CHAPTER 1

Risk Identification Tools

TOP-DOWN AND BOTTOM-UP RISK IDENTIFICATION

The most dangerous risks are those we ignore, as they can lead to nasty surprises. Before organizing risks in a register, it is important to identify the risks that are specific to your own business, not just those based on an external list, and then assess, mitigate and monitor them.

Risk identification in an organization should take place both top-down, at senior management level, looking at the large exposures and threats to the business, and bottom-up, at business process level, looking at local or specific vulnerabilities or inefficiencies. These procedures are different but complementary, and both are vital because it is not sufficient to have one without the other. My favorite analogy for top-down and bottom-up risk management is the crow's nest versus the engine room of a boat, both of which are necessary for a complete view of an organization (see Figure 1.1).

Top-down risk analysis should be performed between one and four times a year, depending on the growth and development of the business and the level of associated risks. The aim is to identify key organizational risks, the major business threats that could jeopardize strategic objectives. Top-down risk identification sessions will typically include senior risk owners, members of the executive committee and heads of business lines. Sessions are best organized as brainstorming workshops with supporting techniques and tools, such as review of exposures and vulnerabilities, risk wheel, and causal analysis of potential impacts and expected revenues. These are explained in the next sections. Top-down risk identification exercises are similar to scenario generation, which is the first phase of scenario analysis. For small to medium-sized firms, I recommend conducting these meetings with both risk identification and scenario generation in mind in order to save time. The results can then be used as inputs to both the risk and control self-assessment (RCSA) exercises and scenario analysis. The links between RCSA and scenario analysis will be explained in Part 2.

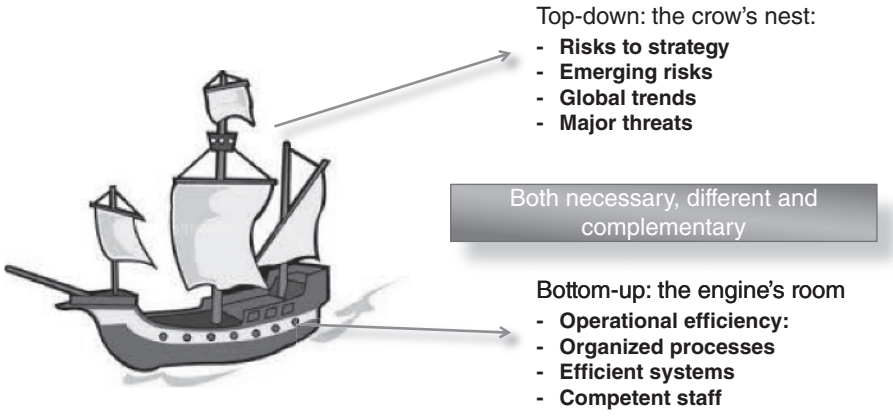

FIGURE 1.1 Top-down and bottom-up risk management: the boat analogy

CASE STUDY: FTSE 100 INSURANCE COMPANY – TOP-DOWN RISK IDENTIFICATION

A large insurer in the UK calls its top-down risk analysis TDRA. It was set up by the chief risk officer (CRO) several years ago and provides a quarterly platform for the executive committee to review principal risks and emerging threats to the business, and to implement any required changes to the firm's risk profile. The insurer calls bottom-up risk identification RCSA, which focuses on the business process level and is the abbreviation for the more classic risk and control self-assessment technique.

Top-down risk analysis is one of the most efficient ways to identify important threats to a business. However, bottom-up risk analysis is still more common in the industry. Bottom-up risk identification is the only type of risk identification in many firms, especially among firms new to the discipline, where the practice is the least mature. In such firms, risk and control self-assessments are carried out as a first step to risk management, at a granular level. If the scope of the bottom-up risk identification exercise is too restricted, too granular, the output will be a disparate collection of small risks, such as manual errors and process risks, which are not always of much value to senior management. In the same way that we might fail to see a beach because we are too busy observing the grains of sand, we may miss the big picture when it comes to risks and their interactions because identification takes place at a level that is too low in the organization. The most common bottom-up risk identification techniques are process mapping and interviews, which we explore in this chapter.

CASE STUDY: TRADING FIRM – COMPLEMENTING TOP-DOWN AND BOTTOM-UP RISKS

Reconciling top-down and bottom-up risks is a goal for many firms and consultants. However, I don't believe it is a useful or even correct approach. Rather than *reconciling*, I would recommend *informing* one type of identification with the other, and *adding* the results of both exercises to obtain a comprehensive view of the operational risks in an organization. This is what we did during an ICAAP (Internal Capital Adequacy Assessment Process) in a trading group in the UK. After performing two risk identification workshops with top management, we compared the results with the findings of the bottom-up risk identification and assessment process. The findings were similar for some risks, but there were also some differences. The sum of both results provided the firm with its first risk universe, which was subsequently organized in a risk register and properly assessed.

EXPOSURE AND VULNERABILITIES

Risk exposure is inherent in every business and relates to key clients, principal distribution channels, central systems, primary sources of revenue and main regulatory authorities. In particular, large company projects and critical third parties are among the typical large exposures for a business. Operational risks related to projects and to outsourcing practices are an increasing focus in operational risk management, and rightly so. Large exposures to certain activities or counterparties aggravate the impact of possible incidents should a failure materialize for one of those activities. We will revisit exposure in Part 4, when we review the key risk indicators (KRIs) of impacts.

Vulnerabilities are the weakest links in an organization. They include inadequate or outdated products and processes, systems overdue for maintenance and testing, pockets of resistance to risk management and remote businesses left unmonitored. Large exposure typically relates to high impact/low probability risks, whereas vulnerabilities relate to higher frequency or more likely risks, hopefully with low impacts, but not necessarily. If vulnerabilities relate to large exposures, you have a heightened threat to the business. Examples of exposures and vulnerabilities are displayed in Figure 1.2.

There are two significant benefits to the risk identification method of exposure and vulnerabilities: it's business-driven and it's specific. Discussing exposures and vulnerabilities with line managers doesn't require risk management jargon. It's a natural process, grounded in the business, which everyone can relate to. The second advantage, shared by the other brainstorming techniques in this chapter, is that it is tailored to a given organization, a given business. In other words, it is individual and specific, which is a characteristic of operational risk. When identifying risks, you may be tempted to

Exposures	Vulnerabilities
• Key distribution channels • Main clients • Main suppliers and third parties • Critical systems • Regulatory exposure • Main drivers of revenues, drivers of value • Brand value • ...	• Weakest links • Fragile systems • Revenue channels at risk • Systems or processes not integrated • Parts of the business resistant to risk management • Small, unmonitored operations or people • Unmaintained systems • BCP due for testing or updates • ...

FIGURE 1.2 Exposures and vulnerabilities as a risk identification tool

use ready-made lists from industry bodies or from the Basel Committee. These lists are useful, but only as an ex-post check, to ensure that the exercise has not missed some significant threat. If used as a starting point, they may miss what makes a business particularly exposed or vulnerable to certain types of event.

THE RISK WHEEL

Popularized by the Institute of Risk Management (IRM) in London, the risk wheel is a classic support tool to spark creativity and imagination during risk identification brainstorming sessions. There are many versions of the risk wheel. The wheel in Figure 1.3 is a modified version of the one from the IRM training course 'Fundamentals of Risk Management', which I have delivered many times over the years. It usually applies to enterprise risk identification in non-financial sectors, but experience has shown that risk managers in the financial industry find it useful to debate themes that are not necessarily considered in financial organizations, such as risks from natural events, supply chains or political and social events. However, these themes are now increasingly considered by the financial sector when looking at outsourcing risk and anticipating business disruption due to extreme weather events, terrorist attacks or social unrest. Between Brexit and the election of Donald Trump, political risks and instability have climbed up the agendas of risk managers across financial services.

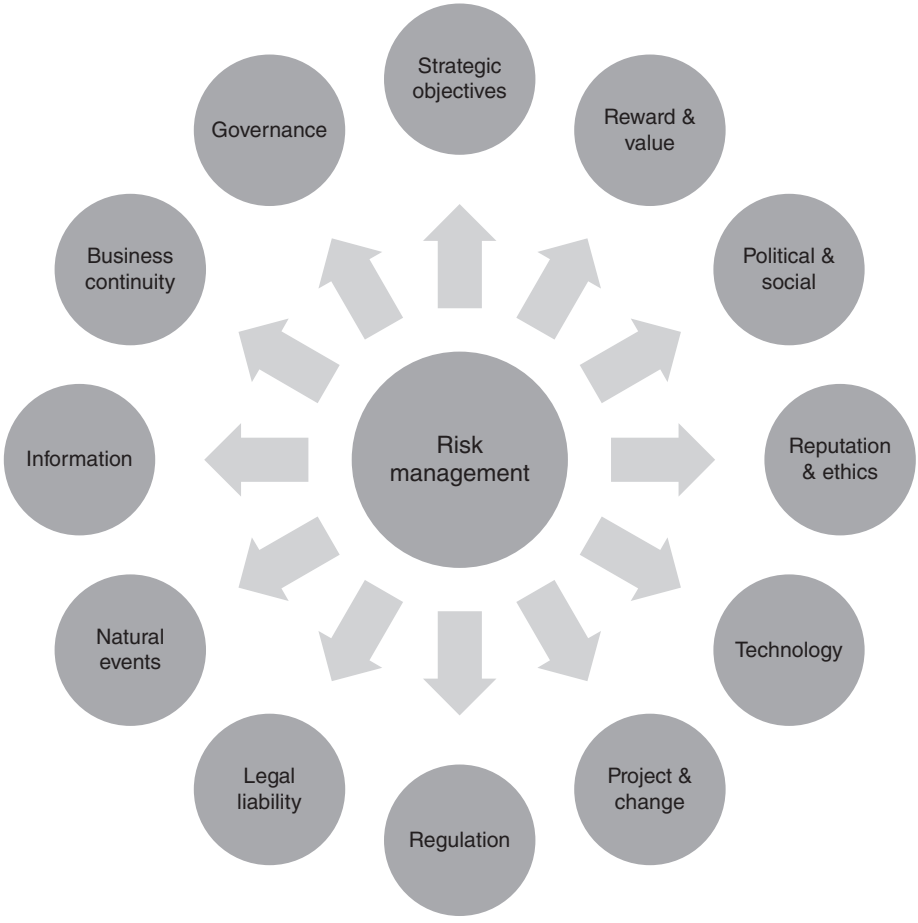

FIGURE 1.3 The risk wheel

By presenting risks – or risk sources – in a circular way, the risk wheel encourages managers to make connections between risk types, highlighting possible chains of causes and effects. The following are examples:

Reward and value → Personal effectiveness → Project and change → Technology → Business continuity → Reputation

Natural events → Supply chain → Business continuity → Reputation

Such causal relationships, even when approximate, help to prioritize risk mitigation. Chapter 4 presents the concept of risk connectivity and illustrates the value for

risk management and mitigation. The evolution of risk lists into risk networks is one of the foreseeable advances in operational risk management.

THE ROOT CAUSES OF DAMAGES AND REVENUES

Apart from incident analysis, the "five whys" and other root cause analysis techniques can also be used to reflect on risks to the business. The starting point can either be an impact to avoid or a revenue source to preserve. By answering successive questions about "why" an accident might happen – or revenues might be affected – managers can build a focused picture of both the threats to the business and the conditions for success, as the case study illustrates.

CASE STUDY: LEASING COMPANY – ROOT CAUSE OF DAMAGES AS RISK IDENTIFICATION TOOL

During a training session on risk identification, a participant from a business line of a leasing company was puzzled by the content and felt unable to start identifying the risks to her business. I asked:

"What is the worst thing that can happen to you?"

" A damage to our reputation," she replied.

"What can cause a damage to your reputation?"

"If the product is faulty, or the price is not right, or the customer service is poor."

"And what could cause those things to happen?"

"If the quality control fails, or there has been a mistake in the pricing of our goods, or if the call center has not been trained properly, or if the broker is fraudulent or disengaged."

"And why would that happen?"

etc.

We had this conversation without mentioning the word "risk." She completely understood the method and was able to start the risk identification of her business, without any established list, because it was rooted in her reality and circumstances.

PROCESS MAPPING

Process mapping is probably the most common risk and control identification approach, bottom-up. It is well developed in information technology, operations and project management, and can also be applied less formally, or at a higher level (e.g., process mapping does not need to be as detailed in other areas compared with IT and operations in any other area). It is useful to establish the tasks performed and to map the different controls with the risks they intend to mitigate. Or it may be easier and more practical to start by observing the controls and inferring which risks they are supposed to address. This exercise should highlight the possible under- or over-control of some risks compared with others.

It may be difficult to decide the appropriate level of analysis. If too granular, the process mapping will be excessively time-consuming and likely to raise only minor issues; if too high-level, it will not be revealing enough. A process description at level 2 or level 3 is usually the right balance, where each step is a significant action and individual key controls are described with their related risks. Figure 1.4 illustrates the principles of process mapping.

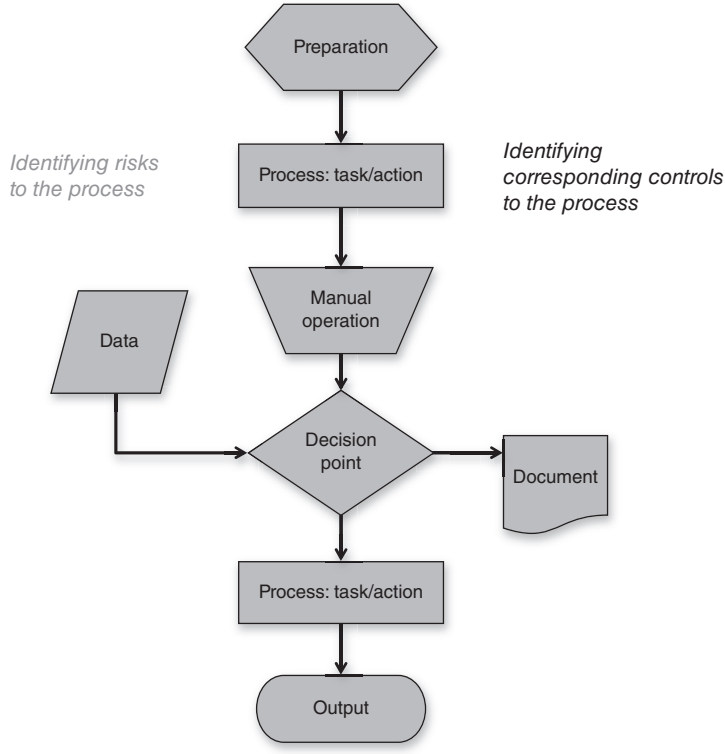

FIGURE 1.4 Common symbols and flows in process mapping

INTERVIEWS OF KEY STAFF

"Ears on the floor are better than any report."

When I was an internal auditor, my boss, who had more than 30 years of experience in the bank, was a great believer in observation and in "auditing with your feet." That means collecting information from the ground up, walking around the office, talking to people, encouraging and overhearing conversations. Similarly, the chief risk officer of a large UK bank once said that the Friday afternoons she used to spend in retail branches provided more valuable information than any credit risk report she ever read.

There is a lesson here for all of us and in particular for operational risk managers: risk-manage with your feet; take the pulse of the business by walking around, talking to people, listening and observing. No risk report is likely to beat first-hand experience.

Two types of employees stand out when it comes to risk interviews. One group is the most experienced employees, who have been with the business since it started and are the living memories of what happened, used to happen, and why things operate the way they do. The other group comprises recent hires, especially those who come from a different firm and culture – and most of all, a different industry. Many things may surprise them about their new company, compared with their previous experiences, and the contrast in practices, good or bad, is a rich source of information about the strengths and weaknesses of a business. Some CROs have distilled these observations into a so-called "amazement report" to highlight the experience of new employees in their first six weeks with the organization, before habit tames their surprise.

WHAT ALREADY HAPPENED: INTERNAL LOSSES, EXTERNAL LOSSES AND NEAR MISSES

Past losses, or "lagging indicators," are often the first things we review in most institutions. While the past is at best an imperfect guide to the future, it is natural for us to look at what has happened when trying to predict what might happen. We all do it. In relatively stable environments, the past may be a reasonable predictor of the future. To refine the approach, we should distinguish between internal losses, external losses and near misses.

Internal losses indicate the concentrations of operational risk in a firm. In banks, these losses typically affect back offices, with financial market activities first, retail next and then the IT department. The number of transactions and the size of the money flows are natural operational risk drivers, especially for incidents related to processing errors, business malpractice and fraud. If repeated internal losses do not represent a systematic failure in internal controls but simply the level at which a business is exposed to operational risk, then those internal losses should probably be budgeted and

accounted for through pricing. If they do come as a surprise, then they may constitute new information regarding risks.

External losses, for risk management in mature organizations, are a systematic benchmark that helps risk identification and assessment. A common good practice in such organizations is to monitor all large incidents communicated by peers and after each one ask objectively: "Could this incident happen to us?" If "yes" and the existing risk controls for that type of incident are deemed inadequate, appropriate mitigation measures must be taken. Although good practice, the review is limited by the reliability of information filtering through from external incidents and their causes.

Near misses are incidents that could have occurred but did not because of sheer luck or fortuitous intervention outside the normal controls. An example of a near miss is leaving a smartphone visible in a car overnight without it being stolen, or forgetting to pay for parking and not receiving a fine (especially in London). In the business context, it could mean mistyping a transaction amount with too many zeros and having it returned because you also made a mistake in the bank account number. Even though most firms claim to record near misses, only the more mature ones actually collect a reliable number of near misses. Those firms typically have a no-blame culture, where teammates feel comfortable admitting mistakes without fearing consequences. It is too easy to sweep things under the carpet when nothing goes wrong in the end, but near misses often provide the most valuable lessons about risk management. We will return to this in Chapter 14 on risk information.