Deloitte.

Insights@Tech Risk
Building an IT Risk department for success

Events of the past few years have presented unprecedented challenges to those working in IT Risk functions at financial services organisations. At times, as they have battled against the latest crisis, it may not have felt like it, but these various crises have served to focus senior executives on the potential risks to reputations, customer bases, and profit figures that can result from risk functions that are badly designed, insufficiently integrated, and under-resourced.

An IT Risk function that is built for success should see itself as delivering a service rather than policing risk.

The incentive to correctly identify IT Risks and proactively intervene to mitigate damage could hardly be clearer. Indeed, some organisations – most notably retail banks – are making progress on this journey. Typically they are driven by the need to cut costs, to realign to higher growth markets, and to meet their regulatory requirements.

Yet, even in these, more advanced organisations, progress is frustratingly slow. Those leading these IT Risk functions are finding that they are not built for success. From the people and skills they have, to the services they deliver, the processes they deploy, and the tools they have at their disposal there is much more that can be done to ensure the IT Risk function measures its effectiveness against business priorities, justifies assigned budgets, and meets regulatory priorities.

Integrated business partner

Successful IT Risk functions are those which have their strategy aligned with those of the broader organisation, which are designed to look forwards as well as backwards and which are structured to correctly identify risks before they materialise and cause an operational, financial or regulatory impact. An IT Risk function that is built for success should see itself as delivering a service rather than policing risk. It should be proactive, looking for ways to mitigate risk whilst working towards shared corporate priorities, rather than purely reactive, putting a brake on progress.

More than anything else it should be seen as an integrated part of the decision-making process within the business, rather than an unwelcome addition to an often complex approval process.

20/20 vision

To achieve this it needs detailed knowledge not only of the business and its technology, but also of the environment within which it operates. They need to have a clear vision of the impact the technological issues have on the wider business. Gaining this understanding requires a painstaking process of mapping stakeholders in both IT, but also the business. Those in the risk function must spend time getting to know the divisional CEOS and CIOs, learning about their activities, their priorities, their challenges.

This is the predominant way to gain that detailed internal understanding and to begin to build the trust which underpins every successful IT Risk function. They can then strengthen that trust by providing clear, timely advice, and so adding significant value to the business.

Obstacles

Reaching that point is far from easy. IT Risk functions face three major obstacles. Firstly, the Head of IT Risk often needs to cross through several parts of the organisation before he or she can begin that dialogue with key senior operational stakeholders. Simply gaining face time is a significant challenge.

Secondly, many organisations lack clarity over who is responsible for specific issues of risk. The three lines of defence approach has much to recommend it, but embedding it operationally can be fraught with challenges, and all too often it leaves operational management, risk management and compliance functions, and internal audit looking at each other wondering why the other failed to act. Getting all three groups to recognise the problems caused by this opacity and then to agree clear remits requires the sort of time and resource that few IT Risk leaders can muster.

Thirdly, there is all too rarely a common language around risk, so IT Risk functions struggle to aggregate and explain risk. To report it internally in terms that will make sense to, let alone resonate with, colleagues, is an ongoing challenge. Often this requires a shift in culture. There needs to be less focus on the technical aspects in isolation, and a greater appreciation of the impact on the wider business.

Taking action

So, what can IT Risk functions do right now to hasten their progress towards that goal? The first step must be to gain clarity on precisely the role they can play within their individual organisations. Once they have identified the areas where they can have the greatest impact, they need to invest time in building a clear strategy to fill that corporate role and, of course, how to measure its success in doing so. It is through this carefully considered process that IT Risk can most effectively add value to business operations.

This process takes time and involves a careful ongoing assessment of the appetite of the business for this sort of engagement from the risk function. At times risk should be leading the business; at others it should lag behind, letting colleagues discover for themselves the need for closer interaction. Push too hard and the business may run scared; sit back and wait and they will never come.

To succeed with all this, it is essential that the business retains talented people who understand the business and its key IT Risks. That is a fundamental pre-condition of success, and it is yet another opportunity for those working in IT Risk functions to embrace. These are exciting times indeed.

At times risk should be leading the business; at others it should lag behind, letting colleagues discover for themselves the need for closer interaction with risk.

Contact us

Chris Recchia
Partner, Tech Risk
crecchia@deloitte.co.uk
+44 20 7007 5159

Stephen Ley
Partner, Tech Risk
sley@deloitte.co.uk
+44 20 7303 7386

Tom Bigham
Director, Tech Risk
tbigham@deloitte.co.uk
+44 20 7007 6931

Designed and produced by The Creative Studio at Deloitte, London. 36748A