4

Risk Evaluation and Control

All courses of action are risky, so prudence is not in avoiding danger, but calculating risk and acting decisively. Make mistakes of ambition and not mistakes of sloth. Develop the strength to do bold things,not the strength to suffer.
– Niccolo Machiavelli, *The Prince*

The ability to understand and manage risk is an important part of BC planning. Until you understand the risks your organization faces and determine the degree to which you are currently resilient to those risks happening, you do not know how robust a BCP you need. You may be running risks you could avoid through simple and often inexpensive risk reduction measures. Risk assessment is part of the background you need to justify risk reduction measures and your BC strategy.

This chapter will help you to:

- *Identify assets, threats, hazards, and risks.*
- *See the potential for loss and vulnerability of assets.*
- *Evaluate risk analysis tools and techniques.*
- *Understand the risk evaluation strategy.*
- *Select the appropriate risk analysis process.*
- *Define the principles of risk avoidance and prevention.*

4.1 Understanding Risk

Risk is all around us. Often it is so familiar that we don't even recognize it as risk. It is important not just to identify risk, but also to understand the impact of a risk actually happening. This impact is covered in business impact analysis (BIA), which will be discussed in Chapter 6. In practice, the aspects of risk analysis (RA) and BIA are often intertwined. Figure 4-1 illustrates the activities, which are explained in more detail in succeeding chapters.

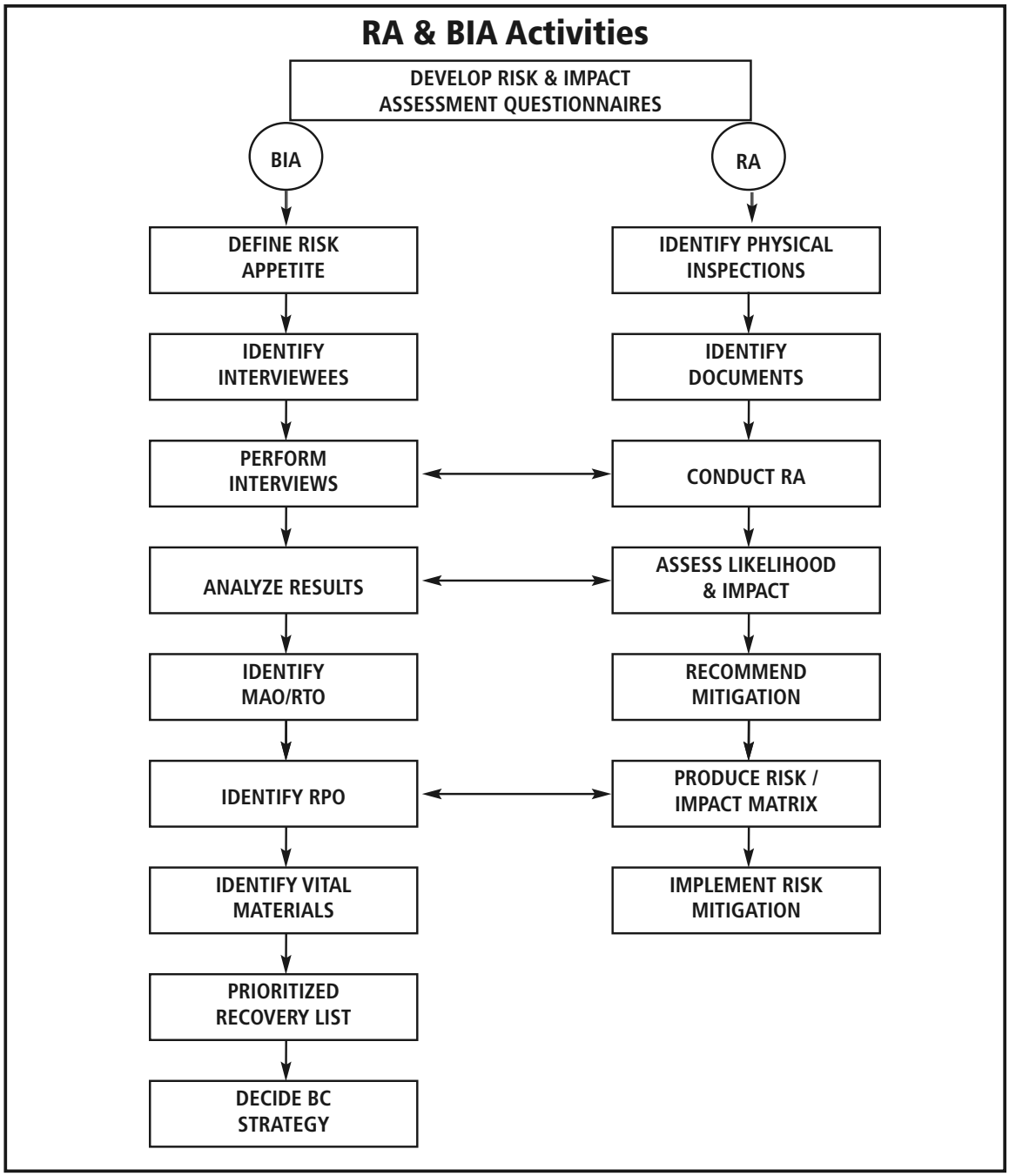

Figure 4-1. RA & BIA Activities

Risk management includes identification of risks, appreciation of their impact on the business and the likely frequency of occurrence, and implementation of steps to reduce that frequency to an acceptable level. Although RA and BIA are often treated as separate activities, for all practical purposes, they are part of the overall process of risk management.

Risk appetite identifies the level of risk the organization is prepared to accept and may be expressed as a cash value, an impact on share price, a percentage of profit loss, a combination of these, or other formula appropriate to the organization.

You may often see the terms *hazards, threats*, and *risks* used interchangeably. For clarification, we will define them, as they relate to assets, in this book as follows:

- *Asset*: something of value; tangible premises, plant, equipment, people, intellectual property, or an intangible quality like reputation.
- *Hazard or threat*: a theoretical exposure to danger.
- *Risk*: a hazard or threat that has been assessed (weighted) as to the probability of it occurring to a specific asset (i.e., how vulnerable a particular asset is to a specific threat).

Threats are identified at a conceptual level (fire, flood, power loss, etc.). Each asset is examined to identify how vulnerable it is to these theoretical threats.

4.1.1 The Need for Risk Assessment (RA)

RA may be required for a number of reasons:

- Protection of life, health and safety.
- The duty of care or corporate governance.
- Legislative requirements.
- Public accountability.
- Compliance requirements.

The objective of risk assessment should be to reduce risk to a level as low as reasonably practicable (*ALARP*).

4.2 The RA Process

Threats are identified at a conceptual level (fire, flood, power loss, etc.). Each asset is examined to identify how vulnerable it is to these theoretical threats. With these vulnerabilities in mind, the risk can be analyzed and countermeasures can be considered to manage or reduce the risk. Cost justification of the risk reduction measures will follow once the BIA has taken place so that the cost of the countermeasure can be balanced against the potential for loss.

The RA process can be seen schematically at Figure 4-2.

4.3 Options for Risk Management (RM)

There are a number of approaches to risk:

- ***Accept*** the risk (do nothing).
- ***Avoid*** the risk (come up with an alternative plan – e.g., do not relocate to a flood plain).

4.14.2 Suppliers – Risk Areas

Supplier risks could include supplier dependence. Many enterprises have reduced the number of suppliers from, literally, thousands of small vendors to a handful of large vendors. Should they lose a key supplier, it may be difficult to find another with sufficient capacity. Moreover, supply chains may be long and opaque – for instance, up to 30 different companies could be involved in providing an Internet-based service.

> **Further, the growth of outsourcing brings with it the serious danger of supplier non-performance – over half of all outsourcing contracts involve dispute.**

Further, the growth of outsourcing brings with it the serious danger of supplier non-performance – over half of all outsourcing contracts involve dispute. We see many contracts in which it has taken several months to negotiate the deal, but termination is on one month's notice – with no chance of finding a replacement supplier and successfully negotiating a sound contract within the termination timeframe. Risk of prolonged service outage is often present, but hidden in support contracts. We frequently find that service availability and reliability commitments are not supported by maintenance arrangements. For instance, by most measurement methods, a 95% per month availability service level means something less than four hours of outage per month. If the maintenance contract has a four-hour "response" or a four-hour "onsite" time, the service will inevitably fail its service level. To succeed, the maintenance contract should, in this example, have a four-hour maximum guaranteed fix time. All key supply contracts should be reviewed as part of your risk assessment to ensure they support mission achievement.

Real Life Issues

- A headquarters building had an archway through the center that gave access to its car park, through which the public had right of way. Unprotected communications cables ran through this archway.
- Another headquarters building had inspection covers in the sidewalk. These could be opened with a standard lifting key. The inspection covers opened to show communications lines to the building. Although the company had dual carriers, both lines ran through the same ducting.
- Unprotected air conditioning fans of one organization were at the back of the building, to which the public could gain access. A metal rod rammed into the fans could take out the air conditioning.
- A dynamic financial institution had grown organically and by merger and acquisition, resulting in many computer rooms and many applications with no overall view of what applications ran where, on what equipment, and with what other dependencies. ICT had to map and document configurations and applications before work could start.

Both in France and UK, we have seen industrial action against government policies taking the form of blockade of refineries, leading to serious fuel shortages.

At the same time, global dependencies and interdependencies within the supply chain over and over again proved fragile.

(***Note:*** *For more about supply chain risk and resilience, see Chapter 5 and Appendix A of this book.*)

Table 4-2. Risk Review Checklist

Risk Review Checklist			
No.	**Action**	**Comment**	**Done**
1	Obtain background briefing material.		
2	Review briefing material – identify queries.		
3	Fix appointment for site visit – physical inspection.		
4	Fix appointments for interviews with: facilities, marketing, CFO, production, operations, CUI, security, audit, HR, health & safety.		
5	Develop/customize risk questionnaire and circulate with explanatory letter.		
6	Conduct physical inspection: general surroundings (site) and premises.		
7	Conduct interviews, covering risks related to business; process; technology; HR; site; premises, suppliers/contracts.		
8	Review insurance and contract issues.		
9	Weight threats to produce a prioritized list of risks.		
10	Consider risk reduction measures; identify and prioritize recommendations.		
11	Draft risk aspects of strategy report.		

Table 4-2 provides a checklist of actions to be undertaken in relation to risk assessment. Clearly, the most significant threats – those that could lead to failed mission achievement, key performance indicators (KPIs) or targets, increased costs, and ultimately to mission failure – should be the first focus of attention.

The hazards or threats may be reported on as shown in Table 4-3.

Table 4-3. Threat/Hazard Report

Threat/Hazard Report								
No.	Hazards Identified	Persons Affected	Existing Controls	Further Action Required	Hazard Owner	Priority		
						H	M	L

It is worth noting that most BCPs will not cover disasters arising from all of these threats: for instance, not covering fraud or industrial action (although these may be covered by separate contingency plans within finance, audit, or HR). In other BCPs, the scope may explicitly exclude some threats. Many public sector organizations are self-insured, or substantive loss to them may be covered by government contingency arrangements. For some, commercial insurance may not be an option. However, where commercial insurance is an option, it usually excludes some threats (e.g., pressure waves, war, or terrorism) and, while extra insurance coverage is available, it may be prohibitively expensive. Some hazards, in our experience, typically are not covered by BCPs. These hazards should be identified and risk mitigation measures put in place wherever practicable.

Table 4-4. Threats that may not be covered by a Business Continuity Plan

Threats that may not be covered by a Business Continuity Plan

- Loss of reputation – criminal act
- Loss of reputation – business error
- Loss of critical customer
- Terrorist activity
- Civil disobedience
- War/invasion
- Contamination
- Neighbor's problems
- Denial of access
- Hacking
- Virus
- Wide-area disaster involving both the normal working premises and the standby site(s)
- Failed business strategy
- Price war
- Recession
- Political interference/policy changes
- Premature obsolescence of technology
- Cheaper alternative products/services
- Acquisition target
- Lack of innovation
- Inadequate management information
- Product contamination
- Loss of supplied services
- Loss of special consumables
- Customer bankruptcy
- Skills/staff shortage
- Pressure waves
- Operator error
- Extortion
- Out of stock situations
- Service level failure
- Quality defects
- Failed outsourcing/supply contract
- Failure of major project
- Lack of innovation
- Failure to manage change
- Security breach
- Starvation/high cost of capital
- Over-trading
- Credit risk
- Interest risk
- Exchange rate risk
- Treasury exposure
- Fraud
- Claims
- Failure to deliver returns
- Share price slump
- Industrial action
- Loss of key staff
- Succession issues
- Espionage
- Breach of confidentiality