Paper

Implementation of information security management system in the small healthcare organization

Jiří Tupa and František Steiner

Abstract— The contribution describes the scope and main subject designed within DIGI-Q project. The paper contains results from subprojects of information security management system (ISMS) implementation, managed by students of DIGI-Q course. Very interesting simple risk assessment method and risk management and their application within in small healthcare organization were developed. Criteria and procedures accepted are described.

Keywords— information security management, personal data protection, risk analysis.

1. Introduction

The subproject solved problems with certification of data management system (DMS) in the private healthcare organization. The objective of this certification is to obtain licence certification mark GoodPriv@cy. The GoodPriv@cy is a certification service available for all IQNet clients interested in the protection of the company information data. Data protection and privacy (DPP) are becoming increasingly significant quality factors in business. It strongly affects the trustworthiness of a company or a public organization. The IQNet GoodPriv@cy specification integrates data protection and related information security requirements in a data protection management system. It supports an organization to manage its data protection and information security aspects proactively and efficiently.

The GoodPriv@cy label testiest that the authorised user: maintains a functioning data protection management system, meets statutory and contractual requirements for data protection and the related information security, continually improves the processes relevant to DPP.

The GoodPriv@cy label allows private and public organizations to document objectively and communicate effectively their own DPP performance vis-à-vis its customers and stakeholders. It's the way to safeguard reputation especially in healthcare public and private area.

The GoodPriv@cy certification can be used for small and medium healthcare organization in relation with quality management system. Example is shown by this paper. The attention is focused on a security of health information system contains medical documentation and sensitive personal data.

Implementation of DMS and its certification according to standards GoodPriv@cy can be way to information security management system (ISMS) building, especially in the health service. Why we are interesting about ISMS? Information is the lifeblood of all organizations and can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by mail or by electronic means, shown in films, or spoken in conversation. In today's competitive business environment, such information is constantly under threat from many sources.

These can be internal, external, accidental, or malicious. With the increased use of new technology to store, transmit, and retrieve information, we have all opened ourselves up to increased numbers and types of threats. There is a need to establish a comprehensive information security policy within all organizations. You need to ensure the confidentiality, integrity, and availability of both vital corporate information and customer information.

What it is ISMS? An information security management system is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems. For example ISO has published a code of practice for these systems – see ISO/IEC 17799 [6].

The personal data are the most important information in the healthcare organization. The goal of ISMS is the patient privacy protection especially privacy protection of sensitive personal data. Healthcare organization use information systems and information technologies for health documentation. This documentation contains sensitive data about all patients. Management and all staffs have to secure and develop system its protection. The GoodPriv@cy certification and audit is the way for good relationships between healthcare organization and patient.

The requirements for personal data protection are described by legislation documents: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications), Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

For example the Czech Republic and Slovak Republic passed the acts about personal data protection, which are

harmonize with legislation of European Union law. These are act No. 101/2000 in the Czech Republic and act No. 428/2002 in the Slovak Republic. All type organizations have to respect these acts for processing of personal data.

2. Subproject description

The subproject was solved as a student work of DIGI-Q course. The DIGI-Q course was the part of project (Quality and On-line Confidence in SMEs e-Business Processes) is funded by the European Commission under contract number IST-2001-38157 of the Information Society Technologies (IST) programme 2002, key action II.1.3. The objective is to develop an ad hoc action of training and awareness for helping SMEs in improving and certifying their business and e-business processes. This will allow to increase the SMEs capabilities in being more competitive in the digital economy age.
Within this project, an advanced course is being developed to provide training to professionals working in SMEs, or in companies working for SMEs. In Czech Republic training course was performed in the Czech Republic by CQS – The Czech Association for the Quality System Certification DIGI-Q Consortium member.
The training course was two parts. First part – classes were given in "weekend blocks" and the second part – student works was solved six month as DIGI-Q subproject. Our subproject was entitled Data Management System Audit according to GoodPriv@cy and was focused on the healthcare area (Mr. Tupa and Mr. Steiner were trained by the course too and Mrs. Šebestová was tutor of training course and subproject). The subproject results were expected:

- audit of data management system;
- GoodPriv@cy certification.

The project results were obtained:

- design of audit checklist according to personal data protection acts;
- design of risks analysis methodology;
- implementation of risks analysis, suggestion how to decrease the risks;
- external audit of DMS according to national law.

The design of risk analysis methodology is the important part for ISMS. Risk analysis methodology was used for risk assessment and for risk management. The methodology was designed accordance with the requirements for personal data protection and according with the results of personal data protection system audit (GoodPriv@cy audit). This audit was made by external audit team.
The GoodPriv@cy audit was realized at a private healthcare organization by external audit team. The authors of this paper were member of audit team. Company was represented by director, quality manager, IT administrator. Audit was performed the way how the organization:

- a formulated and implemented data protection policy;
- an operational and documented DMS;
- compliance with all legal or contractual data protection requirements;
- provision of the information security by appropriate organizational, staff and technical measures;
- effective control and monitoring of processes;
- evolution and continuous improvement of data protection and privacy.

The review of fulfillment requirements with national law was benefit of certification. This act requires execution of external audit of DMS.

3. Implementation of ISMS for personal data protection

Requirements for fulfil of GoodPriv@cy mark is building the security management focused on the personal data protection. For that reason the standards for ISMS (for example standards ISO/IEC 17799 [6]) can be applied adequate for data management security. The ISMS system respected new approach for quality management and the standards for quality management ISO 9000 [7] and ISO/IEC 17799 [6] are harmonised.
The healthcare organization has quality management system (QMS) in accordance to standards ISO 9000:2005 [7] and the standards and documentation for personal data security was implemented to the QMS too.
General requirements for ISMS on the organization are: develop, implement, maintain and continually improve documented ISMS, in this case DMS is focused on the sensitive personal data protection within the context of the organization's overall business activities and risk. For the purpose

Table 1
PDCA description for ISMS

PDCA	Description
Plan	Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do	Implement and operate the security policy, controls, process and procedures.
Check	Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
Act	Take corrective and preventive actions, based on results of the management review, to achieve continual improvement of the ISMS.

of this standard the process used is based on the PDCA model shown by Table 1 and Fig. 1.

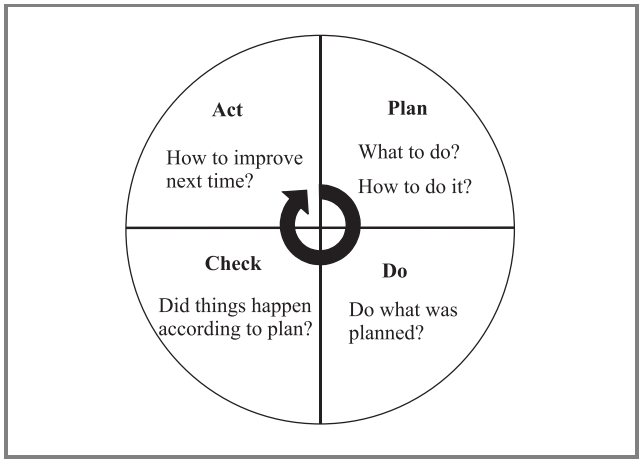


Fig. 1. The PDCA model applied to ISMS process.

The steps for establish the ISMS are:

- define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology;
- define an ISMS policy;
- define a systematic approach to risk assessment;
- identify the risks;
- risks assessment;
- identify and evaluate options for the treatment of risks;
- select control objectives and control for the treatment of risk;
- prepare a statement a applicability.

The next steps in the life cycle of ISMS at the organization are:

- implement and operate the ISMS;
- monitor and review the ISMS.

The important attributes ISMS are documentation (control of documents, control of records), establish the management responsibility (management commitment, resource management, training, awareness and competency), management review of the ISMS (review input and output and internal ISMS audit) and ISMS improvement (continual improvement, corrective action, preventive action) [1].

4. Risk analysis

Risk analysis is most important phase of ISMS establishment. That is process which compares assessed risks with benefit and/or price of possible security control. Standard ISO/IEC TR 13335 [8–10] defines four possible ways of risk analysis. We chose informal access. Advantage of this access is speed and financial modesty.

Base of risk analysis is fulfilment of following activities:

- threats identification;
- estimation of threat likelihood;
- identification of assets (process);
- rating of assets (process);
- determination of vulnerabilities;
- calculation of expected losses at threat impact;
- evaluation of risk analysis.

The interrelationships in risk management are shown in Fig. 2. This diagram helps us to tumble to risk analysis [2].

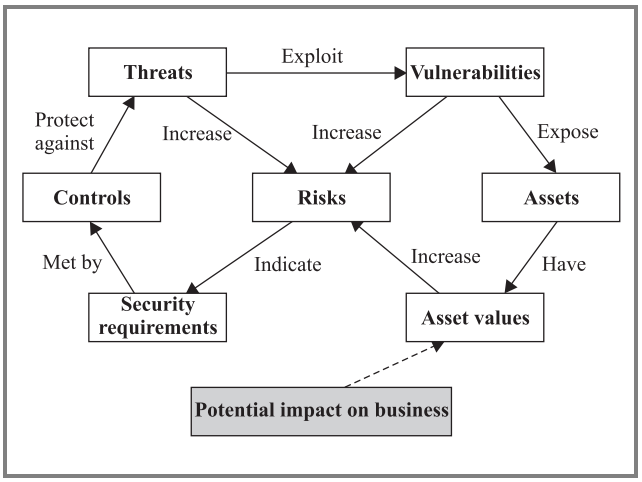


Fig. 2. Diagram of interrelationships in risk management.

The organization can be used standard methodology for example COBRA, CRAMM, etc., but this standards can be complicated and expensive, especially for smart and middle enterprises. In other case organizations can design own risk analysis methodology which will be easy and clear for the responsible management and fulfil the standards for ISMS.

The second case will be recommended for small and middle healthcare organization too.

4.1. Risk analysis key terms

The risk analysis key terms [3, 4] are given below.

Risk. The chance or likelihood of an undesirable event occurring and causing loss or harm. Note that the key element of risk is uncertainty, without which, there is no "risk".

Risk analysis. The process of gathering and analyzing risk-related information in the preparation of a risk assessment.

Risk assessment. A detailed articulation of the risks associated with the information assets and supporting ITC resources at risk, threats that could adversely impact those assets, and vulnerabilities that could allow those threats to occur with greater frequency or impact.

Threat. A potentially undesirable event that could result in loss or harm. The experience of a threat event and its measurable loss or harm is distinct from potential threat events and associated estimates of loss or harm. The aggregation of threat-event experience data provides the basis for estimating expected threat-event loss or harm in the future.

Vulnerability. A lack or inadequate application of a safeguard or control that allows a threat event to occur with greater frequency or impact.

Probability. Measures the chance or likelihood of an outcome or event occurring within a finite universe of possibilities or time, from zero (no chance) to 1.0 (certainty).

Uncertainty. The central issue of risk and risk metrics, reflected as the level of confidence, from zero to 100 per cent, that the associated numbers – and derived results – are credible and useful. Failure to integrate uncertainty into risk analysis/assessment approaches substantially reduces the credibility and utility of their results.

Quantitative risk analysis. It employs two fundamental elements; the probability of an event occurring and the likely loss should it occur. Quantitative risk analysis makes use of a single figure produced from these elements. This is called the "Annual Loss Expectancy (ALE)" or the "Estimated Annual Cost (EAC)". This is calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.
The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated. Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

Qualitative risk analysis. This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

- threats: these are things that can go wrong or that can "attack" the system; examples might include fire or fraud; threats are ever present for every system;
- vulnerabilities: these make a system more prone to attack by a threat or make an attack more likely to have some success or impact; for example, for fire vulnerability would be the presence of inflammable materials (e.g., paper);
- controls.

These are the countermeasures for vulnerabilities.

There are four types:

- deterrent controls reduce the likelihood of a deliberate attack;
- preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact;
- corrective controls reduce the effect of an attack;
- detective controls discover attacks and trigger preventative or corrective controls.

4.2. Risk analysis methodology description – case study

Results of GoodPriv@cy audit made the base for design of the risk analysis methodology [5]. The methodology combines the basic principles of quantity risk analysis with qualitative risk analysis. The principles of failure modes and effects analysis (FMEA) analysis were used for the methodology design too.
The basic ideas of this methodology are:

1. The risks are generated by the processes in the organization that it means that we can search the risks in the processes which processing with the private information about patients and about organization (transfer, record, liquidation, storage, etc.).
2. The processes are part of an object in the organizations. An object makes the assets of organization and contains the processes which processing the information.

The risks are defined and described by individual objects for processes. For each process can be identified one and more risks. The result is defined by number which means risk factor of object. Average of all risk factor determines risk factor of all objects in the healthcare company. The results of risk analysis are recorded and summarized in the risk analysis forms (Tables 2 and 3).
The risk analysis form (Table 2) uses those important terms:

- *Process* – activities in the scope of object.
- *Risk* – description of risk.
- *Risk code* – No. of risk for risk inventory.
- *Risk assessment* – risk assessment contains three date:
  - *consequence* (*C*),
  - *likelihood* (*L*),
  - *risk factor* (*RF*).

Next columns in the form (Table 2) record the current safety precaution and control method of process (internal documentation for process control).

Table 2
Risk analysis form – example of object risk analysis

Object (asset): **Information system**							**(Object code 0.1)**
Process	Risk – identification of undesirable event	Risk code	Risk assessment			Current safety precaution	Control method
			C	*L*	*RF*		
IS administration	Creation of uncontrolled back-up of date and database during IS implementation	1.01	32	10	320	No	No
	The back-up media loss	1.02	16	5	80	Storing back-up media to the safe	Documentation for data administration procedure
IS operating	Fire (over heat)	1.03	8	5	40	No	No

Object risk factor average: **147**

Risk assessment summary (risk class): **Risk class 2** that means increased of risk level, the increase of security level, standards and monitoring of security process is recommended.

Precaution proposal

Risk code	Proposal	Implementation description	Responsible person	Deadline	Estimated cost	Really implementation date
1.01	Procedures and use of model data during implementations IS	IT manager has to prepare procedure for IS implementation	IT manager	15.9.2005	50 EUR	

Table 3
Risk analysis form – example of object risk assessment

Object risk assessment summary

Object code	Name	Object risk factor average	Risk class	Objects (assets) value* [EUR]
0.1	Information system	147	2	6 500
0.2	Physical network architecture	20	1	2 500
0.3	Users desktops	170	2	1 500
0.4	Server	250	3	3 700
0.5	Patient card index	35	2	10 750
0.6	Archive	130	2	17 000
0.7	Server room	120	2	500
0.8	Work room	50	2	12 000
0.9	Laboratory	15	1	7 500
0.10	Medical office	10	1	6 800
	Average (risk factor per organization)	**109**	**2**	**88 750 EUR (sum)**

* Value are determined from accounting system as investment and overhead cost.

Precaution proposal summary

Risk code	Proposal	Implementation description	Responsible person	Deadline	Estimated cost	Priority	Really implementation date
1.01	Procedures and use of model data during implementation IS	IT manager has to prepare procedure for IS implementation	IT manager	15.9.2005	50 EUR	Yes	
1.03	Fire safety system	Installation of electronic fire signalization	Build administrator	31.12.2005	1 200 EUR	No	

Risk consequence. It is determined by Table 4. This table makes to review of an impact. The consequence is calculated as quadrate of risk level (this is expression of the risk intensity in accordance with impact and level). And the table uses the description and characterization of impact to the healthcare organization. This table very easy evaluated the consequence risk.

Table 4
Impact review

Level	Consequence	Characterization	Impact description
1	1	Insignificant	Insignificant infringement of operating procedure in the organization with immediate correction, none financial loss.
2	4	Minor	Low financial loss, infringement of operating discipline, infringement of operating instructions in the IT/SI area.
3	8	Moderate	Unauthorized operating with information in the organization, infringement of security policy and legislative rules, major financial loss, decrease of patients.
4	16	Major	Damage to the goodwill, major decrease of patients, major financial loss, escape insignificant information outside organization, wilful infringement of operating discipline, uncontrolled and unauthorized operating with information and data outside organization.
5	32	Catastrophic	Enormous financial loss, heavy decrease of patients, escapes sensitive information and personal data about patients outside organization, permanent damage to the goodwill.

Likelihood measures the chance or probability of an outcome or event occurring within a finite universe of possibilities or time. We can estimate the likelihood on experience and knowledge basis or from records of incidents and events. The Table 5 shows the likelihood of incident or event in fifth difference level. The different levels reflect the weight of likelihood for the risk factor calculation.

Table 5
Risk likelihood

Risk likelihood	Weight
Practically impossible incident or event.	1
Uncommon incident or event, but coming in specific situation.	5
Possible incident or event, incident or event was identified before.	10
Frequent incident or event.	15
Very often recurrent event and incident.	20

Risk factor (RF) is the numeric value of a risk. Risk factor is the product of likelihood (L) and consequence (C) calculated by Eq. (1):

$$RF = L \cdot C. \tag{1}$$

4.3. Result of risk analysis

Determination of risk class is needed for the improvement of process and ISMS. The classification the risk to the classes gives recommendation how to improve and take safety precaution. The risk factor can be used as classification criterion for risk categorization. In accordance with criterion we can determine risk class for improvement of processes and ISMS. The risk classes are defined by Table 6. The risk class is recorded in the risk analysis forms.

Table 6
Risk class matrix

Risk class	Description
1 ($RF \leq 20$)	Standard risk, the respect of security policy and standards procedures is recommended.
2 ($20 < RF \leq 240$)	Increased of risk level, the increase of security level, standards and monitoring of security process is recommended.
3 ($240 > RF$)	High level of risk, the acceptance of technical, organization, personal and physical proposal is recommended. The organization should be monitoring the security process and re-evaluate the security policy and standards.

Determination of object risk factor and organization risk factor is the next step for summary of process result analysis. The object risk factor can be calculated from all risk factors which were calculated for processes in the object. Average of all objects risk factor determines total risk factor the healthcare organization. The object and total risk factor can be categorized to the risk classes in accordance with Table 6 too.

4.4. Precaution proposal

The precaution proposal is the part of risk analysis for risk elimination and improvement of security processes. The proposal should be implemented if the risk factor exceeds rated value. The rated value of the healthcare organization is for example 180. The limit can be set individually for other type organization. All precaution proposals are summarized to the action plan. For other object can be identified identical processes of course. But the risk and

risk factor of process can be different in dependence on processing information in the object.

5. Conclusion

Real subproject outputs are:

- audit checklists for audit of legal requirements under the GoodPriv@cy certification;
- methodology of risks analysis and its implementation at the healthcare organization;
- GoodPriv@cy certification.

The risk analysis is simple methodology developed for risk assessment and risk management as part of implementation of ISMS in the healthcare organization. Risk analysis methodology, which was design by team, was implemented in the company as part of quality management too. The team cooperated with IT administrator and responsible managers during subproject solution. Cooperation with healthcare organization on the DMS building was very interesting experience from the healthcare area for project team.
The example of the risk analysis is shown in the risk analysis forms (see Tables 2 and 3). The results of risk analysis will be used for design of action plan. The goals of action plan are elimination of risks with high risk factor.
The elements used in accordance with ISO/IEC 17799 [6], which were applied for the clients (patients) information system and databases and for the GoodPriv@cy certificating, are written in this paper in Section 3.
The healthcare organization has the security project in accordance with the legislative requirements too. This project summarizes basic ISMS policy, security analysis and contains physical, technological, personal and organizational proposal, security procedures and incident control, defines the requirements documentation and control of documents, etc. The security project and risk analysis methodology were implemented to the quality management too.

References

[1] *Information Security Management Systems – Specification with guidance use*, BS 7799-2:2002. London: British Standards Institution, 2002.

[2] F. Steiner, J. Tupa, and V. Skocil, "Risk management in manufacturing enterprises", in *Conf. ICPR-18*, Salerno, Italy, 2005, pp. 1–5.

[3] W. Ozier, "Introduction to information security and risk management", http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=543

[4] "Inftroduction to risk analysis", http://www.security-risk-analysis.com/introduction.htm

[5] J. Tupa, "Data Management System Audit according to GoodPriv@cy", DIGI Q – SMEs Project Works. Prague: Czech Association for Quality Certification, 2004.

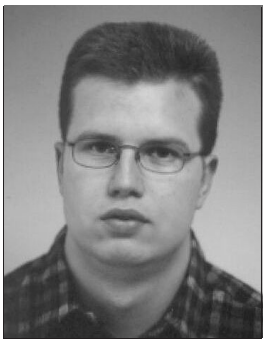
[6] *Information technology – Security techniques – Code of practice for information security management*, ISO/IEC 17799:2005 ed. 2.

[7] *Quality management systems – Fundamentals and vocabulary*, ISO 9000:2005 ed. 3.

[8] *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security*, ISO/IEC TR 13335-3:1998 ed. 1.

[9] *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*, ISO/IEC TR 13335-4:2000 ed. 1.

[10] *Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security*, ISO/IEC TR 13335-5:2001 ed. 1.



Jiří Tupa was born in Czech Republic. He received the M.Sc. and Ph.D. degrees in electrical engineering from Faculty of Electrical Engineering, University of West Bohemia in Pilsen in Czech Republic, in 2002 and 2006, respectively. The main his research interests are business management for electrical engineering industry, integrated management system, electronics technology, information and copyright law, information security. He is lecturer at Department of Technologies and Measurement University of West Bohemia in Pilsen.
e-mail: tupa@ket.zcu.cz
University of West Bohemia in Pilsen
Faculty of Electrical Engineering
Department of Technologies and Measurement
Univerzitní 26
CZ 306 14 Pilsen, Czech Republic

František Steiner was born in Czech Republic. He received the M.Sc. and Ph.D. degrees in electronics from Faculty of Electrical Engineering, University of West Bohemia in Pilsen in Czech Republic, in 1996 and 2001, respectively. The main his research interests are information systems, information security and technology of electronics. He is lecturer at Department of Technologies and Measurement University of West Bohemia in Pilsen.
e-mail: steiner@ket.zcu.cz
University of West Bohemia in Pilsen
Faculty of Electrical Engineering
Department of Technologies and Measurement
Univerzitní 26
CZ 306 14 Pilsen, Czech Republic