Polish Software Compliance Evaluation System

Status: Translation project	**Filename**: System Oceny Zgodności Oprogramowania - v_1_0
	Last change: 2008-11-27 14:40:00
Author: Software Attestation and Standardization Organization members	

Previous version:

Status: -	**Filename**: -
Phase: -	**Last change**: -
Author: -	

Changes:

--

Contents

1. Introduction and references

1.1. Introduction

This document arose in the result of the work of Polish Software Attestation and Standarization Organization. It is describing principles of granting trademarks for software products, called Certificates of Compliance (Quality Certificates).

The software quality as a product is the subject of the research since the time of notion the software engineering. First models of quality (McCall[i] and Boehm[ii]) were published in the 1970's. None of them, and none of models drawn up in subsequent years didn't become the standard in understanding the IT market. Model of the quality, understood as a way (language) of description, also constitutes the language which is used herein for expressing put quality requirements for providing the software compliance evaluation in the polish system. The quality model applied in the document is a model unwound by ISO/IEC JTC1/SC7 which name is SQuaRE[iii] (Product Quality Requirements Software and Evaluation). More information about the quality model is in chapter 1.

Owners of Software Compliance Evaluation System are SASO members represented by bodies listed in SASO Articles of association. Within the scope of Software Compliance Evaluation System will be an appointed Council of certification bodies which expressing its voice stay in the area of the evaluation of the software and principles of applying this System.

Members and the SASO management Board hope that publishing this standard will make the market rich for the possibility of expressing the quality of providing software in the clear form for Customers and Users, as well as will encourage very Producers for investing in the quality its products, as into the essential element of the competitive edge on the market.

1.2. Standard establishment goal

The lack of standards of the quality assessment of the software is depriving Recipients of objective tools enabling the quality assessment of the software. The lack of standards means the lack of independent entities making the research on the software and giving objective informations for IT recipients. As a result, manufacturers are investing resources in software process improvement and certification methods of organizing the company did not treat product quality as a potential source of competitive advantage. The effect of this state are not the products which meet the needs of their customers, or performing tasks in a way that gives users the benefits in relation to the situation of manual work.

Software vendors acting on a highly competitive market, trying to match its costs to the requirements of competitive bids and the factors which guided clients in choosing software. Because users rarely have the

opportunity to assess the quality of the software before purchase, and having no criteria to compare the quality between the products themselves often do not attach much importance to qualitative factors. Creators assume that the Software vendors with available of this standard they will start investing in quality as an important element of competitive advantage in the IT industry, which will be positive impact on the final quality of the products available on the market and consequently to increase the profitability of investing in IT solutions.

1.3. Reference to quality model

Quality description language adopted in this document is the SQUARE model developed by a committee of ISO / IEC JTC1/SC7 and published in a series of standards ISO / IEC 25000.

This model builds on the experience gained by researchers over the last 40 years in formulating the concept, characteristics and sub-characteristics of both the user's perspective (Software Quality in Use), as well as allowing you to decompose these requirements, definitions of technical quality-dynamic (External Software Quality) and technical quality-static (Internal Software Quality). Because this System is intended to be a language of communication customers and software producers, the user perspective was chosen as the basis for terminology.

This system defines 3 areas of compliance testing:
- Compliance in the field of ergonomics as described in chapter 3
- Compliance in the security described in chapter 4
- Compliance of the formal requirements described in chapter 5

Reference to areas of compliance assessment for quality model is shown in Figure 1

Reference to areas of compliance assessment for quality model[iv]
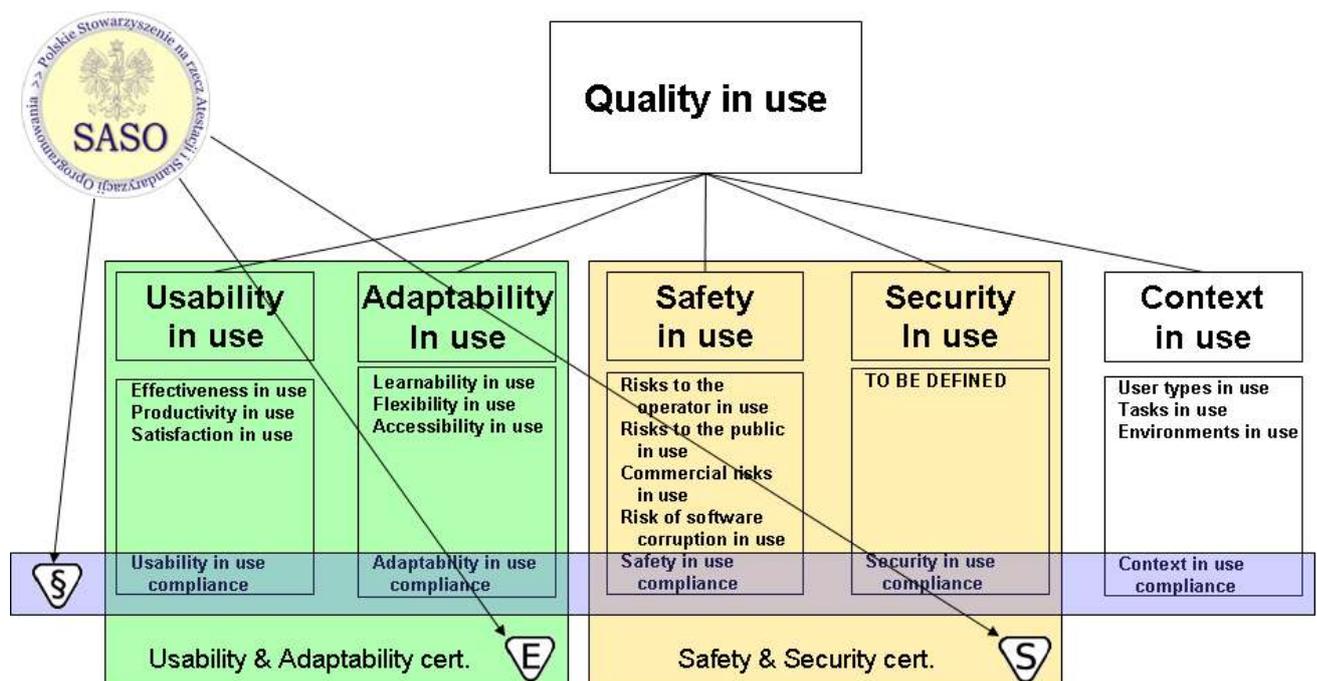
Specific requirements in areas is presented in subsequent chapters.

1.4. Terms

SASO	Software Attestation and Standarization Organization.
Certification Unit	Entity authorized under the agreement with SASO, to award the certificate of compliance after completion of the evaluation procedures described in this document.
Council Units Certification	Body set up to manage the certification process, consisting of representatives of certification units. Pending the appointment of a Council consisting of a minimum of five certification bodies carry out the duties of the Council Board SASO.
Certificate of Compliance	Document issued by the Unit certification in accordance with its powers, and this Compliance Assessment System Software defining the right to use the sign of quality.
Quality Mark	Is a registered trade mark, which is managed by SASO in accordance with Compliance Assessment System Software and the Statute.
Trade Mark	Mark registered in the Republic of Polish Patent Office under the Law on Protection of Industrial Property (DzU 2003 nr 119 poz 1117).
Giving certificate	Grant by SASO, through the Certification Body nonexclusive license to use a particular mark in accordance with this Software Compliance Evaluation System.
Evaluation	Software compliance research process conducted by the Certification Unit in accordance with the contents of this document.
Applicant	Unit submitting the product for evaluation, contracting with the certification unit, determining the scope of the evaluation and applicability.

Security policy[v]

Set of precise and consistent law exacting regulations, rules and procedures by which an organization builds, manages and provides resources and information systems and information. It determines which resources and how to be protected.

Safety profile

Describes the security requirements defined for the selected area of the system or software. The requirements are defined separately for the Software and the environment in which it operates or will eventually work. The safety profile of abstracts from the implementation of individual requirements.

2. Owners of Software Compliance Evaluation System

2.1. System owners

The owner of this Software Compliance Evaluation System are members gathered together in the SASO represented by the bodies mentioned in the Statute of SASO. Owners give the public, non-exclusive license to use this document to all concerned. In the case of duplication of all or part of the contents of this document is required of reference:

Polish Software Attestation and Standarization Organization, Polish Software Compliance Evaluation System, http://www.saso.org.pl*, SASO, Poznań 2008*

Software Compliance Evaluation System consists of two areas: the requirements for a software product and the requirements for the evaluation process. The system is created and modified at the request of members of SASO, while the requirements for the evaluation process for requesting a change may be the Council of certification units, which also participates in the work on this part of System.

This document is the latest version. Rules of software quality marks are published at:

2.2. Evaluation and the supervision process

Evaluation process conducted in accordance with § 5 of the Rules of quality labels and consists of the following stages:

1) The entity interested in certification (Applicant) asks the Certification Unit with the information about software that wants to give the certificate. Information have to contain which trade mark software applied for and what level of certification. Attach to application the declaration of compliance indicating business contexts of use applications.

2) Certification unit shall inform the SASO about application, and for the notifier specifies what documents and materials should be provided to comply with the certification and determine the financial conditions of certification.

3) Applicant shall provide the required materials and application for certification.

4) Certification unit perform the certification planned under the type of application, declaration of compliance , and the required level of certification.

5) Certification unit decides to issue a certificate or refuse to issue the certificate.

6) Certification unit shall inform the SASO to issue or refuse to issue a certificate. SASO making publicly available information about issued certificates, and inform certification units about refuse to issue a certificate.

After the release of Certificate, Certification unit shall exercise supervision over the product when assessing whether the changes are not the place version of the application and affix the mark a different version than the one for which the certificate was issued, investigation is there no changes in interpretation of the declaration of compliance changing application areas of applications. Monitoring is performed under a contract between the notifier and Certification unit.

An important element of evaluation software running on the real environment is access to data stored in the system. In this case, the Certification unit shall have powers to carry out the detailed evaluation, and the scope of its contract with SASO must allow evaluation on running systems.

Certification unit making the certification of products with access to business Applicant secrets, is required to secure adequate Applicant data and the conclusion of SASO in the contract obligations to implement the system of data protection and the relevant clauses with Applicant .

2.3. Contexts of the use

Business contexts implies the use of application specific additional requirements for specific areas of application. Each area defines the requirements to be add to the basic requirements (as defined herein) for each trade mark, distinguishing between levels of certification. Current requirements for individual business areas are publish at the SASO web sight.

In the event when Applicant occur for certification for the new context of use is a agree between SASO and Certification Unit, which will prepare a proposal for the content of requirements for use of this context. Carried out detailed requirements for approval are sent to members of SASO, certification units and other entities co-operating with SASO. If there are not critical objections to the application within 3 weeks from the date of provide specific requirements or in case of a previously approval for the proposed requirements, following requirements are approve and publish at the SASO web sight. Since then, the requirements become effective for the new context of use and become part of the conditions for certification by the applicant who applied for certification for this area.

In circumstances where the Certification unit, Technical Committee on Compliance Assessment System Software, SASO, or other entity through SASO member raised the need to change the requirements detailed in this document or the specific requirements for a given context using the following procedure, similar to the development of new requirements. SASO determined entity who will prepare a new proposal content requirements, which is then send to accept, similar as in the case of new requirements.

Preparing detailed requirements for the various levels of certification for each of the trade marks, should be guided by the level of risk associated with certification of the specificities of the business context of use:

Basic level   there are slight risks seen in the time-use applications

Level ★★   there are slight risks for faulty use of applications, on running application

Level ★★★   there are no risk at the level on running applications

Level ★★★★   there are slight risks visible at the project level, source code, but not at the level on running applications

Level ★★★★★   there is not any risk in the project, source code and running applications

For a new business context use, are made analysis the characteristics of applications, that may raise risk of use.

2.4. <u>The law compliance</u>

Between SASO and Certification unit is concluded contract for licensing rights to the marking trade marks. The Agreement sets out the conditions under which Certification unit may carry out evaluations and issue certificates.

Before concluding contract Certification unit confirms requirements of the specific evaluation of each area and conduct of the evaluation process are accordance with ISO / IEC 25040 (ISO / IEC 14598-5). SASO supervise the evaluation process by the right to audit the evaluation of documents not covered by the mysteries of enterprises, in particular:

 a) the content of submissions from applicants
 b) reports review of declaration of compliance, usable documentation
 c) reports review of evaluation plans
 d) reports review of evaluation
 e) reports review of implementation of supervisory activities

Applicant enters into an contract to carry out research and monitoring certification with the certification unit, which informs the SASO of issued, suspended and revoked certificates in order to publish this information on SASO web pages.

3. Requirements concerning the E area

3.1. Certificate description

E Certificate of Compliance is issued for the area of Ergonomics and Efficiency, and includes characteristics of the SQUARE model: Usability in use, Adaptability in use. Certificate is used for certain areas in the Declaration of Compliance. Certificate is used for certain areas in the Declaration of Compliance. It is required that in user manual or producer website could be seen detailed information on the areas of application of the product for which it was issued a certificate of compliance, and information about what was the hardware on which the measurements made in efficiency.

3.2. Certificate symbol

Giving a certificate is associated with granting the right to a specific version number of the trade mark E, which is presented in Figure 2

Trade mark indicates compliance in the area of ergonomics

Trade mark has to be given a level of certification (see Chapter 3.3), the exact version number and information about the place where you can see the declaration of compliance listing the business contexts of use, and environmental parameters on which investigated the effectiveness of the software.

3.3. Certification Levels

The area includes the certification characteristics of Usability in use, Adaptability in use. For each of characteristics are defined specific performance metrics and their expected value. Giving an appropriate level of certification is related with statement by Certification unit that all requirements meet for a given level (in which case the result of at least one measurement does not meet the minimum requirements specified level of certification may not be granted).

3.4. Detailed requirements

This chapter describes the basic requirements for all applications area. In case specify the declaration contexts of use, should be complemented by a set of measured parameters with the parameters resulting from the use of context. Absence of measurement for the specified context of use together with Certification unit, Applicant and the Council Units Certification shall review the risks associated with the use in this context by publishing the requirements on SASO webpages in accordance with the procedure described in chapter 2.3.

3.4.1. Basic level

Requirement	Required feature (measurement)	Reference to the model
The software does not force the user to wait	For all screens / reports called for the implementation of some steps occur rapidly (the speed is dependent on the frequency of use). The total downtime due to waiting for a reaction to software in a typical manner of use does not exceed 30 minutes to 8 hours.	Usability in use / Effectiveness
User working with the software quickly perform tasks	The software is designed in such a way that the execution of each activity (mean of all the steps in the software that must be performed to achieve the task) by a trained user takes less time than the execution of the same task in an alternative way (without software).	Usability in use / Productivity
The software is user friendly and supports user	The software includes features for the user wich helps do the task, in particular those that allow the use of information once entered, verify the occurrence of simple errors in data entered by the user and suggest what should be done.	Usability in use / Satisfaction
The software is easy to learn and re-learn after a period of non-use (it is intuitive)	Training users to use the software does not take more time than training the user in a situation if tasks are carried without the software. The software has a built-in and easy to find explanations to the user describing how to implement each task.	Adaptability in use / Learnability
The software is compatible with the formal requirements for speed and ease of adapting, if there any	In the case of software used by certain groups of users (reduced mobility and perception) or in certain places (place high intensity light and sound) software meets the formal requirements for such uses.	Usability in use, Adaptability in use / Compliance

Specific requirements for E certification

3.5. Detailed requirements concerning the evaluation

The process of evaluation is closely related to the requirements under the declared contexts of use and with the technical parameters of the system under which the software will run. Evaluation is carried out by the Certification Unit in the system configured accordance with technical parameters, and possibly with other parameters of the system (not covered by the guidelines) set in a random way.

4. Requirements concerning the S area

4.1. Certificate description

S certificate of compliance is issued for the area of security understood as a safety of use (including safety of life, health, assets and the environment) as well as the use of confidentiality (information security). It covers the characteristics of the Square model "Safety in use" and "Security in use". Certificate is issued for certain areas in the Declaration of Compliance application. It is assumed that due to the specific evaluation in range of S Mark is required very close cooperation between the Applicant and Certification Unit. This cooperation focuses on issues relating to the confidentiality of evaluation results and the transfer by the Applicant to the Certification unit the necessary documentation.

Software security as a product is a very strongly associated with the concept of security infrastructure and systems in which software operates. Therefore, in addition to the declaration of compliance wich specify the business contexts of use of evaluation are guidelines safety of the system under which the software is run.

4.2. Certificate symbol

Giving a certificate associated with granting the right to apply for a specific version number of the trade mark S, which is presented in Figure 3

Trade mark indicates compliance in the area of security

Trade mark has to be given a level of certification (see Chapter 4.3), the exact version number and information about the place where you can see the declaration of compliance listing the business contexts of use and guidelines for the safety of the system under which the software will run.

4.3. Certification Levels

The area of certification for compliance with safety requirements include the current versions of the Software Compliance Evaluation System by one level. For this level describes the specific requirements that a product must meet. Giving an appropriate level of certification is related with statement by Certification unit that all requirements meet for a given level (in which case the result of at least one measurement does not meet the minimum requirements specified level of certification may not be granted). The term means a list of the requirements of the security profile assigned to the appropriate area. This list brings together the safety profiles that are a universal description of best practices related to security in the defined area.

The list of areas for quality Mark S:

1. Safety in use
   a) Threats to health and life
   b) Threats to assets
   c) Threats to life environment
2. Security in use
   a) Confidentiality
   b) Integrity
   c) Availability
   d) Identyfication and authentication
   e) Accountability
   f) Autenticity
   g) Undeniability
   h) Reliability

4.4. Detailed requirements

This chapter describes the basic requirements for all applications area. In case specify the declaration contexts of use, should be complemented by a set of measured parameters with the parameters resulting from the use of context. Absence of measurement for the specified context of use together with Certification unit, Applicant and the Council Units Certification shall review the risks associated with the use in this context by publishing the requirements on SASO webpages in accordance with the procedure described in chapter 2.3.

4.4.1. Basic level

Requirement	Required feature (measurement)	Reference to the model
The software ensures the confidentiality of information	The software prevents access (intentional and accidental) to the information by user/software gathered in system to obtain unauthorized access.	Security in use / Confidentiality
The software provides consistency of information	The software prevents the modification of data stored in the software (in a targeted and random) by the user/software to perform unauthorized modification. The software prevents the destruction of the information gathered in system.	Security in use / Integrity
The software ensures the availability of information	The software provides the ability to access user/software authorized to receive information in access time resulting from the declaration of compliance.	Security in use / Availability

Requirement	Required feature (measurement)	Reference to the model
The software does not threaten life and health	In the case of impact on human health and safety, software has safeguards against errors that might result in a threat to life and health.	Safety in use / Risks to the operator, risks to the public
The software does not endanger property	In the case of impact on the security of property software has safeguards against errors that might result in a threat to property. Property means also intangible assets such as reputation of the company's, intangible property etc.	Safety in use / Commercial risks
The software does not threaten the environment	In the case of impact on environmental safety software has safeguards against errors that might result in a threat environment.	Safety in use / Risks to the environment
The software is compatible with the formal requirements for safety	In the case of the impact on the security sphere of operator, other persons, property or the environment, or for storage of protected information (including company's secrets) software provides a level of security consistent with the formal requirements for these areas.	Security in use, Safety in use / Compliance

Specific requirements for S certification

4.5. Detailed requirements concerning the evaluation

The process of evaluation is closely related to the requirements under the declared contexts of use and with the guidelines relating to the security system through which it will run the software. Evaluation is carried out by the Certification Unit in the system configured accordance with these parameters, and possibly with other parameters of the system (not covered by the guidelines) set in a random way.

5.   Requirements concerning the § area

5.1.   Certificate description

§ certificate of compliance is issued for the area of formal conformity, and includes all formal requirements for the software resulting from the context of use . Certificate is used for certain areas in the Declaration of Compliance application. It is required that in user manual or producer website could be seen detailed information on the areas of application of the product for which it was issued a certificate of compliance and guidelines how use software and formal setting (information on what additional documents should exist on the user side, to use the software was fully compatible with the formal requirements, such as policy processing of personal data).

5.2.   Certificate symbol

Giving a certificate associated with granting the right to apply for a specific version number of the trade mark §, which is presented in Figure 4

Trade mark indicates compliance in the area of formal requirements

Trade mark has to be given a level of certification (see Chapter 4.3), the exact version number and information about the place where you can see the declaration of compliance listing the business contexts of use and date for which there is formal compliance with the requirements of (the date of legal status) as well as the formal requirements associated with how to use software.

5.3.   Certification Levels

The certification area includes all characteristics of quality (including certification by the characters E and S), but in terms of formal compliance. Method of certification begins with the identification of the formal requirements and resulting of them characteristics and sub-characteristics and the specific measures and their expected values. Giving an appropriate level of certification is related with statement by Certification unit that all requirements meet for a given level (in which case the result of at least one measurement does not meet the minimum requirements specified level of certification may not be granted).

5.4.   Detailed requirements

This chapter describes the basic requirements for all applications area. If you specify in declaration the contexts of use, should be complemented by a set of measured parameters with the parameters resulting

from the context of use. Absence of measurement for the specified context of use together with Certification unit, Applicant and the Council Units Certification shall review the risks associated with the use in this context by publishing the requirements on SASO webpages in accordance with the procedure described in chapter 2.3.

5.4.1. Basic level

Requirement	Required feature (measurement)	Reference to the model
The software is compatible with the formal requirements for speed and ease of adapting the work, if there any	In the case of software used by certain groups of users (reduced mobility and perception) or in certain places (place high intensity light and sound) software meets the formal requirements for such uses.	Usability in use, Adaptability in use / Compliance
The software is compatible with the formal requirements for safety	In the case of the impact on the security sphere of operator, other persons, property or the environment, or for storage of protected information (including company's secrets) software provides a level of security consistent with the formal requirements for these areas.	Security in use, Safety in use / Compliance
The software is compatible with the rules governing the processing of data stored in the software	Software process and store data in a manner consistent with the provisions, in particular the Law on Personal Data Protection Act, accounting law, banking law, law on business computerization of public service, etc.	Context in use / Compliance
The software is compatible with the requirements of the business context of use	The software meets the formal requirements for the use of areas under the Declaration of Compliance.	Context in use / Compliance
The software is free from legal defects	The software is composed exclusively of components whose use is lawful.	

Specific requirements for § certification

5.5. Detailed requirements concerning the evaluation

Using the software in accordance with the formal requirements requires that the software and how its use is consistent with the requirements. For this reason, the evaluation shall be subject to the requirements arising from the Declaration prepared by the applicant, together with guidelines how use of applications assuming that all things are not specified in the guidelines how use of applications with are not on the user side.

6.   Declaration example of the E certificate requirements compliance

DECLARATION OF COMPLIANCE WITH ERGONOMICS REQUIREMENTS

<Identify the entity making the declaration>

Declares that the software *<software name>*, version *<version number>* is in accordance with the requirements of ergonomics set out in the Polish Software Compliance Evaluation System.

Effectiveness research was conducted on the basis of infrastructure *<description of all elements affecting the efficiency and software usability>* on *<date of research>* by the Certification Unit *<name of Certification Unit>* acting under contract with the Polish Software Attestation and Standarization Organization.

The software meets the basic requirements for compliance *<and the requirements for following areas of use:….>*.

Producer recommendations for how to install, configure and use, to aimed achieving the declared level of efficiency are described *<a link or reference to the user manual where are describes the parameters witch have to be set and rules for the supervision and care, to maintain the level of efficiency>*.

7. Declaration example of the S certificate requirements compliance

DECLARATION OF COMPLIANCE WITH SAFETY REQUIREMENTS

<Identify the entity making the declaration>

Declares that the software *<software name>*, version *<version number>* is in accordance with the requirements of safety set out in the Polish Software Compliance Evaluation System.

Safety research was conducted on the basis of infrastructure with following security *<description of all security elements affecting the security software>* on *<date of research>* by the Certification Unit *<name of Certification Unit>* acting under contract with the Polish Software Attestation and Standarization Organization.

The software meets the basic requirements for compliance *<and the requirements for following areas of use:….>*.

Producer recommendations for how to install, configure and use, to aimed achieving the declared level of safety are described *<a link or reference to the user manual where are describes the parameters witch have to be set and rules for the supervision and care, to maintain the level of safety>*.

8. Declaration example of the § certificate requirements compliance

DECLARATION OF COMPLIANCE WITH THE FORMAL REQUIREMENTS

<Identify the entity making the declaration>

Declares that the software *<software name>*, version *<version number>* is in accordance with the formal requirements set out in the Polish Software Compliance Evaluation System.

Compliance research was conducted based on the following normative acts (state on <date>) *<description of acts: laws, rules, regulations, guidelines which have been identified and taken into consideration during the research>* on *<date of research>* by the Certification Unit *<name of Certification Unit>* acting under contract with the Polish Software Attestation and Standarization Organization.

The software meets the basic requirements for compliance *<and the requirements for following areas of use:….>*.

Producer recommendations for how to install, configure and use, to aimed achieving the declared level of formal compliance are described *<a link or reference to the user manual where are describes the parameters witch have to be set and the regulation of company wich use software, to use it accordance with the requirements>*.

9.   References

[i] McCall J., Richards P., Walters G., Factors In software quality, Griffiths Air Force Base, NY, Rome Air Development Center Air Force Systems Command, 1977

[ii] Boehm B., Brown J., Lipow M., MacCleod G, Characteristics of software quality, NY, American Elsevier, 1978

[iii] Suryn W., Abran A., ISO/IEC SQuaRE. The second generation of standards for software product quality, IASTED2003

[iv] At the time of publication in the voting phase is 55 version of document containing the different division of main characteristics

[v] Source: http://pl.wikipedia.org

http://www.measuringusability.com/papers/p482-sauro.pdf