IT Risk Is Business Risk

By Mike Gill, CISA, CISM, CISMP, ISO 27001 LA, PCIRM

To make a dangerously sweeping generalisation, most folks outside the risk management, finance and technical control sectors frequently see information security and controls as ‘getting in the way’—an inconvenience to business as usual.

Often, business colleagues trying to launch state-of-the-art systems to support marketing initiatives, or perhaps newly redesigned business processes, say they could do without the “hassle” of jumping through all those security hoops (i.e., pre-launch controls assessments and gate reviews). IT risk management is often seen in a negative light when important deadlines are looming. Too often, IT risk (business risk relating to IT usage) is treated as an afterthought, possibly even overlooked completely. Why does this happen?

Similar to the testing phase of the project management life cycle, IT security is often seen as something that can be sacrificed—needless bureaucracy that negatively impacts launch timings. IT risk and enterprise value somehow have become separated. What is needed is a way of integrating IT risk into enterprisewide risk and governance models, so the value of IT risk management can be demonstrated.

Mixed Audiences Require Different Approaches

Of course, it depends on the target audience. Marketing people are not afraid to take risks in business because there are high returns to be had, and such risk taking is essential to a continually healthy business environment; understanding risk appetite and risk tolerance levels in the enterprise is crucial to a successful governance framework.

That approach can be compared to the largely risk-balanced finance community, where gaining support for control initiatives from chief financial officers or finance directors is generally not too difficult to obtain, because the risk/value model is ingrained in the finance community. Alignment of risk appetite can happen successfully only when the right tone is established and communicated from the top down. Another critical success factor in the integration of risk management processes is defining and enforcing personal accountability for operating within acceptable and well-defined risk tolerance levels throughout the enterprise as a whole. ISACA’s Risk IT: Based on COBIT (now incorporated in COBIT 5) introduces a framework that allows IT risk to be aligned and integrated with operational risk models, delivering a method of enabling mature discussion of IT risk at senior levels within the enterprise.

How does one handle such mixed business audiences? In the author’s experience (20-plus years in the automotive, media and finance IT risk management space), this diversity is a healthy asset—essential in fact to that age-old conundrum of assessing risk vs. cost. It is a business balancing act, a necessary reality check.

For example, finance colleagues will not approve purchase requisitions without the inclusion of strong, sound cost-benefit analysis. Marketing colleagues will not accept proposals for new application or infrastructure developments without a rational business case, written in plain language, and without the usual overly dramatic worst-case scenarios. Synchronisation of risk management streams can flourish only by ensuring that the management of IT-related business risk is aligned with the overall enterprise risk management (ERM) initiatives. Risk IT extends and enhances COBIT, so there is no requirement to reinvent
existing IT information and governance frameworks.

Do Not Forget the Need for a Reality Check

Nature has a habit of disrupting day-to-day business: Destructive weather, earthquakes, volcanic ash, for example, periodically test and potentially jeopardise business operations, and humans continue to contribute to the risk mix through fraud, theft, acts of terrorism and, in rare cases, all-out war.

So, risk and cost must be balanced, along with theory vs. practice. Likelihood plays a significant part. In fact, likelihood is key to effective and realistic risk management. How likely is it that a devastating risk will actually manifest itself, really? Be honest. And, even once manifested, what will the impact on the business be? Is it truly likely to threaten the business? Most of the time, the actual impact is not a worst-case scenario at all.

However, the impact on the organisation must be carefully considered. Media outlets run daily stories on IT risk-related scenarios (e.g., identity theft, e-espionage, data loss, significant fraud cases, disgruntled employees running amok), so security professionals no longer need to paint their own risk scenarios and put forward worst-case scenarios to senior executives—they get it! Only by considering real risk factors and environmental risk factors can a balanced and credible view of overall enterprise risk be delivered.

In short, risk management needs an injection of reality, and fast! Scenario planning is a way to deliver that injection. Without scenario planning to insert that realism—theoretical risk explained in easy-to-understand business terms, with credible risk definitions, impact assessments, likelihood statistics and monetary values reflected in risk scores—the information security, risk management and compliance communities will continue to fail in getting their messages to senior management and ensuring that IT risk is always connected to business objectives.

Open Up Communication Channels

Risk must be explained in plain language, with the cost of risk mitigation stated clearly, alongside the projected cost impact of manifested risk. This is not complicated to do.

For example, marketing people understand brand value; risk people understand the potential for reputational damage caused through security breaches. Bolting these two understandings together creates the foundations for realistic risk vs. cost analysis. This reality injection helps promote fair and open communication of IT risk throughout the enterprise and ensures that staff understands that this is a continuous process and an important part of daily business activities. Are there any additional, associated ethical and moral issues that could cause further—in rare cases, irreparable—brand damage? Here is another simple example: How much would sales be impacted if a website were to be defaced or taken down during a high-profile marketing campaign? How much would it cost to secure that website against such attacks? Subtracting one of the monetary values from the other will clearly indicate how much funding needs to be set aside to implement those precautionary methods.

It also helps to focus on the business data, rather than the 'IT clutter' around it: Lost customer data can lead to lost revenue, which is simple to understand. Corrupted data can also lead to lost revenue—also simple to understand. Data not being available when the business needs them is perhaps the easiest to explain in terms of lost revenue.

Risk Management Integration

All that is required is a way of calculating rough figures for revenue losses. This process cannot be fully automated, as up-to-date environmental risk data must be fed in and considered in all cases. Rather, trained, certified and experienced professionals must be utilised to help form a balanced view. In the author's experience, self-created tools and spreadsheets, and even some off-the-shelf applications, while helpful, quickly reveal a critical missing ingredient if used on their own: the human factor.

Risk IT (now incorporated in to COBIT 5) provides tools and techniques to help understand and communicate tangible risk to business operations, as opposed to generic checklists of controls or compliance requirements. Once key enterprise stakeholders have been engaged, IT-related business risk management can be truly integrated into overall ERM.

Risk IT enables enterprises to understand and manage all significant IT risk types. The Risk IT framework provides an end-to-end, comprehensive view of all risk related to the use of IT, as well as a similar view of risk management. The framework fills a gaping hole between generic risk management frameworks (e.g., COSO Enterprise Risk Management and ISO/IEC 31000) and detailed (primarily security-related) IT risk management frameworks.
The key message here is: IT risk *is* business risk—the two can no longer be thought of and treated separately.

**Mike Gill, CISA, CISM, CISMP, ISO 27001 LA, PCIRM**

is managing director of HQ Risk Management Ltd., a company he established in 2005 to help organisations pragmatically translate information security requirements into realistic, achievable and sustainable controls. Gill works with large, multinational corporations in the automotive, media and telecommunications sectors. He can be contacted via LinkedIn at http://www.linkedin.com/pub/mike-gill/1/435/48b or at mikegill@hqrm.com.