Standard Compliance Framework for Effective Requirements Communication

Abstract
Standard Compliance Framework (SCF) is a framework, which supports application of standards at the stages of achieving, assessing and maintaining the compliance. It uses Trust Case language to develop argument structures demonstrating compliance with standards. The paper presents how SCF is applied to increase effectiveness of requirements communication. Relevant mechanisms of the framework are thoroughly described referring to the ISO/IEC 27001:2005 standard. Two case studies of the framework application, one in a project aimed at assessing the compliance, another in a project aimed at achieving the compliance are presented.

Keywords: SCF, Standard Compliance Framework, Trust Case, Trust Case Template, ISO/IEC 27001

Introduction

Standards play an important role on the contemporary market. Statistics show that companies spent about 50 million dollars on ISO publications in 2006 [7], which is only a small fraction of the budget spent on achieving, assessing and maintaining the compliance (e.g. a day of an auditor’s work costs usually much more than the standard itself and the
certification process can take several weeks). And ISO is just one of several organisations developing internationally applied standards.

Therefore, any improvement in effectiveness of standards utilisation can bring significant cost reduction. Presently, only few methods exist which support standards application (for instance COBRA ISO17799 Security Consultant [2]). They are mostly dedicated for specific standards and consequently only the most popular standards are supported in their application by appropriate methodologies.

In this paper we present the **Standard Compliance Framework (SCF)**. The framework is generic and supports application of any standard against which we can identify suitable compliance criteria. SCF can be used at the stages of achieving, assessing and maintaining the compliance. What is important, it can be used together with any additional specific compliance supporting methodology, as such methodologies usually support different (i.e. standard specific) aspects of the standard application processes. In this sense, our approach is more complementary than competitive with respect to the already existing approaches.

The paper stresses mechanisms of the framework, which facilitate effective requirements communication using as an example ISO/IEC 27001:2005 [8], a standard from the domain of security. Application of the framework is presented using two case studies from the ECC-Net and PIPS projects.

**Standard Compliance Framework**

Standard Compliance Framework is based on the observation that assessing and/or achieving the compliance involves producing, gathering and presenting in a legible and understandable way the evidence which demonstrates the compliance. Therefore, argument structures and the related methodologies play the key role in compliance justification. We have chosen the *Trust Case* language for the purpose of structuring the argumentation of standards compliance because of its flexibility and legibility. The language is described in detail in the following chapter.

The main aim of SCF is to develop and maintain a document which justifies the claim of compliance. Such a document is called *standard compliance case*. It is developed from a generic structure called *Trust Case (TC) Template*. A TC template is standard specific and is derived from a given standard. The same TC template can be reused in multiple projects of this standard application. While being applied, the TC template is filled in with project
specific evidence. In addition, the template contains much auxiliary information, which explains and facilitates application of the standard.

Standard Compliance Framework is composed of:

(1) Trust Case language – a language for developing argument structures and Trust Case Templates.

(2) The process of creating templates – which precisely describes how to transform information contained in a standard into a template.

(3) The processes of applying templates – which explain how to use templates in different contexts.

(4) TCT Editor – an on-line editor used to develop Trust Case structures and in particular Trust Case Templates.

A TC template is composed of an argument structure which is called Template Argument Structure (TAS) and additional information placed on the top of TAS and on the bottom of TAS. Together they form three main layers which are depicted in figure 1.

![Figure 1. Trust Case Template structure](image-url)
Layer 1 contains information about the template itself, information about the standard, and information about the purpose of the assessment which can be performed using the template.

Layer 2 includes TAS. It is structured into three sub-layers of abstraction. The top layer is strongly influenced by standard’s structure, the middle layer represents the contents of the standard, and is extended (at the bottom layer) by additional data from other sources external to the standard like the associated documents, historical data and experts’ knowledge. One template can contain more than one TAS. In such a situation, they can demonstrate conformance with a few related standards, or one of them can e.g. claim conformance with a standard and another one can claim that the assessment was performed according to the requirements imposed by the standard (if relevant).

Layer 3 of the template includes information explaining the requirements (represented in TAS) and the mechanisms supporting the template application at the stages of achieving, assessing and maintaining the compliance. This is the place where the majority of mechanisms related to effective requirements communication can be found. They are discussed in detail in the chapter describing the ISO/IEC 27001 template.

Figure 2. Trust Case Template lifecycle

Figure 2 presents the template lifecycle in which we can distinguish four main phases. In the first phase the template from a given standard is derived. This activity is of particular
importance as the quality of the template conditions the quality of the results of the following stages. It is of particular importance that auditors and other experts are involved at this stage. The resulting TC template is a formal document specifying the requirements of the standard as well as the (agreed) way of demonstrating the compliance.

In the next phase the template resulting from the previous phase is used to support achieving compliance. It supports the activity by explaining the meaning of the requirements, identifying interdependencies among them and providing references to the documents which can help in fulfilling specific requirements or which in general describe how to perform the task. The evidence demonstrating that the requirements are met can be integrated in the template through proper links. The result of this process is the standard compliance case in which all claims about fulfilment of the standard requirements are supported by evidence.

The standard compliance case is used as an input for ‘Certify’ phase. The case has the form of a structured argument with the references to the evidential material. It can significantly help the auditor responsible for the certification reducing the amount of his work.

The last phase refers to the problem of maintaining the compliance. The template identifies interdependencies among the requirements, which help in tracing changes and assessing their impact. All the features relevant to achieving the compliance facilitate regaining the compliance with particular requirements, if temporarily lost.

The above description of the framework provides only superficial information necessary to understand the following part of the paper. More thorough explanation can be found in [3].

**Trust Case language**

SCF uses Trust Case language [4, 5, 6] to represent argument structures. The basic logical component in the language is an argument composed of the *claim* to be justified, the *evidence* supporting the claim and the *inference rule* which shows how on the basis of the evidence the claimed property is being achieved. The elements of the language are shown in figure 3.

An *argument* can support the claim or it can demonstrate that the claim is not true (counter-argument). Evidence can have the form of an assumption, claim or fact. The inference rule called *warrant* of an argument can also be represented as an assumption, claim
or fact. Due to the fact that other claims can be used as evidence, the argument structure can be developed recursively.

Assumptions are used to represent preconditions necessary to make the argument valid, but which are not under control of the party which develops the argument. For example, a manufacturer demonstrating safety of a device represents as assumptions the requirements for the device operational environment (for instance, stating that a device is used by trained personnel only). However, if a user of the device argues about safety, he/she may refer to the fact of being well trained. Facts contain information being obviously true or information which is validated in documents external to the argument structure. Such documents can be attached using references, which support a fact or an assumption. References contain only information about a document and its location e.g. URL. Additionally, everywhere in the argument an information node can be added. It contains supplementary information making the argument more legible which, however, does not influence the correctness of the argument.

To eliminate redundancy we admit links in the argument structure.

![Figure 3. Trust Case language](image)

A claim which is not supported by an argument is called open. Similarly, a fact which should refer to an external document but does not, is called open. Open claims and facts are of
particular importance where TC templates are concerned. They represent the ‘holes’ in the argument structure which, for some reasons, are left unfilled at the present stage.

**Template for ISO/IEC 27001**

ISO/IEC 27001:2005 [8] is an international standard defining requirements related to establishment, implementation and effective maintenance of Information Security Management System (ISMS) which is part of the system responsible for information security management. The compliance with the standard confirms the maturity of the organisation concerning security management, in particular that all the activities related to security are based on thorough analysis and the decisions are made taking into account long term goals.

We have developed a TC template for ISO/IEC 27001:2005. The template has been derived mainly from the text of the standard with some references to the external sources of information. The main template structure is presented in figure 4.

```
|   i| I0: Trust case for ISO/IEC 27001:2005 |
|   | i1: Legend                         |
|   | i2: General information            |
|   | i3: References to documents of standards and supporting documentation |
|   | i4: References to documents of the project |
|   | i5: Proof(s) of compliance         |
|   | 🌈 ISO 27001: Compliance with ISO/IEC 27001:2005 |
|   | i6: List of all open claims and facts |
```

Figure 4. Main template structure

Branch ‘I1’ contains information about mechanisms supported by the template. Branch ‘I2’ contains description of the contents of the standard. In branch ‘I3’ all the references to the standard have been located. Storing them in one place makes document management much easier. Bearing this in mind, branch ‘I4’ was also created. It lists all the documents identified by the standard, which are necessary to achieve and demonstrate the compliance. Finally, branch ‘I5’ contains TAS with the claim of the compliance with ISO/IEC 27001:2005. In addition, branch ‘I6’ stores the list of open claims and facts in TAS. TAS is decomposed recursively having in its leaves open claims or facts, each of them representing a particular requirement of the standard.

Representing the TC template as an argument structure explicitly communicates the goals to be achieved for demonstrating compliance: every open claim and fact is a goal which can be achieved by supplying the missing evidence. It can also be easily identified how the main goal (the topmost claim in the structure) is affected by its sub-goals. In this way, the
importance of every piece of evidence is evident and it is easier to understand the meaning of each requirement because it is shown in a broader context. Understanding the way in which the evidence is being used to argue the compliance influences positively the evidence quality.

In the TC template, each requirement of the standard is precisely described using information nodes. An example is given in figure 5 where an open claim representing the requirement related to controls selection from item 4.2.1.g of the standard is presented. The description contains information from the standard, from additional documents and from unpublished sources.

Figure 5. Open claim

The nodes ‘Dependencies’ and ‘Influence’ trace to the interdependent requirements of the standard. Some of those interdependencies are directly stated in the standard but the others had to be discovered by interpreting the document.

The ‘Evidence’ node lists the documents and other requirements of the standard used to demonstrate the fulfilment of the given one. Similar lists are placed in branch ‘I4’ (figure 4). Altogether, these lists make much clearer the requirements for the quality of evidence to be created.

The ‘Examples’ node contains examples of arguments which can be used to justify the corresponding claim. Such examples improve communication of the requirement associated with the claim by showing how to deal with it. In addition to the examples of arguments the node can also include examples of documents containing evidence, negative examples of
mistakes in argumentation strategies or in interpretation of the requirements and other material supporting the template user.

The node ‘Supporting documentation’ references to other useful documents which can be helpful in achieving compliance.

To summarize, the template contains several mechanisms which facilitate communication of the requirements. This involves structuring the requirements in a hierarchical way, providing examples of arguments and evidential documents, and providing structured explanatory information.

Case studies

Trust Case Templates have been used in two case studies realised in EC Joint Research Centre in Ispra in Italy. Both of the case studies used the previous version of the template described in this paper. The template supported utilisation of BS 7799-2:2002 standard [1], which formed the basis of ISO/IEC 27001:2005.

In the first case study a part of an organisation together with a system for ECC-Net (The European Consumer Centre Network) was assessed. The system was supporting an organisation giving the consumers advice, providing them with information on their rights and supporting them in contentious cases. The system dealt with lots of information encompassing private consumers’ data, information about organizations and description of contentious issues. The purpose of the case study was to perform an internal assessment in order to measure the level of the compliance with BS 7799-2. Application of the template proved the usefulness of the framework in providing means for document management and presentation of the achieved results. During the assessment such mechanisms like broad descriptions referring to many documents (e.g. [9-13]) and easy navigation among them turned out to be especially useful. Being enforced to create arguments demonstrating the compliance facilitated understanding of the requirements of the standard and assessing whether they were fulfilled. Information about interdependencies among the requirements increased performance by providing means of better planning the work and improving the level of understanding of the requirements. Finally, the tree structure of the argument and the support provided by the tool to develop Trust Cases made it possible to manage the complexity of the task.

In the second case study a security policy for PIPS system has been developed. The objective of EU 6th FR project PIPS (Personalized Information Platform for Life and Health Services) is to develop a platform of healthcare and lifestyle services for EU citizens. The
platform promotes preventive actions taken to protect health and improve lifestyle. While creating the security policy, the objective was to make it compliant with relevant requirements of BS 7799-2. The main source of those requirements was the TC template for BS 7799-2. The template was extended with examples from the previous case study. The experiment showed that the examples can be useful in explaining the requirements and improving productiveness. It also revealed the value of negative examples.

**Conclusions**

Standard Compliance Framework described in this paper is still under development. Presently the framework implements the full range of mechanisms described above and is supported by a stable Internet based tool. The experiments already performed demonstrated that the framework effectively supports processes of compliance achievement.

Our future plans include running more case studies and measuring the effectiveness of the support provided by the framework by means of metrics. In particular, SCF is to be applied in EU STREP ANGEL (Advanced Networked embedded platform as a Gateway to Enhance quality of Life) as well as in other projects.

**Acknowledgement:**

The work was partially supported by the EU 6th FR IP PIPS. The contribution by Pawel Bodnar to the PIPS related case study is to be acknowledged.

**References:**