01 Introducing employee risk management

Have you ever considered the damage that even one employee can do to your organization? Perhaps if Barings Bank had done so, a derivatives trader by the name of Nick Leeson would not have been able to bring down one of the world's oldest merchant banks in 1995. Equally, do you assume that groups of senior employees can be trusted to not act in a manner that will cost the organization millions or damage its reputation? Mid Yorkshire Hospitals NHS Trust probably thought so before it was forced to pay Dr Eva Michalak £4.5 million in compensation. This followed a campaign of bullying, harassment and sex and race discrimination orchestrated by several senior employees, including the human resources (HR) director. In the United States, JP Morgan Chase had to pay regulatory bodies £572 million (US $920 million) due to senior management's failure to deal with the threats presented by what is known as the 'London Whale' trades. The common denominator in all these examples is the existence of an organizational culture that allowed such risky employee behaviour to flourish.

Introduction

This is where an employee risk management approach comes in. Risk management is conventionally used to assess how threats and vulnerabilities, such as safety hazards, can affect individuals. But what it does not do is put the workforce at the heart of the assessment as the potential source of the threats. Adopting an employee risk management approach shows the harm that individual and group activities can have on unwary employers. Failure to identify, assess and manage these threats can increase the likelihood of legal liability and damage profit margins. In a nutshell, this is what the concept of employee risk management is about. The purpose of this

book is to explain it, describe what areas it covers and show how it can help with HR-related compliance and good practice. A brief introduction is also included here on how the adoption of an employee risk management approach can enhance the profile of HR within an organization, along with a brief overview into how employee risk management can help safeguard an organization's reputation: a theme continually revisited throughout this book.

An overview

The concept of employee risk management comes into its own by focusing on how the actions of employees and others within an organization – such as the board, individual directors, contractors and agency staff – can harm an employer. It is not just limited to compliance issues, but covers a range of threats and vulnerabilities that can originate from the workforce: either as individuals or collectively. It does so by identifying, assessing and prioritizing these threats and vulnerabilities, and then devising a strategy to eliminate, reduce or otherwise manage those found. As a concept, risk management is usually associated with areas such as finance or health and safety. However, its principles can equally be applied to the management of employee risk in the HR context.

I have deliberately used the term 'employee risk management' rather than the better known 'people risk management'. This is because the former specifically refers to a situation where some kind of employment relationship exists, even if a loose one. So it refers not only to employees but other types of individual commonly found in organizations, such as agency staff and self-employed contractors and consultants. It has a broad remit as it covers all grades from the board down to the most junior employee. Outsourcing is also covered due to its increased use by many organizations in recent years. Whilst employers often see outsourcing as an easy route to cost savings, it is not a risk-free strategy. This is due to the reputation damage that may be caused by those who act in an organization's name and are assumed to be employees, but who are not on the payroll. Outsiders such as regulators, shareholders and customers are not included.

The word 'risk' has many definitions that vary according to the particular discipline that is assessing it. For the purposes of this book, I have used it to refer to the likelihood of an organization being harmed by a threat or a loss of some kind, and how serious the harm could be. Risk management itself

refers to the process that systematically identifies, assesses and prioritizes these threats and then devises a strategy to manage them. However, its principles can also be applied to the management of employee risk. This could be as a standalone exercise or part of a wider enterprise risk review. For example, an employer may have already adopted a model of HR risk management as an internal review mechanism that is carried out by HR itself. Alternatively, it may be an area of interest for internal audit (where applicable). If so, employee risk could be seen as a component of a wider HR risk management strategy. Although risk is often seen as something negative for an organization, it can be positive if approached and managed effectively – in that it can lead to more innovative and better working practices.

Areas covered

As employee risk management covers any area where the activities of one or more individuals can harm an organization, its remit is potentially vast. For example, it could be one employee's poor password security that allows cybercriminals to infect the employer's computer network. Or it could be an interviewer asking illegal questions during a recruitment process, which then exposes the employer to a discrimination lawsuit. The availability of resources, or preference, will dictate whether an employer explores only one area of risk management, or multiple areas, at a time. Alternatively, the decision may be taken to invest time into carrying out an organization-wide review into how employee risk is managed. This book (in terms of layout and content) assumes that it is the latter. If this is not the case, however, and risk topics are being assessed in isolation, the chapters can easily be read on a pick and mix basis. Where a comprehensive organization-wide exercise will be undertaken, it is important not to underestimate the time involved in identifying the areas to include. Also, mapping them out will require input from other disciplines than HR in order to ensure that nothing important gets left out. There are several different ways of deciding what areas should be covered.

The first is to identify the different categories that comprise the 'workforce'. This includes the obvious groupings such as directors, employees, agency staff and self-employed contractors. However, it also includes those who are not considered to be workers for the purposes of employment legislation, such as genuine volunteers and interns. It can also include outsourcing, because in the eyes of customers, these third-party workers are effectively

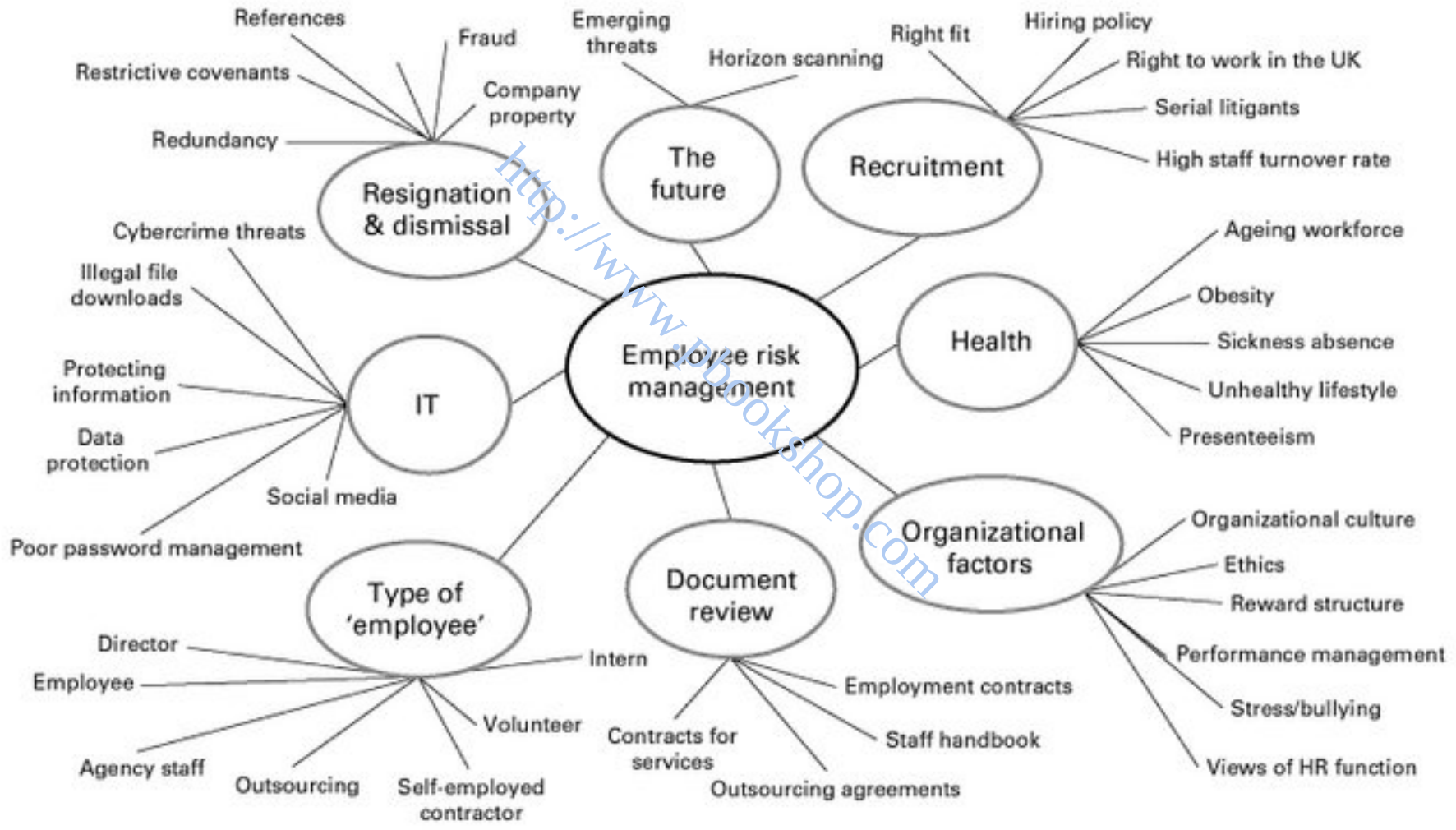
employees. The next stage is to identify the specific areas that will comprise the employee risk assessment. If it is to be thorough and look at an employer from the top down and inside out, it must consider a range of organizational factors, such as culture and the attitude to risk taking (see Chapter 2). It could also examine how the HR function is regarded. Without this, it will be difficult to obtain a full picture as to how well the policies and procedures it produces are viewed.

At this point, decisions on what else to include could be taken from different sources. One option is to look at regulatory requirements, such as compliance with anti-discrimination legislation, for example on age. Another is to examine 'employee' characteristics, such as ill health, obesity or remote workers. Alternatively, employment-related documentation could be reviewed, including the staff handbook and any outsourcing agreements that exist. Priority could then be given to known problems, such as poor disciplinary investigations and a weak social media policy. Alternatively, topic selection can be based on the employment life cycle. This would start with recruitment and work through different areas culminating with the end of employment. Last but not least is a different approach, which looks at key areas of concern. These could be based on those concerns already known to be an issue or suspected weakness in the organization, such as lack of employer control over employee use of social media. The best solution will be to combine these in order to arrive at the coverage that would best serve an organization's particular needs and budget (see Figure 1.1).

Improving legal compliance

A key advantage offered by an employee risk management approach is that it should reduce the likelihood of employment tribunal claims being brought (or threatened). This is because the focus moves to how those responsible for interpreting employment law requirements actually identify, interpret and follow them in practice (see Chapter 10). In this respect, this exercise also becomes a form of 'gap analysis' on how to move from the current state to a desired future state (see Chapter 4). If done well, it will identify any shortcomings in how quickly new or amended employment legislation and case law developments are reviewed and acted upon. It also offers a real-time picture of the level of employee risk that an organization actually faces: it moves the focus onto what an employee actually does in practice, rather than a theoretical review of what a company's mission statement and HR policies

FIGURE 1.1 Areas of coverage



says happens. In other words, the best drafted procedures will not prevent tribunal and other civil court claims if they are not followed.

For example, a textbook disciplinary procedure may exist, but the reality could be a high number of disciplinary hearings and subsequent appeals. A risk management approach can unearth the following: 1) line management failure to deal with problems informally; 2) weak or biased investigations; 3) poorly conducted hearings; and 4) managers failing to follow procedure. If this is so, closer investigation is necessary. A risk-based approach will look for the existence of specific trends, such as a higher incidence of disciplinary hearings in some sites or departments over others. If so, it could be down to a more confrontational or bullying style of management. The risk assessment could continue by drilling down to looking at what training is provided to managers. This would not only be on carrying out a disciplinary investigation, but also on conflict management and the need for early intervention in conduct and capability matters. It could also look at wider issues such as what extra pressures managers may be under locally that do not apply elsewhere.

Enhancing HR's profile

The HR function could benefit from being the initiator of an employee risk management review. Providing it retains ownership of the process, it will provide an opportunity to demonstrate to the board its business acumen and value. This is especially the case for large companies that are subject to regulatory controls such as Sarbanes–Oxley for public companies in the United States and CLERP 9 for their Australian equivalents. In the UK, listed companies are required to comply with the UK Corporate Governance Code (and other organizations may choose to follow its principles as good practice). The relevant section is Section C.2, which makes the board responsible: 'for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.'

It can be argued that the workforce could present a significant risk if various negative factors combine. For example, a disengaged workforce is more likely to perform badly, take time off sick and raise grievances. These problems are not UK-specific and will be costly in terms of money and time to any organization, making them of legitimate concern to shareholders. Thus HR can use the employee risk management process to enhance its standing and involvement

- will help HR demonstrate business acumen;
- is leverage for HR involvement in new areas such as employer branding.

Identifying areas to include can be done by:

- types of 'employee';
- types of characteristic protected by anti-discrimination legislation, eg age;
- other characteristics, such as ill health, obesity or remote workers;
- organizational factors, including culture and attitudes to risk taking;
- documentation, eg staff handbook, employment contracts and contracts for services;
- mapping out key stages in the employment life cycle, eg recruitment and dismissal;
- key areas of concern, such as threats to business reputation.

Threats to reputation are likely to arise where the following trigger points exist:

- disengaged employees;
- high staff-turnover rates;
- higher than expected levels of sickness absence;
- deteriorating employee performance;
- incidences of whistle-blowing;
- industrial sabotage;
- weak financial controls that have led to theft and/or fraud;
- key teams leaving to compete directly/work for competitors.

Chapter 2 looks at the organizational context of employee risk management, including culture, its determinants and how it influences attitudes to risk taking.

02 The organizational context

Introduction

As a concept, employee risk management cannot be fully understood without placing it within the context of the organization itself. This is because such an entity, be it a company, government department or a charity, is largely its workforce. In turn, this workforce will be part of a unique culture that determines the type of individual employed. It is this culture that also dictates the prevailing attitude to risk in general. In addition, each individual will also have their own perception of risk that they will bring to an employer, as well as their own personal ethical values. The first part of this chapter looks at these factors and how they influence employee risk taking, both individually and collectively. It also examines how an organization's leadership can introduce its own threats and vulnerabilities into the mix, as well as how the perception of the HR function influences how it will be viewed internally. Finally, the chapter introduces some work produced by the Institute of Risk Management (IRM), which offers a framework for how the management of risk (including employee risk) can be improved.

Organizational culture

A brief overview

Organizational culture refers to the personality of an organization and 'how we do things around here'. According to Deal and Kennedy (2000), its main determinant arises from the business environment itself. In other words, an organization's reality in the marketplace is largely influenced by its products and services, customers, competitor activities, prevailing technology and

regulatory framework. Values are also important as it is these that define what an organization stands for and what it establishes as standards for achievement. Where these values are strong, the organizational structure tends to be set up to reflect them. For example, companies that operate on high-volume turnover with low profit margins require tight cost control. This is reflected in the high status given to those operating on the financial side and their presence in top management positions. Where commercial success relies heavily on research and development (R&D), premium salaries and status are instead conferred on those working in these areas.

Other influences come from the language of anthropology. For example, those who strongly embody the organization's values are described as 'heroes' and become part of its mythology. This could be a charismatic founder, such as Virgin's Richard Branson or Apple's Steve Jobs, or an ordinary employee who invented a new process. There are also 'rites and rituals'. Rites show staff what is expected via rules and procedures; rituals include activities such as award ceremonies or after-work drinks. There may also be symbolism, such as corporate logos and status symbols. In all cases, their purpose is to reinforce the message of what the organization represents and how it defines success. Last but not least, there is the informal network. Sometimes referred to as a 'hidden' or 'cultural' network, it represents the main channel of communication. In other words, the source of what really happens rather than the official 'corporate-speak'. In fact, knowing who the right people are to get insight from is vital when doing the groundwork for an employee risk assessment!

Taken together, these elements are what differentiate one organization from another. For example, the underlying values and beliefs of a small charity will vary considerably from those of a commercial law firm operating in a highly competitive market. They will also be communicated in markedly different ways. For example, with a small charity, its CEO is likely to be the main source for transmitting its values, whereas a commercial law firm is likely to rely heavily on a slick induction process and glossy internal communications. There will also be established norms for behaviour and ways of working. Newcomers quickly learn what is expected of them via induction programmes and probation. If their face fits, employment is confirmed and the newcomer becomes an accepted part of the 'tribe'. Throughout their employment, they will usually be subject to regular appraisals, which, apart from assessing how well they perform in their role, will be another opportunity

to reinforce organizational values and beliefs. Whether these are positive or not is another matter entirely.

How culture influences risk taking

The dangers of 'groupthink'

Organizational culture plays a key role in determining attitudes to risk taking. This is because culture is created by those at the top with the power to impose their own values and beliefs onto the workforce. One factor in influencing this is the degree to which groupthink operates amongst the C-suite or managing board. This arises where groups desire a state of conformity to the extent that conflict is minimized and healthy debate on acceptable levels of risk taking is discouraged. As a result, probable threats and vulnerabilities inherent in a specific course of action are either not considered, or ignored. Also, the group dynamics evolve to such a degree that any independent thinkers will be deemed to be showing disloyalty to the group. By discouraging dissension, the groupthink mentality is elevated to a state where its members start believing in their own invincibility. This leads to a belief that their leadership and decision making is the only way forward – and thus the group becomes increasingly isolated from its workforce. As a consequence, directors, both as individuals and collectively, can introduce many threats and vulnerabilities into their organization.

The reason that groupthink can gain a foothold is due to the homogeneity of the decision makers. Since the recent banking crisis, much has been made of the fact that the boards of many private companies are dominated by white middle-aged men from similar social backgrounds (in other words 'male, pale and stale'). One reason for this is that it is natural to recruit in your own image. This is a safety factor, as it is assumed that those who are similar will share the same values and beliefs. In turn, this further reinforces and perpetuates the groupthink mentality. Also, headhunters wish to keep the fees rolling in by forwarding the same type of candidates that they successfully fielded before. In fact, it was only after the global downturn that the homogeneity of boards was seriously challenged. For example, Christine Lagarde (Head of the International Monetary Fund) commented, 'if it was the Lehman Sisters, the crisis might look quite different'. This has led to pressure within the European Union for the introduction of quotas to get more women on boards.

physical isolation from the workforce. Instead, profligate pay awards are still in evidence. For example, the independent, non-party think tank, the High Pay Centre (2013), found that UK high-street banks paid nearly 1,000 senior bankers over £1 million in bonuses in 2012 alone. This was accompanied by redundancies and pay freezes for the rest of the workforce. Such a damaging culture inevitably had a negative impact on the rank and file worker. According to the Chartered Institute of Personnel and Development (CIPD), *Employee Outlook: Focus on Rebuilding Trust in the City* (2013), fewer than one in three employed in financial services (outside senior management ranks) say that they are proud to work in the sector. Over 1,000 employees were interviewed and 65 per cent believe that some individuals in their business are being rewarded in a way that encourages poor behaviour.

So it is not surprising that in 2013, the UK's Chartered Institute of Internal Auditors updated its guidance to its members working in financial services. It recommends that internal audit should extend its scope to specifically examine the risk and control culture of the organization. This involves assessing whether or not decision making and the 'tone at the top' fits with the stated values, ethics and policies of the organization. The advice given in the publication is to assess the attitude and approach taken at all management levels towards risk management. Interestingly, this expressly includes looking at poor customer treatment that could lead to conduct or reputational threats. It goes on to suggest that internal audit should evaluate whether or not the organization is acting 'with integrity' in how it deals with customers and interacts with relevant markets. The point about relevant markets is a nod to the massive fines levied on several banks by the EU regulator for the LIBOR and EURIBOR scandal. Deutsche Bank had the largest fine at €725.36 million. Others fined include Royal Bank of Scotland and France's Société Générale.

Relationship to how HR is perceived

The organizational culture will heavily influence how HR is regarded. If, for example, it is seen as merely a support function separate from the real decision making, there will be no HR presence in the C-suite. In fact, according to Groysberg, Kelly and MacDonald in their *Harvard Business Review* article 'The New Path to the C-suite' (March 2011), HR is still struggling to gain influence. In qualitative interviews with global business leaders, they found that whilst the top people-management roles exist, they are being populated by non-HR professionals from other disciplines such as corporate

law, operations or marketing. This is largely due to the preference of CEOs for 'metrics-driven' leaders. In fact, this research found that the HR role was still viewed mainly as being administrative with HR directors mainly relegated to managing policies and cultural initiatives. In other words, HR is marginalized to more 'fluffy' activities that are not at the heart of the business.

The problem comes back to the organizational culture and the tone from the top. The harsh reality is that if the C-suite or equivalent decision makers have questionable ethics, and are inclined towards reckless behaviour, they are hardly likely to employ the type of HR director who will challenge it. If they do, that individual's tenure is likely to be a short one. There is also the question of remoteness, in that the more isolated senior management is from its workforce, the less likely that HR is to possess a high status. If senior HR staff lack access to the decision makers, and are unable to build relationships with them, the opportunity to be able to influence them is seriously limited. As a result, the C-suite or equivalent leadership are not exposed to the benefits that a good HR function can offer. A classic example of this is the banking sector, where HR lacked the proximity (and authority) to successfully challenge how the reward culture operated. Yet the paradox is that talent management is consistently a major concern of CEOs globally.

Impact of international culture

Another factor that influences the link between culture and risk taking is the particular country under the microscope. Given that cultures vary between countries this is reflected in how different organizations assess and view risk generally. For those operating internationally, it is vital that the differences that will be encountered are understood. The comparative work of social psychologist Geert Hofstede on national culture is useful here. Hofstede has created six 'dimensions' as a means of analysing different cultural values. In the context of propensity to take risks, some of the dimensions he outlines are more relevant than others. For example, he calls one dimension 'individualism–collectivism'. Individualistic societies are those that expect a high degree of self-reliance and for its citizens to look out for themselves and their immediate families. Naturally, this individualist outlook transfers itself to the workplace. So the UK, United States, Canada and Australia score highly here whereas countries such as China and Saudi Arabia score low. Collectivism is the opposite of this, with the dominant focus being on the needs of the group.

often be averted. Even if it is not, it still presents a chance to learn from any mistakes by turning them into a learning opportunity. This can then be shared across the organization and used to devise better systems and practices. Equally, there may be opportunities that can be utilized by those organizations that move fast enough to exploit them before their competitors. A good example is organizations that quickly harnessed the power of social media as both a marketing and recruitment tool, rather than just seeing the downsides.

The global consulting firm McKinsey has examined the traits of strong risk cultures and the part that risk managers have to play. In its article 'Managing the people side of risk', published in McKinsey Insights in May 2013, Krivkovich and Levy found that a key trait is being able to respond to emerging threats quickly. Another is the ability to break through rigid governance mechanisms to get the right people on board to tackle them. They also recognize that acknowledging risk requires a certain confidence. Not only must the environment (and its senior management) be strong enough to support this approach, but the policy framework must also be robust enough. Such a culture is likely to exist in an organization that openly discusses risk and looks for emerging trends (see Chapter 4). Unfortunately, though, such transparency and forward thinking is uncommon. Instead, there is either a flourishing blame culture, or attempts are made to ignore or suppress what is happening.

A good example of suppression is the US retailer Wal-Mart and the allegations made against it by a whistle-blowing employee in 2005. These involved the payment of alleged bribes worth over US $24 million to Mexican officials. Their purpose was to facilitate the speedy purchase of construction permits that would enable Wal-Mart de Mexico to achieve rapid market dominance with their stores. The company sent in investigators who found evidence of payments, as well as the fact that Wal-Mart de Mexico's leadership had deliberately concealed their existence from Wal-Mart's US headquarters. In the report, the lead investigator recommended that the investigation be widened, as it was believed that both US and Mexican laws had been violated. Yet, following an independent examination by the *New York Times*, it appears that Wal-Mart's bosses shut down the investigation. Not only this, but no law enforcement official in either country had been notified of developments.

In an article entitled 'Vast Mexico Bribery Case Hushed Up by Wal-Mart After Top-Level Struggle' published in the *New York Times* on 21 April 2012, reporter David Barstow also said that no one was disciplined. In fact, Wal-Mart de Mexico's chief executive, who was named as the driving force behind the bribery, was promoted to vice chairman of Wal-Mart. Until media involvement in the affair, it appears that much time and effort had been spent on damage control rather than getting to grips with the scale of criminality involved. One example of this was a rapid modification of protocols for internal investigations. Its purpose was to give those being investigated more control over the process and to add layers of bureaucracy, such as requiring a cost-benefit analysis before agreeing to a full investigation. Only when the allegations against Wal-Mart were published, did Wal-Mart inform the US Justice Department of possible violations of federal law.

Improving organizational culture

All the examples given above are of environments where the organizational culture needs to be reviewed and changed. Until this happens, sufficient buy-in to the adoption of an employee risk management approach is unlikely. If it does occur, it will have only a limited impact as the senior level support essential to its embedding throughout the organization will be lacking. To combat this, two pieces of work produced by the IRM (as set out below) provide frameworks on what a healthy risk culture looks like. The first is a generic model on risk (see Table 2.1) and the other is a questionnaire on ethics. They have been chosen because: 1) they are straightforward and not complicated; 2) they are compatible with each other and the concept of employee risk management; and 3) both offer new opportunities for HR to proactively contribute to improving an organization's employee risk culture. Another advantage is that both models can be used together, as they complement each other.

The model is fairly self-explanatory. Developed by the IRM, it is called a 'Risk Culture Aspects Model' (Hindson: IRM, 2012). This model proposes eight 'aspects', grouped into four 'themes'. All must be in place to ensure that an organization has a healthy risk culture.

TABLE 2.1 Risk culture aspects model

Theme	
Tone at the top	Risk leadership: clarity of direction • senior management set clear and consistent expectations for managing risks • leaders role model risk management thinking and actively discuss tolerance to risk issues Responding to bad news: welcoming disclosure • senior management actively seeking out information about risk events • those that are open and honest about risks are recognized
Governance	Risk governance: taking accountability • management are clear about their accountability for managing business risks • role descriptions and targets include risk accountabilities Risk transparency: risk information flowing • timely communication of risk information across the organization • risk events are seen as an opportunity to learn
Competency	Risk resources: empowered risk function • the risk function has a defined remit and has the support of leaders • it is able to challenge how risks are managed Risk competence: embedded risk skills • a structure of risk champions support those managing risks • training programmes are in place for all staff
Decision making	Risk decisions: informed risk decisions • leaders seek out risk information in supporting decisions • the business's willingness to take on risks is understood and communicated Rewarding appropriate risk-taking • performance management linked to risk-taking • leaders are supportive of those actively seeking to understand and manage risks

Reproduced with kind permission of the Institute of Risk Management

Whilst this model refers to both risk in general and the existence of a dedicated risk function, it can easily be used in the context of employee risk. In fact, all four themes of: 1) tone at the top; 2) governance; 3) competency; and 4) decision making are revisited to varying degrees throughout this book (see Chapter 12 in particular). There is a possibility that where risk managers are employed, they may already be familiar with this model (especially if they are members of the IRM). The same applies to any internal audit team in place. If so, the model may already have been implemented in some form or other. Should this be the case, HR could suggest that this model's use be extended to formally incorporate employee risk. Should the model not be already in place, HR could propose its introduction by the board; even if only initially used in the context of managing employee risk.

Where there are also serious concerns over an organization's ethical standards, a questionnaire produced by Peter Neville Lewis for the IRM's document 'Risk Culture: Resources for Practitioners' (2012) can help get it back on track. Equally, it is a good benchmark for those employers who may wish to improve their organization's reputation. The questionnaire is called a 'risk and ethics culture assessment' (RECA) and its purpose is to ensure that the right standards are in place. This is to: 1) minimize risk; 2) protect an organization's reputation; and 3) maximize what Lewis refers to as sustainable profit. This model contains 10 questions that come with the advantage of having a global application and relevance (see box below).

Risk and ethics culture assessment, by Peter Neville Lewis

1. How well disciplined is your organization to meet the emerging public and regulatory demand for demonstrating risk-balanced and ethical decision making in the way you transact business with ALL your stakeholders in the global economy?
2. How clearly does your organization articulate and communicate its values in order to guide risk-balanced and ethical decision making at all levels? Where are the roadblocks to risk evaluation?
3. How well examined is your Values Statement to determine if these are based on true moral values like courage, self-discipline, fairness, trust etc rather than desired outcomes (eg reputation or efficiency)?
4. How committed is your organization to putting moral values and moral purpose, which affect ALL stakeholders, before just value for shareholders?

5 How strongly does your CEO (which might equally imply Chief Ethics Officer) champion a culture for balanced risk taking and decision making – A Culture of Enlightened Integrity?

6 How well emphasized in your Risk Register are 'RIGHT' (see below) decision making and effective measures to mitigate reputational risk caused by careless thinking? Is there a clear framework?

7 How open and properly supported at grass roots are your whistle-blowing culture and speak-up processes, to encourage people at all levels to speak the truth?

8 Have you identified or appointed independent Risk and Ethics Ambassadors at all levels to advise on and monitor risk and ethical dilemmas and to report to appropriate line managers (HR/Legal/Risk if appropriate)?

9 How clearly articulated is your organization's remuneration and reward structure to encourage and reward balanced risk taking and ethical decision making?

10 How firmly is your organization opposed to individual gain and corporate excess in its relations with ALL its stakeholders?'

Reproduced with kind permission of the Institute of Risk Management

Note

'RIGHT' stands for:

- **R-ules:** do we know and operate within them?
- **I-ntegrity:** do we act out ALL 10 moral values that could be held to make up integrity?
- **G-ood:** is our decision making intended to do good? For whom?
- **H-arm:** will our decision making cause unintentional harm? To whom?
- **T-ruth and T-ransparency:** can we stand behind our decision with a clear heart?'

Organizational culture influences the acceptability of risk taking via:

- the extent to which the board is susceptible to 'groupthink';
- where independent thought is discouraged and leaders believe in their own invincibility;
- how physically isolated the top management become from the workforce;
- how homogeneous the board is in terms of being 'male, pale and stale';
- the ethics that the board bring with them, both individually and collectively;
- the manner in which business ethics are set from the top and filtered downwards;
- a link between a lack of ethics and greed that is supported by a short-term business outlook;
- having a weak HR function that lacks the clout to challenge rewards systems;
- a cultural view of how risk taking is viewed in the country that the enterprise operates in.

Organizational culture and how HR is regarded:

- research found that CEOs want 'metrics-driven' leaders in the C-suite;
- top people-management roles are taken by non-HR professionals;
- the more isolated the board, the less likely HR is to possess a high status;
- isolation means that HR lacks the opportunity to demonstrate its value;
- organizational culture and how HR is regarded:
  - will influence how well the workforce respects and follows HR policies;
  - determines whether HR is seen as value adding or merely a support function.

The link between culture and risk taking is significant as it:

- determines how senior management will react to unavoidable problems;
- influences whether or not staff feel they can report potential threats and vulnerabilities;
- defines whether or not serious problems are treated as a learning opportunity.

Improving the culture:

- is necessary to obtain buy-in to an employee risk management approach;
- board level commitment is needed in order to embed it throughout the organization;
- can be achieved by using the IRM's 'Risk Culture Aspects Model' – this looks at 'tone at the top', governance, competence and decision making;
- can be achieved by incorporating a risk and ethics culture assessment (RECA) into the organization.

Chapter 3 looks at the essential pre-assessment groundwork that should be covered before the project starts.