Reprinted from Managing business risk,
6th edition Reuvid, J (ed), Kogan page, London

4.1

Managing information risk and other areas of operational risk: routes to success

Marco Kapp and Simon Oxley, Citicus Limited

In 1999, the Organisation For Economic Co-operation and Development (OECD) – a body where 30 of the most economically advanced nations of the world come together to devise policies to foster economic growth and the expansion of world trade – published its *OECD Principles of Corporate Governance*. This highly influential report argued that identifying and managing risk are a fundamental part of top management's job, and that boards of directors should:

- establish a risk policy;
- institute a system for risk management;
- be fully informed about risk (ie be provided with accurate, relevant and timely information, and training if necessary);

- deal with risk with due diligence and care;
- disclose (eg by publishing in their annual report) all material risk factors and how risk is monitored and managed by their organization.

The OECD principles were endorsed by OECD ministers in 1999 and revised in 2004. They are now the international benchmark on corporate governance for policy makers, regulators, investors, corporations and other stakeholders worldwide.

Developments over the last five years – including those presently unfolding in the home loans and banking sectors – underline the importance of strong corporate governance and effective risk management practices. Notable events include:

- high-profile collapses of firms such as Enron Corporation, WorldCom and Parmalat, which led to the US federal government passing the Sarbanes–Oxley Act 2002;
- rogue trading losses at AIB, Barings, National Australia Bank and Société Générale;
- improper disclosure of sensitive data that millions of citizens entrusted to government or private companies;
- flawed risk management practices that led to the 2008 'credit crisis' – which is still unfolding.

The OECD principles and subsequent events show that managing risk well is important because policy makers, regulators and investors *require* that it is done well. It is indeed a crucial part of good management – with the potential for *catastrophic* loss if not done well, ie loss at a level that the organization concerned cannot sustain without outside assistance, or at all.

As a result, today, annual reports report on risk management practices and highlight key risks with increasing clarity and sophistication. Given the global credit crisis, it doesn't take a crystal ball to see that the pressure to manage risk well will intensify in the near term.

What does managing risk well mean?

So what does a business need to do to manage risk well? Some businesses have excellent methods in place for managing particular areas of risk. For example, insurance companies rarely get into trouble with motor insurance business. This is because:

- motor insurers have learned exactly what information to collect to evaluate the risk to them of insuring different categories of vehicles or drivers;

- there is abundant information around on incidents and claims;
- they have systematized, repeatable processes in place to price policies and write exclusions that control their exposure;
- they can track whether these processes lead to profitable business over time;
- the vocabulary, mechanisms and procedures for measuring and managing risk are built into the fabric of the organization – and everyone complies with them.

Their success enables them to predict the likelihood of suffering claims and their magnitude with sufficient accuracy for decision makers. This is the purpose of any risk management process. Thus their practices provide a solid starting point for looking at how to manage *information risk* and other areas of *operational risk* well.

What is 'information risk' exactly?

Information risk can be defined as the 'chance or possibility of harm being caused to a person or organization as a result of a loss of the confidentiality, integrity or availability of information'. This definition has stood up to inspection for many years and has been widely adopted. It can be applied to all types of information and all means of capturing, storing, handling or transmitting it. Its use it therefore strongly commended.

How well is information risk managed at the moment?

So how well is information risk managed at the moment? Just going about your normal day-to-day life will tell you that the answer is 'not very well'. Systems go down, process information incorrectly and disclose it to the wrong people so often that it's part of the day-to-day reality of modern life.

To take a couple of incidents at random, a UK town council recently managed to publish a list of 'safe houses' for victims of domestic violence on its public website – a shocking violation of victims' confidentiality; and a glitch at the UK's main air traffic control centre led to flights being cancelled at London's busy Heathrow airport – less shocking but still pretty irritating for the travellers whose flights were cancelled or delayed.

To put the likelihood of suffering a major 'information incident' on a quantitative footing: in leading companies there is over a 50 per cent chance of a business-critical system suffering a major incident like this a year. Modern public and private sector enterprises will be supported by tens, hundreds or thousands of such systems, which is why major glitches are so evident to employees and the people who rely on their efforts.

Detailed statistical analysis reveals that the harm caused by such incidents can be minimized simply by adopting good practice (eg testing that back-ups can be restored successfully within the critical timescale of a business application, rather

than just assuming they can). Controls like these can slash the chance of suffering a major incident – and often cost little or nothing to implement. So why don't people adopt them? The answer is that:

- Security people often focus on threats like hackers and viruses rather than the more mundane and far, far more common types of event (eg human error) that lead to a loss of confidentiality, integrity or availability. The effect is to unbalance efforts to guard against incidents.
- There are too many controls that need to be in good shape for any one person to focus on all of them, so key weaknesses are often overlooked.
- There's no real consensus about what 'good practice' is.
- Increasingly, systems are connected to other systems, so weaknesses in one can foul up another.
- 'Ownership' of individual systems is often unclear – and 'owners' don't really know how to manage risk down.

The net effect is that business-critical systems that support leading organizations tend to have controls that are in 'variegated' condition: typically, in great shape in a few control areas, weak in other equally critical areas and 'average' in the rest.

Why information risk is so needlessly high?

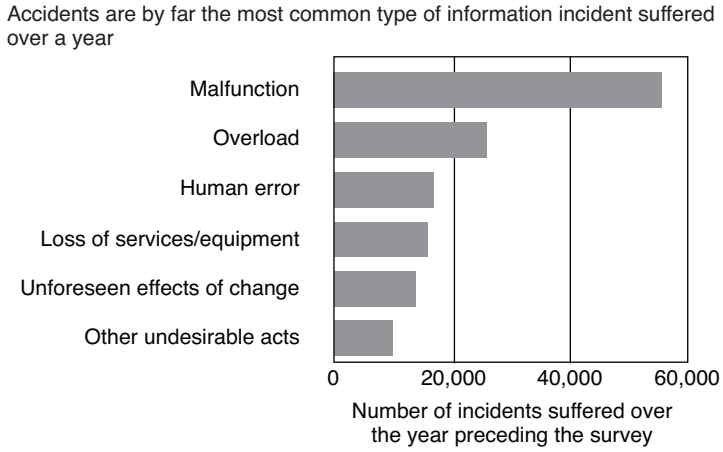
Detailed inspection of the controls applied to thousands of systems and their experience of incidents shows that to drive risk down a very different pattern of controls is essential. Specifically, controls need to be in pretty good condition across the full spectrum of control areas. This is *the* key finding from a massive programme of research into what makes controls effective.

About 10 per cent of business-critical systems that support leading organizations have controls in this condition. That's why information risk is so high.

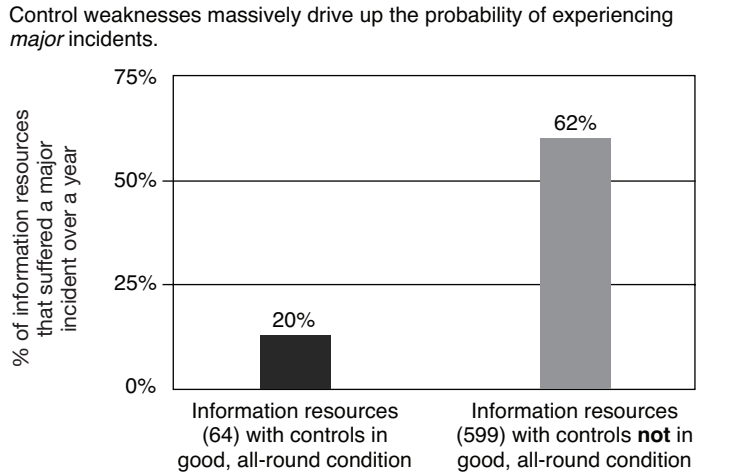
Figure 4.1.1 shows what sorts of incidents actually lead to a loss of confidentiality, integrity or availability of information and why getting controls into 'pretty good all-round condition' is worthwhile. The four charts in Figure 4.1.1 show that incidents are disturbingly common and, while most have minor impact, some can have very serious consequences. The cumulative effect of such incidents erodes profits and makes enterprises underperform.

Benefits of driving risk down

By getting controls in good shape, organizations can substantially reduce information risk. They can also significantly improve their bottom line, since good controls reduce the chance and financial impact of major incidents, and cut the number of minor incidents suffered day to day and the inefficiencies that go with them. Thus the benefits of driving risk down are substantial.



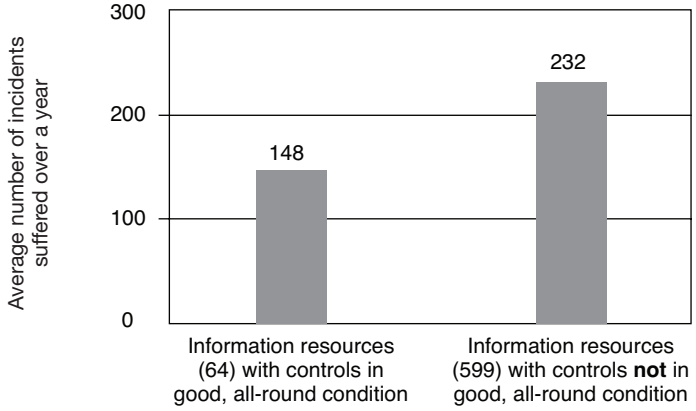
Source: Citicus analysis of 139,000 incidents affecting 558 'live' information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.



Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.

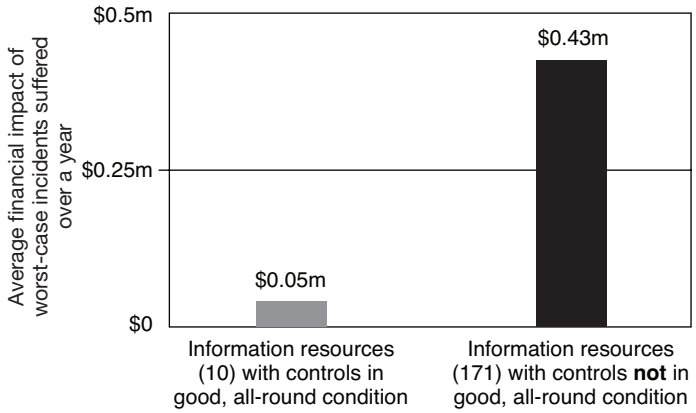
Figure 4.1.1 Statistical insights into information risk

You can expect to suffer substantially (36%) fewer incidents when your controls are in good, all-round condition.



Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information security status survey.

Where controls are in good, all-round condition, the average financial impact of worse-case incidents is only a fraction of what it is elsewhere.



Source: Citicus analysis of 181 worst-case incidents affecting 181 information resources 'on the ground' covered by the Information Security Forum's 2000–02 information status survey.

Figure 4.1.1 continued

Causes of failure in managing information risk down

To get the benefits, you have to go about managing risk in the right way, and avoid the pitfalls that lead to failure.

As part of the research we've carried out, we've examined factors that cause information risk management initiatives to fail and to succeed in a wide variety of case-study organizations.

Key causes of failure

Here are the key things to avoid:

- inability to measure risk *objectively*;
- overly complex approaches that yield results business people don't believe in or understand;
- turf wars between proponents of competing risk methodologies;
- lack of tools to automate the process in a reproducible way;
- lack of cooperation on the ground;
- lack of resources to drive and run the risk management initiative;
- immature processes and reporting structures;
- weak programme management;
- questionnaire fatigue.

Each of the above is a potential 'programme killer' – but an *inability to measure risk objectively and in business terms* will bring any programme into disrepute, so that's possibly the most crucial one to get right.

Secrets of success

The secrets of success that emerged from the research we conducted are strongly reinforced by our experience in helping organizations of different types and sizes around the world manage risk successfully. They can be summarized as follows:

- Before you start, gain top management commitment.
- Get the organizational arrangements right.
- Have a strong, personable programme manager who has the drive, skill and experience to deal with business, people, and technical issues as well as to drive a company-wide programme.
- Base your approach on a crystal-clear definition of risk that addresses what needs to be protected and both the magnitude and the probability of harm.
- Measure the five determinants or indicators of risk that your insurance company considers when assessing the risk posed by drivers (criticality or value at risk; status of controls; special circumstances, eg complexity or scale; experience of incidents; and the business impact of incidents).

- Ensure the risk management process is constructive rather than blame oriented (otherwise people will evade or sabotage the programme).
- Ensure the risk management process is continuous rather than a series of one-off evaluations (so improvements can be tracked over time).
- Make risk management a *personal* responsibility of individual business 'owners' of your 'targets of evaluation'.
- Keep evaluations simple, efficient, objective and business oriented.
- Ensure the process is proportionate (when resources are limited it makes sense to focus them where they will have the greatest payback rather than spreading them evenly across everything).
- Produce meaningful results that capture the attention of busy decision makers – particularly business 'owners'.
- Introduce an element of competition between facilitators and 'owners' (eg by publishing risk league tables).
- Cause pressure to filter down so it motivates others to act (eg by showing dependency risk).
- Embed risk management into the fabric of the organization (eg make criticality assessments become part of project approval and procurement processes).

Putting principles into practice

Over the last eight years, our company has had extensive experience with putting these principles into practice in a wide variety of organizations operating in virtually every country in the world. Figure 4.1.2 gives a quick overview of the constructive evaluation process we advocate.

Our software enables a busy business 'owner' to complete a *criticality assessment* of an information resource in minutes in a coherent, business-oriented fashion, using a company-wide 'harm reference table' to highlight the types of harm that need to be considered. Because the approach is systematized, hundreds of such evaluations can be completed in two or three weeks; thousands take a bit longer (say three to four months).

Criticality assessments focus not on the probability of a harmful event or how it might be caused (which business 'owners' are not equipped to assess through their own experience). Instead, they assess the *worst that could happen if confidentiality, integrity or availability were to be compromised for whatever reason*. This ensures that the assessment of risk takes the worst that can happen into account, which is crucial.

Once criticality has been assessed, the programme manager can decide which information resources warrant a full evaluation of risk using a *balanced risk scorecard*. Such evaluations can be conducted at a high level or in more detail using the scorecard plus subordinate checklists, thus achieving proportionality in the depth of each evaluation.

The balanced risk scorecard verifies the assessed *criticality* of a 'target of evaluation' and establishes the status of its *controls* – this is the factor that mainly determines the likelihood of suffering incidents in future. But it doesn't stop there. It also assesses three other factors that highlight or otherwise indicate risk, namely:

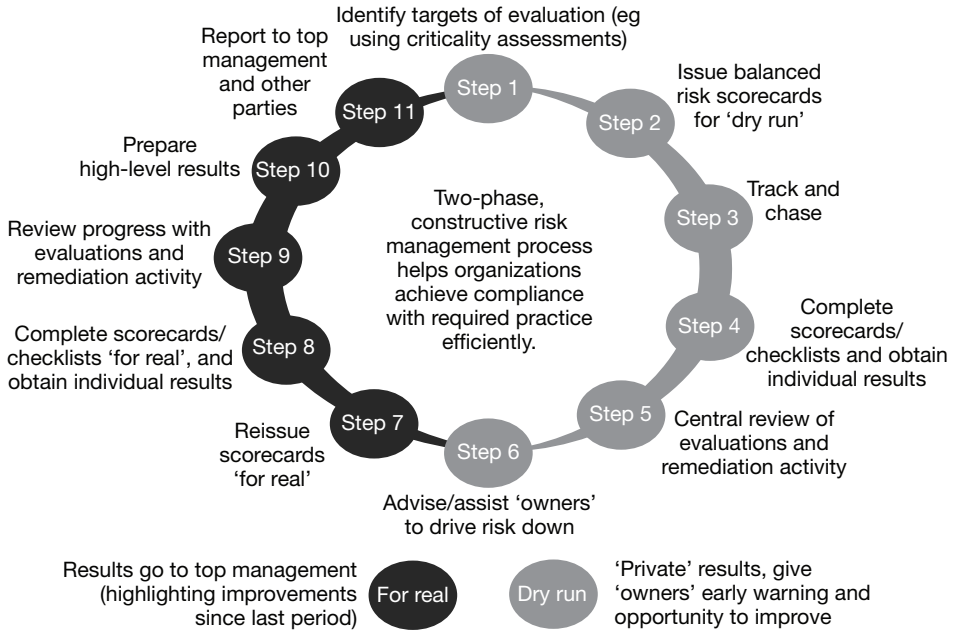


Figure 4.1.2 A constructive evaluation cycle

- *special circumstances*, such as immaturity, scale or complexity (these increase the likelihood of suffering incidents);
- *the number of incidents* suffered over the last year (these provide an independent indication of whether controls are effective and are highly predictive of the chance of suffering major incidents in future);
- *the business impact of such incidents* (these provide a business-oriented indication of what incidents have cost the organization so far).

By design, these five factors echo the ones your insurer considers when setting the price of your car insurance (eg the value of your car, its roadworthiness, your age, your occupation, where you live, and your history of driving offences and claims). Thus measuring them yields a sound, factual picture of the risk posed by individual systems, which can be aggregated for decision makers.

A full evaluation like this is usually conducted initially at a three-hour risk workshop and can thereafter be updated in minutes (eg as improvements are made that reduce measured risk).

For completeness any serious risk management programme worthy of the name also needs to keep track of remediation activity, which our approach does, and show 'owners' of individual systems the risk status not just of their own system but of the other systems it is linked to. This can be visualized using a dependency risk map such as the one shown in Figure 4.1.3.

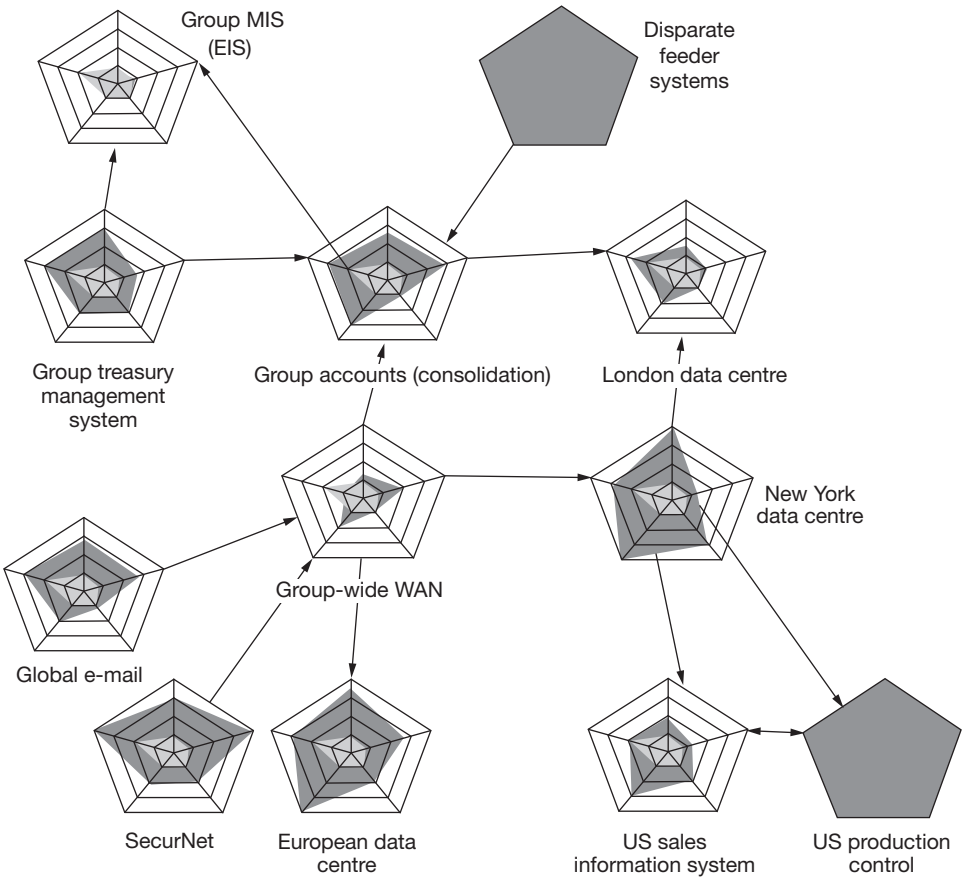


Figure 4.1.3 A dependency risk map

Benefits of a sound approach

Since we started in 2000, our software has been used to carry out thousands of evaluations, in over 150 countries. Typically, the process of managing information risk starts with a 'discovery' phase, which of itself delivers many benefits.

> When we started, we didn't know whether we had 6,000 or 60 business-critical systems in Germany alone and had only very patchy information about their 'owners'. Now we know exactly what's critical we can focus attention on the ones that matter most.
>
> Risk manager, global consumer products company

Our customers are also finding that sound risk data help in deciding which systems should be co-located and which kept separate and the precise grade of service each one needs. This can save millions when services are delivered by an outsource partner.

Extending the approach to other areas of risk

When we started, our focus was on developing a business-oriented and scalable method of evaluating information risk systematically, which could be successfully applied by organizations of all types and sizes. Since then, we've found that the same principles can be applied to other areas of operational risk; it is just the fine detail of the process that needs adjusting.

By 2008, we found that our customers and prospects were excited about applying the same approach to multiple areas of risk and focused in particular on information risk plus three other areas of operational risk, namely:

- *supplier risk*;
- *site risk* (this covers security and health and safety of employees, visitors and neighbours);
- *privacy of personal data* (this is of ever-growing importance as regulations tighten and more and more breaches emerge).

The reaction we've seen is telling us that there is pent-up demand for a method of measuring and managing risk based on sound principles. We hope this chapter has given you a good feel of what these might be and helps you plot a route to success that avoids the pitfalls others fall into.