Peer reviews with a perspective based approach as an alternative to implement ISO 9001 audits

Alvaro Ruiz de Mendarozqueta, Pablo Oliva, Martín Domínguez, Gonzalo Bonigo

Abstract— In this work we show a technique to implement a quality management system for software development companies which complies with the ISO 9001 standard and also with agile development methodologies. We show how the principles of ISO 9001 have much in common with Agile principles, and how both of them can be combined to get improved results. In particular, we show a way to implement Peer Reviews as an extension of the audit concept, ensuring compliance with the ISO 19011 standard. We also discuss how the practices "inspect" and "adapt", from agile methodology, are related to the Plan–Do–Check–Act (PDCA) Deming cycle. We evaluate our approach analyzing the experience in two software enterprises who obtained their ISO 9001:2008 certification while using Agile methodologies.

We conclude that peer reviews are an excellent tool for training and the audit process, where experienced people can be easily involved. We think that our approach is suitable without any major adjustments for the 9001:2015 version.

Index Terms—ISO 9001; Peer reviews; Reviews; Agile

1 Introduction

In his landmark paper, "Characterizing the Software Process: A Maturity Framework" [7], Watts Humphrey suggested that the responsibilities of quality assurance should be assigned to an independent team. He stressed the importance of audits to evaluate process performance in his book, "Managing the Software Process" [5], but warned that an incorrect audit can actually be counter-productive.

Rubio et al, in the paper "An integrated improvement framework for sharing assessment; lessons learned" [8] compiled 40 assessments in different companies using CMM, CMMI and ISO 9001 models. All the findings were normalized to fit CMMI [14] format and categorization.

A quantitative and qualitative analysis was performed: within the main results, the Process and Product Quality Assurance (PPQA) area was determined to be among the most error prone. Also, a risk analysis was performed based on the impact of each finding, considering the difficulties to reach a goal implementation fulfillment. For (PPQA), the Generic Goal 2 – (GG2 - Institutionalize a Managed Process) was the highest risk regarding the goal fulfillment.

In almost all companies there was either a quality group, or an individual that performed quality audits. In the qualitative analysis for the same assessment data base, the paper "Un enfoque para la mejora continua basado en los principios ágiles" [9] showed that the quality areas considered in the study [8] were assigned to personnel that did not have neither the skills nor the experience for performing the PPQA role, and there was very little involvement of experienced people from other areas.

The ISO 19011 standard [4] details the different skills an audit team member should have. It also exemplifies the necessary skills, considering the field where the audit will be performed, and quality management is included. It is evident that the skills needed for performing an audit can only be found in experienced people, at least for the main activities of it.

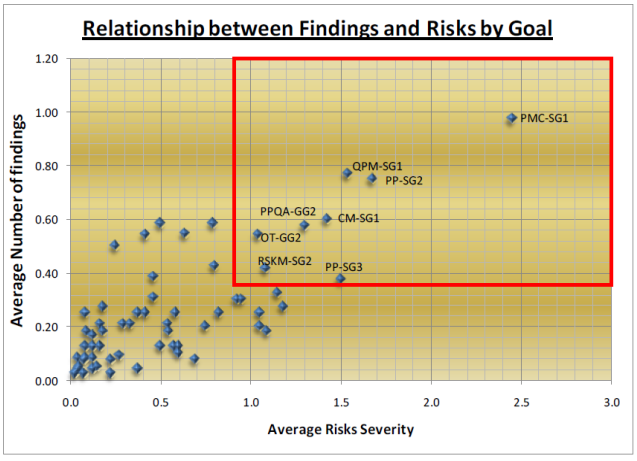

Figure 1 Relationship between findings and risks by goal

On the one hand, there is a link between a lack of experience in the quality area with the difficulties for institutionalizing the activities for performing an effective PPQA (W. Humphrey [5] pointed out that this is one of the main reasons why an SQA area is ineffective) and, on the other hand, we can think that audits performed by

- *Esp. Ing. Alvaro Ruiz de Mendarozqueta. UTN FRC E-mail: aruizdemendarzoqueta@gmail.com.*
- *Lic. Pablo Oliva. UTN FRC. E-mail: pablomigueloliva@gmail.com.*
- *Dr. Martín Domínguez. FaMAF, UNC. E-mail: mardom75@gmail.com.*
- *Lic. Gonzalo Bonigo. UTN FRC. E-mail: gonzalobonigo@gmail.com*

inexperienced personnel, were one of the causes for the difficulties in the implementation of a successful PPQA group and activities.

2 Peer Review

One of the most widely accepted software engineering techniques to detect errors and defects is the Peer Review. Freedman et al [6] said that the main reason for reviewing technical work is: *to err is human*. Also, they indicate that *large classes of errors escape the originator more easily than anyone else*.

Humphrey explained, in his book "Managing the Software Process" [5], the different types of reviews and their intended use; he emphasized them as a key practice to increase the maturity of the development process.

Gilb et al [11], in the book "Software Inspections", defined a rigorous approach for setting a software inspection process. The process they described maps easily with several of the elements of the audit process defined by ISO 19011 [4].

An interesting focus for the peer review is the perspective based approach. In the book "A Handbook of Software and Systems Engineering", Enders et al [12], explained that "*a perspective is the view a certain stakeholder has on the system*". The basic idea is to ask different reviewers to review from differents point of view and to perform the review based primarily on that perspective. Boehm et al [13], established that "*perspective-based reviews catch 35 percent more defects than nondirected reviews*".

For peer reviews and inspections, Enders et al [12] observed three main laws as showed is table 1:

Table 1: Main laws for peer reviews

Law	Statement
Fagan´s	Inspections significantly increase productivity, quality, and project stability.
Porter–Votta	Effectiveness of inspections is fairly independent of its organizational form.
Basili	Perspective-based inspections are (highly) effective and efficient

We can conclude that peer reviewing is an effective technique, its effectiveness is only slightly influenced by the organizational form, and the use of a perspective-based approach is especially effective and efficient.

3 Agile

Given the known problems of traditional software development (massive delays, products that did not fulfill its purpose adequately after years of development), a group of pioneers thought of a radical paradigm shift. The traditional paradigm tries to establish the requirements comprehensively at the beginning of the project (whose duration is fixed) and then to estimate, based on the development plan, the effort, necessary resources, and schedule to be fulfilled.

There are multiple examples of failure, delays and problems in such estimation. In the new paradigm [17] [18], as shown in Figure 2, a fixed time window is established, a small team of developers is organized and functionality is estimated, with the permanent help of the "owner" of the requirements.

Agile methods are based on values and principles that are expressed in the Agile Manifesto [16]:

"*We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:*

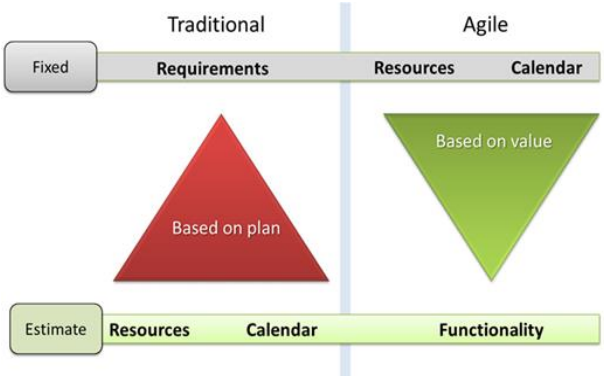

Figure 2 Paradigm shift in Agile

- *Individuals and interactions over processes and tools*
- *Working software over comprehensive documentation*
- *Customer collaboration over contract negotiation*
- *Responding to change over following a plan*

That is, while there is value in the items on the right, we value the items on the left more. "

The manifesto is complemented by 12 principles [16], that highlight goals such as customer integration in the development process, ownership by the entire team of everything that is produced, and a sustainable pace of work.

4 What is ISO 9001

ISO 9001 [2] is an international standard developed by ISO, that specifies the requirements for a quality management system (QMS) [3] that can generate the ability to consistently provide products and services that meet customer requirements, effectively and efficiently, and to improve continuously. It can be used by any organization, large or small, regardless of its field of activity. In figure 3 we can see the basic components [2] of the ISO 9001 standard. ISO 9001 can be certified and registered by an independent certification body and there are some implementations guidelines based on the type of service. In the software domain, the ISO 90003 guideline [21] provides guidance for organizations in the application of ISO 9001:2008 to the acquisition, supply, development, operation and maintenance of computer software and related support services.

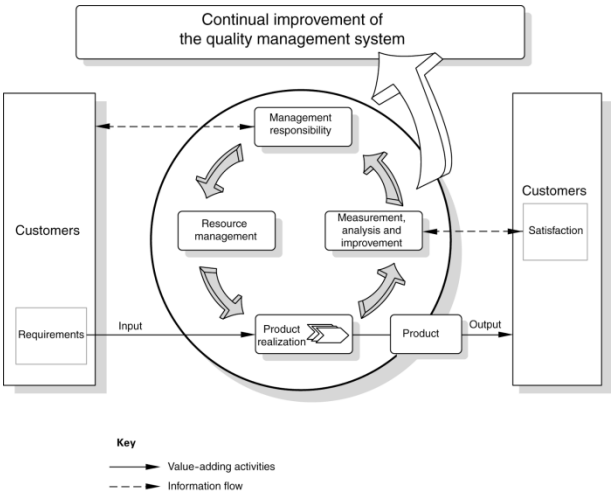

Figure 3 ISO 9001 overview

5 ISO AND AGILE

A straightforward way to understand that ISO 9001 can be implemented using the Agile philosophy is to analyze their principles. In table 2 we can see that most of the quality management principles [3] defined by ISO can be mapped with Agile principles [16] and practices.

ISO quality management principles [3]	**Agile**
Customer focus	Our highest priority is to satisfy the customer through early and continuous delivery of valuable software. [16] Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage [16]
Involvement of people	Business people and developers must work together daily throughout the project. [16] The most efficient and effective method of conveying information to and within a development team is face-to-face conversation [16] Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely [16]
Process approach	Methods that implements Agile principles like Scrum and Extreme Programming defined a process [15] [17]
System approach to management	As Agile implies a new paradigm defined by the manifesto and principles, and instantiated in different methods, is quite obvious that a systemic approach is needed in order to understand its advantages and how to use it. [9].
Continual improvement	At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly. [16] Continuous attention to technical excellence and good design enhances agility [16]
Factual approach to decision making	Working software is the primary measure of progress. [16] At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly. [16]

Table 2: Comparison between quality management principles and Agile principles

6 AGILE AND PEER REVIEWS

There is a strong mapping between Agile principles and practices and Peer Reviews characteristics as shown in table 3.

Peer Review	**Agile**
Detects lots of defects [6] [12]	Working software is the primary measure of progress. [16]
	Continuous attention to technical excellence and good design enhances agility.[16]
	Fix bugs that are identified as highest priority as soon as possible [18]
Basically is a group activity [6] [11]	Individuals and interactions over processes and tools [16]
	The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.[16]
Review team is	Collective code ownership [15]

responsible for the quality of the review outcome [6]	
Reviewed assets are shared by the reviewers [6] [11]	Increase visibility [17]

Table 3: Map between peer review and Agile principles

We can conclude that there is a strong matching between peer reviews and agile principles. The implementation of peer reviews, as well as other proven software engineering practices, while implementing agile practices, could lead to a more successful deployment of Agile.

7 Peer Reviews and Audits

In table 4 we can see that peer reviews can implement the audit principles [4].

Audit	**Peer Review**
Independent [4]	Team members from groups that are not responsible of the asset being reviewed, increase the independence.
Systematic [4]	Has a defined process so it can be repeated, measured and improved [5]
Documented [4]	Must be defined so it must be documented [11]
Evidence-based approach [4]	Findings are directly assigned and decisions are taken, based on the actual asset being reviewed [6] [11]
Due professional care [4]	Peer reviews requires training, expertise and practice [11]
Fair presentation [4]	The group is responsible for the review outcome [6] so it is easier to reach a consensus and to reflect accurately the results of the review
Confidentiality [4]	Gilb et al [11] indicate that the leader of a peer review is responsible for the confidentiality of the documentation and review
Integrity [4]	As peer review is an activity performed by professionals, they should work under the umbrella of a professional code of ethics that always includes integrity

Table 4: Map between peer review and audits

The CMMI model [14] stated in the PPQA key process area that objectivity can be reached using: "*Formal audits by organizationally separate quality assurance organizations. Peer reviews, which can be performed at various levels of formality In-depth review of work at the place it is performed (i.e., desk audits). Distributed review and comment of work products Process checks built into the processes such as a fail-safe for processes when they are done incorrectly*"
It also mentions that the quality assurance activity can be embedded within the processes and activities of the organization as we can see in: "*For example, in an organization with an open, quality oriented culture, the process and product quality assurance role can be performed, partially or completely, by peers and the quality assurance function can be embedded in the process. For small organizations, this embedded approach might be the most feasible approach*."
We can say that a peer review can clearly implement the defined principles for an audit and is one of the ways to implement objectivity suggested by the CMMI model.

8 Reasons to prefer Peer Reviews with a perspective based focus over traditional audits

As we mentioned before, traditional audits were used in several companies to implement the PPQA activities required [14] by CMMI and audits required by the ISO 9001:2008 [3].
According to the studies, the results tended to be poor.
Traditional audits need to set an audit meeting. Usually, these meetings are planned at an organizational level driven by quality groups or departments, so their schedule clashes with those of the projects and sometimes the quality department has no visibility of organizational plans. However, projects do plan and implement Verification and Validation (V&V) activities (required by the models [14] [3]); if peer reviews, including an "audit" perspective, were planned as V&V activities, there would be no clash between project and organization level planification, thus removing the need for extra meetings in order to perform the audits.
Having different perspectives and reviewers helps to understand the audit point of view, increases the possibility for detecting more findings, and is better suited to reach the consensus needed for the conclusions of the review, due to the fact that findings occur while the whole team is performing the review [6] [11]. In the traditional approach, demands for clarification of a finding and discussions regarding its impact often demand additional effort and meeting time.
Peer reviews are an excellent way to implement the "Engagement of people" Quality Management principle [3], as more people are involved and the participants are trained by performing the reviews themselves as a secondary benefit [11]

9 A CASE STUDY IN TWO COMPANIES: TALLER TECHNOLOGIES AND ESOLUTIONS

In both companies, the delivery of software products and services were implemented using the Agile philosophy. The management system was designed from the bottom up, taking advantage of the various processes that were operating in the different projects. The aim was to design a minimal viable version of the processes and start using them, and to review them, as soon as possible; even without waiting for all processes to be defined.

As agility focuses on adding value to the customer, who is the one who sets priorities, the organization's managers were chosen as the internal customers of the continuous improvement activities.

One of the most common problems with the implementation of a quality management system is the use of preset recipes [9]. If a design was successful in a company, it is usual to copy the processes because they already had "success" in the certification. As Gerald Weinberg says [19] "*There are no two software organizations exactly alike. There are not two totally different software organizations*", thus the decision was made to design processes to improve what was already being done, such that the new processes were perceived to be an improvement and not an imposition. Some recommendations and lessons learned were used, but no "packed" implementations were copied.

As software development is a creative task, specifying all the steps to follow during its creation would be harmful for the productivity and morale of its creators. We prefer, in all instances where possible, to describe which artifacts a process should produce, rather than detailing the steps of each process. This also allowed us to adjust the objectives to the pre-existing processes in each project.

In order to be able to cover the variations that the different projects have and, at the same time, be as simple and flexible as possible, very high level processes were designed that contain a conceptual definition of what needs to be done in projects.

Each project, through the project plan, is responsible for defining how to implement what the process defines.

The heuristic used is as follows: the software development process is instantiated in each project plan, using guides that determine how the process is defined: for the project plan, the configuration management activities, scrum implementation, etc.

In order to make the instantiation, a business and/or management criterion is used according to elements such as: complexity, size, impact on the business, quantity of people, skills and abilities of the participants, among others.

The defined process tells what needs to be done and the project determines how to do it.

Taller Technologies

Taller Technologies is a software development services company; it is specialized in developing customized solutions and strongly aligned with Agile methodologies.

They provide services to customers in different countries, in three main areas: embedded and real-time software development for mission critical and high-availability systems, software development for mobile devices and software development for web services and applications.

Project Review

Each project was reviewed periodically by a specialized quality team, with the project team being represented by their project manager. While this was normally closer to a standard audit, team members were invited to participate from time to time in the review, not only to answer questions but also to ask them. These mixed reviews were found to be more effective than the standard audits.

Release Readiness Review

To comply with the requirements of a mission critical software for avionics, a release audit called Release Readiness Review was implemented. Its aim was to ensure that all the quality requirements of the software had been met, to provide corrective actions when non compliances were found, and to discuss possible process enhancements. It required the participation of at least three team members plus an external reviewer with the main goal of considering the point of view of the quality management system and ISO compliance perspective. The review findings were treated as non conformances, being brought up in retrospective meetings and handled to prevent them from reoccurring.

Esolutions

Esolutions is a software services and products company; it specializes in the development of custom tailored software for telecommunication companies and for face to face customer support. It uses Agile methods both for software development and for its internal processes.

The overall improvement project included the design and implementation of the quality management system, the roll out of the agile philosophy and the implementation of several engineering practices, one of which was the peer review.

The approach was to use an agile implementation so monthly improvement sprints were deployed. In the case of peer review, the deployment was evolving and it was used to implement both the technique and the audit process.

Each team presented its own definition of processes in a Project Plan. These plans were reviewed to ensure that they were both sufficiently rigorous and actually followed. The reviews were performed by a mix of people from external teams (whose own projects were audited in turn), and team members.

Also, non-compliances found during a weekly meeting of all team leaders were added to an improvement backlog, with status updates on subsequent weekly meetings. This acted as a form of "Managerial Peer Review", ensuring that correct processes were followed by all the teams in the organization

10 LESSONS LEARNED

The approach worked very well. Both companies ob-

tained the ISO 9001:2008 certification, while showing an actual improvement in the maturity of their processes.
Peer reviews also worked as excellent tools for training: the participants learned about engineering best practices, organizational processes, and methods. The involvement in the reviews made the necessity for a rigorous following of processes evident for all those involved.
Reaching consensus about the findings was much easier when the findings appeared to emerge from the group itself, since the auditor was seen as another member of the team.
Experienced people were easily involved, and their knowledge was shared more fluently with the rest of the team.
The Verification and Validation (V&V) activities were enhanced with the perspective based focus.
Having an ISO and quality management perspective in the reviews improved the quality of the peer review outcomes.
The maturity of V&V practices is critical; if peer reviews are not an established practice in the organization, training and pilot projects should be carried out before the perspective based peer review implementation.

11 FUTURE WORK

A quick analysis of the requisites of ISO 9001:2015 shows that the approach is suitable with no changes.
On top of this, we believe that the emphasis on risk analysis and management that has the 2015 [20] version of the ISO 9001, will help a lot in order to use the same approach. Based on the risk assessment per project it will be easier to tailor the defined process, using a business criterion, into the project plan.
The ISO 9001:2015 also emphasized leadership; the peer review approach is an excellent fit due to the fact that it provides an environment for enhancing leadership and participation [3].
We have already started the migration of this approach to the requirements of the ISO 9001:2015.
A guideline based on the ISO 90003 [21] structure is being developed; it will describe how to implement the ISO 9001:2015 for the software domain using the agile philosophy, principles and methods, and also using proven software engineering techniques.

ACKNOWLEDGMENT

The authors wish to thank to Ana Belén Mercado, Fabio Bustos, Fabio Grigorjev, Omar Chaig, Álvaro Loeschbor, Miguel Insaurralde and Maximiliano Ugarte.

REFERENCES

[1] ISO/IEC, IEEE, “International Standard ISO/IEC/IEEE 24765, Systems and software engineering — Vocabulary”, Switzerland: ISO/IEC IEEE, 2010.
[2] ISO, “International Standard ISO 9001, Quality management systems — Requirements”, Switzerland: ISO, 2008.
[3] ISO, “Quality Management Principles”, Switzerland: ISO, 2008.
[4] ISO, “International Standard ISO 19011, Guidelines for auditing management Systems”, Switzerland: ISO, 2011.
[5] W. S. Humphrey, “Managing the Software Process”, Addison-Wesley, 1989.
[6] D. P. Freedman, G. M. Weinberg, “Handbook of Walkthroughs, Inspections, and Technical Reviews”, Third Edition Dorset House, 1990
[7] W. S. Humphrey, “Characterizing the Software Process: A Maturity Framework”, Technical Report CMU/SEI-87-TR-11 ESD-TR-87-112, June 1987
[8] D. Rubio, N. Andriano, A. Ruiz de Mendarozqueta y C. Bartó, “An integrated improvement framework for sharing assessment lessons learned”, CACIC 2008, Universidad Nacional de Chilecito, La Rioja - Argentina, 2008.
[9] A. Ruiz de Mendarozqueta y N. Andriano, “Un enfoque para la mejora continua basado en los principios ágiles”, ASSE 2014, Universidad de Palermo, CABA - Argentina, 2014
[10] A. Davis, "15 Principles of Software Engineering," Manager Column, IEEE Software, 11, 6, November 1994.
[11] T. Gilb. D. Graham, "Software Inspection," Addison-Wesley, 1993
[12] Albert Endres, Dieter Rombach, “A Handbook of Software and Systems Engineering”, Addison-Wesley, 2003.
[13] Barry Boehm, Victor R. Basili, “Software Defect Reduction Top 10 List”, IEEE Computer, January 2001
[14] CMMI Product Team. CMMI for Development, version 1.3. Pittsburgh, Pennsylvania, USA : Software Engineering Institute (SEI), November 2010.CMU/SEI-2010-TR-033
[15] J. Shore, S. Warden, “The Art of Agile Development”, O’Reilly, 2008
[16] K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R.Martin, S. Mellor, K. Schwaber, J. Sutherland, D. Thomas; “Principles behind the Agile Manifesto”; 2001; available at: http://agilemanifesto.org/principles.html
[17] A. Cockburn, “Agile Software Development”, Addison-Wesley, 2007.
[18] J. Sutherland, “Agile Principles and Values”, Microsoft; available at:: https://msdn.microsoft.com/en-us/library/dd997578.aspx
[19] G. Weinberg, “Quality Software Management (Vol 1 Systems Thinking)”; Dorset House, 1989.
[20] ISO, “International Standard ISO 9001, Quality management systems — Requirements”, Switzerland: ISO, 2015.
[21] ISO, ISO/IEC 90003:2014, “Software engineering -- Guidelines for the application of ISO 9001:2008 to computer software”, Switzerland: ISO, 2014