# IP Risk and IP Risk Management

## What should an IP risk management process look like?

**Introduction**

Hello and welcome to the Academy by PatSnap course on IP Risk. We're delighted to welcome our partners and experts in this field, Chawton Innovation Services, who will continue to guide us through the complex environment of risk and how it relates to intellectual property. I'm happy to introduce Donal O'Connell, Managing Director of Chawton Innovation Services, who will be our host for this session. In this second module, we'll investigate the components of IP risk and begin exploring the fundamentals of IP risk control and management. So let's join Donal now, who starts with a recap on IP related risks and, more specifically, where these risks can arise…

**Donal O'Connell:**

Hello again everyone and thanks for joining us on this second video. As we mentioned in video one, risk is the chance of something going wrong, and the danger that damage or loss will occur. By its very nature, there are both rewards and risks associated with IP. For anyone involved in IP, then IP related risks are part of working life. However many ignore the risks associated with IP or only react when the risk has materialised, which is most times too late.

The obvious IP related risk is that a business may infringe the IP rights of a 3rd party. However, there are many other IP related risks to consider, for example:

- Having too narrow a definition of IP, and ignoring potentially valuable IP assets
- The IP terms and conditions in some development or commercial agreements with 3rd parties
- The publishing activities of the business
- Embracing open source software
- Being involved in certain interoperability standardisation activities
- Getting involved in some open innovation initiatives
- The use of subcontractors
- One's own IP out-licensing program
- Employees stealing IP from the company
- The scourge of Counterfeit products
- Trademark disputes with 3rd parties
- And lastly… Trade secrets not being properly managed
-

That said, not all IP risks are the same:

… far from it, in fact. Not all IP risks are the same and they may be broken down into a variety of different categories, such as the form of IP involved (such as patents, trademarks, copyright,

and so on), the source or origin of the IP related risk, the impact and probability of the IP risk, the date when the risk is likely to materialise, 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, and other such considerations.

Many mistakenly assume that all IP risks originate from competitors, but IP related risks may originate from a variety of sources. These include:

- The activities of one's own company and its people
- The activities of entities within one's own eco-system (suppliers, partners, distributors, customers)
- The activities of one's competitors
- The activities of other entities such as non-practising entities, or NPEs
- Changes to Government policies related to IP
- The activities of illegitimate entities such as hackers and counterfeiters

Ok, so what are the components needed for IP risk management:

IP risk management is not easy and a number of components need to be in place for a company to truly master this aspect of IP. I strongly suggest that the following components are needed:

- Good IP and IP related Risk awareness and education
- A robust fit for purpose IP Risk Management process
- IP Risk Management system / tool
- Data (IP related risks, actions, documents, reports)
- A variety of IP Risk Mitigation solutions
- IP Risk Management resourcing (people, budget)
- Proper IP Risk Management governance

I suggest that IP awareness and IP governance are like the bookends, keeping everything else in proper order. Governance here is about management putting IP risk on their agenda and regularly asking themselves whether they have the right culture, people and processes in place.

I should also highlight that the skills needed to succeed with IP risk management do not match exactly those needed to be successful with the other key IP processes, such as IP creation, IP portfolio management, IP exploitation and IP enforcement. The mind-set is just different for those charged with IP risk management.

Let's now look at the IP Risk Management Process:

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, analyzing and addressing IP related risks to make sure organizations achieve their objectives. So it must be proportionate to the complexity and type of organization involved. 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.

Let's look at the key steps in the IP risk management process:

A process is an interrelated set of activities designed to transform inputs into outputs, which should accomplish your pre-defined business objectives. Processes produce an output of value, they very often span across organisational and functional boundaries and they exist whether you choose to document them or not.

A process can be seen as an agreement to do certain things in a certain way and the larger your organisation, the greater the need for agreements on ways of working. Processes are the memory of your organisation, and without them a lot of effort can be wasted by starting every procedure and process from scratch each time and possibly repeating the same mistakes.
At a very top level, the IP risk management process involves the following key phases:

- Identification
- Analysis
- Review
- Mitigation
- Monitoring

IP Risk Management Standard:

The IP risk management process an organization adopts must be proportionate to the complexity and type of organization involved.

It is important not to underestimate or exaggerate the risks associated with IP. As IP relates to innovation and creativity, it can sometimes be an emotive subject and some care is needed.
ISO 31000:2009 is a standard relating to risk management codified by the International Organization for Standardization. The purpose of this standard is to provide principles and generic guidelines on risk management.

The ISO with this standard seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

The ISO 31000:2009 standard is not specific to any industry or sector. It is able to be applied to any sort of risk. It is able to be applied to any kind of organisation. It is intended that it should be tailored to suit the needs of a specific organisation.

It definitely can be applied to IP and IP risk management.

The generic approach described in the standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner, and within any scope and context.

The standard includes:

- Principles and Guidelines on Implementation
- Risk Assessment Techniques
- Risk Management – Vocabulary

One of the key paradigm shifts with this standard is a controversial change in how risk is conceptualised. The definition of "risk" is no longer "chance or probability of loss", but "the effect of uncertainty on objectives" ... thus causing the word "risk" to refer to positive possibilities as well as negative ones.

The standard provides a risk management framework as well as a top level process description.

The standard provides a list on how to deal with risk, namely:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Accepting or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

The standard provides a structured credible foundation for discussions about risk and risk management. It provides a starting point for creating a risk management process if none exists today. It also gives some standard vocabulary related to risk and risk management.
ISO 31000:2009 is clear, sensible and brief. It was not developed with the intention for certification.

Next, let's focus on top down vs bottom up IP risk assessment:

The two 'halves' of IP risk management are IP risk assessment and IP risk mitigation. Risk assessment is about the identification, quantification and prioritization of IP related risks facing an organization.

In the top-down approach, IP risk management begins at the highest conceptual level and works down to the details, with the major IP related risks being identified by senior management.

In the bottom up approach, it begins down with the details and works up to the highest conceptual level, with IP related risks being identified by middle managers and individual contributors, and with the higher probability and/or impact IP related risks then being passed up to senior management.

Top down and bottom up are both strategies of information processing and knowledge ordering, used in a diverse range of fields, including in the area of IP risk management. The two approaches may be seen as a style of thinking. Processing here is just a simpler way to say taking in IP related risk information, analysing it, and drawing conclusions or taking action. In a top down approach, an overview is formulated, with the details beyond that overview specified but not delved into. A bottom up approach is the piercing together of different details. It should be stressed that both have the same goal, namely to ferret out the key IP related risks facing the organization.

Success depends on using a combination of top down and bottom up approaches to first identify, classify and prioritize the IP risks facing the organization.

Combining top-down with bottom-up approach is especially needed when the IP environment is continuously changing and consequently, the organization's IP risk map is shifting. In such circumstances, the top-down approach gives IP risk management the necessary strong foundations whereas the bottom-up approach give it some flexibility. The combined approach also keeps everybody in the organization involved in the IP risk management process and ensures accountability and improves compliance.

For organizations tackling IP related risk management for the first time, it is recommended to start initially with a top down approach but then to roll out a bottom up approach to reach out across the entire organization over time. The bottom up approach may for example become an annual exercise conducted across the organization.

Ok, so finally: Who should be interested in IP risk management?

Anyone with interests in IP should take IP risk management seriously. It should be of particular interest to anyone who is:

- Operating in an IP litigious environment
- Coming up for exit or listing

- Anxious to get IP risk management under control
- Facing an executive management team that are demanding visibility of IP related risks
- Experiencing major business changes
- Facing a major IP risk and realising that they are unprepared
- And who is… Interested in proper governance of IP

Regardless of why one is interested, it is best to master IP risk management when things are calm rather than when one is tackling a major IP risk, when pressure is intense and everything seems chaotic and dis-organized. This is not the right time for a GC, CIPO or IP Manager to have to go to the Board and explain that the IP risk management process is to 'panic widely and run away'.

**Conclusion**

And that concludes our second module on IP Risk Management. Many thanks to Donal there. Do join us on our third module, in which we will turn our attention to risk mitigation solutions, so do join us for that.

In the meantime, thanks for watching and until next time, goodbye.