A UML APPROACH IN THE ISMS IMPLEMENTATION

Andrzej Białas
Institute of Control Systems, 41-506 Chorzów, Długa 1-3, Poland; e-mail: abialas@iss.pl

Abstract: The paper deals with the modelling of the Information Security Management System (ISMS). The ISMS, based on the PDCA (Plan-Do-Check-Act) model, was defined in the BS7799-2:2002 standard. The general model of the ISMS was presented. The paper focuses on the Plan stage elaboration only, basing on the previously identified ISMS business environment. The UML approach allows to achieve more consistent and efficient implementations of the ISMS, supported by the computer tools. The paper shows the possibility of the UML use in the information security domain.

Key words: Information Security Management System; ISMS; PDCA model; IT security framework; risk management; development; computer-aiding; security engineering; UML; modelling.

1. INTRODUCTION

The paper presents the concept of modelling the Information Security Management System (ISMS), using the Unified Modelling Language (UML)[1-2]. The ISMS was defined within the BS7799-2:2002[3] standard as "*the part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security*" in the organization. The ISMS, based on the PDCA (Plan-Do-Check-Act) management model, should be created and refined in accordance with other management systems (business, quality, environment, etc.) coexisting in the organization The ISMS implementation is unique for every organization and depends on its business needs, environment features, and related risk concerning the factors that disturb the achievement of business objectives by the organization. The standard[3]

provides general directions how to establish and maintain the ISMS within the organization. Every organization needs more detailed implementation methodology, basing on a wider group of standards and know how.

The paper features the UML-based approach to the implementation of the ISMS to achieve more consistency and efficiency offered by this language. Using graphical symbols instead of textual descriptions, the UML language allows intuitive, semiformal presentation of ideas and concepts. The basic knowledge of the UML elements is usually sufficient. The modelling approach is growing and the UML approach is commonly used, not only by IT developers but also in such domains as business management, logistics, transportation and telecommunications, to solve their specific modelling problems. The paper presents how the UML can be used by security managers and developers. This will be exemplified by very basic elements of this language, i.e. class and activity diagrams. It will also be shown that a computer-aided tool supporting information security management processes within the organization can be developed on the basis of this ISMS model.

The works on UML extension, called UMLsec[4], provide a unified approach to security features description. These works deal with modelling the IT security features and behaviours within the system under development, but they do not focus on the IT security management process. Some works deal with modelling complex security-related products[5] which consist of other security-related products and require advanced composition methods based on the Common Criteria[6]. The composition problem was considered there a modelling problem with security as its subject domain. Other papers[7] focus on the UML-based development method, constraints languages and tools used for advanced Java smartcards designs that meet the highest evaluation assurance levels (i.e. EALs) defined by the standard[6].

Usually, implementation methodologies are the consultants' know-how and are seldom published in details. An example of the ISMS implementation methodology, including the simple risk analysis method, is presented in the SANS Institute publication[8] but it is not based on the UML approach.

The paper presents a new concept of using UML in ISMS modelling and development. It will be shown that the general UML specification of the ISMS is feasible and, due to its coherency, the ISMS:

- can be better understood by a wider group of its potential users, while ISMS deployment,
- enables more effective information security management,
- allows to create computer-aided tools, based on the UML specification.

By nature the ISMS systems are based on the risk approach. This requires proper risk analysis and management methodology implementation. The paper shows how to solve this problem using the UML modelling approach.

The paper refers to more extensive works on the UML-based ISMS implementation[9-11]. It focuses on the elaboration of the Plan stage processes, i.e. ISMS scope, policy and risk issues. The processes are exemplified by simple UML class or activity diagrams. Some of them have conceptual meaning only, for the ISMS idea presentation. Others were refined during the development of the computer-aided tool.

2. UML REPRESENTATION OF PDCA MODEL

The general model of the ISMS, defined in the standard[3] and based on the PDCA concept, was developed and presented in the Figure 1.

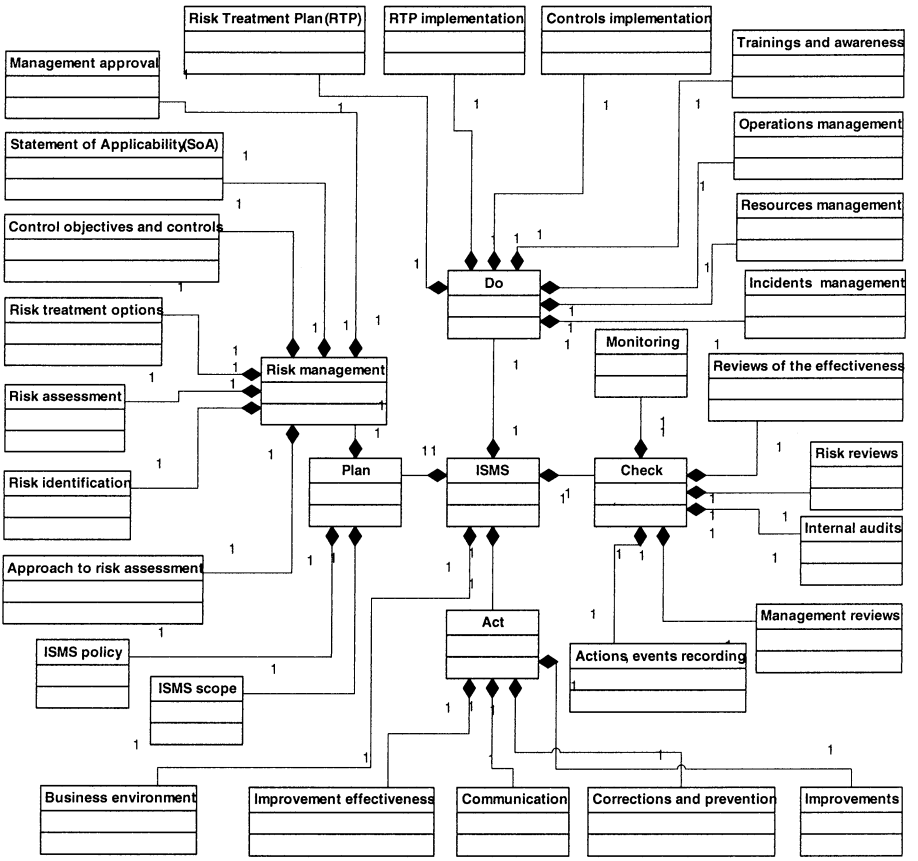

Figure 1. General structure of the ISMS.

There are four stages in the entire ISMS: Plan, Do, Check, and Act, each containing elements defined by the standard. Every class, concerning security management processes or their sub-processes, represents: ISMS documents, like ISMS policy, risk treatment plan; or ISMS operations, like tools for the risk analysis, monitoring or security management support. In reality, the classes shown in the Figure 1 represent a set of classes grouped in hierarchical complex structures that are not discussed in this paper.

Please note that there is one additional class in the Figure 1. It concerns high-level risk analysis and is called *Business environment*. This class represents ISMS entry into business processes and ensures appropriate positioning of all ISMS elements to meet business needs of the organization.

Starting from the *ISMS scope* and going clockwise to *Improvement effectiveness*, all ISMS elements specified in the standard[3] can be met. Please note aggregations linking classes on the class diagram.

3. BUSINESS ENVIRONMENT OF THE ISMS

The ISMS is a part of the overall management system of the organization and must reflect its business needs and existing risks. All relationships between information security and business processes should be identified. The standard[3] focuses on this topic but does not specify in details how this can be achieved.

To specify properly these relationships the *Business environment* class was defined (Figure 2). This class encompasses *Business domains*, where *Business objectives* are reached by means of processes (*Process description*), using *Underlying IT system*, with respect to the *Quality or Environment management requirements* (please note marked dependencies), if the latter exist. Discussions on business environment[11] show that the ISMS business environment will be viewed by the set of *Business level security objectives* expressing security needs. The identification of business environment concerns the high-level risk analysis. Information on risk issues is gathered and analyzed on the basis of interviews-workshops methodology. This information is represented by the set of attributes of the *Business domain* class. The derived global risk value is expressed by the *HighLevelRisk()* operation results. To assess these issues, some predefined quality measures[11] were defined. (please note these classes on the diagram).

All business processes providing business objectives should be analyzed and their importance for the organization should be assessed (attribute: *criticality4organization*). The other question is the level of participation of IT systems in the development of these processes, represented by the *ITDependencyDegree* attribute.

Protection needs regarding security attributes i.e. information integrity, availability and confidentiality are identified for each of the business processes. The business impact, caused by loss of these attributes, is analyzed with the use of predefined damage scenarios (e.g. from BSI[13], like those used by SANS[8]).

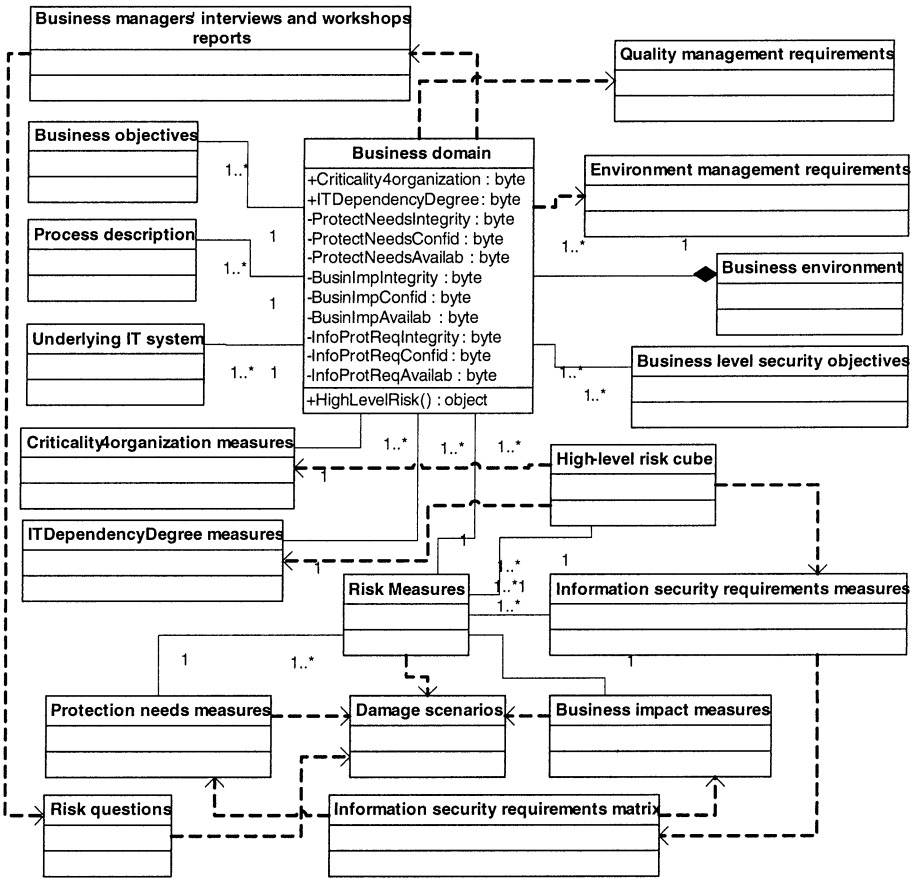

Figure 2. General structure of the ISMS business environment.

The information security protection requirements are derived from: protection needs regarding the security attributes, and business impacts caused by the loss of values of these attributes (please note all mentioned attributes). These requirements are based on the assumed matrix of predefined risk values.

The information security protection requirements, the criticality level, and the IT dependency degree – expressed in the assumed predefined scales – constitute a three dimensional measure of the high level risk within the

business domain. This measure is represented by the "risk cube", by analogy with the risk matrices. On this basis, filters and risk views can be implemented, allowing the users to trace different risk factors.

Additionally, the information security requirements can be considered separately for every attribute, allowing to trace the risk within the integrity/confidentiality/availability cross-sections. They can also be considered globally, using a cumulated measure for all attributes.

Different aspects of the above mentioned high-level risk factors and their assessed values can be used for the following tasks, concerning Plan stage processes elaboration:

- to order business processes with respect to their criticality level, IT dependency degree, and information security requirements,
- to set business level security objectives for all business domains, expressing what should be done to meet the security needs,
- to choose adequate risk management options for the organization or its business domains,
- to formulate risk acceptance criteria for the organization.

All these collected data serve as input for a detailed risk analysis performed within the selected domains when appropriate. This approach is a type of a high-level risk analysis, compliant with the standard[12], refined by BSI[13] and used there for partitioning all IT systems of the organization into domains which can be covered by the base control, or safeguarded on the basis of risk analysis results.

4. PLAN STAGE ELABORATION – EXAMPLE

The Plan stage focuses on the information security policy and on planning the controls relevant to the assessed risk level. Before that, however, the area of the organization covered by the ISMS must be precisely defined, regarding different aspects. The basic elements of the Plan stage, concerning the ISMS scope and policy, are presented in the Figure 3. Others, concerning low-level risk management, will be discussed later.

This class diagram is another example of using the UML for the ISMS specification. Both the *ISMS scope* and the *ISMS policy* are expressed as classes, aggregating their subclasses. Their names, belonging to the information security management domain[3], suggest responsibility of each class. The *Plan* includes also the third class, *Risk management*, that groups all low-level risk management elements (Figure 1).

The elaboration process of the *ISMS scope* elements placed in the Figure 3, based on the *Business environment* (Figure 2), is shown in the Figure 4 as an example of the UML activity diagram. Any activity may use objects

(please note underlined names) of given classes on input, producing or modifying other objects on its output. Some actions can be done concurrently. Generally, it is the simplest way to present an activity during the elaboration process, though sequence or collaboration diagrams can also be useful. The UML sequence diagrams are similar to well known block schemes of algorithms.

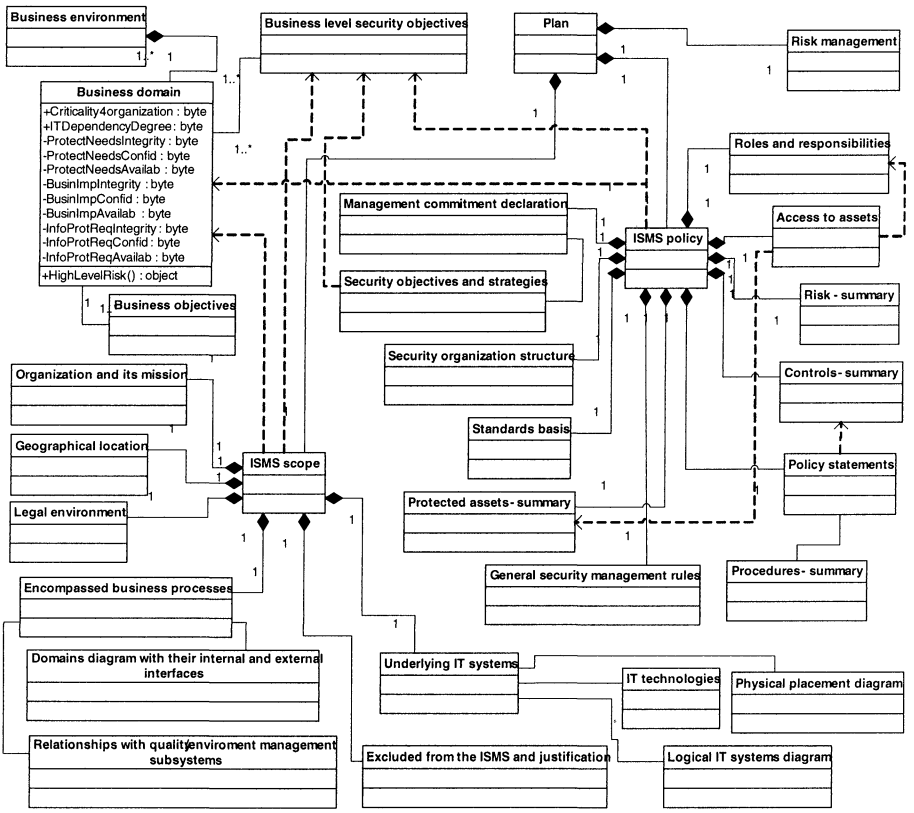

Figure 3. The Plan stage elements – the ISMS scope and policy.

Starting from a short presentation of the organization's mission (i.e. previously identified business objectives), geographical location, legal environment (acts and statutory regulations should be compliant), a business processes map is created with consideration of the underlying IT systems and their placement. For some areas of the organization excluded from the ISMS, justification is needed. Any organization ought to have assets inventory, encompassing different types of assets, including sensitive information. The presented approach assumes identification of assets based on the previously specified business domains. The assets may have different

roles assigned, e.g. owner, administrator, responsible person, etc. For this reason the adequate security organization structure and roles should be established. Please note that most of the *ISMS scope* specification elements can be derived directly from the previously specified objects of classes belonging to the *Business environment* class.

For well defined management scope, the management rules can be assumed, described by the *ISMS policy* class. Its basic elements are presented in the Figure 3.

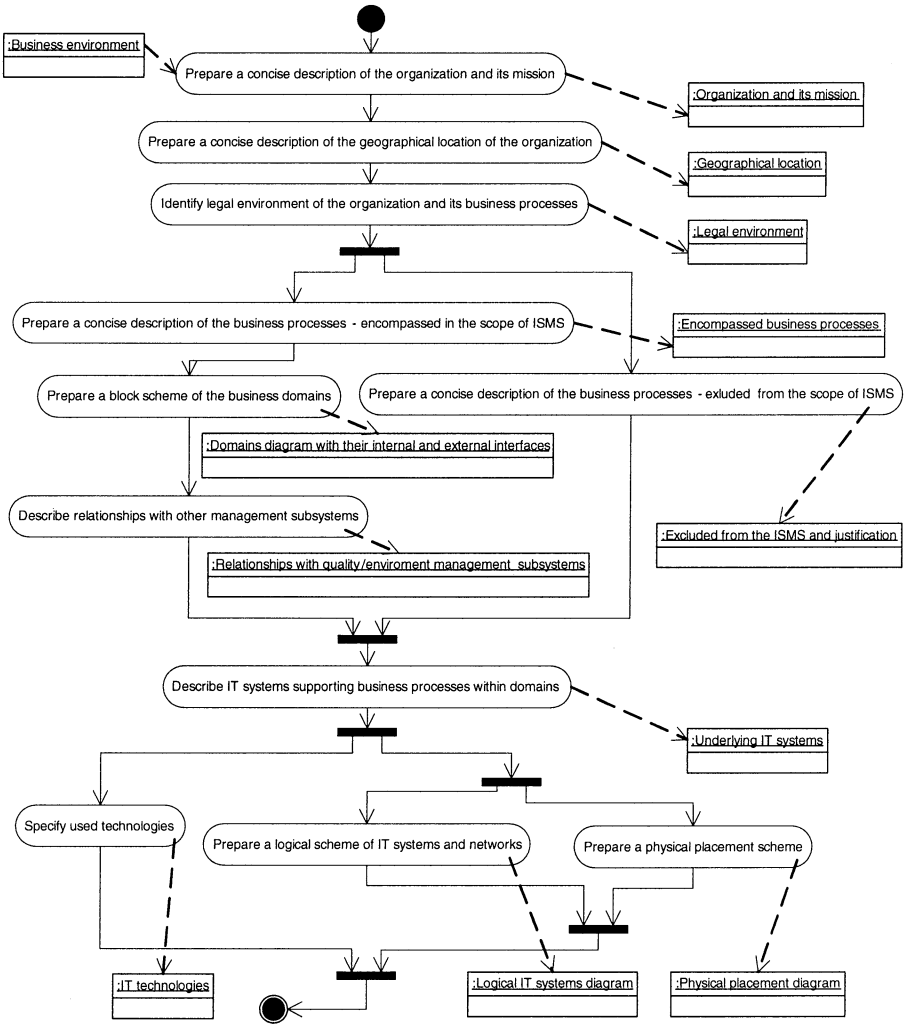

Figure 4. The ISMS scope elaboration.

The Figure 5 features another UML example, showing how to elaborate them.

Please note that the *ISMS policy* can be completed as a result of risk assessment and treatment.

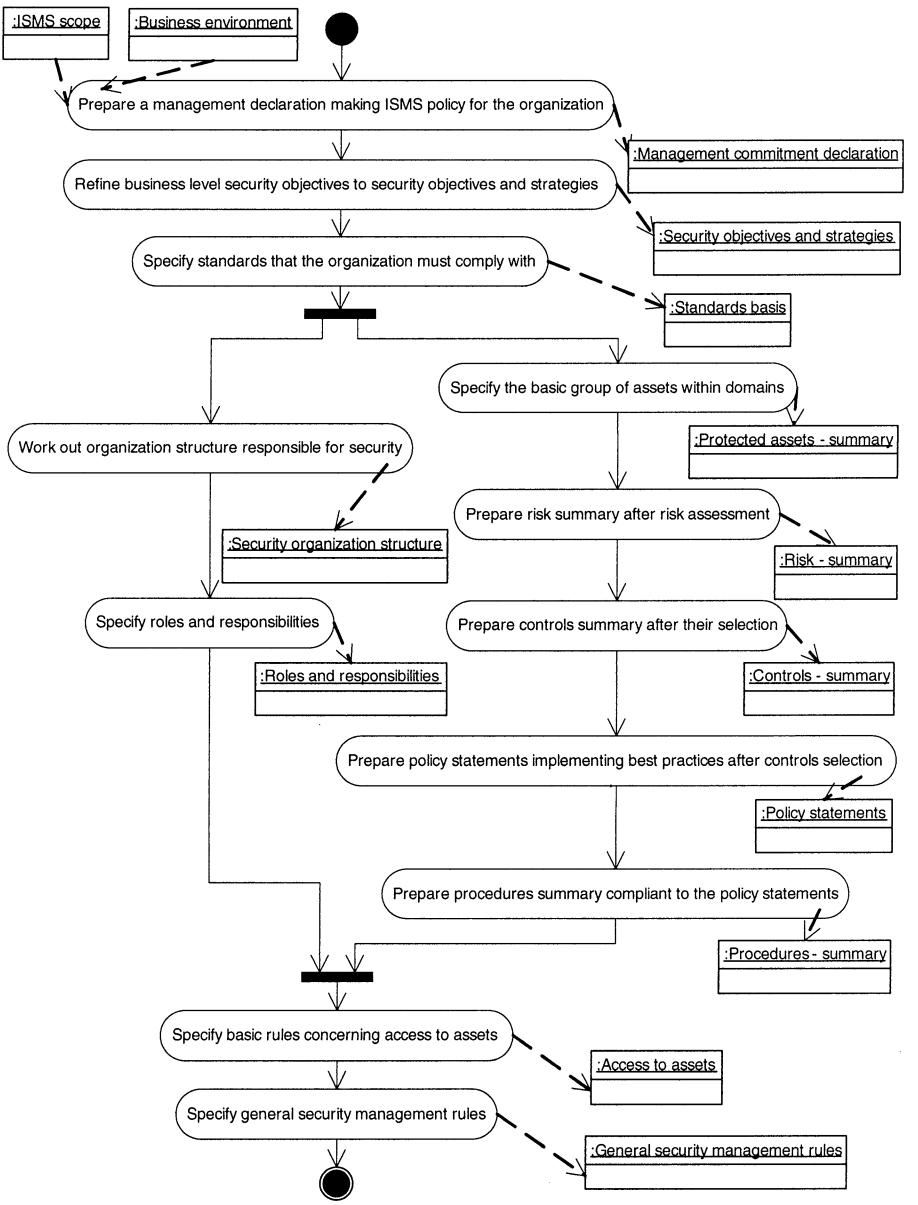

Figure 5. The ISMS policy elaboration.

The main *Risk management* elements belonging to the class *Plan*, and access control elements are presented in the Figure 6. The business domains usually differ from one another with respect to the following: high-level risk assessed, underlying IT systems and working environment. Thus, low-level risk management can be provided separately for every domain in accordance with the risk approach applied by the organization.

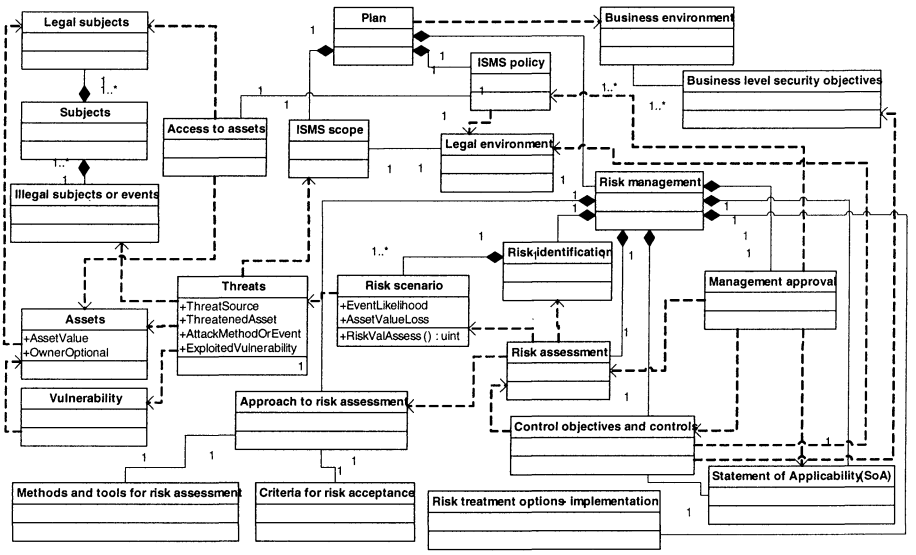

Figure 6. The Plan stage elements dealing with low-level risk management.

A detailed (low-level) risk analysis approach[12] was implemented. The elaboration of the *Risk management* elements is not discussed in detail but it is very similar to the actions previously presented on activity diagrams. The diagram also presents access control management to assets. Similarly to the concept presented in the author's paper[14], *Legal* and *Illegal subjects or events* classes were specified. The *Access to assets* class specifies access rules of any *Legal subject*.

The *Illegal subjects or events* class represents forces exploiting *Vulnerability* and initiating *Threats* for the *Assets*. Any of these undesirable events is described by the *Risk scenario*. The assessed risk value depends on the loss of the asset value and the event likelihood (please note appropriate class attributes). The presented detailed risk analysis can be qualitative, quantitative or mixed mode. Please note that some risk management issues, as summary information, can be added now to the *ISMS policy*.

The *Control objectives and controls* are derived from the *Business level security objectives*, *Risk assessment* and *Legal environment* classes, and will

be used to obtain a set of recommended safeguards during control implementation (Do stage is not discussed). They need justification (why selected/rejected) represented by the *Statement of Applicability (SoA)* class. At the completion of the standard Plan stage efforts, all data needed for the risk treatment plan elaboration and deployment are prepared (Do stage). The elements presented in the Figure 6 provide a risk management framework for the ISMS, used and updated during the whole ISMS life cycle.

5. CONCLUSIONS

The paper deals with the ISMS specification based on the UML. It encompasses all PDCA stages including the introductory high-level risk analysis for appropriate positioning of the whole model within the organization. The UML-approach for the ISMS specification was exemplified on the Plan stage elaboration. Using Plan stage specification, all structures – Do, Check, and finally, Act, can be successively elaborated, but it is not discussed there. Only main class diagrams and activity diagrams were shown in the paper. Use-case models, the assumed 4-layer software architecture and its implementation were not discussed there either.

The presented concept was used for the development of the prototype of a computer-aided tool[15], supporting information security managers, shown in the Figure 7 as the example. The application window contains main Plan stage elements, developed on the basis of high-level risk analysis results presented in the business environment window.

All main PDCA elements are implemented in the current version of the prototype at the basic level, while some details and features are still under development. The first feedback from customers shows that the tool is useful during security management – all activities are coordinated, records are sampled, the integrated tools and documents can be quickly reached, and internal security audits/reviews can be performed. Aside from BS 7799 compatible checklists, the tool has many others built in, concerning different legal and technical issues.

The first developers' experiences show that:

- taking advantage of the UML approach is fully possible for the ISMS implementation, just like in many other areas of the UML deployment,
- thanks to the UML it is possible to specify the entire ISMS and its processes in a modular way – methods, measures, tools, document templates can be changed,
- this flexibility allows tailoring the ISMS according to the size and specific needs of the organization (document templates defined for the assumed organization profiles).

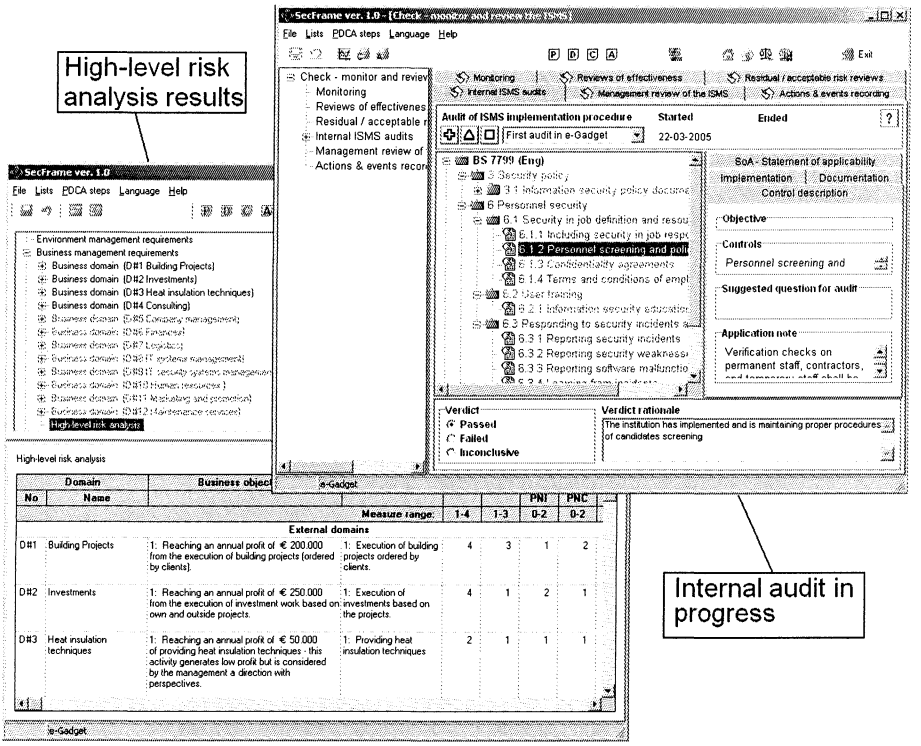

Figure 7. Information security management supporting tool[15].

In the same way it is possible to specify: business and its managing processes, security and its managing processes, IT systems and their managing processes and other assets – it is possible to create a unified information security management framework, well positioned within the business environment, basing on the UML approach. It can be assumed that the UML approach should be promising for the information security management as well, although this research area still needs further investigation.

REFERENCES

1. Booch G., Rumbaugh J., Jacobson I.: UML - Przewodnik użytkownika , Wyd. II, WNT, Warszawa 2002, (UML – User Guide).
2. UMLsite http://www.omg.org/uml/
3. BS-7799-2:2002 Information security management systems – Specification with guidance for use, British Standard Institution.
4. Jürjens J.: Secure Systems Development with UML, Springer-Verlag, 2004.

5. Galitzer S.: Introducing Engineered Composition (EC): An Approach for Extending the Common Criteria to Better Support Composing Systems, WAEPSD Proc., 2003.
6. Common Criteria for IT Security Evaluation, Part 1-3, ISO/IEC 15408.
7. Lavatelli C.: EDEN: A formal framework for high level security CC evaluations, e-Smart' 2004, Sophia Antipolis 2004.
8. Kadam Avinash: Implementation Methodology for Information Security Management System, v.1.4b, SANS Institute 2003.
9. Białas A.: IT security modelling, The 2005 International Conference on Security and Management, The World Congress In Applied Computing Las Vegas, June 20-23, 2005.
10. Białas A.: Designing and management framework for ICT Security, Joint Research Centre Cyber-security workshop, Gdansk, 9-11 September 2004.
11. Białas A.: The ISMS Business Environment Elaboration Using a UML Approach, KKIO (National Conference on Software Eng.), Cracow, 2005 (to be published by IOS Press).
12. ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the management of IT Security, Part3: Techniques for the management of IT Security.
13. IT Grundschutz Handbuch, BSI – Bonn: http://www.bsi.de
14. Białas A.: IT security development – computer-aided tool supporting design and evaluation, In: Kowalik J, Górski J., Sachenko A. (editors): Cyberspace Security and Defense: Research Issues, NATO Science Series II, vol. 196, Springer 2005.
15. SecFrame: http://www.iss.pl

ACKNOWLEDGEMENT

The author wishes to thank the Director of the Institute of Control Systems for the permission to publish screenshots of the SecFrame application (Figure 7).