

IP Risk and IP Risk Management

What is an IP risk register?

Donal O'Connell

Introduction

Now, any company faces a variety of IP related risks, some foreseen others unforeseen. I have yet to meet a company who does not have one or more IP related risks to consider. Not all IP related risks are the same and they may be broken down into a variety of different categories, such as the form of IP involved (e.g. patents, trademarks, copyright, trade secrets, etc.); the impact and probability of the risk; the source or origin of the IP related risk; the date when the risk is likely to materialise; the IP activity impacted; the geographical nature of the IP risk; whether they are generic or specific in nature; the group or sub-group most impacted by this risk in the organisation; etc.

IP litigation is a threat to all businesses, large and small but it is by far not the only form of IP related risk. There are indeed many different types of IP related risks that a company may face.

Ok, so now on to IP risk management:

IP risk management is a practice that deals with processes, methods, and tools for managing IP risks in a project, business unit or organization. It is initially about the identification, assessment, and prioritization of IP related risks followed by the coordinated and cost-effective application of resources to reduce or eliminate the probability and/or the impact of these IP related risks to the organization.

IP risk management involves understanding, analysing and addressing IP related risks to make sure organizations achieve their objectives. Proper IP risk management is an integrated and joined up approach to managing IP related risks across an organization and its extended networks.

IP risk management is about ensuring that the business really understands its IP related risks, and then mitigates pro-actively. The rationale for this may be driven by the need for freedom to use technologies already in use or being considered for use in the company's products, but there are many other reasons why businesses need to take IP risk mitigation seriously. The focus should be on risk mitigation and not just of risk evaluation.

Risk mitigation covers efforts taken to reduce either the probability or consequences of a threat. Risk mitigation efforts may range from physical measures to financial measures.

Ok, now where does the IP Risk Register fit in?:

The IP Risk Register is much more than just a simple list of IP related risks. It is much more sophisticated than that. An IP Risk Register is an important component of the overall IP risk management framework. The IP Risk Register is used to identify, assess, and manage IP related risks down to acceptable levels through a review and updating process. The purpose of the IP Risk Register is to record the details of all IP related risks that have been identified along with their analysis and plans for how those IP risks will be treated. The IP Risk Register will also contain IP risk metadata. Metadata is a set of data that describes and gives information about other data. Metadata is simply data that describes other data. Meta is a prefix that in most information technology usages means 'an underlying definition or description'. IP risk metadata summarizes basic information about the risk, which can make finding and working with particular instances of data easier.

That brings me on to the idea of an IP Risk ID:

Each IP risk logged in the IP Risk Register should have an IP risk ID. This is a unique identification number used to identify and track the IP risk in the IP Risk Register. Each IP risk should also have a brief description of the potential IP risk. The IP Risk Register should also ideally contain a classification system. An IP Risk Register should ideally also log the actions to analyse these IP risks and the actions to mitigate these IP risks plus metadata associated with these actions. Next, it should also contain a document management component to help track the various documents associated with IP related risks, IP risk analysis actions and IP risk mitigation actions. Metadata associated with these documents should also be logged into the IP Risk Register.

A cost module should definitely be included, to help track the costs associated with the IP risks if and when they materialise and the costs associated with the actions to first analyse and then mitigate these IP risks. And finally... good search and reporting functionality should also be built into the IP Risk Register if it is going to be a truly value adding IP management tool.

Ok, next we'll explore how the IP Risk Register should support the IP Risk Management process:

The system should support the process and not vice versa. It is therefore imperative that there are features and functions within the IP Risk Register which underpin all five phases of the IP risk management process, namely ...

- Identify, characterize, and gauge IP related threats to the organization.
- Review the vulnerability of critical assets to specific IP related threats.
- Determine the expected consequences of specific IP related threats.
- Determine ways and means to reduce each of these IP related risks.
- And lastly... Implement IP risk mitigation measures based on the overall IP strategy.

Let's consider now: Where is this IP Risk Register located?

Typically the IP Risk Register will be located within the in-house Legal / IP function and operated by people within that function. Given the nature of some IP related risks, access to

and access control of the IP Risk Register are crucial issues for consideration. However there are a number of Legal and IP Firms who have designed, developed and deployed an IP risk management service offering for their operating company clients and these firms locate and operate the IP Risk Register within the firm but on behalf of their clients.

Factors to consider when selecting an IP Risk Register:

I suggest that one needs to take many of the following issues into consideration...

First of all, under the umbrella of user experience, one might consider:

- User interface design and ease of use
- Overall user experience
- Functionality
- Features
- Reliability
- User documentation
- Training, that's pre and post launch -and by whom
- As well as...Ease of getting good quality, useful reports out from the system or tool

Another area to consider is around the features and functionalities of the solution, which would include:

- Architecture of the solution
- Hardware requirements
- Hosting, in-house or externally
- Ease of configuration
- Inter-operability with other patent systems and tools in use within the Patent Creation Factory
- Inter-operability with systems and tools in use across your key interfaces
- Inter-operability with general office type systems and tools
- Manageability of the system
- Access control
- Performance, particularly under load and stress conditions
- Security such as data storage encryption, data transmission encryption

Of course, there are also the points that relate to the business case and implementation:

- Initial costs
- Costs over time
- Support at the launch and post launch
- Maintenance over the life-time of the tools
- Ability to upgrade over time and adapt to future needs

And finally, questions and considerations concerning the relationship with the vendor, such as:

- Roadmap from the vendor showing future enhancements planned
- Ownership and financial status of the vendor
- Current industry reputation of the vendor
- Past performance of the vendor
- References from other customers
- Competitive situation regarding your vendor
- Any other agreements between you and the vendor

In summary then:

An IP Risk Register is a crucial tool to support the IP risk management process. A robust fit for purpose IP Risk Register which underpins the IP risk management process is key. A good IP Risk Register helps ensure that the process is an efficient and effective one. It can improve data integrity as well as better support how IP risks are articulated and reported. It should be easy to install, easy to configure and easy to take into use, otherwise there is a great danger that the system become a 'white elephant'.

As stated initially, IP related risks are an issue of concern for most businesses. It is therefore critical that the company's IP Risk Register is fit for purpose, ensures the effectiveness and efficiency of its IP risk management process, brings great value to those using the system, allows the user to convert the IP risk related data contained therein into information, and ultimately helps add value to the business.

Duncan Clark:

Well, once again, many thanks there to Donal O'Connell for this fantastic overview of the IP risk register. In our next session, we will join Donal again to explore how IP risks can be visualised. In the meantime, thanks for watching and see you on the next module.