THE LEGAL AUDIT PROCESS IN THE SOFTWARE DEVELOPMENT LIFECYCLE: A WAY TO MANAGE LEGAL RISKS IN SOFTWARE PROJECTS

Ricardo Rejas

Universidad Francisco de Vitoria
Ctra. Pozuelo-Majadahonda Km. 1,8
28223 Pozuelo de Alarcón,
Madrid, Spain

J. J. Cuadrado-Gallego

Universidad de Alcalá
Ctra. de Barcelona, Km. 31,7
28805 - Alcalá de Henares
Madrid, Spain

D. Rodríguez

Dept of Comp Science
The University of Reading
Reading RG6 6AY
UK

Abstract

All systems during their lifecycle, no matter how simple, will generate legal implications that need to be managed. The potential cost of an inadequate management of legal aspects can even imply the failure of the project. As a consequence, legal risk management should not only be a major activity of the development lifecycle, but it needs to be performed by qualified personnel following well-defined procedures and standards. However, current software process improvement models neglect processes to handle the legal aspects inherent to all software systems.

This work presents a process for managing legal risks. It is organised by a series of activities to be performed at each stage of the software development lifecycle to eliminate or minimize the risk of project failures for legal reasons.

Key words: Legal Audit, Software Process, Software Systems, Legal Risks, CMMI, ISO 15504, Software Lifecycle.

1. INTRODUCCION

The ever increasing importance of software systems in all economic and social sectors implies an important increment of legal aspects in the software lifecycle.

An inadequate management of such risk can increment the possibility of failure of a project, for example, not having a clear ownership of the product when the product has been developed by a third-party, other cases can related to legal claims by third-parties or even public administrations.

The most important software process improvement and assessment models (CMMI – Capability Maturity Model Integration [1] – or ISO 15504 [2]) do not properly include processes for legal audits and more concretely legal risks management for each phase of the software development lifecycle. Only in CMMI, it is possible to find scattered mentions to contractual or legal aspects in the requirements section.

Neither in industry related to manage legal risks of software projects is possible to find well-defined and standardised projects. Activities performed in this area depend on the perception of the risk by management. Generally such activities do not follow any temporal pattern to systematically perform them but the most common activity consists of performing a *Due Diligence* or legal audit before marketing the product. This lack of standardised process means that legal risks are handled reactively instead of proactively.

This work presents legal audit activities to be performed as part of software process assessment and improvement models. The aim is to provide industry with a framework for efficiently manage legal risks inherent to all software projects. Such a framework allows us to move from a reactive risk strategy to a proactive one.

The organisation of the paper is as follows. Section 2 identifies the most common legal risks involving software projects. In Section 3 is analysed, on the one hand, how risks are treated by major software assessment and improvement processes, and on the other hand, how those are actually managed in industry. Section 4 provides an standardised framework for legal audits to manage legal risks. Finally, Section 5 concludes the paper and future work is outlined.

2. LEGAL RISKS FOR SOFTWARE PROJECTS

With the aim of providing a high level view of legal risks and not being completely exhaustive (a comprehensive coverage of all risks is impossible), we provide a Web project as an example. In such type of project, we could find legal risk in the following areas:

2.1 Intellectual Property Area

The design and development of a Web site needs protection in two different ways:

1. As a graphical representation, it is an artistic creation and therefore, it is protected by royalties.

2. As a computer program. it contains source code, e.g., XML HTML, Visual Basic JavaScript, etc. that are also protected by intellectual property rights.

In this area, there are two groups of legal risks:

1. Legal Risks related to the ownership of the product. Deficiencies or the lack of a proper contract with developers can generate claims about its ownership.

2. Legal risks related to the infringement of a third party intellectual property. On the one hand, a Web site can include content or design developed by a third party with their rights. Not acting with caution and ignoring audits to check such infringements can generate legal claims involving expensive settlements and even penal offences.

2.2 Aspects related to current regulations

Designs and contents included in a Web site can violate a large number of juridical regulations designed to protect all kind of activities related to the Web. This can generate legal claims by third parties or penalties by public administration with fines, expedients or even penal actions. These risks can be classified in the following areas:

1. Related to the publication of products or services via Web with the infringement of:

    a. Regulations about advertising.
    b. Regulations about users' rights.
    c. Trading standards
    d. Intellectual property rights

2. In the commercialization of products or services, it is possible the infringement of:

    a. Regulations about electronic business.
    b. General legislations about contracts.
    c. User's rights and obligations

3. In relation data protection, i.e., to how user's personal data are used and treated.

4. In relation to services properly registered, i.e., certain service providing sites must be registered properly by public administrations to carry out the intended business. Not doing so can generate penalties form public administration bodies.

5. Some Web sites and specially those that belong to public administrations must comply with certain level of accessibility defined by the W3C [13] or the European Union.

The previous points highlight the fact of the variety and large possible risks that must be considered when carrying out a software project. Some of those are serious risks that need to be managed properly to avoid the failure of the project.

3. RISK MANAGEMENT IN SOFTWARE PROCESS ASSESSMENT AND IMPROVEMENT MODELS

After commenting the seriousness and importance of a proper management of legal risks in a software project, it is of paramount importance to have procedures and

activities defined beforehand to minimize or eliminate such risks. We now analyse how those activities are taken into account by the most important assessment and improvement models, and in particular those related to software engineering. In this analysis we have taken into account the CMMI model [1].

After analysing the CMMI model, we concluded that there is no process area containing legal aspects in a systematic and organised way. There are, however, scattered references to legal aspects of the project mainly in relation to contractual rights and obligations. These references include:

1 Basic Management Process Area: The Supplier Agreement Management process area. This process area consider the assumption in which "*a product component is identified and the supplier who Hill produce it is selected , a supplier agreement is established and maintenance…", "The purpose of Supplier Agreement Management is to manage the acquisition of products from suppliers for which there exists a formal agreement."* and it includes as Specific Goal (SG1) *"Establish Supplier Agreements".*

2 Advanced Management Process Area: Project Management, Integrated Project Management for IPPD. The SG 2 Coordinate and Collaborate with Relevant Stakeholders in the SP 2.2-1 Manage Dependencies establish in its subpractice -4 point-: "*Review and get agreement on the commitments to address each critical dependency with the people responsible for providing the work product and the people receiving the work product".*

3 Advanced Management Process Area: Project Management, Integrated Supplier Management. The SG 2 Coordinate Work with Suppliers dedicate the SP 2.3-1 to *"Revise the Supplier Agreement or Relationship"*

4 Engineering, Requirements Management. The SG 1 Manage Requirements include in its points SP 1.1-1 and SP 1.2-2 to *"Obtain an Understanding of Requirements"* and *"Obtain commitment to Requirements"*, respectively.

4. A LEGAL RISK MANAGEMENT PROCESS

4.1. Setting up legal audits within the CMMI framework

The first step to consider as a process all activities to manage legal risks related to software projects consist of locating such a process in the CMMI scheme; more specifically, we need to define which of the Process Areas could include legal audits.

First, we need to define which category of the CMMI Process Areas (Process Management, Project Management, Engineering and Support) is the most appropriate. After analyzing the scope of each Process Area, we believe that the most suitable place to locate such activities is the Project Management area, as it is defined: "*Project Management process areas cover the project management activities related to planning, monitoring, and controlling the project*".

The process of legal audit is a set of activities related to both the planning and control of the project. Legal audits are related to planning as it must include activities and resources to minimize legal risks. More concretely, legal audits must include control activities; such activities need to control the legal aspects and avoid any risk during its life-cycle.

The next step, following the categories defined by CMMI v1.1, consists of locating the most suitable Process Area with within Project Management for the legal audits activities. The Process area Risk Management aim is "*to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives*."
According to this definition, the audit process must be integrated in the process area Risk Management; it complies with its aim, concretely, to identify potential legal problems before they occur. The legal activities and measures must be planned and invoked as needed across the life of the product or project to avoid or mitigate adverse legal impacts on achieving objectives.

Finally, with the objective of structuring the legal audit process in the Risk Management Process Area, it is necessary to divide it into 3 parts following the Introductory Notes:

- *Defining a legal risk management strategy*. It defines a legal audit process for legal risk management inherent to all software projects. A generic definition will consider two main issues: (i) the type of software to be developed because the activities will depend on it (for instance, we will need to carry out different activities depending on if the systems is an invoice system or a Web site); (ii) the software development lifecycle, as it is the cornerstone of all project activities and it will be necessary to locate the legal audit activities.
- *Identifying and analyzing legal risk.* For identifying and analysing the legal risks that can endanger a project, it is also necessary to take into account both the type of software to be developed in technical terms, i.e., its design and development, and its functionality, what the system is suppose to do. These considerations will allow us the identification and posterior analysis of the legal risk related to the project. With knowledge about the technical aspects, it will be possible to identify and associated legal risks, i.e., intellectual property. On the other hand, if we take into account its functionality, we will be able to identify legal risks derived from its use in the market or when the system is in production, for example, legal risks associated with current regulations.
- *Handling identified risk.* As a consequence of the risks that need to be managed, legal audits need to follow a structured process with omnipresence throughout the software development lifecycle. It cannot be an autonomous process but on the contrary, it needs to have relationships with other activities that need to be audited in a proactive way. In this way, once legal risks and the activities have been identified, it is needed to analyse the software development lifecycle, establish its phases and set the legal activities in the most appropriate place. For example, in a project where legal risks related the intellectual property have been identified as a result of subcontracting part of the product, the legal activities related to minimize such risk must be set up in the software lifecycle. In this case, those will be mainly contractual at the beginning of the project (planning) because once the product is being developed; the ownerships of the project can generate legal conflicts.

5. CONCLUSIONS AND FUTURE WORK

In all software projects, a proper management of legal activities is a key area for a successful project. It will mitigate legal risks associated to the project and also it will increment its quality (a project with legal or potential conflicts is a serious defect in terms of quality). However, the most important process improvement and assessment models such as (CMMI o ISO 15504) do not include legal audit processes to manage during the software development lifecycle legal activities. Neither, current practices in industry do manage such issues properly.

This work tries to provide a framework to minimize such risks within the software industry. It presents legal audit activates as an extra process to be implemented in the software assessment and improvement processes inherent to all software processes. Such a way of dealing with risk is a proactive way of instead of reactive. In the CMMI model, the legal audit process should be included as part of Project Management and more concretely, within the Risk Management area.

Future research work will be the detailed description of the audit process in terms of generic and specific goals. Also, the benefits of such audit process will need to be evaluated in a quantitative way.

ACKNOWLEDEMENTS

We would like to thank the Spanish Ministry of Science and Technology for supporting this research (Project CICYT TIN2004-06689-C03) and Prof Javier Dolado for his useful comments.

BIBLIOGRAPHY

1. CMMI-SE/SW/IPPD/SS, V1.1 Capability Maturity Model Integration. CMMISM for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing

2. SPICE – ISO 15504. Information Technology - Software Process Assessment

3. Directive 2001/84/EC of the European Parliament and of the Council on the Resale Right for the Benefit of the Author of an Original Work of Art

4. Directive 91/250/EEC of the European Parliament and of the Council on the legal protection of computer programs

5. WIPO International Forum on the Exercise and Management of Copyright and Neighboring Rights in the Face of the Challenges of Digital Technology. 1997

6. Directive 91/250/EEC of the European Parliament and of the Council relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising

7. Directive 98/6/EEC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers

8. Directive 97/7/EEC of the European Parliament and of the Council on the protection of consumers in respect of distance contracts

9. WIPO Intellectual Property Handbook: Policy, Law and Use.2004

10. Directive 2000/31 of the European Parliament and of the Council on certain legal aspects of information society services

11. Directive 97/66 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector

12. Directive 2002/58 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector

13. W3C World Wide Web Consortium. Web Site: http://www.w3c.org/