Checklist support for ISO 9001 audits of software quality management systems

AJ Walker

Software Engineering Applications Laboratory
Electrical Engineering, University of the Witwatersrand, Johannesburg, South Africa

Abstract: This paper presents an overview of a national project to develop a checklist to support audits and assessments of quality management systems in the field of software in terms of the compliance requirements of the ISO 9001 international standard for quality management. This national project is reviewed in terms of: project requirements , quality objectives and quality management practices; participation by industry locally and internationally; the use of the Internet for communication and document distribution; the product development and review process; the trialling (or validation) of the product; the incorporation of guidance from the Software Engineering standards emerging from ISO\IEC\JTC1\SC7. These standards offer guidance on international good practices over a broad range of topics, and the medium and long-term benefits and impact of the development of this product.

1 Introduction

ISO 9001 [1] has emerged as the undisputed international benchmark for quality management. Since its introduction in 1987 enterprises in more than 70 countries have established quality management systems based on the ISO 9000 family of International Standards. Tens of thousands of these organisations (more than 100 000 by end 1995) have invested in independent verification by 'registration' - or 'certification' - bodies that their quality systems conform to ISO 9000 standards. The ISO 9000 certificates then issued by the registrars to these enterprises can be used by the latter to create confidence among their clients in their ability to deliver goods and services that meet the clients requirements. The number of ISO 9000 certificates issued world-wide is expected to exceed 250 000 by the year 2000.

The ISO 9001 standard is a generic model for quality assurance in design\development, production, installation and servicing. The requirements of the standard have to be interpreted by each organisation wishing to be registered formally as evidence of meeting its requirements.

While the primary market demand for ISO 9001 has come from the manufacturing sector, the standard is now being applied to all aspects of economic activity, including software development, health care, security services, project management, and many others.

The development of software was regarded as sufficiently important for ISO to release a guidance document in 1991 providing an interpretation of the application of ISO 9001 to the development of software products and services (ISO 9000-3)[2]. This initiative was followed up in the UK by the Department of Trade and Industry who developed a sector-specific registration scheme for the software industry, known as the TickIT Scheme. Today this scheme has registered more than 900 companies in the UK alone, with strong interest in the scheme being shown in many European countries and Australia.

With the exception of the TickIT scheme [3], there is little commonality in the approach to auditing software companies against the requirements of ISO 9001. This lack of uniformity creates a serious problem for companies which seek registration to ISO 9001 in the field of software development, since there is a large gap between the ISO 9001 clauses and their interpretation for the field of software. So much so that this creates considerable problems for those who create and maintain software quality management systems against the ISO 9001 standard, and those who interpret those requirements for compliance purposes (quality systems auditors).

One of the commonly used tools in quality management is a checklist, which may contain a set of criteria against which the efficacy of a process is judged.

Remarkably there is no internationally (or nationally) agreed checklist against which compliance of software systems to the requirements of ISO 9001 can be assessed.

In view of this a project was initiated in November 1994 by the Software Engineering Applications Laboratory (SEAL) to develop a national standard (or more accurately *Recommended Practice*) under the auspices of the South African Bureau of Standards Technical Committee for Information Technology (TC71.1) for this purpose.

This paper presents an overview of this national project in terms of:

- project requirements , quality objectives and quality management practices

- participation by industry locally and internationally,

- the use of the Internet for communication and document distribution

- the product development and review process

- the trialling (or validation) of the product

- the incorporation of guidance from the Software Engineering standards emerging from ISO\IEC\JTC1\SC7. These standards offer guidance on international good practices over a broad range of topics.

- the medium and long-term benefits and impact of the development of this product.

2 A Checklist for auditing software quality management systems

At the May 1995 meeting of SABS National Committee for Information Technology (TC71.1) a project was launched to develop a Checklist for auditing software systems in terms of the requirements of the international standard for quality management ISO 9001. The goal of the standard is to provide a common framework for assessments and follow-up audits for companies engaged in the development of software for supply to an external customer, or where software is developed on a large scale for internal applications.

It was believed that such a tool would go a long way to reducing the all too frequent adversarial relationship between the quality assurance manager on the one part, the software developers on the second part, and the external quality system auditors on the third part. Although there is a considerable need in this area, an investigation revealed that there were no suitable checklists available for this purpose, either locally or internationally.

Current international practice is, however, moving towards the use of checklists for conducting assessments\audits of ISO 9000 quality management systems, largely to bring harmony to audit and assessment practices.

In view of this the main purpose of this project is to develop a checklist to support ISO 9001 compliant audits and assessments of organisations or organisational units engaged in software development where the customer for the developed software product or service may be internal or external to that organisational unit.

It is believed that this Checklist will be useful to

- internal quality system auditors and quality managers, and

- to individuals or bodies who conduct 2nd or 3rd party surveillance assessments/audits of quality management systems in the software industry.

3 Project requirements

3.1 Product requirements

The first task of the project team was to develop, review and approve the Requirements Specification for the Checklist. These requirements were categorised into those which can be considered as *functional* and *non-functional* .

Functional requirements are tangible and can be measured, while non-functional requirements can be viewed as desirable goals or objectives for the project - nice to have but impossible to measure.

The following *functional* requirements were identified:

a. The requirements of ISO 9001 (as indicated by the 'shall' in each clause) will be probed by a searching question (or series of questions) to identify the extent of compliance of the system under review.

b. The Checklist will address the domain of software.

c. The development of the Checklist questions will be strongly guided by current and emerging international good practices, and will seek to use compliance indicators being used for this purpose elsewhere.

d. The Checklist shall be available in both hardcopy and electronic format.

e. The layout of the Checklist will be guided by applicable SABS Recommended Practices i.e. ARP 013: Drafting and Presentation of Standards [4].

f. The header of the Checklist table will support the conduct of the audit\assessment, and make provision for recording:

   i. Client

   ii. Date

   iii. Reference number for the assessment/audit

   iv. Person(s) interviewed (Shown as a table, with the headings of name, initials, function).

   v. Auditor(s)\Assessor(s)

   vi. The columns of the Checklist table will support the conduct of the audit\assessment by making provision for: Auditor initials, Assessee\ Auditee initials, Checklist\ Compliance question, Company document identification, Result: [Categories A and B: Compliance; N - Non-compliance] [Categories C - F: P - Present; A - Absent] X - Not applicable, Implementation/ Observation/ Comments, Implementation Result,

expressed in the [Categories A and B: Compliance; N - Non-compliance] [Categories C - F: P - Present; A - Absent] X - Not applicable, Reference to Findings Report

Note: These categories are provided to differentiate between what is audited for *compliance* (A, B) , and what is what may be asked in terms of *good practice* (C - F).

The following *non-functional requirements* were identified:

a. The use of the Checklist will serve to:

    i.   enhance customer confidence in the client quality management system

    ii. improve the effectiveness and efficiency of audits\assessments

    iii. improve the objectivity of the assessment\audit

b. That international recognition of the product will be promoted.

3.2 Quality requirements

Besides identifying technical requirements for the product, quality objectives were identified for the process applied to the development of the Checklist and extent to which the product met the technical requirements.

3.2.1 *Project quality objectives*

The quality requirements for the process applied to developing the Checklist were defined as:

a. To manage this product development in compliance with ISO 9001 requirements.

b. The Committee Draft stage will be used to apply the Checklist in practical assessment/auditing situations to determine the utility of the questions and to elicit feedback for validation purposes.

3.2.2 *Product quality objectives*

On the other hand, the quality objectives for the questions comprising the Checklist were required to demonstrate [5]:

a. **Objectivity**: a question is objective if it is possible to provide the answer without the opinion of the Checklist user.

b. **Completeness**: a question is complete if all the components needed to specify its meaning are present.

c. **Repeatability**: a question is repeatable if applied several times by the same Checklist user always produces the same answer.

d. **Reproducibility**: a question is reproducible if applied by different users always produces the same answer.

e. **Usefulness**: a question is useful if its answer contributes to the evaluation process.

f. **Measurability**: a question is measurable if it is possible to determine the attributes and their measures.

g. **Specific:** a question results in an attainable response.

h. All the *shall* requirements of ISO 9001 are addressed in the Checklist.

The extent to which these quality characteristics are exhibited by the Checklist questions may be evaluated by field trialling and by the application of formal inspection and review techniques.

4 Local and international collaboration

The project drew upon the following resources:

a. **Core Group Members:** (13) Individuals who are software quality system managers in local companies.

b. **Extended Core Group Members:** These include colleagues overseas experienced in software quality management (9) and a number of individuals locally who have shown interest in trialling the product in their companies (3 at the present time).

c. **Organisational Representatives of the SABS TC71.1 Information Technology Committee:** This group of individuals is responsible for approving the developed product.

5 Project practices

5.1 Project communication

Project communication depends heavily upon the use of the Internet for communication and document distribution.

The SEAL File Server is the repository of the project documents and records.

All core group members have username and password access to the management products, technical products and records supported on the SEAL File Server.

The emerging Checklist technical products are publicly available and are accessible using anonymous FTP access to the SEAL File Server thereby providing access to the Checklist products for trialling and validation. (See Appendix A).

A mail list has been created to support exchange of information and ideas between core and extended core group members. (See Appendix B)

5.2   Document management and control

The ISO 9001 Clause 4.5 document control requirements are comprehensively applied to all documents recorded and emanating from the project.

Briefly, the impact of such compliance includes:

a.   Revision control is applied to all documents.

b.   All documents and records are numbered and recorded in the project Master Document List (MDL).

c.   Documents are 'issued' by placing them on the SEAL File Server and then issuing an e-mail 'Document Issue Notice' which advises members of the Document Name, Revision, Number and file path. Each individual is responsible for downloading the updated documents using ftp.

5.3   Configuration management

All project artefacts are supported by a Configuration Management Plan, which describes the:

a.   Document naming conventions

b.   Record naming conventions

c.   Description of project directory structure

d.   Archiving arrangements

These conventions were defined at the start of the project and have ensured a common understanding of the project artefacts as the project has evolved.

5.4   Project tracking and control

The Project Management Plan supports details of the following:

a.   Project dependencies

b.   Human resources required

c.   Human resources available

d.   Team roles and responsibilities

e.   Hardware and software required

f.   Any training needs

g.   The Work breakdown Structure (WBS), obligations and schedule, and log of completed tasks

Items a) - f) were assembled at the start of the project and are largely static. The WBS is actively managed as the project evolves.

5.5   Product reviews

Three types of reviews are used in the project:

a.   **Project reviews:** These are undertaken in the context of formal meetings of the core group members. The purpose of the meeting is to review the status of the project and to plan in detail the next phase of product development.

   i.   *Meeting Inputs*: Meeting agenda, minutes of last meeting, Project work breakdown structure - schedule and log of completed activities

   ii.   *Meeting outputs:* Meeting minutes; updated Project work breakdown schedule and log

b.   **Product development meetings:** These are undertaken by small taskgroups comprising 4 or 5 core group members. They are held specifically to elaborate the technical aspects of the Checklist questions.

   i.   *Meeting inputs:* Applicable software engineering standards, ISO 9000 series quality assurance and quality management standards; current revision Checklist questions.

   ii.   *Meeting outputs:* Next revision Checklist questions.

c.   **Product inspection meetings:** These are undertaken by small tasks groups comprising 4 core group members. Formal product inspection methods are used. The primary purpose of the meeting is to apply quality control measures to the Checklist questions and to provide confidence that the product technical and quality requirements are met.

   i.   *Meeting inputs:* Current revision Checklist questions; forms for recording inspection and review decisions;

   ii.   *Meeting outputs:* Next revision Checklist questions; quality records comprising the completed inspection and review forms.

5.6   Product development management

Developing national or international standards is unavoidably a resource intensive and time-consuming process. The goal is to achieve consensus amongst the

various stakeholders on the technical attributes of a new product - which may exert a considerable impact on prevailing practices, particularly if the standard affects contractual arrangements or legislation.

In view of this management authorisation operates on a number of different levels and is governed by product progress through the Working Draft, Committee Draft and Draft SA Standard stages, which are formally governed by SABS Recommended Practice ARP 017 [6].

a.   New Work Item (NWI)

The requirements specification for the proposed Checklist was assembled and submitted to SABS Information Technology (TC71.1) in June 1995. The NWI proposal was formally approved in November of the same year.

b.   Working Draft Stage (WD)

The first project-level meeting was held in early December 1995 where the team concentrated on two tasks: refining the product requirements and secondly, defining the project and product quality criteria. Effort was then committed to developing the front-end support document (i.e. front page, table of contents, and supporting information), the Checklist framework, and a basic set of questions to support ISO 9001. The output of this stage was Rev 0.20 comprising 21 documents, including the Introduction and a document supporting each clause of ISO 9001.

This task was completed by the target date (1 April 1996) and the product set was released as the Working Draft for a 6 week formal review period. A Call for Review was extended to the Core, Extended Core (electronic format) and to members of TC71.1 (circulated using hard copy).

The scope of the review was defined as the structure of the Checklist, rather than the detail supplied in the Checklist questions - which would be subjected to retailed review in the CD stage.

c.   Committee Draft Stage (CD)

The project is presently in this stage of development. Effort is being devoted to the elaboration of the Checklist questions taking account of relevant international standards in Software Engineering (used as a source of indicators on good industry practices) and standards dealing with quality assurance (ISO 9001) and Quality Management (largely covered by the ISO 9004 series).

The output of this stage will be Revision 0.30 of the product set with development taking place over the period June to September 1996. Formal inspection reviews will be conducted on the 20 sub-products during a 3-day workshop scheduled from 4 - 6 November 1996.

While this stage is in progress the various sub-products comprising the Checklist will be tested (trialled, or validated) against the technical requirements and quality criteria.

The product (Revision 0.3) will be formally released in late November 1996 for a project level review with electronic distribution to core and extended core members, and hard copy distribution to TC71.1 members.

Should this review elicit only minor comment the product will be updated to take account of these concerns, and then forwarded to the Draft South African Standard stage.

d.   Draft SA Standard Stage (DSS)

This stage is regarded as a formality in which only changes of an editorial nature are allowed. If serious technical concerns are raised the product is returned for a further CD review.

6   Product trialling and validation

The development path taken by this project is unusual in the emphasis placed on active testing of the product at each stage of the standardisation process. Indeed, the only way in serious feedback can be elicited is by testing the subproducts in actual audit or assessment situations.

The net result of this process is to enhance confidence in the use of the Checklist.

7   Medium to long-term benefits

This project is being viewed as a potential prototype of how standardisation activities might be conducted on a wider scale in this country in future.

The following aspects of the process are novel to this project:

a.   the use of a formal quality management system to support the product development at all stages of the process. (The SEAL was awarded an ISO 9001 list for software development in July 1995).

b.   the exclusive use of electronic networks for exchange and distribution of documentation and for project communication. Paper based documentation

is only used where the project has to interface to the wider, non-electronic world.

A major consequence of applying these support processes to the project has been to dramatically reduce the development and review cycle, making it feasible to undertake the necessary technical development and review activity in a tight timeframe of 24 months, from initial New Work Item submission to SABS, to issue of the Checklist as a National Standard.

8 Impact of emerging SE standards

The questions in the Checklist are subdivided into two key categories: those which test compliance to a standard (ISO 9001) and those which offer guidance on the implementation of ISO 9001 in the software domain.

Until very recently, there were few software engineering (SE) standards which could be regarded as international, the most influential being the US Department of Defence MIL SPEC standards, and secondly the IEEE Software Engineering standards series.

The problem with the Military standards is that they are geared to the needs of that specific sector i.e. mission critical, long life cycle products. There are exceedingly few instances of the MIL Standards being voluntarily applied in the commercial domain - largely on account of the perceived higher development cost.

While the IEEE standards have been available for a decade or more, they have not been widely applied outside of the quasi-classified product community, and essentially unknown or at best ignored by the commercial software sector.

Both standards series suffer from the limitation that they are regarded as industry specific and controlled by a powerful stakeholder i.e. the defence community.

The software engineering standards being assembled by the Software Engineering Standards Committee (SC7) operate under the Joint Technical Committee for Information Technology (JTC1) run under the auspices of the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

SC7 presently supports 9 active workgroups resourced by ~200 international SE technical experts from 22 countries in the following technical areas:

a. **WG2: System Software Documentation:**
    Development of standards for the documentation of software systems.

b. **WG4: Tools and Environment:**
    Development of standards and technical reports for tools and Computer Aided Software/System Engineering (CASE) environments.

c. **WG6: Evaluation and Metrics:**
    Development of standards and technical reports for software products evaluation and metrics for software products and processes.

d. **WG7: Life Cycle Management:**
    Development of standards and technical reports on Life Cycle Management.

e. **WG8: Support of Life Cycle Processes:**
    Development of standards and technical reports on Life Cycle Management processes.

f. **WG9: Software Integrity:**
    Preparation of standards, technical reports, and guidance documents related to software integrity at the system and system interface level. In this context, software integrity is defined as ensuring the containment of risk or confining the risk exposure in software.

g. **WG10: Software Process Assessment:**
    Development of standards and guidelines covering methods, practices and application of process assessment in software product procurement, development, delivery, operation, evolution and related service support.

h. **WG11: Software Engineering Data Definition and Representation:**
    Development of standards and technical reports to define the data used and produced by software engineering processes, establish representations for communication by both humans and machines, and define data interchange formats.

i. **WG12: Functional size measurements:**
    To establish a set of practical standards for functional size measurement. Functional size measurement is a general term for methods of sizing software from an external viewpoint and encompasses methods such as Function Point Analysis.

The SEAL Server is the national repository of these standards in electronic format where they are supported in Working Draft (WD), committee (CD) and Draft International Stages (DIS). Once a standard reaches the stage of International Standard (IS) then it can only be obtained from the ISO head office in Geneva or from the national standards body (i.e. SABS).

Standards in electronic format are also subject to copyright protection, and are only made available for review or to support standards development activity.

At the present time there are 53 standards in various stages of development from WD to IS. This high level of activity places a tremendous review burden on local technical experts. To put this issue in perspective, the flagship Standards Committee is TC 176 which dealt with the ongoing development of the ISO 9000 series. TC 176 supports a work group per standard document, while in the SC7 context each work group might have between 3 and 30 standards to manage!

9   Lessons learned

Many software developers might react to a project of this nature with a big yawn. The processes described above seem to be a far cry from the chaotic practices of the conventional software development enterprise.

The project and its context i.e. the development of national and international standards in software engineering, must be taken seriously for the following reasons:

a.   South Africa is now part of the world community - and conditions affecting our capacity and capability for international trade are vitally important to the national survival and well-being.

b.   Compliance to the requirements of the ISO 9001 standards is a given condition for doing business with much of the industrialised world - as many companies in this country are discovering to their cost.

c.   The software engineering series of ISO \IEC\JTC1\SC7 are being used as compliance indicators when evaluating the effectiveness of quality management systems of software companies seeking ISO 9001 certification.

d.   The flagship standard of the SC7 series (ISO 12207 [7]) is now a required reference point for the development of all future ISO SE standards and is exerting a strong influence on the process model under consideration for the next revision of ISO 9001, due for release in the year 2000.

e.   There are strong moves in large local corporate users of Information Technology to take software quality management seriously. Evidence of this is the number of instances in which ISO 9001 requirements are now indicated in contracts from software product and service suppliers.

Tertiary education in this country, with a couple of exceptions, is largely ignorant of the pressures being brought to bear on local companies. In view of this, new graduates need to be technically skilled and well-versed and experienced in key project support processes (i.e. software project management, software quality assurance, software configuration management and requirements management.)

10 Acknowledgements

11 References

[1]   SABS ISO 9001 (1994) Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing

[2]   SABS ISO 9000-3 (1996) (DIS) 28 June 1996 Quality Management and Quality Assurance Standards, Part 3 - Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software

[3]   The TickIT Guide, Appendix 1: European IT Quality System Auditors Guide, Rev 3.0, 4 September 1995, IT & Software Engineering Department , BSI Quality Assurance

[4]   SABS ARP 013: 1990 Drafting and presentation of standards

[5]   Evaluating evaluation instruments, F Fabbrini, N Format, M Fusani, S Gnesi, Proceedings, Software Quality Management '95, 8 - 9 November 1995, South African Society for Quality and Software Engineering Applications Laboratory.

[6]   Procedures for the Technical Work in the preparation of South African Standards, ARP 017:1993, GR 14.

[7]   SABS ISO 12207 (1995) Software Life-Cycle Processes

Contact Details: Professor A.J. Walker, Software Engineering Applications Laboratory, Electrical Engineering, University of the Witwatersrand, Private Bag 3, P.O. Wits, 2050, Johannesburg, South Africa. Ph: +27 11 716-5469 Mobile: +27 82 452-0933; Fax: +27 11 403-1929. E-Mail: walker@odie.ee.wits.ac.za

Appendix A: Access to the Checklist

The audit Checklist can be downloaded from the SEAL Server via FTP at the following site:

seal.ee.wits.ac.za

The files are available in the directory:

ftp/pub/iso-acl/install

The following files must be downloaded:

- **isoacl2p.exe** - Self-extracting archive of Revision 0.2+ of the Word for Windows 6.0 files for the ISO 9001 Audit Checklist for Software product.

- **instal2p.txt** - Installation instructions

- **review2p.txt** - Product review invitation form

For convenience the file ISOACL2P.EXE is also supplied in uue encoded format, as a file named ISOACL2P.UUE.

The de-archived files will occupy about 2.5 M Bytes of file space.

The file format is Word for Windows Version 6.0.

Appendix B: Subscribing to the Checklist mail list

All details concerning product updates are distributed using the SEAL Mail List Server.

To receive these notices on a regular basis and to participate in discussions with other users we ask you to subscribe to the Mail List.

This registration is performed by sending an e-mail note as follows:

E-mail address: mail-list@seal.ee.wits.ac.za

Subject: -   <leave empty:

Copies to: <leave empty>

Message:

subscribe iso-acl

(No other information must appear in the body of the message).