



Legal risk management: A proactive, integrated approach



Jiří Černý

Legal, Compliance & Corporate Security Director,
Board member, Tesco Europe

The management of legal risks is a crucial part of the broader risk management discipline.

In risk management, it can be so easy to become lost in tactical responses to a myriad of risks, without actively managing them at the strategic level. Which is why my first recommendation for all practitioners is to apply a general risk management methodology. This will help you best identify, assess, mitigate and monitor legal risks, highlighting the areas you need to prioritise.



01 Distinguishing legal risks

When separating legal risks from other risks, I tend to focus on the legal team's involvement. I consider legal risks as those that are actively managed, or that should be managed, by a legal team. In other words, if they materialise, the legal team will be responsible for dealing with them.

It's rare that risks are managed solely by legal teams, with responsibility usually shared with other internal functions. If you're looking to define these separate responsibilities, I'd advise using an RACI matrix. This will drive clarity and save you from making assumptions around whose responsibility the risk might be.

An RACI Matrix defines different levels of responsibility as follows:

R – Responsible: The team that is responsible for the correct completion of the task

A – Accountable: Someone who is delegated tasks across the project

C – Consulted: Subject matter experts – including lawyers – who are consulted where necessary

I – Informed: The teams kept up to date with ongoing progress



02 Prioritising your risks

Once you've identified which risks count as legal – and the extent to which that's the case – you'll need to prioritise them. The best way to do so is by keeping your company's values and each risk's possible impact on business KPIs at the front of your mind.

A legal team's time is a constrained resource, and the way you use it needs to strive for the best return. If it is distributed to all legal risks equally, some areas will be underinvested, and some overinvested. Keep them connected to business outcomes and a path for prioritisation becomes clear.

A great way to consider which legal risks to put higher on your agenda, is to go through individual categories of risk – Privacy, Cybersecurity, Competition law, and so on. Keep considering how these risks could impact delivery of your business KPIs. All risk categories have their own subcategories, which should be assessed on their own merit.

03 Respect to fundamental principles

In spite of Point 2, there are certain principles that should be respected irrespective of their impact on company KPIs – categories like anti-bribery, health and safety compliance, and truthful and accurate accounting. These fundamental principles are a matter of integrity, and should be separated from legitimate risk assessment.

There might be moments when a risk assessment is blurred by various contradicting motivations. In these situations, I go back to basics, looking into the company's purpose and measuring the risk against it. In the absence of the company's purpose, you could consider how confident you and your organisation are in defending your position, should it ever go public.



01 The importance of acknowledging risk

Risk acknowledgement and acceptance of residual risk will always be a part of the risk management routine, and should never be replaced with risk denial.

Risk denial happens when we deny the risk exists, or when we discount its likelihood and materiality.

The risks we are not aware of are those we should be worried about the most. When such risk materialises, it brings a moment of surprise and possible disruption your organisation might not be ready for, as well as raising a legitimate question: **what could the legal team have done differently to have identified it?**

05 Defining success

Despite their best efforts, no legal team can completely mitigate against legal risks.

While we may not always control our external environment, we can control our response to it, and we should always be looking for opportunities to improve the way we react to, and reduce the effects of, new legal risks when they do arise.

When your house is on fire, your immediate response is not to focus on how to avoid the next fire, but instead to extinguish the existing one. Similarly, when faced with a competition authority dawn raid, you're not looking at how to design your next competition law training. But, when that moment of crisis is over, these materialised risks give you the best opportunity to learn and reassess your response to individual risk and overall risk management.

The definition of success in managing legal risk is not to avoid all risks. That's impossible. Instead, it's about setting a culture of learning and improvement that looks to better your management of legal risks, reduce their impact, identify hidden risks, and avoid any misinterpretation of how they might materialise.

