of risk management is mitigating the risk to an acceptable level by compiling a proper Risk Treatment Plan. One of the premises underlying the model is that all actions which are performed in it are effective and carried out in a continuous and systematic way (e.g. monitoring, reviews).

General characteristics of information security risk assessment methods

In theory and in practice several dozens of methods for information security risk assessment and evaluation are utilised. These methods can be divided into 3 following groups:
- quantitative methods,
- qualitative methods,
- hybrid methods.

Qualitative methods

Qualitative risk assessment is most often a subjective evaluation which is based on best practices and experience. The outcome of such an assessment is a list of threats ranked by their risk level (low, medium, high). Qualitative methods are

very flexible and open to various kinds of modifications. Owing to their flexibility and modifiability they provide the organisation with fast and cost-effective results when identifying threats and deploying security measures is concerned. However, because of the flexibility the scope and cost of risk assessment in different organisations can vary to a significant extent. That is why, depending on the available financial resources allotted for this purpose in the budget the scope of risk assessment may change in the course of time.

In qualitative risk analysis all risks and potential effects of their occurrence are presented in a descriptive way. It means using risk scenarios and determining the effects of potential realisation of risk. The scenarios should include numerous details which are helpful in taking specific actions and choosing proper security measures. In widespread use, there are various scales to describe specific situations and incidents.

Quantitative methods

In quantitative risk assessment it is essential to determine two basic parameters; the value of effect and the probability of occurrence of a specific risk.

The potential effects may be determined by evaluating the effects of risk events or extrapolated on the basis of data from the past. The consequences of risk events may be expressed by means of different categories (e.g. financial, technical, operational, human resources).

The overall quality of the analysis depends on the accuracy of indicated values and statistical validation of the deployed model [ENISA 2006, pp. 22–23].

Hybrid methods

Both quantitative methods and qualitative methods have some disadvantages. First of all, they are too general. Second, they do not identify all the needs with regard to information security in a precise way. Apart from that, they do not provide the organisation with sufficient information concerning the cost analysis when deploying new security. Because of this, the majority of companies make use of the combination of the two approaches. On one hand, qualitative analysis founded on scenario-based methods is used to identify all risk areas and potential effects of specific risks. On the other, quantitative analysis is used to determine the costs associated with the effects of risk occurrence. This also leads to significant increase in knowledge related to processes realised in an organisation and raises awareness on the potential risks.

Guidelines on risk assessment specified in ISO/IEC 27001:2005

The model of the process of information security risk assessment described above is a standardised approach to the analysed issue which has been described and propagated in the ISO/IEC 27001:2005 standard. The standard describes the components which should be taken into consideration when a risk assessment method is designed. It does not, however, specify the specific outline of the final method. Thus, this approach may be regarded as advantageous since the security standard does not impose any single method on the organisation and in this way gives it a free choice. This, above all, can be justified by diverse employment size and structure in organisations, as well as by the characteristics of conducted activity or the area of activity.

The standard, however, requires that a specific method of risk assessment be selected[2]. This, in turn, shall safeguard that through a methodical approach to risk assessment it will be possible to compare the results in the course of time. It shall be also possible to ensure repeatability of the results. Apart from that, it is vital that risk acceptance criteria be drawn up and acceptable risk levels be determined. Diverse methods of risk assessment have been published and are commonly used in organisations. Obviously, it is also possible for a particular organisation to use individual methods which are based on own experience. The most popular methods for information security risk assessment shall be presented in the following chapter.

Risk assessment according to ISO/IEC TR 13335-3[3]

The ISO/IEC 27001 standard does not specify which particular method should be used. It does, however, give some remarks on the examples of risk assessment methods discussed in ISO/IEC TR 13335-3, *Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security.*

The ISO/IEC 13335-3[4] published in 1998 is one of five parts of the standard devoted to information technology. It is a set of guidelines (instructions) for people responsible for the management of IT Security. This third part includes techniques for forming a three-level security policy. So it discusses the problem of risk analysis, implementing security plans and reacting to incidents. Moreover, it presents the methods of risk assessment as far as information security is concerned.

---

[2] A number of key methods for risk assessment are described further in this paper. These methods are not only used in their basic version, but are also modified to meet the needs of a particular organisation. Apart from the methods mentioned in this paper, some other authors point out to the following ones: TRIKE (Treat modelling framework with simulaties to the Microsoft threat modelling processes), AS/N2S 4360:2004 Risk Management (Australian/New Zeeland Standard), CVSS (Common Vulnerability Scoring System).

[3] ISO/IEC TR 13335, often abbreviated to GMITS (Guidelines for the Management of IT Security) is a technical report of significant importance to ISMS. The report consists of five parts.

[4] National organisational units (which belong to ISO or IEC) draw up international standards through the agency of technical committees performing work in specific areas. In the area of IT technology ISO and ICE founded a Joint Technical Committee ISO/IEC JTC 1. The basic task of the technical committees is drawing up international standards. A technical committee, however, sometimes publishes a technical report marked with the "TR" symbol.

The OCTAVE Method

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a set of guidelines developed at Carnegie-Mellon University in 2001 [Alberts & Dorofee 2003]. This method is used, for instance by the US army, and is getting more and more popular in other, especially large, organisations.

The OCTAVE approach defines a risk-based strategic assessment and planning technique for security. The method is directed to all types of organisation. It is based on the premises that the employees of an organisation are responsible for establishing a security strategy in it. Its principles should be implemented by a small interdisciplinary analysis team (consisting of three to five of the organisation's own personnel). The team should collect and analyse data, determine the strategy for using security measures, as well as mitigation plans based on organisational security risks. In order to implement the OCTAVE Method in an efficient way, the team should have comprehensive knowledge about the activity of the business activity of the organisation and its security processes [ENISA 2006, p. 36].

The OCTAVE method uses a three-phased approach. The first phase is based on analysing the critical assets in an organisation, identifying the current practices, reviewing the requirements related to security, determining the organisational vulnerabilities and existing threats. The second phase is aimed at identifying technological vulnerabilities. The third phase is developing a protection strategy and risk mitigation plans.

Failure modes and effects analysis — FMEA

The Failure Mode and Effect Analysis (FMEA) is mainly a method to support quality management, however the concept and rules of risk assessment (organisational and technological) may also be applied in case of information security risk assessment.

Initially, the FMEA method was used in the USA in the 1960s for production in space travel and automotive industry[5]. The method was used to verify the projects of different elements of spaceships and its main aim was ensuring the participants' safety in the space expeditions. The success of this method in case of NASA contributed to its implementation in other branches. In 1970s and 1980s, it became popular in Europe where it was used in the chemical, electronic and automotive industry. In the last of the three it was deployed in the most dynamic way. In 1990s the method was adapted as a part of the ISO 9000 standard and particularly the QS 9000 (ISO/TS 16949) standard specifically dedicated to automotive industry.

[5] Using FMEA is obligatory for suppliers in the automotive industry (OE – original equipment, OES – original equipment services) – [AIAG 2008; Łuczak 2008, p. 103 and other].

The method is based on determining and analysing cause and effect relationship as far as potential product failures are concerned. It also takes into consideration the severity of a given risk. The main goal of the method is to consistently and systematically identify potential product/process failures/defects so as to eliminate them or mitigate the risk related to them [Łuczak 2008, pp. 164–174].

In other words, assessing risk according to this method is based on the assessment of risk factors. FMEA lists three criteria which are ranked with points from 1 to 10. In case of information security risk assessment, the following criteria can be distinguished:

- significance for the company/or Customer,
- probability of loss of integrity, availability and confidentiality,
- effects of potential loss of one of the features of information security (confidentiality, integrity, availability).

When the conventionally defined limit (number of points) is concerned, it is necessary to prepare and deploy a risk mitigation plan. The plan should specify the objectives, realisation times, people held responsible and risk assessment. It should anticipate the effectiveness of specified actions.

The CRAMM Method

The CCTA Risk Analysis and Management Method (CRAMM) is a risk analysis method developed by the British Central Communication and Telecommunication Agency (CCTA) whose name was changed to Office of Government Commerce (OGC). The integral part of this method is a special IT tool for risk assessment (CRAMM). Using the method without the CRAMM software tool can be difficult.

The first edition of CRAMM (methods and tools) was based on best practices of British government organisations. Nowadays, CRAMM is the preferred method of risk assessment for the British government, but it is also used by many organisations in other countries. This method is particularly useful for large organisations, such as governmental agencies or in case of industry [ENISA 2006, p. 31].

The CRAMM is a method realising the requirements of standards by: conducting a gap analysis, preparing a security improvement programme, producing an information asset register, defining the scope of the information security management system, as well as compiling documentation for implemented security measures [Molski & Łachota 2007, pp. 98–99].

The COBRA Method

The Control Objectives for Risk Analysis (COBRA) is a complete risk analysis method designed for the board and management of an organisation to thoroughly evaluate the profile of risks related to the conducted activity. Particular attention is paid to the security of the image, conformity with applicable legal regulations and laws and to internal control mechanisms.

The structure of the COBRA method consists of the six following areas:
- Inherent Risk,
- Control Activities & Procedures,
- Human Resources Risk,
- Security Risk,
- Financial Statement Compliance,
- Disaster Readiness.

Apart from the above, there are 33 subcategories and 429 control questions [Molski & Łachota 2007, pp. 99–100].

The MARION Method

The method MARION (Methodology of Analysis of Computer Risks Directed by Levels) was developed by the CLUSIF (Club de la Sécurité de l'Information Français), and the last update was performed in 1998. Nowadays, CLUSIF does not longer finance nor promote the method as the financial resources were reallocated to another, newly developed, method, i.e. MEHARI. However, this method is still used by many organisations.

It is based on a methodology of audit, which, as its name indicates, allows for estimating the level of IT security risks of a company through balanced questionnaires giving indicators in the form of notes on various subjects relative to security. The objective of the method is to determine the level of security which is estimated based on 27 indicators distributed in 6 large subjects; each of them is assigned a grade between 0 and 4. The level 3 is the level to be reached to ensure a security procedure/measure is considered as sufficient and acceptable [ENISA 2006, p. 35].

The MEHARI Method

Methode Harmonisee d'Analyse de Risque (MEHARI) was developed by security experts from CLUSIF. This approach is based on defining the parameters to measure risk reduction corresponding with the targets of the organisation. The MEHARI provides:
- a risk management model,
- modular components and processes of the model,
- tools to analyse risk situations,
- tools to determine vulnerabilities through audit,
- a specific approach to threat identification and vulnerability characteristics,
- rules for optimal selection of corrective actions [ENISA 2006, p. 36].

MEHARI realises the guidelines of ISO/IEC 27001:2005 and ISO/IEC TR 13335 standards by using a uniform risk assessment system, properly selected security measures and proper allocation of assets.

The ISACA Standards

The Information Systems Audit and Control Association (ISACA)[5] standards regarding the IT audit give a number of methods of risk evaluation in Information Systems.

One of them risks assessment measurement evaluation with eight key variables. Each unit/area in the IS audit will be rated on these eight key variables using a numeric descriptive value ranking of 1 (low) to 5 (high). The results of these rankings are then multiplied by significance weighting factors that range from 1 (low) to 10 (high) to give an extended value. These extended values are added together to give a total. Once the totals have been obtained, the auditable units/areas are ranked by risk [Molski & Łachota 2007, p. 97].

Author methods

The ISO/IEC 27001 does not specify which method should be deployed. Thus, it is possible for the organisation to use its own methods which are compiled based on industry knowledge and experience. This approach, however, is only appropriate for large organisations which have proper organisational structures to compile and validate such a method. The biggest advantage of it is being fully aware of the method as well as the whole risk assessment process by all people involved in the processes related to it. Obviously, there is a danger that the developed method may turn out to be ineffective and that the organisation shall not be granted a recommendation during the certification audit. In consequence, it may also not be awarded a certificate. For this reason, small businesses do not decide to develop their own methods and prefer to choose one of the methods which are already available. Such methods are usually approved of auditors during certification audits. Finally, small businesses do not usually have sufficient human resources to develop their own methods.

Conclusions

Information security, and a basic part of it – risk management is nowadays of great significance and only an efficient information security management system can ensure it. The 'driving force' of such a system should be risk management. This is the general conclusion and guiding principle of the authors of this paper. Selecting the basis for ISMS is also important. Although, the basis in each and every case does not have to be the ISO/IEC 27001 (and certification against this standard is

[5] The Information Systems Audit and Control Association (ISACA) is the biggest organisation dealing with the problems of audit, control and management in the IT environment.

not crucial), it may be advisable to make use of the said international standard, as it is a selection of best management practices. Irrespective of the organisation's size, the characteristics of its processes it may be highly advantageous to take ISO/IEC 27002, COBIT, ITIL, ISO 20000 and other standards (especially related to risk assessment methods) into consideration. However, wide reading knowledge, expertise and experience with regard to the organisational aspects is required in this case. In similar vein, each time special attention should be paid to the fact that the solutions within the ISMS and general management system for every company (especially for government offices) should be scaled, in other words fitted to real needs.

References

AIAG, 2008, ISO/TS 16949:2009, *FMEA MANUAL.*

Alberts, Ch., Dorofee A., 2003, *Managing Information Security Risks*, The OCTAVE Approach, Addison-Wesley, Boston.

ENISA, 2006, *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment methods and tools* [online] http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf.

ISO/IEC TR 13335 *Guidelines for the management of IT Security.*

ISO/IEC 27001:2005 *Information technology – Security Techniques – Information Security Management Systems – Requirements.*

Łuczak, J., 2008, *System zarządzania jakością dostawców w branży motoryzacyjnej*, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań.

Molski, M., Łachota, M., 2007, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice

PN-I-13335–1, 1999, *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych.*

Whitman, M.E., Mattord, H.J., 2006, *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston.

ZARZĄDZANIA RYZYKIEM JAKO PODSTAWA SYSTEMU ZARZĄDZANIA NA PRZYKŁADZIE URZĘDÓW ADMINISTRACJI PUBLICZNEJ W POLSCE

Streszczenie: W pracy omówiono problem zarządzania ryzykiem z punktu widzenia systemu zarządzania bezpieczeństwem informacji i całościowego systemu zarządzania organizacją. Artykuł jest także przeglądem zagadnień najistotniejszych dla systemu zarządzania bezpieczeństwem informacji, w tym organizacji i procedur. Głównym celem niniejszego opracowania jest przegląd metod i koncepcji wykorzystywanych w ramach systematycznego podejścia do zarządzania bezpieczeństwem informacji i dyskusja w zakresie możliwości ich aplikacji – jako podstawy kształtowania systemu zarządzania. Artykuł uwzględnia specyfikę administracji publicznej w Polsce, bazuje na doświadczeniach autorów w tym względzie. Dokument skupia się na procesie oceny ryzyka w polskich urzędach, który można uznać za fundament zarządzania organizacją.