DRAFT

full paper published in:

The Proceedings of International Conference of Dependability of Computer Systems DepCoS-RELCOMEX, Szklarska Poreba, Poland, 2008, pp 95-102

Paper published in the journal and presented at the conference

Standards Conformity Framework in Comparison with Contemporary Methods Supporting Standards Application

Łukasz Cyra, Janusz Górski
Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland
lukasz.cyra@eti.pg.gda.pl, jango@pg.gda.pl

Abstract

Achieving and assessing conformity with standards and compliance with various sets of requirements generates significant costs for contemporary economies. Great deal of this is spent on fulfilment of safety and security requirements. However, standards application is not supported sufficiently by the tools available on the market. Therefore, Standards Conformity Framework (SCF) containing methods and tools which provide support for application of standards was proposed. The framework is based on trust case methodology being used to provide arguments demonstrating properties of IT systems. The article describes SCF and shows how it fits into the processes of achieving and assessing conformity. It identifies other methods and tools supporting standards application and compares them with the framework.

1. Introduction

Compliance and conformity achievement and assessment involves significant costs in contemporary economies. It is estimated that in US over 1.4 trillion $ being 15% of the GDP is spent yearly to this end [1]. Additionally, the costs have been increasing dynamically at the rate of 40% for the last 15 years [2]. Similar tendencies can be observed all over the world.

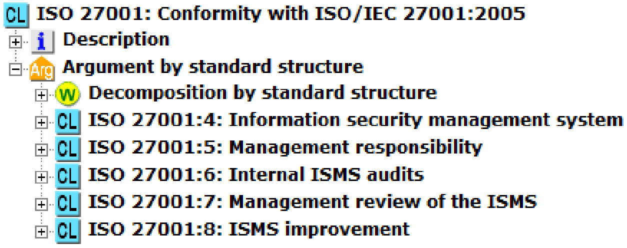
Despite the importance of the subject, it has not yet been addressed adequately in the market. According to the survey published in [3], 74% of organizations base their compliance effort on manual or mostly manual methods (e.g. text editors, spreadsheets, etc.), indicating lack of existence of satisfactory solutions in 37% of cases.

Standards Conformity Framework (SCF) is a generic framework supporting standards application. It has already been successfully applied in relation to safety and security standards. The article presents the framework, its application process and a tool supporting SCF. Then a number of methods and tools related to standards application and financial and security audits, presently available in the market, are compared with SCF. In conclusion we briefly summarize the results of this comparison.

2. Standards Conformity Framework

Standards Conformity Framework (SCF) is based on the observation that assessing and/or achieving conformity mainly involves producing and gathering the conformity demonstrating evidence and then presenting it within a legible and understandable argumentation. Therefore, argument structures and the related methodologies can offer a direct support to this end.

The *Trust Case* language, being developed as part of the *Trust-IT* methodology [4-6], was chosen for the purpose of structuring the argument of standards conformity. It was selected because of its flexibility and legibility. Trust Case is a powerful language, which can be easily applied to situations where uncertainty resulting from lack of evidence is unavoidable. It is also an expressive language which can be used to represent formal as well as informal reasoning being much in common in real-life situations. Trust Case is a graphic language of simple syntax. The argument has a tree-like structure, being composed of a number of simpler sub-arguments developed recursively. Each of the sub-arguments is decomposed in further until it is possible to base the inference on available evidence. So a Trust Case tree encompasses all the evidence and justification related to a certain problem. It is easy to comprehend because it recursively decomposes the problem into sub-problems that to large extent can be considered in isolation. It also leads the user through subsequent abstraction layers which correspond to the subsequent level of the argument tree.



```
CL ISO 27001: Conformity with ISO/IEC 27001:2005
⊞ i Description
⊟ Arg Argument by standard structure
    ⊞ W Decomposition by standard structure
    ⊞ CL ISO 27001:4: Information security management system
    ⊞ CL ISO 27001:5: Management responsibility
    ⊞ CL ISO 27001:6: Internal ISMS audits
    ⊞ CL ISO 27001:7: Management review of the ISMS
    ⊞ CL ISO 27001:8: ISMS improvement
```

Figure 1. Trust Case

An example of a Trust Case is given in figure 1. In the root of the tree it contains a claim (denoted CL) of conformity with ISO/IEC 27001:2005 standard. Below this claim there is an argument node (denoted by Arg) that explains the chosen argument strategy to argue about the claim (the strategy is to argue by referring to the standard structure). There is also an information node (denoted i) which includes additional information which helps the user to understand the argumentation. Justification of the claim is based on five more specific claims, each of which states that requirements of a particular chapter of the standard are fulfilled. The inference is explained and justified in the warrant (denoted W). Each of the five sub-claims can be decomposed further, which is not presented in figure 1. Finally, at the bottom of the structure the inference is based on facts rather than claims, and the facts are directly referring to available evidence.

The main objective of SCF is to develop and maintain an (electronic) document which justifies the claim of conformity. Such a document is called a *standard's conformity case*. It is derived from a generic structure called a *Trust Case Template*. The template is standard specific and its structure reflects the structure of a given standard. The same template can be reused in multiple projects of this specific standard application. While being applied, the template is filled in with project specific evidence.

The process of SCF application is presented graphically in figure 2. The process distinguishes four steps of the framework application. The first step involves derivation of the template from a given standard. It is a formal document specifying the requirements of the standard as well as the (agreed) way of demonstrating conformity. This step is of particular importance as it conditions the results of the following steps. Auditors and other experts are involved at this step to provide for quality and to decide about the final acceptance of the template.

In the next step the template drives the process of achieving conformity. It identifies the evidence which must be created, guides in positioning this evidence in the argumentation tree and provides criteria for assessing its quality. The template explains the meaning of the requirements of the standard, explicitly represents interdependencies among them, and lists the additional documents required by the standard and the external guidance documents, which can be helpful in fulfilling the requirements. The result of this process is a standard's conformity case in which all claims about fulfilment of the standard requirements are supported by explicit justification.

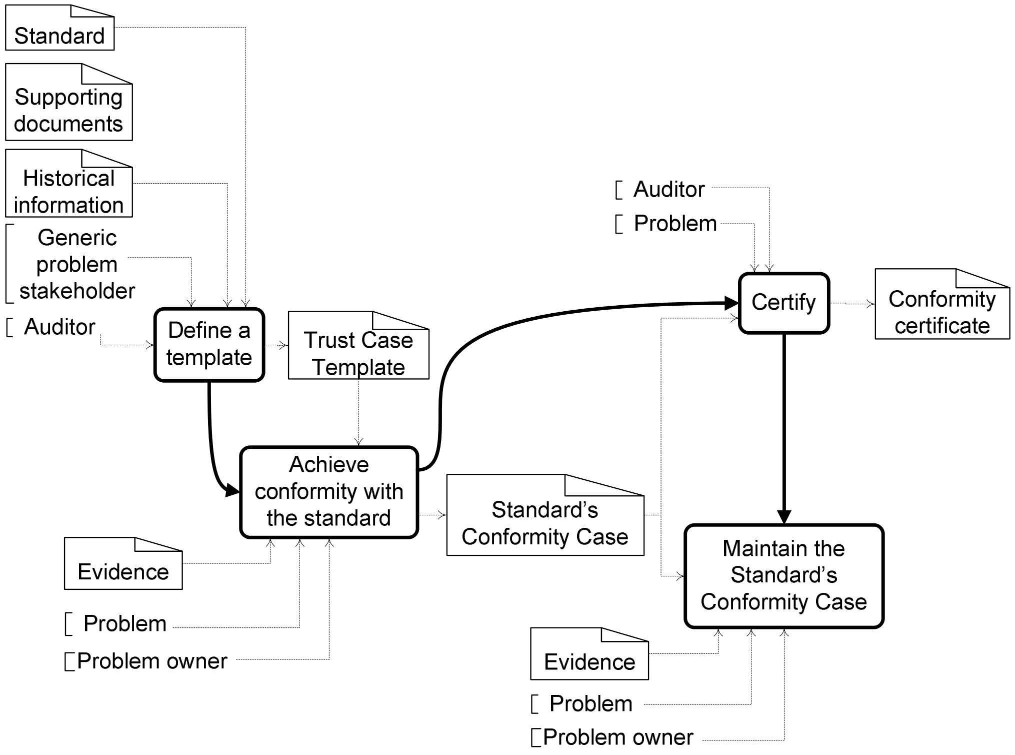


Figure 2. SCF application process

The standard's conformity case is used as the input to 'Certify' step. Presenting a complete justification of the claim of conformity in the form of a conformity case significantly facilitates this step. The task of the auditor it to examine and assess the conformity case with the main focus on the scope and quality of the evidence included in the case. In this particular step the effort put in the earlier preparation of the template pays back by providing explicit argumentation which can be followed by the auditor, and by providing easy access to the evidence supporting this argumentation.

Finally, as numerous standards require regular reassessment, SCF supports the process of maintenance of conformity. The template identifies interdependencies among the requirements, which help in tracing changes and assessing their impact. And in the case conformity is temporarily lost, all the advantages relevant to the conformity achievement step can be again exploited for quick conformity restoration.

The whole process of SCF application is supported by a software tool, called the TCT system. The TCT system is a fully on-line, Internet based tool, which provides for development, dissemination and maintenance of Trust Case templates and standard's conformity cases. Among many others it supports teamwork, remote access and document management. It is easy to use, which is particularly important considering involvement of non-technical people in the conformity related projects.

More thorough explanation of SCF can be found in [7,8].

3. Comparing SCF to other conformity supporting approaches

The main purpose of the analysis was to compare and assess the support provided by SCF with respect to other methods presently available on the market. The analysis did not pretend to cover all the approaches supporting standards application; nevertheless it covers a representative sample of the available solutions. The support for security standards was considered with special care because of the importance of this domain and the availability of several matured standards. We have also included the financial audit and security audit tools and methods because of many similarities between conformity audit and other types of audits.

The following methods, tools, guides, and standards were identified and taken into account in the analysis: *Audyt Asystent* [9], *AutoAudit* [10], *BindView* [11], *BIP 0070* [12-15], *BS 7799-3:2006* [16], *Callio Secura 17799* [17], *Cobra* [18], a tool from Commonwealth Information Security Center [19], *Compliance Audit Reference Manual* [20], *CRAMM* [21], *CuteDraw* [22], *EA-7/03* [23], *EBIOS* [24], security audit standards from ISACA [25], *ISO 19011* [26], *ISOCharter* [27], *ITAF* [28], *LP-A* [29], *MARION* [30], *Microsoft Visio 2007* [31], *Office of the Auditor General of Canada Guide* [32], *PD 3000* [33-37], *Podręcznik audytu wewnętrznego w administracji publicznej* [38], *Proteus* [39], *Ra2* [40], *SecCert* [41], *SecFrame* [42], a tool from TeamInfoSec [43], *TeamMate* [44], *Trenox ISO Toolkit* [45].

The main conclusion from the analysis was that there is presently no generic solution supporting application of a range of standards. Each approach is targeting at a small set of similar standard (mostly just one standard). *SecFrame* is an exception and supports application of seven different standards, however, all of them from the same domain. For some standards there are no solutions available at all (ISO 14971 [46] is an example).

3.1. Conformity achievement and maintenance

Considering conformity achievement, the solutions available provide very divers support. Many of them define the process of conformity achievement and try to help to manage it (*CRAMM*, *EBIOS*, *PD 3000*, *BIP 0070*, *Ra2*). However, the main focus of all of the methods is to help in fulfilling particular requirements. For some standards, there are guidelines which help in business process modelling (*Trenox ISO Toolkit*, *ISOCharter*), risk analysis (*TeamInfoSec*, *Callio Secura 17799*, *MARION*, *CRAMM*, *EBIOS*, *PD 3000*, *BS 7799-3*, *Proteus*, *Ra2*, *AutoAudit*), security controls designing and assessment (*SecCert*, *SecFrame*) and so on. In addition, some of the proposed approaches facilitate development of the documents required by standards by providing document templates (*BindView*, *PD 3000*, *BIP 0070*), supporting cost analysis (*CRAMM*) and many others. Certain solutions include recommendations of how to base decisions on the data gathered about the object of analysis (*Cobra*, *CRAMM*) or support change management in relation to conformity with a standard (*ISOCharter*).

Only one of the proponents identified and represented interdependencies among standards' requirements which is very crucial concerning the process definition and conformity maintenance (*SecCert*, *SecFrame*). In all the solutions the problem of justifying conformity was not addressed at all or treated very superficially. The most advanced solutions in this respect provide means of giving explanations in words (*Callio Seucra 17799*, *SecFrame*) and one of them provides provisions to attach external files (*Callio Secura 17799*).

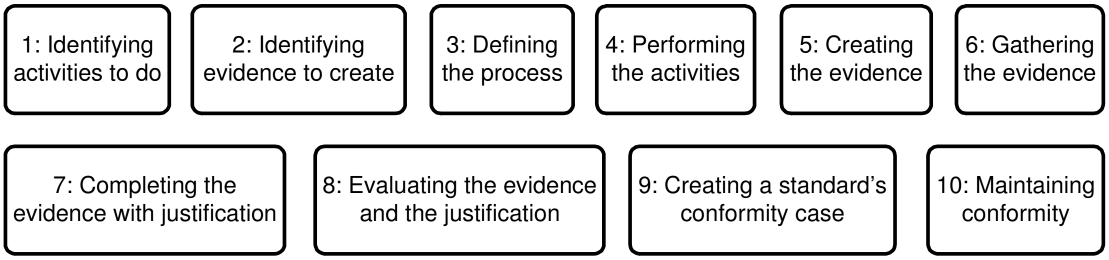

1: Identifying activities to do
2: Identifying evidence to create
3: Defining the process
4: Performing the activities
5: Creating the evidence
6: Gathering the evidence
7: Completing the evidence with justification
8: Evaluating the evidence and the justification
9: Creating a standard's conformity case
10: Maintaining conformity

Figure 3. Conformity achievement and maintenance comparison criteria

Figure 3 shows the detailed criteria related to conformity achievement and maintenance, used during our assessment. The analyzed solutions concentrate on 1 and 4, some of them support 3. As for 2 and 5 they address them partly, supporting only development of documents required by standards. Criteria 6, 7, 8 and 9 are treated superficially. 10 is addressed only by a few solutions. By contrast SCF fully meets 2, 6, 7, 8 and 9, addresses 3 and 10 and refers to the already existing solutions in relation to 1, 4 and 5. The result of the comparison is given in table 1.

Criterion	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Available solutions	+	+-	+	+	+-	+-	+-	+-	+-	+
SCF	+-	+	+	-	-	+	+	+	+	+

Table 1. SCF vs other solutions for conformity achievement and maintenance

This analysis has shown that the available solutions are rather complementary than competitive to SCF. It has also shown that SCF together with a method which meets criteria 1, 4 and 5 (e.g. *SecFrame* for ISO 27001 [47]) can well support the whole process of conformity achievement and maintenance.

3.2. Conformity assessment

Concerning conformity assessment the available solutions can be classified as follows. Some address the rules of performing audits, like impartiality of the auditor (*ISACA*, *Office of the Auditor General of Canada*, *Podręcznik audytu wewnętrznego w administracji publicznej*). Some state how audit should be performed, and define requirements for the process e.g. the steps to be taken, the roles to be played and the related responsibilities, the necessary competencies, the way of reporting the audit results, and so on (*EA-7/03*, *Podręcznik auditu wewnętrznego w administracji publicznej*, *LP-A*, *TSIM*, *ITAF*, *Compliance Audit Reference Manual*, *ISO 19011*). Other define the certification process (*BIP 0070*, *PD 3000*) or support drawing charts of audit processes and procedures (*Microsoft Visio 2007*, *CuteDraw*). Many of the solutions focus on supporting assessment of conformity with particular requirements of a standard e.g. security assessment (*SecCert*, *PD 3000*, *BIP 0070*) or give precise instructions how to assess conformity with particular requirements (*BIP 0070*, *Proteus*). Additionally, some of the solutions provide audit document templates (*Office of the Auditor General of Canada*, *Podręcznik audytu wewnętrznego w administracji publicznej*, *LP-A*, *ITAF*).

In all the solutions, the problem of evaluation of evidence was not addressed or treated superficially. In most cases, the only support is by providing checklists, a few provide some means of managing the evidence and support a bit more refined assessment. The most advanced solutions use a four level scale which makes it possible to state whether the requirement is fulfilled, not fulfilled, not relevant, or it is inconclusive, and to explain textually the decision (*SecFrame*). None supports explicit arguments of conformity. By contrast SCF provides means of evaluation of validity and strength of the justification and evidence, giving a very powerful method of conformity assessment.

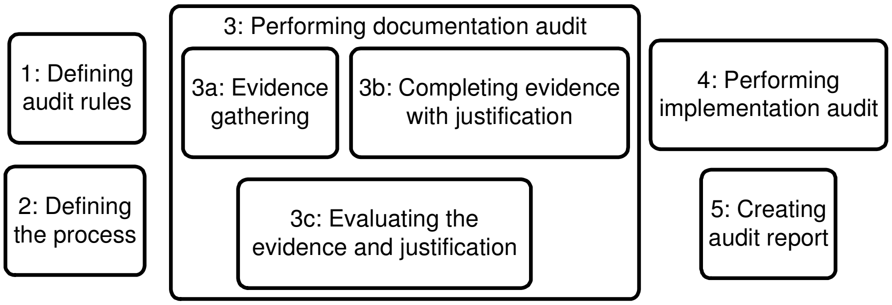

1: Defining audit rules
2: Defining the process
3: Performing documentation audit
3a: Evidence gathering
3b: Completing evidence with justification
3c: Evaluating the evidence and justification
4: Performing implementation audit
5: Creating audit report

Figure 4. Conformity assessment comparison criteria

Figure 4 shows the detailed criteria used for the conformity assessment aspect. SCF does not support criterion 1. Criterion 2 is covered only on a generic level and does not go into detail considering aspects not directly related to features of the framework. Both criteria are well covered by the existing solutions. The major difference between SCF and other methods is that SCF fully meets 3a and 3b before the audit starts. By contrast, the other methods leave meeting of those criteria as the responsibility of the auditor. The approach promoted by SCF can have a positive impact on costs, as it can be much more cost effective to gather all the evidence and justification before the audit. There are people in organizations who have the knowledge to perform this task effectively and usually their revenues are lower than the auditors'. Criterion 3c is very well supported by SCF and only partially addressed by some of the other solutions. Criterion 4 is quite well addressed by some of the considered solutions and is not addressed at all by SCF. Criterion 5 is quite well addressed by some of the considered solutions and is also well addressed by SCF.

Criterion	1	2	3a	3b	3c	4	5
Available solutions	+	+	+	+-	+-	+	+-
SCF	-	+-	+	+	+	-	+

Table 2. SCF vs other solutions for conformity assessment

This analysis has shown that SCF is a good alternative for the considered methods which address documentation audit. Because of taking a different approach than other methods conformity assessment is largely simplified. Advanced functions related to argument evaluation implemented in the tool supporting SCF can propose a new quality in this field. On the other hand, SCF does not define the audit rules and defines the audit process only superficially. These criteria, however, are very well addressed by other solutions and there is a room for complementarity as in the case of implementation audit and creating the final audit report.

4. Conclusions

Standards Conformity Framework described in this paper is a complete and ready to use methodology supporting achieving, assessing and maintaining conformity. The framework is supported by an Internet based tool which supports all the stages of SCF application.

The analysis presented in the paper showed that SCF is complementary to the other methods for conformity achievement and maintenance available on the market, and is a good alternative for the existing conformity assessment solutions. It has already been applied in several real-life case studies giving very promising results. It was also highly assessed by auditors from one of the leading international certification companies. A number of further experiments and case studies in cooperation with industrial partners are under preparation.

5. References

[1] M. Hodges, Grandfather Economic Report, http://mwhodges.home.att.net/regulation.htm, visited on 20.09.2007

[2] International Standard, Conformity Assessment, and U. S. Trade Policy Project Committee, Standards Conformity, Assessment, and Trade. Into the 21st Century, National Academy Press, Washington, 1995

[3] Companies Struggle with Compliance: Survey, Elsevier, Computer Fraud & Security Volume: 2006, Issue: 8, August, 2006, pp. 3

[4] J. Górski et al.: Trust Case: Justifying Trust in IT Solution. Reliability Engineering and System Safety, Volume 89, Elsevier, 2005, pp. 33-47

[5] J. Górski: Trust Case – a Case for Trustworthiness of IT Infrastructures. Kowalik J. & Gorski J. & Sachenko A. (Eds.), Cyberspace Security and Defence: Research Issues, NATO ARW Series, Springer-Verlag, 2005, pp. 125-142

[6] J. Górski: Collaborative Approach to Trustworthiness of Infrastructures. Proceedings of IEEE International Conference of Technologies for Homeland Security and Safety. TEHOSS 2005, 2005, pp. 137-142

[7] Ł. Cyra, J. Górski, Supporting Compliance with Safety Standards by Trust Case Templates, Risk, Reliability and Societal Safety : Proceedings of the European Safety and Reliability Conference 2007, ESREL 2007, Norway, vol. 2, London : Taylor and Francis, 2007, pp. 1367-1374

[8] Ł. Cyra, J. Górski, Standard Compliance Framework for Effective Requirements Communication, 14th International Multi-Conference: Advanced Computer Systems, Międzyzdroje 2007

[9] InfoAudit, Audyt Asystent's User Manual, 3.00.19 Version, http://www.infoaudit.com.pl, visited on 07.09.2007 (in Polish)

[10] Paisley Homepage, http://www.paisley.com, visited on 07.09.2007

[11] BindView Homepage, http://www.bindview.com, visited on 17.09.2007

[12] T. Humphreys, A. Plate, BIP 0071 Guidelines on Requirements and Preparation for ISMS Certification based on ISO/IEC 27001, BSI 2005

[13] T. Humphreys, A. Plate, BIP 0072 Are You Ready for an ISMS audit based on ISO/IEC 27001?, BSI 2005

[14] T. Humphreys, A. Plate, BIP 0073 Guide to the Implementation and auditing of ISMS controls based on ISO/IEC 27001?, BSI 2005

[15] T. Humphreys, A. Plate, BIP 0074 Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001?, BSI 2006

[16] British Standards Institution, BS 7799-3 Information Security Management System. Part 3: Guidelines for Information Security Risk Management, 2006

[17] Callio Technologies Homepage, http://www.callio.com, visited on 07.09.2007

[18] C & A Security Risk Analysis Group Homepage, http://www.security-risk-analysis.com, visited on 07.09.2007

[19] R. Prieto-Diaz, Security Impact Analysis Visualization Research, Internal Report, Phase 1 Report, 2003

[20] Forest Practices Board, Compliance Audit Reference Manual Version 0.6, 2003, http://www.fpb.gov.bc.ca/, visited on 07.09.2007

[21] CRAMM Homepage, http://www.cramm.com, visited on 12.09.2007

[22] CuteDraw Homepage, http://www.cutedraw.com, visited on 12.10.2007

[23] EA C5 WG7 on Information and Communication Technology, EA-7/03 EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems, 2000

[24] IT Works Homepage, http://www.itworks.lu, visited on 12.09.2007

[25] ISACA, Standardy wytyczne i procedury audytowania i kontrolowania systemów informatycznych, 2002, http://www.isaca.org.pl, visited on 28.09.2007 (in Polish)

[26] International Organization for Standardization, ISO 19011:2002 Guidelines for Quality and/or Environmental Management Systems Auditing, 2002

[27] M. Olszewski, ISOCharter:rISOwnik, PCkurier 19/1998, http://www.pckurier.pl, visited on 07.09.2007 (in Polish)

[28] ISACA, IT Assurance Framework Exposure Draft, https://www.isaca.org, visited on 12.09.2007

[29] K. Liderman, A. Patkowski: Metodyka prowadzenia audytu z zakresu bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki, nr 19, 2003, http://centrum.bezpieczenstwa.pl, visited on 12.09.2007 (in Polish)

[30] M. Molski, M. Łacheta, Przewodnik audytora systemów informatycznych, Helion, Gliwice, 2007 (in Polish)

[31] Microsoft Homepage, http://www.microsoft.com, visited on 02.10.2007

[32] Office of the Auditor General of Canada Homepage, http://www.oag-bvg.gc.ca, visited on 07.09.2007

[33] British Standards Institution, PD 3001:2002 Preparing for BS 7799-2 Certification, 2002

[34] British Standards Institution, PD 3002:2002 Guide to BS 7799 Risk Assessment, 2002

[35] British Standards Institution, PD 3003:2002 Are You Ready for BS 7799-2 Audit?, 2002

[36] British Standards Institution, PD 3004:2002 Guide to the Implementation and Auditing of BS 7799 Controls, 2002

[37] British Standards Institution, PD 3005:2002 Guide on the Selection of BS 7799 Part 2 Controls, 2002

[38] Polish Department of Finance, Podręcznik audytu wewnętrznego w administracji publicznej, 2003, http://www.mofnet.gov.pl, visited on 12.09.2007 (in Polish)

[39] Information Governance Limited Hompeage, http://www.infogov.co.uk, visited on 21.09.2007

[40] AEXIS Security Consultants Homepage, http://www.aexis.de, visited on 21.09.2007

[41] Centrum Bezpieczeństwa Systemów Teleinformatycznych Instytutu Systemów Sterowania Homepage, http://www.cbst.iss.pl, visited on 04.10.2007

[42] A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowo-Techniczne, Warszawa 2006 (in Polish)

[43] TeamInfoSec Homepage, http://www.teaminfosec.com, visited on 07.09.2007

[44] PriceWaterHouseCoopers Homepage, http://www.pwc.com, visited on 07.09.2007

[45] G. Berdebes, ISO 9000: Achieving & Retaining Certification For Professional Services Organizations and Internal Service Departments, 2003, http://www.tenrox.com, visited on 29.09.2007

[46] International Organization for Standardization, ISO 14971, Medical Devices – Application of Risk Management to Medical Devices, 2007

[47] International Organization for Standardization, ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements, 2005