Daniel GĄSKA[*], Antoni ŚWIĆ[**]

THE STANDARDIZED AUDIT OF SAFETY AND THE RELIABILITY OF ERP SYSTEMS

Abstract

The paper presents the possibility of the realization of the evaluation of the security of the Enterprise Resource Planning (ERP)systems following the regulations specified by European and Polish norms which relate to the safety of computer systems (information systems) in enterprises with the special regard to the ERP systems. It also introduces the possibility of creating the security system programme and the actions executed during the evaluation.

1. INTRODUCTION

ERP systems are characterized by the modular structure, that is each system contains several modules which create the complete entity. The modules can work in various configurations, which means that the firm does not have to buy the whole system. It is enough to buy the chosen modules which will co-operate with each other, thus exchanging the introduced information.

Assuring the safety to the computer resources of firms is currently one of most popular services on the IT market. However, the majority the services aiming at the evaluation and the improvement of the computer safety in the firm do not take into account the regulations specified by Polish and European norms. Thanks to the introduction of the norms into the process of the evaluation of the computer safety of the firm it will be possible to compare various ERP systems in relation to the safety. The standardized process of the evaluation of the safety will give us the true representation of the system and its protections.

The safety of the ERP system is the necessary element to ensure the correct functioning of the whole enterprise. Because all the elements of the enterprise are integrated with the ERP system, the possibility of maintaining the safety of the system

[*] M.Sc. Eng. Daniel Gąska Lublin University of Technology, Institute of Technological Information Systems, Lublin, Poland, e-mail: d.gaska@pollub.pl
[**] D.Sc. Eng. Assoc Prof. Antoni Świć Lublin University of Technology, Institute of Technological Information Systems, Lublin, Poland, e-mail: a.swic@pollub.pl

seems to be the essential element in the context of the utilization of ERP systems in the enterprises which introduced the system [1].

2. AUDITING ERP SYSTEMS ACCORDING TO THE DIRECTIVES OF SACA

ISACA (Information Systems Audit and Control Association) is an international association of the people in charge of the issues concerning the audit, control, safety and other aspects of the management of the information systems.

It is one the ways of introducing the reliable evaluation of the information systems and, in particular, of the ERP systems. The association proposes solutions which enable the execution of the audit of the information system realized on the basis of standards specified in SISA Standards for Information Systems Auditing [4].

It is imperative that the organization's system management fully understand and support the IS auditor's role(s) as it relates to the ERP system or implementation project .The IS Auditing Guideline should be reviewed and considered within the context of the ERP system and related initiatives of the organization (Fig. 1.).

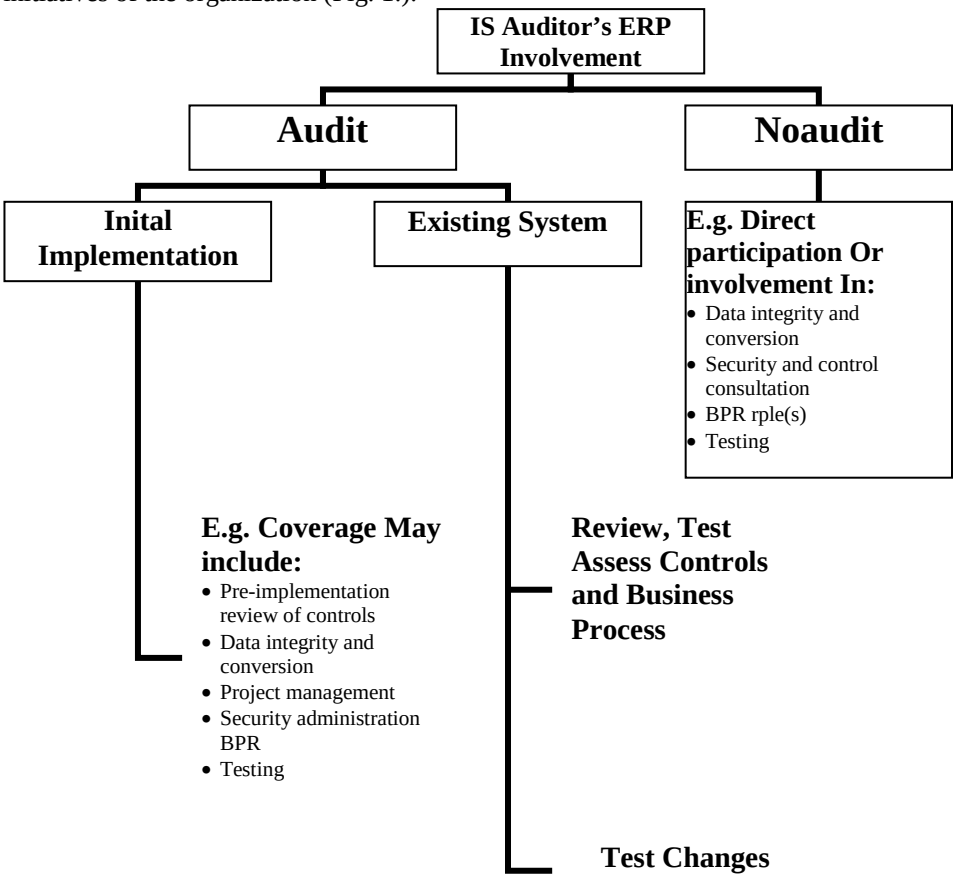

Fig. 1. IS Auditor's ERP Involvement [3]

ERP Knowledge and Skill Requirements [3]

	ERP System	**Implementation Project**
Background knowledge of the IS auditor	An understanding of financial and management controls and control risks generally A thorough understanding of the application of professional IS auditing standards A thorough understanding of IT related controls and control risks in the following areas: • IT environment • Applications/processing An understanding of client/server architectures An understanding of operating systems and database management systems A general understanding of ERPs and their design and deployment philosophies, including their effect on the audit trail An understanding of the ERP modules and how they are configured, integrated and deployed An understanding of security and authorization concepts in an ERP setting	An understanding of project management practices and controls generally An understanding of project management practices and controls in the area of IT An understanding of IT-related systems development methodologies and standards, including change management An understanding of business process reengineering principles and application of such
Skills of the IS auditor	A seasoned IS audit professional who is able to focus on the key areas of control risk in an ERP setting An understanding of computer-assisted audit techniques (CAATs) and how to apply them in an ERP setting. An ability to recognise where additional skills/expertise (such as financial and regulatory) are required	Experience in the review and assessment of implementation projects

How to Acquire skills	Certification as a professional auditor Certification as a professional IS auditor, such as CISA ERP learning opportunities especially as part of the end-user community Practical, on-the-job experience Self study, research, Internet, etc.	Enroll in specialist training courses focusing on Practical, on-the-job experience Self study, research, Internet, etc.

While carrying out the audit of the ERP systems, you should consider the most important areas of the system. Fig. 2 shows which areas you should examine more exactly.

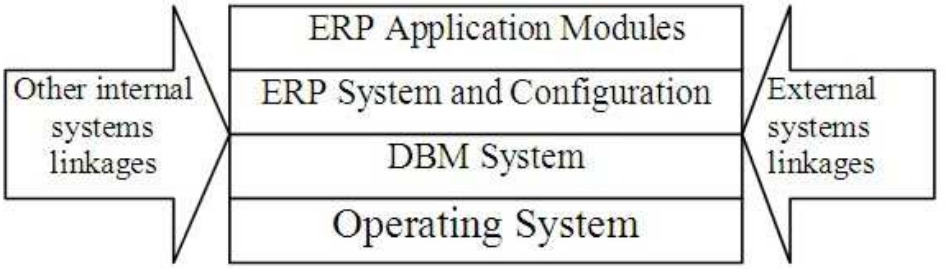

Fig. 2. General Elements of and Questions on ERP System Implementation

3. THE FEATURES OF THE SECURITY

Every component feature of the security depends on the architectural organization of the modules of the ERP systems and on the properties of the security of these modules.

Every component feature on the level of the system can depend on several component features on the level of the module [6].

The security of the ERP systems cannot be described by one feature. Some of the features can be expressed as probability, other features are deterministic some elements can be introduced quantitatively, whereas other aspects can only be described qualitatively.

The examples of the analysis of the security of ERP systems on the level of modules can be situations in which:

- thearchitecture of the system contains redundancy, the readiness of the system depends on the features of the integrity of the redundant modules;
- if the architecture contains the mechanisms of the protection of the system, the protection of the system depends on the features of the readiness of the modules which realize the mechanism of the protection;
- if the architecture contains modules controlling internal passing of the information between the various parts of the system, then the security of the system depends on the features of the protection of these modules.

In order to realize the evaluation of the security of the ERP systems, the program of this evaluation needs to be defined. This is possible after defining the aims of the evaluation of security, the requirements of the system and the specification of the system. Figure 1 represents three elements of the full analysis of the system, with the third element of the analysis being the evaluation of the security of the ERP systems [13].

It is important to remember that the information given in the document relating to the system requirements (SRD) and in the document relating the specification of the system (SSD) must be complete and exact to make the evaluation of the system possible.

If it turns out that at any phase of carrying out the evaluation, some information is missing or is incomplete, the consultation with the authors of SRD and SSD is required. By asking them detailed questions, it will be possible to receive the required information. It is important that the received additional information is specified in suitable documents [15].

4. EVALUATION CRITERIA ERP SYSTEMS ACCORDING TO THE DIRECTIVES OF INTERNATIONAL STANDARD ISO/IEC 15408

Information held by ERP system is a critical resource that enables organizations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in ERP products or systems remain private, be available to them as needed, and not be subject to unauthorized modification. ERP products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term ERP security is used to cover prevention and mitigation of these and similar hazards.

Many consumers of ERP lack the knowledge, expertise or resources necessary to judge whether their confidence in the security of their ERP products or systems is appropriate, and they may not wish to rely solely on the assertions of the developers. Consumers may therefore choose to increase their confidence in the security measures of an ERP product or system by ordering an analysis of its security (i.e. a security evaluation) [10].

The Common Criteria (CC) with international standard ISO/IEC 15408 can be used to select the appropriate ERP security measures and it contains criteria for evaluation of security requirements.

The Common Criteria (CC) with international standard ISO/IEC 15408 plays an important role in supporting techniques for consumer selection of ERP security requirements to express their organizational needs. The Common Criteria (CC) with international standard ISO/IEC 15408 is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.

Consumers can use the results of evaluations to help decide whether an evaluated product or system fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different products or systems. Presentation of the assurance requirements within a hierarchy supports this need.

The Common Criteria (CC) gives consumers — especially in consumer groups and communities of interest — an implementation-independent structure termed the Protection Profile (PP) in which to express their special requirements for ERP security measures in a Target of Evaluation (TOE).

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform.

The Common Criteria (CC) does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations. Figure 3 depicts the major elements that form the context for evaluations.

Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgment and background knowledge for which consistency is more difficult to achieve.

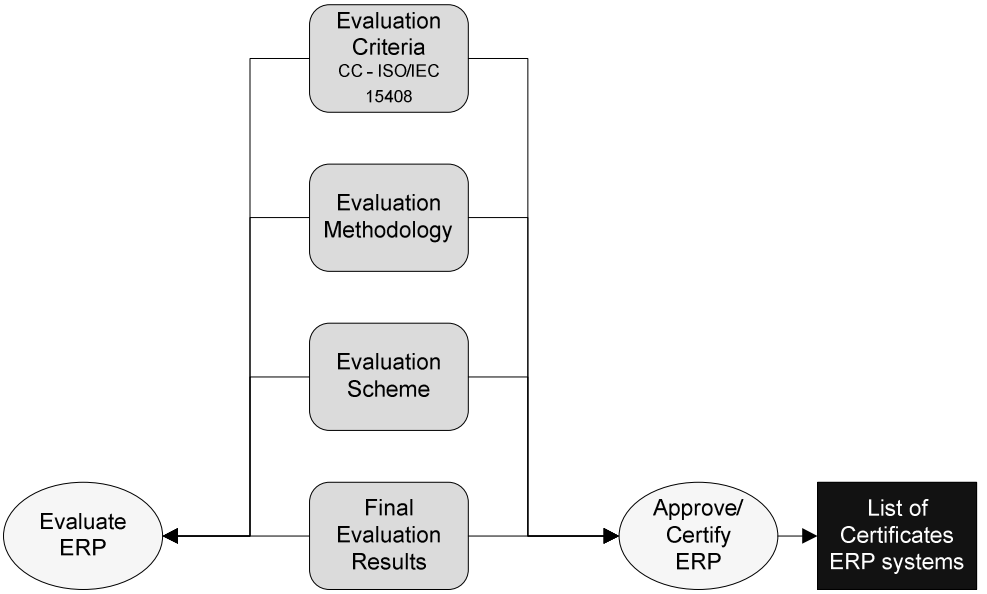

Fig. 3. Evaluation context

In order to enhance the consistency of the evaluation findings, the final evaluation results could be submitted to a certification process. The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval. The certificate is normally publicly available. It is noted that the certification process is a means of gaining greater consistency in the application of ERP security criteria.

Security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets. All categories of threats should be considered; but in the domain of security greater attention is given to those threats that are related to malicious or other human activities. Figure 3 illustrates high level concepts and relationships.

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Owners will perceive such threats as

potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security specific impairment commonly includes, but is not limited to, damaging disclosure of the asset to unauthorized recipients (loss of confidentiality), damage to the asset through unauthorized modification (loss of integrity), or unauthorized deprivation of access to the asset (loss of availability) [10].

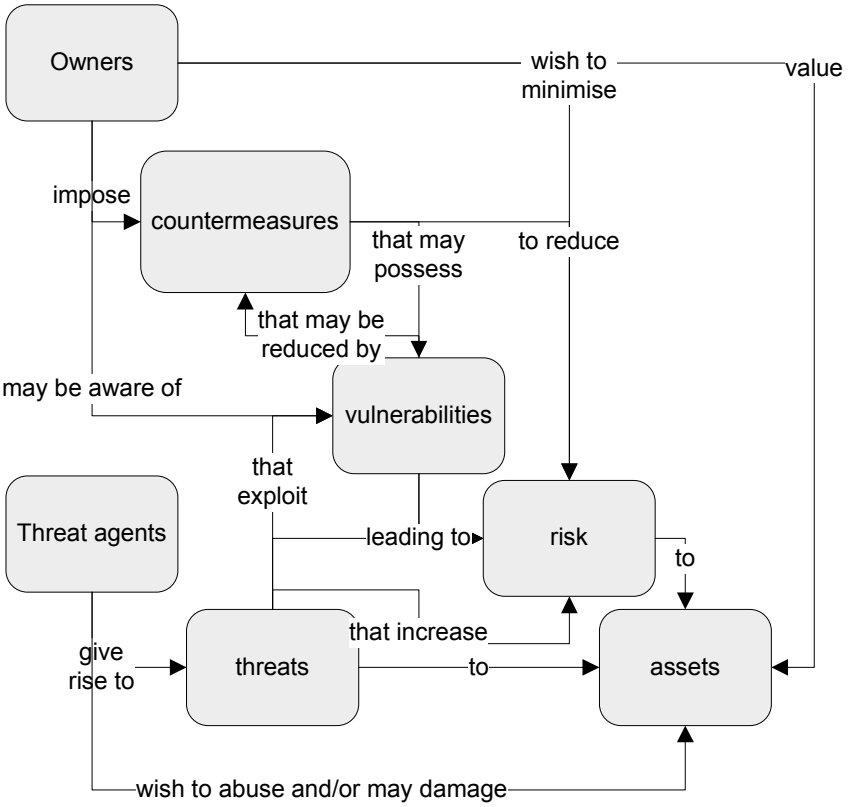

Fig. 4. Security concepts and relationships

The owners of the assets will analyze the possible threats to determine which ones apply to their environment. The results are known as risks. This analysis can aid in the selection of countermeasures to counter the risks and reduce it to an acceptable level.

Countermeasures are imposed to reduce vulnerabilities and to meet security policies of the owners of the assets (either directly or indirectly by providing direction to other parties). Residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets. Owners will seek to minimize that risk given other constraints.

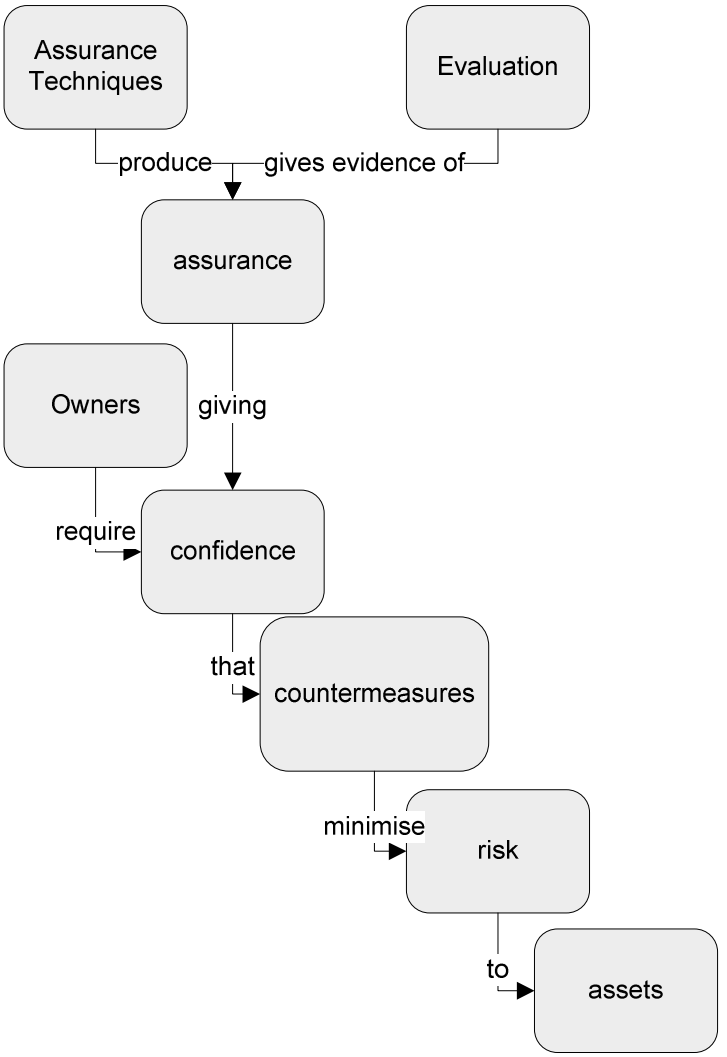

Fig. 5. Evaluation concepts and relationships

Owners will need to be confident that the countermeasures are adequate to counter the threats to assets before they will allow exposure of their assets to the specified threats. Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures. The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets. The statement assigns an assurance rating of the countermeasures, assurance being that property of the countermeasures that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats. Figure 5 illustrates these relationships [11].

Owners of assets will normally be held responsible for those assets and should be able to defend the decision to accept the risks of exposing the assets to the threats. This requires that the statements resulting from evaluation are defensible. Thus, evaluation should lead to objective and repeatable results that can be cited as evidence.

Many assets are in the form of information that is stored, processed and transmitted by ERP products or systems to meet requirements laid down by owners of the information. Information owners may require that dissemination and modification of any such information representations (data) be strictly controlled. They may demand that the ERP product or system implement ERP specific security controls as part of the overall set of security countermeasures put in place to counteract the threats to the data ERP systems are procured and constructed to meet specific requirements and may, for economic reasons, make maximum use of existing commodity ERP products such as operating systems, general purpose application components, and hardware platforms. ERP security countermeasures implemented by a system may use functions of the underlying ERP products and depend upon the correct operation of ERP product security functions. The ERP products may, therefore, be subject to evaluation as part of the ERP system security evaluation [11].

4.1. COLLECTING THE INFORMATION FOR EXECUTING THE EVALUATION OF THE SECURITY

Before beginning the realization of the audit of the security of the ERP system, it is necessary to execute the review of the system in order to relate the system to its mission. The system should be decomposed into modules and elements. It is also necessary to remember that the process of decomposing leads to demonstrative schemes/patterns and additional descriptions.

It is recommended that while realizing the process of decomposing of the ERP system the description should include:

- all modules of interface to the process, to the application, to the database and to external systems;
- communication channels which in the large measure decide about the security of the system;
- processing modules connected with the application;
- the interaction of the modules;
- existence of the divisions and the distances between the divisions of the firm.

After completing the process of decomposingit is important to know that the majority of ERP systems are based on module architecture which where he separate modules freely combined.

In order to conduct the evaluation of the system, it is essential to extract the necessary information from SRD and SSD documents.

It is recommended to combine the requirements specified in SRD and the level of security assured by the system, as specified in SSD, and the comparison between them in order to arrive at the precise quantitative and qualitative definition and the range of their value, if this can be applied, in following casess:

- thelimits of the ERP systems;
- thekind of threats and their ways of spreading;
- the influencing conditions which can create the threat inside the system;
- the ways of reducing the risk of the situations which may pose the threat;

- the ways of reducing the risk of the situations of connecting various phenomena which, in turn, may pose the threat;
- the allocation of the security of modules and the elements of the system;
- the way in which various modules and the elements of the system interact and the possibility losing the security which can happen as the result of the interaction;
- matters which are outside the range of the system;
- thegenerally accessible knowledge and the range within which the security of the system is to be evaluated.

4.2. ACTIONS EXECUTED DURING THE EVALUATION OF THE SECURITY OF THE SYSTEM

The list of the actions to be realized during the evaluation process comes from the reduced list of the objects of the evaluation broadened by the subjects included in the evaluation in which we should consider:

- thekind of analysis and defining of the proprieties required for the justification of the evaluation of the security;
- thelevel of the priority of every action which is part o the evaluation of the security;
- theknowledge and skills necessary for the execution of the required analysis and the definition of the properties;
- limitations in the schedule of the evaluation of the security, resulting from the long time of marking the different proprieties of the system;
- theavailability of the chosen staff;
- tools and services necessary for the execution of required analyses and delimitation of the propriety of the system;
- estimation of the cost and duration of every analysis and the definition of the properties of the system.

It is often necessary to combine several techniques which will be complimentary and will make it possible to define the security of the system realizing earlier planned actions.

The programme of the evaluation of the security of the ERP systems should contain such elements as:

- the object of the evaluation;
- the criteria which need to be taken into consideration;
- the actions taken during the evaluation;
- therequired increase of the level of the confidence;
- the schedule of the evaluation in which you should consider the long time of the duration of some investigations.

4.3. TECHNIQUES OF DEFINING THE PROPRIETIES OF THE SYSTEM FOR FURTHER EVALUATION

Chosen techniques could be either analytic, using only the documentation of the system or experimental, requiring the access to the realized system [2].

The results received with the help of the alternative techniques of defining proprieties can be quantitative or qualitative, or can also be the combination of both kinds.

Various methods of defining properties can be applied, but it is recommended that in each case, the report of the evaluation contained the reference he documents describing the applied methods.

The following steps should be executed with reference to each kind of the threat:

- check if the threat exists and if it does, check if there is the accessible certification and if it is valid in the working conditions specified in SRD or if it follows the regulation;
- if the satisfying certification is not available it is recommended to execute the suitable analysis of the risk.

The experimental techniques of defining the proprieties of the system are the supplement of the analytic techniques.

Every time the analytic techniques cannot guarantee the evaluation of the security level of the system, the execution of experimental defining of the proprieties, in order to evaluate those aspects which do not have complete data.

5. THE REPORT OF THE EVALUATION OF ERP SYSTEMS

The report of the evaluation of the safety of the ERP system should also contain the following information:

- the compilation of the data from the document relating to system requirements and the document relating to the specification of the system of, for example the requirements of safety, working conditions, service, etc.;
- theanalysis of the system, its modular and functional structure, the risks to which the system was subjected, elements and components and the relationship between them, etc.;
- thelist of actions recommended for further evaluation of the analysis and further investigations.

8. SUMMARY

Summing up should affirm, that the performance of the standardized programme of the opinion of the safety of the ERP systems will make possible the creation such conditions the work, which will give the tool to the enterprise thanks which what level of the safety of the ERP systems the qualification possible will be he is in the enterprise. Does the introduce methodology give the answer what to the safety of one of the most important links of the firm.

REFERENCES

1. *Benjamin B. Bae, Ph.D., and Paul Ashcroft, Ph.D.*: Implementation of ERP Systems. Accounting and Auditing Implications, ISACA Journal Volume 5, 2004.
2. *Standards*, Guidelines and Procedures for Auditing and Control Professionals, Published by Information Systems Audit and Control Association, February 2007.
3. *Steve Maguire*, Writing solid code: Microsoft's techniques for developing bug-free C programs, Published by Microsoft Press Washington 1993.
4. *PN-I-13335-1*: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.

5. *PN-I-02000*: Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.
6. *PN-ISO 10011-1*: Wytyczne do audytowania systemów jakości. Audytowanie.
7. *ISO/IEC 17799*: Technologie informacyjne. Zasady postępowania w zarządzaniu bezpieczeństwem informacji.
8. *PrPN-I-13335-2*: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Aspekty zarządzania i planowania.
9. *PrPN-I-1335-3*: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Techniki bezpieczeństwa.
10. *ISO/IEC 15408-1*: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.
11. *ISO/IEC 15408-2*: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components.
12. *ISO/IEC 15408-3*: Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components.
13. *PN-EN 61069*: Pomiary i sterowanie procesami przemysłowymi. Wyznaczanie właściwości systemu w celu jego oceny: Część 2: Metodologia oceny.
14. *PN-EN 61069*: Pomiary i sterowanie procesami przemysłowymi. Wyznaczanie właściwości systemu w celu jego oceny: Część 5: Ocena niezawodności systemu.
15. *PN-EN 61069*: Pomiary i sterowanie procesami przemysłowymi. Wyznaczanie właściwości systemu w celu j**e**go oceny: Część 7: Ocena bezpieczeństwa systemu.