Defining a Legal Risk Management Strategy: 
Process, Legal Risk and Lifecycle 

Ricardo J. Rejas-Muslera\textsuperscript{1}, Juan. J. Cuadrado-Gallego\textsuperscript{2}, and Daniel Rodriguez\textsuperscript{2} 

\textsuperscript{1} Universidad Francisco de Vitoria 
\textsuperscript{2} Universidad de Alcalá 

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 do not properly include processes for legal audits and more concretely legal risks management for each phase of the software development lifecycle. Neither in industry related to manage legal risks of software projects is possible to find well-defined and standardised projects. This lack of standardised process means that legal risks are handled reactively instead of proactively. 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. 

Keywords: Legal Risk, Software Process, Software Systems, CMMI, ISO 15504, Software Lifecycle.

1 Introduction 

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 \cite{1} – or ISO 15504 \cite{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: