Introducing the Risk Grid

by Andrew Katz[a] and Shane Coughlan.[b]

(a) Moorcrofts LLP
(b) Opendawn Consulting

Abstract
A Special Interest Group of the European Legal Network discussed issues around the commercial procurement of Free/Open Source Software, and methods to reduce or contain risk in transactions related to the supply chain. The initial focus of this group was on creating generic contractual language for use by Customers when establishing a relationship with a Supplier. However, it quickly became apparent that for a true solution far more than generic contractual language was required. There needed to be a guidance document to contextualise the scope of potential issues and to describe the potential remedies available for both Customer and Supplier regardless of their relative experience in Free/Open Source Software. To do this the members of the Special Interest Group created the Risk Grid, a table designed to describe the different ways in which publicly available code could be infringed, with rows to separate out each instance, and with example wording to help in drafting procurement contracts for software projects which make use of Free/Open Source Software components.

Keywords
Law; information technology; Free and Open Source Software; Risk management, contract law,

Introducing The Risk Grid

In 2008 the European Legal Network founded a Special Interest Group to discuss the commercial procurement of Free/Open Source Software. The group initially focused on producing generic contractual language to minimise risk when sourcing code or products potentially involving such code. This was envisioned as text to be used by companies relatively knowledgeable in the field to regulate their relationships with suppliers. The implicit assumption – borne of market experience – was that suppliers might not adhere to Free/Open Source Software licence terms without explicit prompting from their customers.

While such an approach had its merits, it quickly became apparent that far more than generic contractual language was required. There needed to be a guidance document to contextualise the scope of potential issues and to describe the potential remedies available, and this document needed to be accessible to both the Customer and the Supplier irrespective of their relative experience in dealing with Free/Open Source Software. Andrew Katz, Malcolm Bain and Amanda Brock from the Special Interest Group began work on such a document, and created an overarching Risk Grid as a proposed solution to the problem.

The Risk Grid is envisioned as a document that describes various actions or risks involving software, and allocates each risk to the Customer and/or Supplier as appropriate. It is designed to describe the different ways in which publicly available code could be infringed, use table rows to separate out each instance, and provide example wording to help in drafting procurement contracts for software projects which make use of free/open source components. The assumption underlying the Risk Grid is that the best contracts are those which:

1. Explicitly identify the risks which arise from the transaction, and allocate those risks appropriately to the parties;

2. Recognise that risk can always be priced. However, the party generally best placed to bear the risk is the one which has control/knowledge of the circumstances giving rise to the risk and is therefore likely to be able to price it most appropriately. Indemnities are one appropriate mechanism for allocating risk;

3. Try to manage the expectations of the parties;

4. Are easy to understand.

The Special Interest Group focused on the areas which typically generate the most controversy in contract negotiation, and tried to encapsulate the arguments typically used by the supplier and the customer in relation to each area. Rather than being prescriptive, the Risk Grid suggests sample wording with various options to outline approaches that may be taken by either party. It is acknowledged that there cannot be a universal contract that will adequately provide for the requirements of a market where at one extreme there are software distributions being provided gratis and at the other there are bespoke management systems being built for specialised uses.

The Risk Grid is intended to assist with negotiation, and its utility extends beyond Free/Open Source Software. The document can equally assist in contextualising proprietary software transactions, or those where a mixture of Free/Open Source Software and proprietary software are involved. However, it is a work in progress and will by necessity be expanded and refined by those making use of it. Parties in different market segments and in various national jurisdictions may require quite substantial additions to ensure relevance. For example, in some jurisdictions, there is an emerging market providing insurance for IP infringement, and this has ramifications for the language used to off-set risk in purchasing contracts.

We are also working on skeleton wording for a precedent purchasing agreement, with definitions and terminology consistent with the Risk Grid, and enabling the chosen sample wording to be inserted in appropriate places. (The Risk Grid uses a number of terms which are capitalised - such as “Publicly Available Code”. Their meaning should be clear from the context, but the intention is that these terms will be defined in the precedent purchasing agreement).

Suggestions for improvement to the Risk Grid are welcome. The primary maintainer is Andrew Katz, and he can be contacted at <Andrew.Katz@moorcrofts.com> to discuss potential additions, alternations or ancillary guidance in applying the document.

The Risk Grid

Text of final risk grid is attached at the end of this paper. Current version is 8. It is licensed under the conditions set forth at the end of this paper.

Appendices

The Risk Grid is intended to be a largely self-contained reference document, but it will also be usable in conjunction with the planned precedent purchasing agreement. However, to assist with contextualising the transaction between Customer and Supplier it makes references to three appendices. These would have to be created by the Customer and/or Supplier to meet their requirements and annexed to the final contract between the parties. There is an overview of the intended content of each appendix below. These appendices will also be referred to in the planned precedent purchasing agreement.

Appendix [1]

This appendix should list the locations from which any and all Publicly Available Code incorporated in the Software has been acquired.

Appendix [2]

This appendix should list any and all guidelines to be followed to accurately document the source of each acquisition of Publicly Available Code incorporated in the Software.

Appendix [3]

This appendix should list any and all licences regarded by the Purchaser as acceptable for the purposes of this transaction and/or the contractual relationship directly related to this transaction.

Licence and Attribution

This paper was published in the International Free and Open Source Software Law Review, Volume 1, Issue 1 (July 2009). It originally appeared online at http://www.ifosslr.org.

This article should be cited as follows:

Coughlan, Shane; Katz, Andrew (2009) 'Introducing the Risk Grid', IFOSS L. Rev., *1(1), pp 33 – 35*