Legal Risk Management Process in Software Projects: An Action Research Study

Ricardo J. Rejas-Muslera
Universidad Camilo José Cela
rrejas@ucjc.edu

Miguel A. Sicilia Urbán
Universidad de Alcalá
msicilia@uah.es

Alain April
École de Technologie Supérieure
alain.april@etsmtl.ca

Abstract

For the software industry, legal risk management is a growing concern. In some cases it can be a serious threat to the commercial and financial success of software systems. Software engineers cannot find guidance on legal assurance, as it is not covered in the software best practice frameworks and international standards. Project Management standards, such as the Project Management Institute's PMBOK (Project Management Body of Knowledge), the Maturity models (MM) such as the CMMI and ISO/IEC 15504 and the international standards such as ISO/IEC 12207 do not currently offer explicit guidance for software engineers on the topic of legal assurance. This paper proposes extensions to the current international standards life-cycle processes and maturity models to add legal management processes targeted to provide guidance for the management of the legal risks associated with systems and software. A case study using these extensions is also presented. Our findings indicate that a formalized legal management process is a suitable way for helping companies in mitigating, diminishing or avoiding legal risks in software development projects.

1. Introduction

Risk analysis and management is a major issue for management and leadership standards [37], and particularly for information systems and software engineering [38] [39]. On the other hand the ever-increasing relevance of software systems in all economic and social sectors implies a growing importance of the legal implications related with the development, procurement and use of software systems [25]. Consequently, legal aspects are not only important with the end product, but they also need consideration during each activity performed through the software development lifecycle [1]. Although there is little published data about the cost of litigation in the software industry [28], there is a current perception – notable by the growing literature published recently on this topic – about the need to better manage the contractual and legal aspects during the software project lifecycle.

Figure 1 presents a number of legal concerns that software engineers should consider when planning the development of a new product that includes software.

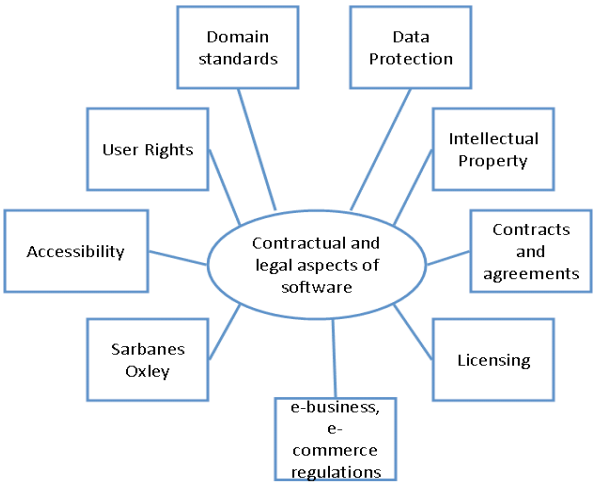

Figure 1. Legal concerns in software engineering

The legal concerns [26] detailed in Figure 1 can be summarized as follows:

- Data Protection. Regulations on the personal data protection when software systems are used to its treatment
- Intellectual Property. Regulation on the allocation of property rights on software
- Contracts and agreements. Regulation on the commercial transactions between developer and client/costumer
- Licensing. Legal aspects related with the license design and use
- E-business and e-commerce regulations. Regulation on market activity when ICT are used
- Sarbanes Oxley. Regulation on accounting duties and responsibility
- Accessibility. Regulation on accessibility duties in certain sectors as Public Administrations
- User Rights. Regulations and law protection of costumer rights
- Domain Standards law, such as web accessibility policies and regulations [36]

For example, some of these concerns arise with the use of Open Source Software (OSS), which is recognized by the Gartner Group as one of the five most important software engineering trends of the industry in 2005 [2]. When faced with using open source software components, the project manager is faced with a number of licensing options [3]; the Lesser General Public License (LGPL), the strong-copy left GNU General Public License (GPL) and the more permissive licenses such as the BSD licenses or the MIT Licenses. From a management and legal perspective, there are consequences with using one of these licences, for example, if the system software development is based on a viral license like the GPL, the final product must be licensed with the GPL, relevantly affecting its marketing in intellectual property terms [4-10].

Another sign of the growing importance of legal issues in software engineering is the growing number of regulations that are appearing in the industry. For example, the growing need to be compliant with Sarbanes-Oxley (SOX) Section 404 requirements [11] adds another legal concern to be considered by software engineers. A growing number of publications also describe the legal issues associated with compliance to ISO 9001 and maturity models such as the ISO/IEC 15504 and

the Capability Maturity Model Integration (CMMI) [12], (where 4 out of 6 of SOX control objectives are addressed by ML2 process areas [13][1]).

Thus, as the IT industry context grows more complex every year, managing the many legal concerns are becoming more and more important to management. The legal management process for software should be considered as being of increasing importance that, without adequate management, could increase the possibility of failure of a software product or at least present an unknown financial risk. However, current process and maturity models fail in providing an explicit support for legal issues proactively. The objective of this paper is to propose a legal management process, which would help in defining the legal conformance audit activities that could be performed as part of the quality assurance of a software project. This process could also be useful for software process assessment and improvement with the objective of minimizing potential litigation associated with software projects. The paper provides the definition of such a process and reports on a case study aimed at evaluating the potential usefulness of the proposed approach in a practical situation.

The rest of this paper is structured as follows. In Section 2, a summary of related work and models is provided. Then, Section 3 provides the description and rationale of the proposed legal management process. Section 4 presents the results of a case study conducted to assess the proposed approach. Finally, conclusions and outlook are provided in Section 5.

2. Related work

Legal concerns need to be considered within existing software engineering practice. Consequently, a first analysis was carried out to understand if it is taken into account in the current software engineering "maturity models" which proposes exemplary practices for the IT industry. An inventory of software engineering maturity models can be found in [15][2]. Looking at all the major maturity models, we have not found any explicit recommended practices on legal management. A second literature review took place in the area of risk management. Risk management and contract management is often concerned with legal issues [1]. We investigated more closely the risk maturity model literature. The first model investigated was INCOSE's Risk Management Maturity Model (RMMM) [16], which is based on the Crosby's Quality Management Maturity Grid [30]. This proposal presents a grid crossing four maturity levels (1: ad-hoc; 2-initial; 3-repeteable; 4-managed) and five dimensions (definition; culture; process; experience; application) where there is no mention of legal aspects of software. The next two risk maturity models investigated were: 1) the RMM - Enterprise Risk Management [17] and 2) the IACMM CMM [18] on contract management. Also in these two proposals we did not find any concepts of legal management.

With few guidance found, we proceeded with a third area of inquiry looking for the presence of explicit legal guidance in project management literature. Looking at project management maturity models such as: Portfolio-Programme-Project Maturity Model (P3M3) [19], Prince2 Maturity Model (P2MM) [20] and PMI Organizational Project Management Maturity Model (OPM3) [21], we could not find explicit legal management topics.

Finally, our literature review looked at the most important software process assessment and improvement models such as the Capability Maturity Model Integration (CMMI) [14] ISO/IEC standards on process models (12207 for System and Software Engineering [22] and 15288 for Systems Engineering [23]) and the related assessment model provided by the 15504 series [24], and the Software Maintenance Maturity Model (S3M) [15]. We can report that none explicitly include specific practices targeted to adequately manage legal issues. However, recently we see encouraging signs of change where both the SEI and ISO/IEC process models propose a new group of processes, called "Acquisition" that is introducing some legal concerns:

---

[1] The four control categories covered are: Change Control process, Emergency Changes, Project Life Cycle, Testing, while "Application Logical Access Control" and "Access Administration Control" are not covered by CMMI.

[2] See also http://www.semq.eu/leng/proimpsw.htm.

- in the ISO/IEC 15504 process exemplar model is composed by five processes (ACQ.x)[3], introduced with the two amendments dated 2002 and 2004, now recently incorporated into ISO 12207:2008;
- in CMMI, a new constellation (CMMI-ACQ [31]) was released on November 2007, including five processes inserted between the existing processes ML2 and ML3[4].

In both cases such practices are presented from an acquirer's perspective, while our objective in this research is to propose legal guidance for the project manager during planning and construction of software and systems. Looking more closely at the ISO/IEC 15504-5:2006 [24] practices, it is possible to find scattered mentions of contractual and legal issues in the:

- *Acquisition group processes* (ACQ) (e.g. for the collaboration with other companies or the acquisition of software product to be re-engineered, etc.)
- *Requirement Elicitation* (ENG.1) process,(e.g. for the implicit or explicit requirement to manage all possible legal implication in working on a software project);
- *Risk Management* (MAN.5) process (e.g. for the project management risks associated with the improper management of legal issues and for the need to take it into account in re-planning/ monitoring during the project lifecycle).

Also quite recently we have found other maturity models starting to address legal issues. The automotive SPICE recently proposed a legal and administrative requirements process group. The process proposed in this paper differs in its scope, location in the maturity model and execution steps. The main differences with the automotive SPICE proposal are:

- *Scope of the process*. The scope chosen for legal concerns in automotive SPICE aims at fulfilling the legalities in contracts, while this paper proposal includes legal activities across the product life cycle. The proposed approach aims at protecting also the rights outside the organization (i.e. competitors, public, etc.)
- *Location of the process within the model*. Automotive SPICE located its legal process in a process group named ACQ. This location means affecting mainly the supplier-customer area. This paper proposal locates the legal concerns in a management process (MAN) therefore affecting any activity in the product development, maintenance/evolution and operation.
- *Legal activities execution steps*. In automotive SPICE the legal activities are executed mainly when supplier-customer interactions are performed, that is, generally at the beginning of the product life cycle. Legal activities and measures proposed in this paper are to be carried out throughout the whole product life cycle.

Legal concerns are better incorporated into management processes due to the following reasons:

- Legal assurance typically implies practices that may be used by anyone who manages any type of project or process within a software life cycle. The legal issues, in organizations, are addressed by specialized staff and sometimes only by project managers. It is their responsibility to identify the legal risks and to put in place mitigation measures to avoid possible future sanctions or legal claims;
- Similar to risk management, legal concerns need to be assessed and mitigated throughout the whole product life cycle, from the planning phases and requirements capture to maintenance/evolution and operation activities.

---

[3] ACQ.1: Acquisition Preparation; ACQ.2: Supplier Selection; ACQ.3: Contract Agreement; ACQ.4 : Supplier Monitoring ; ACQ.5 : Customer Acceptance.

[4] ML2: Agreement Management (AM); Acquisition Requirements Development (ARD). ML3: Acquisition Technical Management (ATM); Acquisition Validation (AVAL); Acquisition Verification (AVER).

However, it is debatable when and how legal activities should be conducted during the life-cycle phases of a software development or maintenance project, and further research is needed to confirm a consensus and best practices in this area. Legal activities highly depend on the managers' perception of risks. Currently, legal activities typically consists of performing a due diligence or legal audit before marketing the final software product. Our findings confirm that legal risks are currently handled reactively instead of proactively. This leaves the topic mostly unexplored and without guidance that can be readily used by software engineers and project managers.

3. A proposal for a legal management process

In order to properly address all legal aspects of a software project throughout its development lifecycle, organizations will need to define and use a legal management process. An example of such a legal management process, based on SOX conformance, was presented in [29]. Such a process should take into account legal risks identified by the project, and assess the conformance and actions that are actually adopted to avoid or minimize such risks at each phase of the lifecycle.

First, at a high level, we identify the link between this proposed legal management process with ISO/IEC 12207 requirement stated in clause **6.4.1.3.2.3 '***The project shall define a representative set of activity sequences to identify all required services that correspond to anticipated operational and support scenarios and environments*'. It is important that we can link the proposed legal management process with the software engineering life cycle standard. Further more, our proposal for a legal management process consists of 6 items:

1. **Process identification**: The legal management process would be assigned the next available management process number (MAN.7) in ISO/IEC 15504. We have chosen this category because the management process category consists of processes that contain practices of a generic nature that may be used by anyone who manages any type of project or process within a software life cycle;
2**. Process name**: We propose to name this new process 'Legal Management' to reflect the need to plan, define, delegate and conduct surveillance of the legal issues of a software project. These are key management activities;
3. **Process purpose definition**: The legal management process area would have the following purpose:

"To deal with the possible legal issues arising in the software lifecycle, establish a protection strategy, measuring the legal exposure and conducting appropriate actions in order to prevent or avoid litigations or legal penalties";

4. Define **process outcomes**: as in ISO/IEC 15504-1 [24], they must be 'an observable result of the successful implementation of a process'. For each base practice (*see item 5*) defined, a list of outcomes would be proposed;
5. Propose **a set of base practices** and specify the requirements, the design, and the behaviour and other characteristics of the process to ensure it is comprehensive, precise and verifiable;
6. Propose **quantitative practices** to measure the extent to which the legal management recommended practices are implemented in the project[5].

Concepts leading to this process has been initially presented and described in [25][26][27] being developed and evaluated in this work by using an action research study. The specific objectives in this paper are:

- to present an overview of the legal management process (using an ISO/IEC 15504-like architecture), and;
- to detail the MAN.7 set of base practices and guidance to measure them.

[5] This last step will be implemented in a next future work, after the proposed process will be revised and more stable.

- to report on a case study research in which the processes and practices proposed have been put into practice.

The initial action research carried out provides an initial evaluation of the applicability of the practices and highlights pitfalls that may be found in other applications of the processes.

3.1. Elements to be mapped in the ISO/IEC 15504 language

In [25][26] an initial proposal for a legal process was formulated in a free-style manner, starting from the initial assumptions and then focusing on its description and finally proposing a way to quantify and measure the "legal risk" at each phase of a software project.

In the following sections the formulation for the proposed legal assurance process group is presented, focusing on the two key dimensions addressed by a maturity model: 1) the process dimension and 2) the capability dimension. Because the new ISO/IEC 12207 has numerous categories of life-cycle processes we will focus our description on the software implementation processes only.

3.2. Process Dimension: Base Practices (BP)

This section of the paper describes the MAN.7 process base practices using the ISO/IEC 15504 architecture.

In current industrial environments, a major differential factor between companies is their ability to create and commercialize knowledge [10]. This is a strategic ability especially in the software market due to the intangible nature of software products and its associated intellectual properties. As a result, a proper protection of these assets is a key element in the management of software organizations. Taking into account a strategy to manage legal issues will generate and optimize business opportunities in the areas described in the next base practices (BP). The first two BP face the process motivation and targets: for this reason in the following a more detailed description has been provided. The remaining BPs (BP.3 to BP.8), that essentially contain specific legal assurance measures, are sketched in Table 1.

MAN.7.BP1 Define the objectives for the Legal Management process

An inexistent or inadequate legal protection can reduce or even eliminate the commercial life of a software product. A successfully commercial product will generate clones that will be commercialized at a much lower cost avoiding development costs. It is therefore required to clearly define the objectives for a legal assurance process aligned with the organizational goals and policies. Objective of this practice is to verify the existence of a legal assurance process within the organization, in order to properly manage legal issues the organization has to deal with.

Sub-practices:
- Establish the legal assurance scope;
- Define the legal assurance measures according with the software lifecycle and specifications.

Outcomes:
- Legal assurance plan is established;
- Software development process is properly protected in legal terms

MAN.7.BP2 Reduce or minimize risks for the Legal Management process

A proactive and all-encompassing management of legal risk is a key aspect to project success, e.g. an adequate intellectual property protection will provide a powerful financial instrument that can be used to: guarantee credit applications; attract venture capital, or even and/or apply for government benefits and grants for Research and Development (R&D). As in the logic of a scorecard approach, part of financial resources obtained from the last fiscal year should be reinvested in the processes allocated in the so-called "Learning & Growth" perspective, related to innovation & infrastructure and people-related processes. Objective of this practice is the verification of the organizational capability to achieve this goal during time.

Sub-practices:

- State available legal assurance activities;
- Perform a descriptive analysis of previously defined activities;
- Establish the legal assurance measures in concrete points within the product life cycle.

Outcomes:

- Software product is respectful with Intellectual Property of others companies;
- Software product is properly developed, in terms of staff involved, staff contracts and IP agreements which protect it against staff claims. Risk of reclamation is assessed.

In addition to the possibility of maximizing business opportunities, the proposed legal management process aim to reduce risks or potential threats derived from the failure to comply with the law or inadequate conformance to legal regulations. Such threats, if not addressed, can lead to litigation from third parties, economic sanctions from governments/local authorities, and even penal actions. The problem of organizing legal assurance activities within the software implementation processes is not a trivial process because specific quality assurance activities aimed at assessing the legal compliance must be applied at the right phase, i.e., the efficiency of legal assurance activities depends on applying the right action at the right time.

Therefore, it is not enough to perform legal audits or due diligence once the project has been moved to its maintenance. In the case of performing ordinary legal audits before launching a product, it is possible to find potential threats that force modifications of certain aspects of the project; usually such unplanned modifications are very expensive or cannot be performed without delaying the product delivery. E.g. in software with dedicated functionality to the personal data processing, the in-force law requires to implement systems for the protection and integrity of such data. If this is detected in a final legal audit, the software must be modified to include the above security measures. XXX

In addition to the identification and incorporation of legal assurance activities in each phase of the project, the management of these activities will be greatly improved if supported by a process that includes legal exposure measurements (from a quantitative point of view) about the protection level required and attained at each phase of the software project.

Next table summarizes in a SPICE-like style the above-mentioned elements for the definition and description of the candidate MAN.7 process.

Table 1. MAN.7 process

Process ID	MAN.7
Process	Legal Management

Name	
Process Purpose	The purpose of the Legal Management process is to deal with the possible legal issues arising in the project lifetime, establish a protection strategy, measuring the legal exposure and conducting appropriate actions in order to prevent or avoid litigations or legal penalties.
Process Outcomes	As a result of a successful implementation of the Legal Management process: 1) Legal assurance plan is established. 2) Software product is conform with in force law, especially data protection law, industrial property law, antitrust law, and e-business regulations, if a website is developed. 3) Software product is respectful with Intellectual Property of others companies. 4) Software product is properly developed, in terms of staff involved, staff contracts and IP agreements which protect it against staff claims. Risk of reclamation is assessed. 5) Software Intellectual property is registered and ready to be opposed against eventual infringements. 6) Software development contract is developed. Object of the software development contract is clearly-defined by means of the requirement document reinforced by means of the requirement document's signature. 7) Software is protected against illicit copies or piracy, the introduction of elements as innocuous code, bestow a relevant evidence against illicit copies upon the developer. 8) Software commercialization is regulated by means of licenses or default contracts.
Base Practices	**MAN.7.BP.1: Define the objectives for the Legal Management process**. Identify and define the objectives for a legal management process aligned with the organizational goals and policies. [Outcome: 1, 2] Sub-practices: ▪ Establish the legal assurance scope ▪ Define the legal assurance measures according with the software specifications
	MAN.7.BP.2: Reduce or minimize risks for the Legal Management process. Provide an adequate intellectual property protection by risk management. [Outcome: 3,4] Sub-practices: ▪ State available legal assurance activities; ▪ Perform a descriptive analysis of previously defined activities; ▪ Set temporally the legal assurance measures according with the product life cycle
	MAN.7.BP.3: Legal exposure at the implementation phase. After determining the scope and list of possible project legal threats, each must be assessed by the individuals responsible of such issues and obligations,

	verifying the presence of mandatory clauses in contracts and regulations. [Outcome: 5, 6,7] Sub-practices: ▪ Establish the rights and obligations by responsible personnel ▪ Establish the rights and obligations due by internal personnel ▪ Verify the presence of mandatory legal clauses on the software development contracts
	MAN.7.BP.4: **Legal exposure at the requirements phase.** An important step aims at defining of the scope of possible legal risks during the project life cycle. Moving from the project requirements, it is requested to find all possible explicit and implicit legal threats the project could express. [Outcome: 2, 3, 6] Sub-practices: ▪ Approve and sign the requirements in legal document/form; ▪ Verify the completeness and consistency of the requirement traceability document; ▪ Approve and sign the prototype document limiting their use.
	MAN.7.BP.5: Legal exposure at the architectural and detailed design phases. As a second step, the verification of collected elements against the applicable software licenses after the SRS is completed and before the Coding phase starts. This task represent an important step for quantifying the legal risk, if it would take place in the near future and therefore impacting on the project budget. [Outcome: 6] Sub-practices: ▪ Verify and ensure the compliance to all the applicable software licenses; ▪ Verify and ensure the performance of personnel data protection regulation.
	MAN.7.BP.6: Legal exposure at the construction phase. During the coding phase, it is requested an analysis of the source code produced by the organization, paying attention to the elements produced/incorporated within the software solution, as meta-tags or other DRM-related issues. [Outcome: 2, 6, 7] Sub-practices: ▪ Ensure intellectual property rights for the product ▪ Verify the legal conformance of incorporated web elements
	MAN.7.BP.7: Legal exposure at the integration and qualification testing phase. During the Test and Release phase, the accompanying actions requested on the legal side will face the duties for an eventual registration of the software product, according to kind of license established between the parties as well as the licensing documentation to be provided to the customer at the release. [Outcome: 5, 8] Sub-practices:

	▪ Ensure the software improvements intellectual property rights : aplication form copyrights, patents, notarial deposit ▪ Write the licensing document and a template for the acceptance of the delivered product
	MAN.7.BP.8: Legal exposure at the Maintenance phase. the maintenance phase will require an update on a regularly basis of the legal assurance on the current contracts. [Outcome: 8] Sub-practices: ▪ Software maintenance is regulated; ▪ Proper SLA terms are established. ▪ Software intellectual property rights are assured and improvements are developed (new functionality or adaptation of the existent).

Table 2. MAN.7 associated work products

Work Products	
Inputs	**Outputs**
Project Plan and Life Cycle model (outcome 1)	Legal Assurance Plan (outcome 1)
Human resource management plan and supplier selection (outcome 4)	Contracts and agreements with responsible, internal personnel and staff working for subcontractors (outcome 4)
Agreements with the client and high level's software specifications (outcome 6)	Contract Software Development Sketch (outcome 6)
Requirement specification (outcome 6)	Signed Requirement Specification (outcome 6)
Signed Requirement Specification (outcome 6)	Development contract adding Signed Requirement Specification (outcome 6)
Prototype design (outcome 6)	Prototype Document (outcome 6)
Licenses used in the development (outcome 3)	Obligations and liabilities Licenses report (outcome 3)
Software functionality document (outcome 6)	Obligations on data protection law report (outcome 2)
Low level software design and source code (outcome 7)	Low level software design including stenography (outcome 7)
Graphical design and Low and high level design (outcome 7)	Legal Web Report (outcome 2)
Requirement specification, Low and high level design (outcome 7)	Applications form to register Intellectual Property rights (copyrights, patents, register into notary...) (outcome 5)
Commercialization policy (outcome 8)	Licenses and default contracts to the software commercialization (outcome 8)
Installation and maintenance plan (outcome 8)	Maintenance contract (outcome 8)
Maintenance strategy (outcome 8)	SLA contract (outcome 8)
Improvement software design and source	

code (outcome 8)	

4. Case study

In order to apply the proposed Legal Management Process in a real business setting and get an initial evaluation, an action research project was conducted, linking theory and practice. The procedures followed are in the form of process consultation [32], and the main elements of action research practice were considered explicitly [33].

The action research study was based in a Researcher–Client Agreement (RCA) using an iterative approach, where mutual behaviour and responsibilities was established and the research methodology was detailed. The research setting involved two teams, a software and telecommunications services company (Telecom Solutions S.L.) with registered address in Madrid (Spain), and a researcher team integrated by members of four universities. Telecom Solutions had undergone a failed attempt to manage legal risk in a previous software development project and for the company was seeking for a process to avoid or minimize such kind of risk was a key target.

Five phases were set up to conduct the action research [33]: Project Infrastructure, Intervention Diagnosis, Action Planing, Action Taking and Outcomes Analysis, as showed in Figure 2.

Figure 2. Action Research Phases

Project Infrastructure

The project Infrastructure was supported in three key elements:

1. A formal group composed of researchers and company staff:
   - Researchers: The team included an experienced team leader (LT); a researcher with a strong practical background in the application area (Legal Risk Management and software development project) and a researcher expert (RE) in software engineering management as senior consultant.
   - Company Staff: Later the team expanded to include the Chief Operating Officer (COO), the Project Manager (PM) a programmer analyst (PA) and the in-house attorney.
2. A communication plan structured in:
   - Scheduled Communication, with a General Meeting to start the action research in order to se up the action planning. A Phase Meetings starting each project stages, in order to organize the legal assurance actions, a week meeting to resolve incidental issues and, at the end of the action research project, past the first year of software running, a Final Meeting to the outcome analysis.
   - Express Communication. Supported in e-mail and mobile phone to resolve pressing troubles
3. The action plan described further

Intervention Diagnosis

The initial diagnosis discovered that previous software projects were deeply exposed to risks by the inexistence to proactively address legal risks. Legal concerns (see figure 1) were not considered in this project management activities: the company staff reported intellectual property infringements, in a previous project, related with the use of a GPL license. This project required external legal consultancy in a reactive way, with high economic impact in order to address this legal issue. Following this incident, the management team closely attended the need to establish a proactive and institutionalized legal risk management process for software projects.

The management team realized quickly that there were very practical problems to be address for software projects in this area: first, there were no trained or experienced attorneys in the company and second the current process was ad hoc.

As a result of this initial diagnosis, the management team focused on addressing the lack of legal risk management process in order to obtain the following benefits:

4. A proactive management of legal issues;
5. A legal risk management strongly connected to general management of the project linking legal risk and software life cycle;
6. A legal risk management process fully institutionalized.

Action Planning

The action plan consisted in a trial application of the Legal Management Process presented above in a new software development project: a VoIP Billing Solution (BillVoiP), taking the project lifecycle as the backbone of the process, as showed in Table 1. The action plan was detailed in the Legal Assurance Plan, with the following key goals:

Goal 1. Identify and define the process objectives (BP1)
Goal 2. Identify and define the project lifecycle phases
Goal 3. Identify and define the required legal assurance activities in each phase, in order to identify legal risk (BP2)
Goal 4. Identify and take legal measures to avoid o minimize identified legal risk (BP2)
Goal 5. Hold in check Legal risk materialization during the first year of software running
Goal 6. Outcome Analysis

In order to establish the action planning goals described, were linked with Project Infrastructure as summarized in Table 3.

Goals	Meeting	Researcher Members	Company Members
Goal 1	General Meeting	TL and SC	COO, PM and PA
Goal 2	General Meeting	TL and SC	COO, PM and PA
Goal 3	Phase Meetings	TL and SC	PM and PA
Goal 4	Phase Meetings	TL and SC	PM and PA
Goal 5	Express Communication	TL and SC	PM and PA
Goal 6	Final Meeting	TL and SC	COO, PM and PA

Table 3. Action Planing Goals

The action planning resulted in the Legal Assurance Plan (Process Outcome 1)

Action Taking

Goal 1 and 2 were established in a general meeting. The process objectives were identified and defined. The implantation of a Legal Risk Management Process followed to deal with the possible legal issues arising in the software lifecycle. This established a strategy protection, measuring the legal exposure and conducting appropriate actions in order to prevent or avoid litigations or legal penalties. The existing software project lifecycle was structured using the following five stages sequentially: Project Planning, Requirements Elicitation, Design, Construction, Integration and Testing. The legal risks of the maintenance phase were not addressed in this research. Accordingly five phase meetings (legal reviews) were required. Each of these meeting was planned at the end of each phase in order to prepare the Legal Management Process activities for the next one.

The Legal Management Process was applied to each phase and as a result the legal risks were identified early. Accordingly the base practices of the model were recommended and, outcomes and work products were generated. Table 4 summarize the work produced by the team.

Phase	Identified Risk	Process Base Practice	Process Outcome	Associated Work Product
Project Planning	Human resources claims by inadequate contracts	BP3: New contracts	Outcome 4	Contracts and agreements with responsible, internal personnel and staff working for subcontractors
Requirements Elicitation	No Legal Risk	N/A	N/A	N/A
Design	Use of a dualLicense	BP5: Verify and ensure the compliance to all the applicable software licenses	Outcome 3	Obligations and liabilities Licenses report
	Personal data processing	BP5: Verify and ensure the performance of personnel data protection regulation	Outcome 2	Obligations on data protection law report
Construction	Source-code piracy	BP6: Ensure intellectual property rights	Outcome 7	Low level software design including stenography
Integration and Testing	Source-code piracy	BP7: Ensure the software intellectual property rights	Outcome 7	Applications form to register Intellectual Property rights

Table 4. Legal Management Process Application

Detailing the information presented in table 4, the major risks identified and corresponding management actions were:

- Human resources issued inadequate contracts. As a result of an audit of the HR project contracts, two inadequate contracts were detected. Two existing employees who were to be

involved in the project as developers were hired as administrative assistants, not as developers. A conversion of these contracts was recommended.

- Use of a dual License: The software development project used the *Asterisk* open-source software [34] as its basis. *Asterisk* is a software implementation of a telephone private branch exchange (PBX) released under a complex legal model: A GPL for non-commercial aim, and a proprietary license in case of proprietary distribution. In the Licenses Report the main economic duties, and responsibilities were located, emphasizing the obligation to release the BillVoiP software under a GPL license for domestic distribution and, in particular, the obligation to pay royalties in the event of a future commercial distribution.

- Personnel data processing: The BillVoIP´s functionality included personal data. The system allows storage of data from customer calls: callers' identification and date, time and duration of the call. Such personal data is considered baseline data for the current regulations in Spain. Based on this consideration the legal requirements were identified in two stages: Requirements in the development stage involving the obligation to implement identification and authentication functionality for user, and requirements in the operational phase consisting of declaring the personal data files to the Regulatory Agency.

- Source-code piracy: Piracy is an endemic risk for any software development project [35]. In order to minimize the source-code piracy risks, two measures were recommended to protect and ensure intellectual property of BillVoIP: Stenography based on Digital Watermarking, including relevant information about the copyright: owner, year and license. The second measure recommended to formally register the software to the Intellectual Property Office.

Outcomes Analysis and Lessons Learned

The initial outcome resulted in a number of concrete actions that effectively reduce the risk exposure of the project. In the Final Meeting the outcome analysis was performed. Final Meeting consisted of a standardized interview supported on four key open questions on different parameters, focused on checking if the process purpose was reached. The meeting results can be summarized as follows:

Parameter	Question	Results
Process Capability	Do you consider that Legal Risk Management Process has reduced the legal risks exposure of BillVoIP project?	Managers felt that the process is a strategic tool to manage legal risks
Process failures, weakness, and improvement opportunities	Have you identified any failure or weakness of the process?, What about a improvement opportunity?	No Failures Weakness: the need of a in-house attorney with a strong practical background improvement opportunities: A software to support the process
Process performance	Has a legal risk materialized during the first year of BillVoIP operation?	No legal risk aroused in the first year
Process future	Does the process of legal risk management will be institutionalized and implemented in the next software development projects?	The company´s management were positively satisfied and motivated to institutionalize Legal Risk Management Process.

WinuE 11-4-5 17:17
Deleted:

Table 5. Final Meeting

Also, we found that the results of technical processes were also significant. Legal risks were identified and actions for a proactive management were proposed and were executed. The Final outcome was successful likewise. A review of the project after more than a year since the end of the project showed that no legal issues have occurred, and the company has decided to deploy the Legal Management Process in all future projects.

In general terms the company came to terms with the importance of a proactive legal risk management in software projects, and the need of a standardized process. Particularly the company validated how Legal Risk Management Process can be a suitable tool to avoid or minimize legal risks in software development projects, linking legal risk management with software development lifecycle. On the other hand, researchers have a strong indication that the proposed process achieves the purposed it was defined for. It also confirmed that combining maturity models and legal management is a successful way to deal with legal issues in software development projects.

on the other hand the need for a good in-house attorney with a strong practical background; a scarce and expensive professional profile was observed.

5. Conclusions

The research results, presented in this paper, aim at improving the management of legal issues in the ICT industry. In order to achieve this goal, we proposed to manage legal issues adding a new process in ISO/IEC 15504 software process assessment and improvement model.

This new process proposes a series of legal assessment activities to be included within the software project lifecycle. In order to structure legal risk assessment activities in a process model, the ISO 15504 process architecture has been used. The proposed process also included the main goals and practices for the new proposed MAN.7 process.

In order to evaluate the proposed approach, an action research project (case study) was conducted. The case study was based on a formal agreement between researchers and a company, and was structured in five stages. In the first stage, the project Infrastructure was established, defining the formal working group, the communication plan, and the project plan. During the Intervention Diagnosis stage, major organizational weaknesses and needs were identified; taking such inputs as a starting point, Action Planning was designed supported by six key goals. Actions to achieve such goals were taken in the Action Taking stage, where the execution of Legal Risk Process Management was conducted. Finally, in the Outcome Analysis stage, process capability, performance, weakness and future improvement were assessed.

The findings of the Action Research project validated the approach proposed in this research, confirming that connecting legal risk management and software project lifecycle using maturity models recommendations is an effective and efficient way to minimize or avoid legal risks in software development projects software.

Our next research objective will be to adapt the proposed process to others maturity models (like the CMMI and S3M, considering the lessons learned and, in particular, addressing the weaknesses and future improvements identified.

6. References

[1] R.J. Rejas-Muslera, J.J. Cuadrado-Gallego, and D. Rodríguez, "Defining a Legal Risk Management Strategy: Process, Legal Risk and Lifecycle", in Proceedings of the 14th European Conference on Software Process Improvement (EuroSPI 2007), Potsdam, Germany, September 26-28, 2007, Lecture Notes in Computer Science 4764 Springer 2007, pp. 118-123 , ISBN 978-3-540-74765-9

[2] D.W. Cearley, J. Fenn, D.C. Plummer, "Gartner's Positions on the Five Hottest IT Topics and Trends in 2005", Gartner, Publication Id. G00125868, 12 May 2005, URL: www.gartner.com/DisplayDocument?doc_cd=125868 {accessed 2009-12-22}

[3] FSF, Free Software Foundation – Licenses, URL: www.fsf.org/licensing/licenses/ {accessed 2009-12-22}

[4] R.J. Rejas-Muslera, J.J. Cuadrado-Gallego, J. Dolado, and D. Rodríguez, "The open source software vs. proprietary software debate and its impact on technological innovation", *Upgrade* [Online]. *6(5)*, October 2005, pp.35-39. ISSN: 1684-5285. URL: www.upgrade-cepis.org/issues/2005/5/upgrade-vol-VI-5.html {accessed 2009-12-22}

[5] Olliance Group, "2007 Open Source Think Tank: The Future of Commercial Open Source", Executive Summary Report, URL: http://web.archive.org/web/*/http://thinktank.olliancegroup.com/ostt2007report.pdf {2009-12-26}

[6] J. Urban, "Legal Uncertainty in Free and Open Source Software and the Political Response", from The Politics of Open Source Adoption (POSA), version 1.0, Social Science Research Council (SSRC), Eds: Karaganis J. & Latharn R., May 2005, pp. 68-82, URL: http://www.ssrc.org/wiki/posa/ {accessed 2009-12-22}

[7] J. Haislmaier, C. Hamley and A. Cohn, "Open Source License Enforcement Actions. What you can expect when there is a knock on you door", Presentation, May 23 2007, URL: www.hro.com/resources/custom/publications/HRO%20Publications/opensourceppt.pdf {2009-12-05}

[8] K. Moyle, "Total Cost of Ownership and Open Source Software", Research Paper, July 2004, Dept. of Education and Children's Services (DECS), Government of South Australia, URL: www.curriculum.edu.au/verve/_resources/total_cost_op.pdf {2009-12-05}

[9] O. Tazi, "A Practical Strategy for Leveraging Open Source", Presentation, ObjectWebCon2006, 5th ObjectWeb Annual Conference, January 31 February 2 2006, Paris (France), URL: objectwebcon06.objectweb.org/xwiki/bin/download/Main/DetailedSession/O-Tazi.pdf {accessed 2009-12-22}

[10] WIPO, Records of the Intellectual Property Conference of Stockholm (Stockholm, June 11 to July 14, 1967), Volume II, pp. 283-330, URL: http://www.oup.com/uk/booksites/content/9780198259466/15550029 {2009-12-05}

[11] Sarbanes-Oxley Act, January 23 2002, URL: http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf {2009-12-05}

[12] L. Janssens, "Auditing CMMI Maturity and Sarbanes-Oxley Compliance", ISACA Journal Online, 2007, Vol.3, URL:

http://www.isaca.org/Template.cfm?Section=JOnline&CONTENTID=35756&TEMPLATE=/ContentManagement/ContentDisplay.cfm {2009-12-26}

[13] J. Tower, "IB Technology Examples of CMMI Benefits", JP Morgan, version v1.4, August 2004, URL: www.sei.cmu.edu/library/assets/2004-CMMI-020.pdf {2009-12-05}

[14] CMMI PRODUCT TEAM, CMMI for Development, Version 1.2, CMMI-DEV v1.2, CMU/SEI-2006-TR-008, Technical Report, Software Engineering Institute, August 2006, URL: www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm {accessed 2009-12-22}

[15] A. April, A. Abran, *Software Maintenance Management: Evaluation and Continuous Improvement*, Wiley-IEEE, 2008, ISBN 978-0-470-14707-8, pp.313

[16] INCOSE, Risk Management Maturity Level Development, RMRP 2002-02, Version 1.0, April 2002, URL: www.pmi-switzerland.ch/fall05/riskmm.pdf {2009-12-05}

[17] RIMS, RIMS Risk Maturity Model (RMM) for Enterprise Risk Management, November 27 2006, URL: www.rims.org/RMM {accessed 2009-12-22}

[18] IACCM, IACCM Capability Maturity Model, August 2007, URL: http://www.iaccm.com/maturity/index.php {accessed 2009-12-22}

[19] OGC, Portfolio, Programme & Project Management Maturity Model (P3M3), version 1.0, February 1, 2006, URL: www.ogc.gov.uk/documents/p3m3.pdf {2009-12-05}

[20] OGC, Prince2 Maturity Model (P2MM), v1.0, March 2006, URL: www.ogc.gov.uk/documents/PRINCE2_Maturity_Model_Version_1.pdf , 2006. {2009-12-05}

[21] PMI, Organization Project Management Maturity Model (OPM3), Project Management Institute, URL: http://opm3online.pmi.org/ {accessed 2009-12-22}

[22] ISO/IEC, IS 12207:2008 – Information Technology – Software Lifecycle Processes, International Organization for Standardization, Genève, March 18, 2008

[23] ISO/IEC, IS 15288:2008 – Systems Engineering – System Life Cycle Processes, International Organization for Standardization, Genève, March 18, 2008

[24] ISO/IEC 15504 - Information Technology - Software Process Assessment, Parts 1-6, 2003-2007, URL: www.isospice.com {accessed 2009-12-22}

[25] R.J. Rejas-Muslera, "Proceso De Gestión De Riesgos Legales Para Proyectos De Desarrollo De Software", Ph.D Thesis, Universidad de Alcalá, Departamento de Ciencias de la Computación, Madrid (Spain), May 2007.

[26] R.J. Rejas-Muslera, J.J., Cuadrado-Gallego, M.A. Sicilia, D. Rodríguez, "SLA: A legal assurance process model for software engineering Management", Software Process: Improvement and Practice (SPIP), Wiley & Sons, Vol.12, Issue 2, March-April 2007, pp.191-198.

[27] L. Buglione R.J. Rejas-Muslera, J.J. Cuadrado-Gallego, "Strengthening Maturity Levels by a Legal Assurance Process", Proceedings of EuroSPI2008, Dublin (Ireland), September 3-5 2008, ISBN 978-87-7398-150-4, pp. 11.25-11.35

[28] T. De Marco, T. Lister, “Both Sides Always Lose: Litigation of Software-Intensive Contracts”, Crosstalk, February 2000, URL: www.stsc.hill.af.mil/crosstalk/2000/02/demarco.html {accessed 2009-12-26}

[29] A. April, R. Ouanouki, “IT Process Conformance Measurement: A Sarbanes-Oxley Requirement”, 17th International Workshop on Software Measurement (IWSM/MENSURA 2007), Palma de Mallorca, Spain Nov 5-7, 2007, pp 26-37.

[30] P. Crosby, *Quality is Free*, McGraw-Hill, NY, 1979, ISBN 0070145121.

[31] CMMI PRODUCT TEAM, CMMI for Development, Version 1.2, CMMI-DEV v1.2, CMU/SEI-2006-TR-008, Technical Report, Software Engineering Institute, August 2006, URL: www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm {accessed 2010-12-22}

[32] Baskerville, R. and A. T. Wood-Harper. (1998) "Diversity in Information Systems Action Research Methods" European Journal of Information Systems, (7) 2, pp. 90-107.

[33] Davison, R. Martinsons, M. and Kock, N. (2004) “Principles of canonical action research” Information Systems Journal, 14 pp. 65-86

[34] Asterisk Open Source Software Communications. URL: http://www.asterisk.org/ {accessed 2010-01-22}

[35] Seventh Annual BSA and IDC Global Software Piracy Study. Business Software Alliance, November 2010, URL http://www.bsa.org/globalstudy {accessed 2011-01-22}

[36] Web Content Accessibility Guidelines (WCAG). Web Accessibility Initiative (WAI) , URL: http://www.w3.org/WAI/intro/wcag {accessed 2010-02-22}

[37] ISO. ISO 31000 – Risk management. URL: http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/risk_management.htm {accessed 2011-01-22}

[38] Charette, R. “Software Engineering Risk Analysis And Management” (1992). Computer Standards & Interfaces, Elsevier Vol.14, Issue 2, pp 180

[39] David C. Chou, Amy Y. Chou, “Information Systems Outsourcing Life Cycle And Risks Analysis”. Computer Standards & Interfaces, Elsevier, Vol. 31, Issue 5, pp 1036-1043

WinuE 11-4-4 18:53
Formatted: a, Font:(Default) Arial, 11 pt, English (UK)

Unknown
Field Code Changed

WinuE 11-4-5 17:01
Formatted: a

Unknown
Field Code Changed

WinuE 11-4-5 17:01
Formatted: a

WinuE 11-4-4 18:04
Deleted:

6. Appendix A: List of Acronyms

ACQ	Acquisition group processes (in ISO 15504)
BSD	Berkley Software Distribution
CMMI	Capability Maturity Model Integration
CMMI-ACQ	CMMI for Acquisition
CMMI-DEV	CMMI for Development
COTS	Commercial Off The Shelf software
DRM	Digital Rights Management
ENG	Engineering process group (in ISO 15504)
FSF	Free Software Foundation
GNU	General Public Licence
GP	General Practice
GPL	General Public License
IACMM	International Association for Contract & Commercial Management membership
IEC	International Electrotechnical Commission
ISO	International Standard Organization
LGPL	Lesser GPL
MAN.7	(proposed) Legal Management Process
MIT	Massachusetts Institute of Technology
ML	Maturity Level [where MLx stands for Maturity Level x]
MM	Maturity Model
OPM3	Organizational Project Management Maturity Model
OSS	Open Source Software
P2MM	Prince2 Maturity Model
P3M3	Portfolio, Programme and Project Management Maturity Model
PA	Process Area
PMBOK	Project Management Body of Knowledge
RMMM	Risk Management Maturity Model
R&D	Research & Development
SEI	Software Engineering Institute
SG	Specific Goal
SL	Service Level
SLA	Service Level Agreement
SLAP	Software Legal Assurance Percentage
SDLC	Software Development Life Cycle
SOX	Sarbanes-Oxley
SP	Specific Practice
SPICE	Software Process Improvement Capability dEtermination (ISO/IEC 15504)

S3M	Software Maintenance Maturity Model
UR	User Requirement