Process Assessment for Digital Records Preservation and Information Security

Lucas Colet
Public Research Centre Henri Tudor
29 avenue John F. Kennedy
L-1855 Luxembourg
+352 42 59 91 - 2421
lucas.colet@tudor.lu

Alain Renault
Public Research Centre Henri Tudor
29 avenue John F. Kennedy
L-1855 Luxembourg
+352 42 59 91 - 2758
alain.renault@tudor.lu

ABSTRACT
In this paper, we describe a way to help organizations, mostly SMEs, implementing records management, digitization, digital preservation and information security on the basis of ISO standards. In order to achieve this, we target the development of an assessment method for digitization, digital records preservation and information security. The result is made up of three tools: a Gap Analysis, giving a big picture of the system by evaluating the gap between its current status and the requirements of the ISO standards, a Lite Assessment tool, and a TIPA® for Electronic Records Management tool, the last two are more complete interview-based assessment methods.

General Terms
Management, Measurement, Standardization.

Keywords
Process Assessment, Electronic Records Management, Standardization, PSDC, Luxembourg.

1. INTRODUCTION
Today is a world of information. In order to be compliant with regulations or for management purpose, more and more of this information needs to be long-term stored, especially for organizations. Moreover, in order to keep its legal value, this information needs to have the following properties, according to ISO 15489-1 [12]: authenticity, reliability, integrity and usability. With these properties, information is then called records for the organizations.

The Public Research Centre Henri Tudor started to work on the integration of some of the standards related to Records Management, Digitization and Information Security. Our objective was to create a framework of tools and methods in order to help organizations (especially SMEs) to gain awareness on these topics. We have used Process Assessment as a mean for helping organizations in this way.

Indeed, when dealing with Records Management systems, improving the efficiency of the processes that manage these systems improves the overall quality. Higher efficiency can be reached by working on the various aspects of process maturity. Process maturity can be built by going up the levels of the maturity scale, each level building on the previous one.

Learning from a reference framework's best practices in a particular domain, as ISO 15489-1 for Records Management, is an effective way of improving processes but this implementation is not straightforward. Process assessment is a powerful tool to start such an improvement initiative. Assessment results represents where the current practices in the organization stand compared to the reference process.

Moreover, process assessment is useful to identify improvement opportunities and setup priorities within an improvement plan. It enables to measure the progress accomplished during an improvement project and thus facilitates buy-in from the management. The process maturity approach structures the improvement initiative by providing a step-by-step roadmap.

Our work is carried out in several steps: first, we select different relevant standards. Then, we analyze them in order to find atomic requirements; we could therefore identify and extract processes, objectives and activities, thanks to the requirements that tend to the same objectives. We developed a Process Assessment for Electronic Records management, on the basis of the ISO standard for Process Assessment, ISO/IEC 15504-2 [5], which allow organizations to be assessed against best practices. We also defined another tool, which allows organizations to identify the gap between their existing system about Records Management, Digital Preservation and Information Security, and a system with a defined set of standards. We present in this paper a three-steps assessment approach with: a Lite Assessment, a TIPA® for Electronic Records Management Assessment, and a Gap Analysis.

2. CONTEXT IN LUXEMBOURG
In the specific context of Luxembourg, a lot of companies, especially banks, retain important information on paper records. Paper documents are difficult to manage, essentially when an organization wants to retrieve a specific one. To face the amount of data to be preserved, to increase efficiency and to reduce storage cost, the use of digital records is the common answer of organizations. However, organizations in Luxembourg often did not take the chance to digitize their paper records: indeed, they could not destroy paper (and therefore save space) because of a flaw in the current legal context: the CSSF (*Commission de Surveillance du Secteur Financier*, financial supervision of

Luxembourg) even recommends in 2008 not to destroy paper records, without an adapted legal framework for this [1] [4].

A new legal framework is currently under development in Luxembourg (actually waiting to be voted), in order to allow this destruction without any legal ambiguity. This new legal framework will be supported by technical requirements developed by ILNAS (Luxembourg national body regarding standardization, *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*) called "Technical regulation requirements and measures for certifying Digitisation or Archiving Service Providers (PSDC)" [20] (called hereafter "technical regulation for PSDC") in order to ensure the reversal of the burden of the proof (if there is a litigation, the opponent will have to prove that the defender's records, digitized and stored according to the technical regulation, were not managed in an adequate manner and therefore cannot be accepted in front of the court; today, the defender has to prove that its records have been digitized and stored according to the state of the art; this proof could be difficult and costly to bring). This technical regulation is strongly based on the ISO/IEC 27001 [7] and ISO/IEC 27002 [8] standards, foundation of Information Security.

In this context, the objective of Public Research Centre Henri Tudor is to help organizations (especially SMEs) to raise awareness on Records Management, Digital Preservation and Information Security, and to enhance the adoption of the PSDC technical regulation by adding to them requirements for Records Management and Digital Preservation.

3. STANDARDS SELECTION

Our initial task consisted in selecting relevant standards in the field of Records Management, Digitization, Digital Preservation and Information Security, the latest being important for Luxembourg as it is the basis of the technical regulation for PSDC. We then used this technical regulation as a basis for our work (and by ricochet ISO/IEC 27001 and ISO/IEC 27002). We added a layer of Records Management on top of this Information Security layer by selecting a complementary standard to ISO/IEC 27001 in the field of Records Management: ISO 30301 [14]. Indeed, both standards are Management System Standards (MSS) developed by ISO (International Organization for Standardization) on the same skeleton but adapted to different fields. The heart of the management systems is the continuous improvement, linked to the PDCA cycle (Plan, Do, Check, Act, as pictured with the cycle in ISO 30301 in Figure 1).

These standards help organizations, above all top management, to formalize their approach of a topic by giving guidelines to define policies, procedures, implement them and check whether they are compliant with what had been defined, and improve the system. Another standard that we included was ISO 9001 [15], defining requirements to set and improve a Management System for Quality.

Below this management-layer, we investigate standards in the field of Records Management and Digital Preservation, i.e. standards for keeping records, for keeping information on a long-time period, and for digitization. We shortlisted three standards:

[1] *"En l'absence d'un cadre juridique plus adapté, qui devrait néanmoins voir le jour, la CSSF recommande aux professionnels financiers de ne pas détruire les documents communément admis comme preuve devant les instances judiciaires et qui restent principalement sous forme «papier»"*

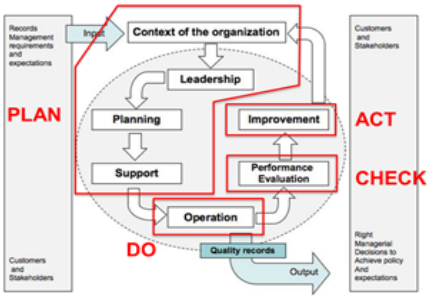

Figure 1. PDCA cycle in ISO 30301.

ISO 15489-1 (which gives example of processes for Records Management), ISO 14721 [11] (aka. OAIS, which gives guidelines for electronic long-term preservation), and ISO 13028 [10] (which gives guidelines for Digitization). Our idea was to combine these standards to create the best combination for an organization which wants to efficiently digitize analogue documents, and to keep electronic records by preserving the legal value on the long-term. Separately, each standard covers only a part of this idea. Together however, they bring a good answer to this challenge.

We have selected relevant standards for our goal; we then have to analyze them, find requirements and define processes.

4. DEFINE PROCESSES

In order to perform Process Assessment, ISO 15504-2 requires that a Process Assessment Model (PAM) shall be based upon a suitable reference source of process definitions – one or more Process Reference Models (PRM). The PRM gives a high-level definition of the process based on its name, purpose and outcomes, whereas, in addition to this, the PAM lists the process base practices and work product that can be used as process indicators during a process assessment.

We have a set of standards, and we have to define a PRM in order to create a PAM. We sliced up the standards into atomic requirements, to know what is really needed in a system, by using a method developed in [2], mostly based on a vocabulary cutting (when there is a "shall" in the sentence, it is a requirement, if there is a "and" in the sentence, this sentence has to be split up in two requirements to encompass both parts – before and after the "and"). None of the standards for Records Management, Digital Preservation and Digitization provides requirements, but rather guidelines. In order to achieve our goal, we turned these guidelines into requirements, in order to provide the best system at the end. These "requirements-guidelines" are traced to know if they are really mandatory (as a real requirement) or not (as a guideline). Furthermore, OAIS is structured in such a way that it is difficult to extract requirements or guidelines from its content. That is why we used ISO 16363 [13] instead, This standard is based on OAIS and gives requirements for Digital Preservation.

With the same method, we can organize and structure these requirements according to their objectives. We can define the outcomes and the process purposes, identify common purposes upon those requirements, factorize outcomes from the common purposes, and group activities together under a practice and attach it to the related outcomes, allocate each practice to a specific capability level. Goal-oriented requirement engineering techniques were mostly used for doing so, as detailed in [24]. We would then have a set of processes, as a process is a "set of

interrelated or interacting activities which transforms inputs into outputs" [5].

However, by looking into a Management System Standard like ISO/IEC 27001 or ISO 30301, it is difficult to identify such processes. Some work has been done on the definition of processes for Management System Standards [29] or the integration of Management System Standards [17] [19]. The processes given in the first paper are too detailed: about 30 processes are defined, which could be too much for our goal, as we target SMEs. [21] defined 12 management processes for ISO/IEC 27001, but as stated before, it still is too much, as we will also have to add processes for Digital Preservation, Digitization and Records Management. However, they give a good basis to start building and defining less processes with a broader scope. Furthermore, the papers on Integrated Management System helped on the identification of the recurrent requirements in MSS. The requirements were then grouped together according to their goals, the outcomes, and the purposes.

The processes definition for Records Management, Digitization and Digital Preservation followed the same method, and was driven by ISO 15489-1, ISO 13028, ISO 16363 and the PSDC technical regulation. The whole set of processes, defined thanks to goal trees, is given in Figure 2. Five management processes are defined, with two support processes, and six business processes (Records Management, Digital Preservation and Digitization core).

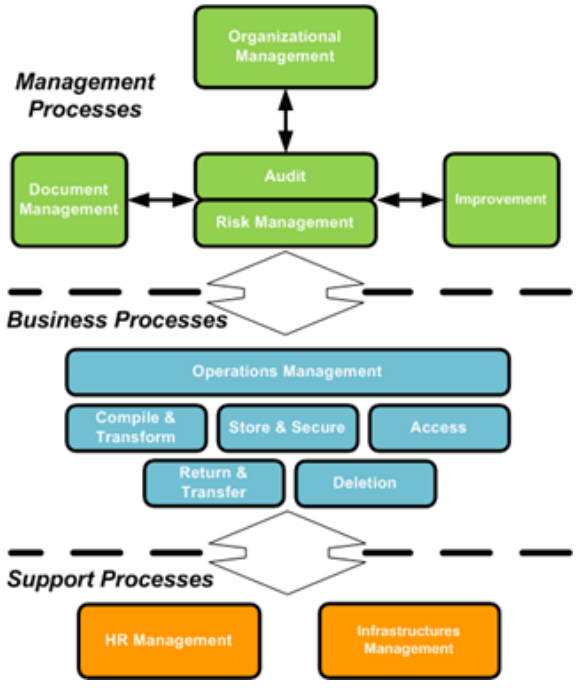

Figure 2. Set of 13 defined processes for Digital Preservation, Electronic Records Management, Digitization and Information Security.

ISO 15489-1 defines seven processes: Records capture, Registration, Classification (all three covered by Compile & Transform), Storage and handling (covered by Store & Secure), Access (covered by Access), Tracking, and Implementing disposition (covered by Return & Transfer and Deletion).

Technical regulation for PSDC defines, for the digitization part, four processes: Compilation of analogue documents, Creation and temporary storage of digital documents (both covered by Compile & Transform and by Store & Secure), Temporary storage of analogue documents (covered by Store and Secure), Restoration, transfer, and potential destruction of analogue documents and deletion of digital documents (covered by Return & Transfer and Deletion).

Technical regulation for PSDC defines, for the archiving part, three processes: Compilation of digital documents, Creation and conservation of digital files (both covered by Compile & Transform and by Store & Secure), Restoration, transfer and deletion of digital files (covered by Return & Transfer, Access, and Deletion.

On top of these business processes, Operations Management is needed in order to steer the Digitization and Archiving. We have 13 processes defined in the PRM.

We have then to define the PAM that will be the reference for performing assessments, and the method to use it.

5. ASSESSMENT

We defined two levels of assessment based on our PRM (plus a Gap Analysis that will be developed below): one called Lite Assessment, that confronts the whole organization to the relevant standards without any possibility to tune it to a single process, and one called TIPA for Electronic Records Management (ERM) that could be tuned in order to assess a part of the organization and a subset of processes. The first one is shorter in duration than a full TIPA for ERM assessment, as it is an integrated method created to directly assess the whole organization, whereas the TIPA for ERM is really based on a possibility to assess in depth some processes. TIPA for ERM is based on the TIPA framework, as depicted in Figure 3, where the TIPA Process Model is tuned to reflect the specific domain of Records Management, Digitization and Information Security.

Figure 3. Structure of the TIPA® framework.

TIPA (Tudor IT Process Assessment) has been chosen because it is published [3] and documented. To build TIPA, the authors have experimented and published a transformation process [2] to support the development of robust process models be them based on informal process descriptions or on collection of requirements. Furthermore, a complete toolkit is available to support the assessment method (see Figure 4). This interview-based assessment method is now widely trained and used internationally [18] [16]. TIPA® is an interview-based assessment method that is developed on the basis of ISO/IEC 15504-2 assessment approach. It provides an objective and structured view of the current maturity level of the practices of an organization.

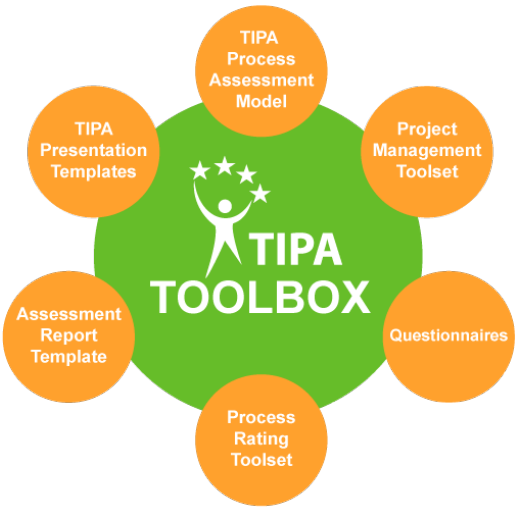

Figure 4. The TIPA® toolbox.

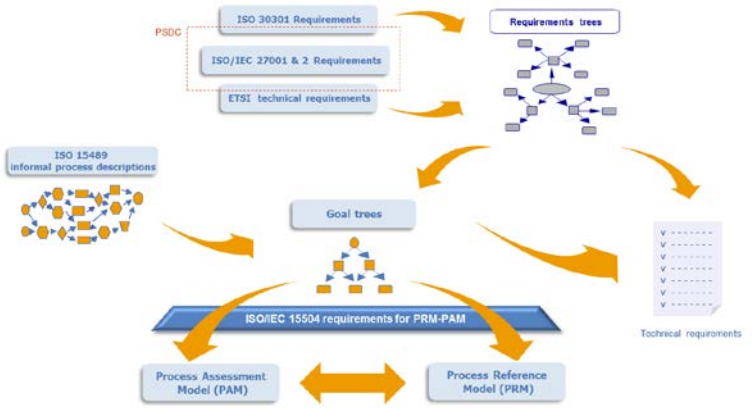

Figure 5. The TIPA® transformation process for ERM.

The ISO/IEC 15504 assessment approach states that we have to look inside the processes in order to know on which maturity level a specific process is.

The ISO/IEC 15504-2 standard (and the TIPA® assessment method) defines 6 levels of process maturity that cover various aspects of process effectiveness:

- Does the process achieve its purpose and outcomes? (Level 0 if not, Level 1 if yes)
- Is the process performance managed and are its work products managed? (Level 2)
- Is the process well-defined and performed in a standard way throughout the company? (Level 3)
- Is the process quantitatively managed? Are there indicators to predict the process activity? (Level 4)
- Is the process continuously improved? (Level 5)

However, TIPA® has not been applied to Records Management, Digitization, or Information Security.

To build this assessment for these specific topics, each reference document has provided inputs (atomic requirements or best practices) for the creation of a Process Reference Model (PRM). This PRM has been defined; we can couple it to our already developed TIPA® Measurement framework, add process indicators to this PRM, and create a specific Process Assessment Model (PAM).

For creating a PRM and a PAM, we will have to identify for each process its purpose, its expected results, and its base practices and work products. Base practices are typical activities that help achieve the expected results of the process, and that are performed in order to fulfill the process's purpose. They will be useful in order to know if the Level 1 is reached. Moreover, it is possible thanks to this approach to verify the inputs and outputs of the process (Work Products in ISO/IEC 15504-2). Our approach to create PAM and PRM is given in Figure 5.

Our methodology for Lite Assessment and TIPA® for ERM uses an interview-based assessment for the collection of indicators as an effective way to gather information about the Process implementation and the Process maturity. This methodology has been developed for TIPA® and already been tested and used with success with ITIL v2 [22] and v3 [23] (Information Technology Infrastructure Library), with the ISO/IEC 20000 standard [6], with CMMI [26], and with ISO 10006 [9].

6. GAP ANALYSIS

With our set of requirements encompassed in a set of processes, we also created a tool called Gap Analysis.

In order to implement these standards, organizations will first usually evaluate the gap between their current status and the requirements of the standards, in order to know what could be reused from the actual system and to estimate the resources needed to fill the gap. This step is often referred to as a gap analysis. This task could be really complicated and costly. Indeed, an Information Security Management System is composed of 150 normative requirements and 133 security controls, a Management System for Records is composed of about the same normative requirements, etc. [27]. In order to reduce this step, especially in the SMEs context, this Gap Analysis tool has been created.

This tool will help organizations to position themselves against our relevant standards or a selection of them. Our Gap Analysis was developed on the basis and with the method of a previous work [27]. As stated in this paper, based on [1], three steps have to be followed: modelling of the standards requirements, design of the assessment tool, and experimentations. The first step has been greatly facilitated thanks to our work for creating the PRM and PAM for our integrated approach. The second step consists of creating a questionnaire covering and regrouping all the requirements of all the studied standards, with the only possible answers are "Yes" and "No" (example: "Do you do regular reviews of the management system efficiency, particularly after significant changes?"). The third step is in progress: we are testing this tool in several organizations in Luxembourg. Furthermore, this tool has been extensively tested with the ISO/IEC 27001 part [28]. It is really a useful tool for SMEs, as it is a quick and cheap assessment, even if it gives only a big picture of the existing system.

7. CONCLUSION

We presented three different tools, each of them having a certain accuracy in assessing an organization against our relevant standards (Gap Analysis tool is the less accurate, Lite Assessment give a far better accuracy of the whole system, TIPA® Assessment gives the best accuracy and could be used for only a set of processes and not the whole system), and each of them have a certain human cost (Gap Analysis tool is the cheapest, as it needs only two days to be used, Lite Assessment is greedier, as it needs 15 days, and TIPA® Assessment needs more resources if the whole system is assessed, but could be tailored for the needs of the organization).

The TIPA® Assessment and Gap Analysis have already been largely experimented. We are currently testing there application to ERM. Moreover, we are still developing the Lite Assessment method in the frame and with the help of the TIPA development team.

The next steps for these tools and this framework around Digitization, Electronic Records Management, Digital Preservation and Information Security will be to prove the consistency of the models. This will be done by investigating the possibility to enhance the governance and compliance of these processes against these relevant standards, thanks to feedbacks from industry or research specialists, Requirements engineering techniques (GORE) and Business Process Modeling, in order to allow a very good level of confidence when using these models. Furthermore, another lead could bring us to measure the impact of processes for products / services or optimize them by strengthening our skills and tools (i.e. how to measure (IT) Service Quality and make the link with process maturity?).

Lastly, we would investigate in which circumstances and in which proportions our approach could enhance and facilitate the certification of an organization, as we use an integrated approach [25].

8. REFERENCES

[1] David E. Avison, Francis Lau, Michael D. Myers, and Peter Axel Nielsen. Action research. *Commun. ACM*, 42 (1): 94–97, January 1999. ISSN 0001-0782. doi: 10.1145/291469.291479. URL http://doi.acm.org/10.1145/291469.291479.

[2] B. Barafort, A. Renault, M. Picard, and S. Cortina. A transformation process for building prms and pams based on a collection of requirements – example with iso/iec 20000. In *Proceedings of the International Conference SPICE2008, Nuremberg, Germany*, 2008.

[3] B. Barafort, V. Betry, S. Cortina, M. Picard, M. St Jean, A. Renault, O. Valdés, and Tudor. *ITSM Process Assessment Supporting ITIL : Using TIPA to Assess and Improve your Processes with ISO 15504 and Prepare for ISO 20000 Certification*. Van Haren, Zaltbommel, Netherlands, 2009.

[4] CSSF (Commission de Surveillance du Secteur Financier). Rapport annuel, 2008.

[5] International Organization for Standardization. Iso/iec 15504-2:2003: Information technology – process assessment – part 2: Performing an assessment, .

[6] International Organization for Standardization. Iso/iec 20000-1:2011: Information technology – service management – part 1: Service management system requirements, .

[7] International Organization for Standardization. Iso/iec 27001:2005: Information technology – security techniques – information security management systems – requirements, .

[8] International Organization for Standardization. Iso/iec 27002:2005: Information technology – security techniques – information security management systems – code of practice for information security management, .

[9] International Organization for Standardization. Iso 10006:2003: Quality management systems – guidelines for quality management in projects, .

[10] International Organization for Standardization. Iso/tr 13028:2010: Information and documentation – implementation guidelines for digitization of records, .

[11] International Organization for Standardization. Iso 14721:2012: Space data and information transfer systems – open archival information system (oais) – reference model, .

[12] International Organization for Standardization. Iso 15489-1:2001: Information and documentation – records management – part 1: General, .

[13] International Organization for Standardization. Iso 16363:2012: Space data and information transfer systems – audit and certification of trustworthy digital repositories, .

[14] International Organization for Standardization. Iso 30301:2011: Information and documentation – management systems for records – requirements, .

[15] International Organization for Standardization. Iso 9001:2008: Quality management systems – requirements, .

[16] R. Hilbert and A. Renault. Assessing it service management processes with aida – experience feedback. In *EuroSPI*, 2007.

[17] British Standards Institution. Pas 99:2006: Specification of common management system requirements as a framework for integration.

[18] ITPreneurs. About tipa®, tudor it process assessment, 2013. URL http://www.tipaonline.org/en/tipa/about-tipa.

[19] Stanislav Karapetrovic and M. Casadeús. Implementing environmental with other standardized management systems: Scope, sequence, time and integration. *Journal of Cleaner Production*, 17 (5): 533 – 540, 2009. ISSN 0959-6526. doi: http://dx.doi.org/10.1016/j.jclepro.2008.09.006. URL http://-www.sciencedirect.com/science/article/pii/S0959652608002394.

[20] ILNAS (Institut luxembourgeois de la normalisation de l'accréditation de la sécurité et qualité des produits et services). Technical regulation requirements and measures for certifying digitisation or archiving service providers (psdc), 2013.

[21] Olivier Mangin, Béatrix Barafort, Patrick Heymans, and Eric Dubois. Designing a process reference model for information security management systems. In *12th International Conference, SPICE 2012, Palma, Spain, May 29-31, 2012*, 2012.

[22] Office of Government Commerce. Itil (information technology infrastructure library) v2, 2001.

[23] Office of Government Commerce. Itil (information technology infrastructure library) v3, 2007.

[24] André Rifaut and Eric Dubois. Using goal-oriented requirements engineering for improving the quality of iso/iec 15504 based compliance assessment frameworks. In *International Requirements Engineering, 2008. RE '08. 16th IEEE*, 2008.

[25] Santos, Mendes, and Barbosa. Certification and integration of management systems: the experience of portuguese small and medium enterprises. *Journal of Cleaner Production*, Vol. 19, Issues 17-18: 1965–1974, 2011.

[26] Carnegie Mellon University. Cmmi (capability maturity model integration), 2010.

[27] Thierry Valdevit and Nicolas Mayer. A gap analysis tool for smes targeting iso/iec 27001 compliance. In Joaquim Filipe and José Cordeiro, editors, *ICEIS (3)*, pages 413–416. SciTePress, 2010. ISBN 978-989-8425-06-5. URL http://dblp.uni-trier.de/db/conf/iceis/iceis2010-3.html#ValdevitM10.

[28] Thierry Valdevit, Nicolas Mayer, and Béatrix Barafort. Tailoring iso/iec 27001 for smes: A guide to implement an information security management system in small settings. In Rory V. O'Connor, Nathan Baddoo, Juan Cuadrago Gallego, Ricardo J. Rejas-Muslera, Kari Smolander, and Richard Messnarz, editors, *EuroSPI*, volume 42 of *Communications in Computer and Information Science*, pages 201–212. Springer, 2009. ISBN 978-3-642-04132-7. URL http://dblp.uni-trier.de/db/-conf/eurospi/eurospi2009.html#ValdevitMB09.

[29] Alastair Walker. Towards iso 9001:201x: Transitioning from process quality to product quality. In *12th Annual SAATCA International Auditors Convention*, 2009.