

Take the right steps  
9 principles for  
building the Risk  
Intelligent Enterprise™









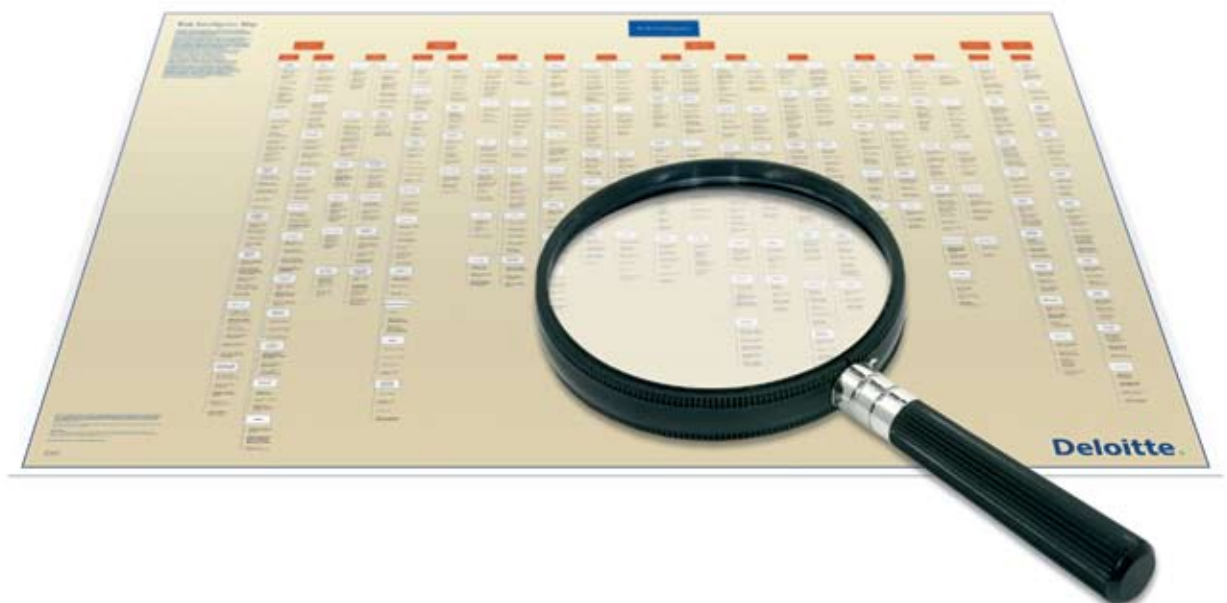
# Preface

This publication represents the first part in Deloitte's series on the fundamental principles of Risk Intelligence. The papers in the series are intended to offer simple descriptions of the basic elements of a Risk Intelligence programme, as well as insights and practical steps you may consider for incorporating the concepts within your own organisation.

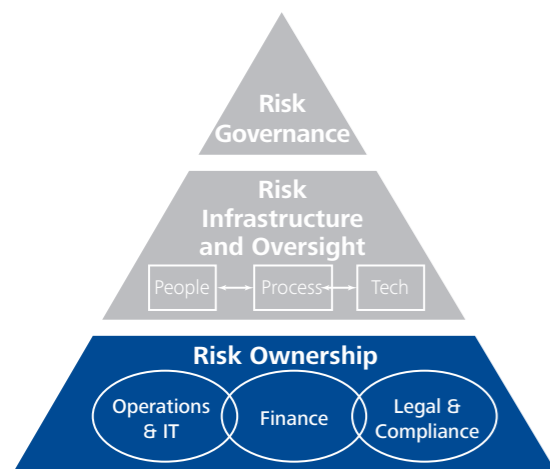
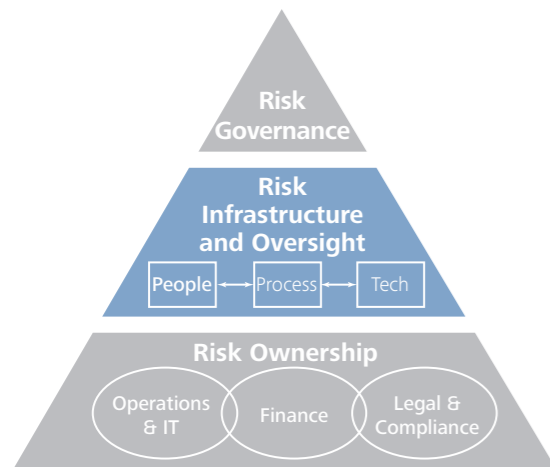
On each of the following pages, you will find a statement describing a single principle of a Risk Intelligence programme, along with an elaboration on the topic. We believe application of these principles as a whole will help create a Risk Intelligent Enterprise.

Although this paper is the first in our 'Fundamental Principles' series, it is by no means our initial words on the subject of Risk Intelligence. In fact, we have published over a dozen related titles as well as numerous podcasts and webcasts. You may access all of this material free of charge at [www.deloitte.com/RiskIntelligence](http://www.deloitte.com/RiskIntelligence).

Open communication is a key characteristic of a Risk Intelligent Enterprise. Please consider sharing this publication with the other executives, board members, and key managers in your organisation. The issues and concepts outlined here should provide an excellent starting point for a crucial dialogue on enhancing your organisation's Risk Intelligence.



## 9 principles for building a Risk Intelligent Enterprise



### Risk Governance

**#1** – A common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organisation

**#2** – A common risk framework supported by appropriate standards is used throughout the organisation to manage risks

**#3** – Key roles, responsibilities, and authority relating to risk management are clearly defined within the organisation

**#5** – Governing bodies (e.g., boards, audit committees, etc.) have appropriate transparency and visibility into the organisation's risk management practices to discharge their responsibilities

### Risk Infrastructure and Oversight

**#6** – Executive management is assigned with primary responsibility for designing, implementing, and maintaining an effective risk programme

**#4** – A common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities

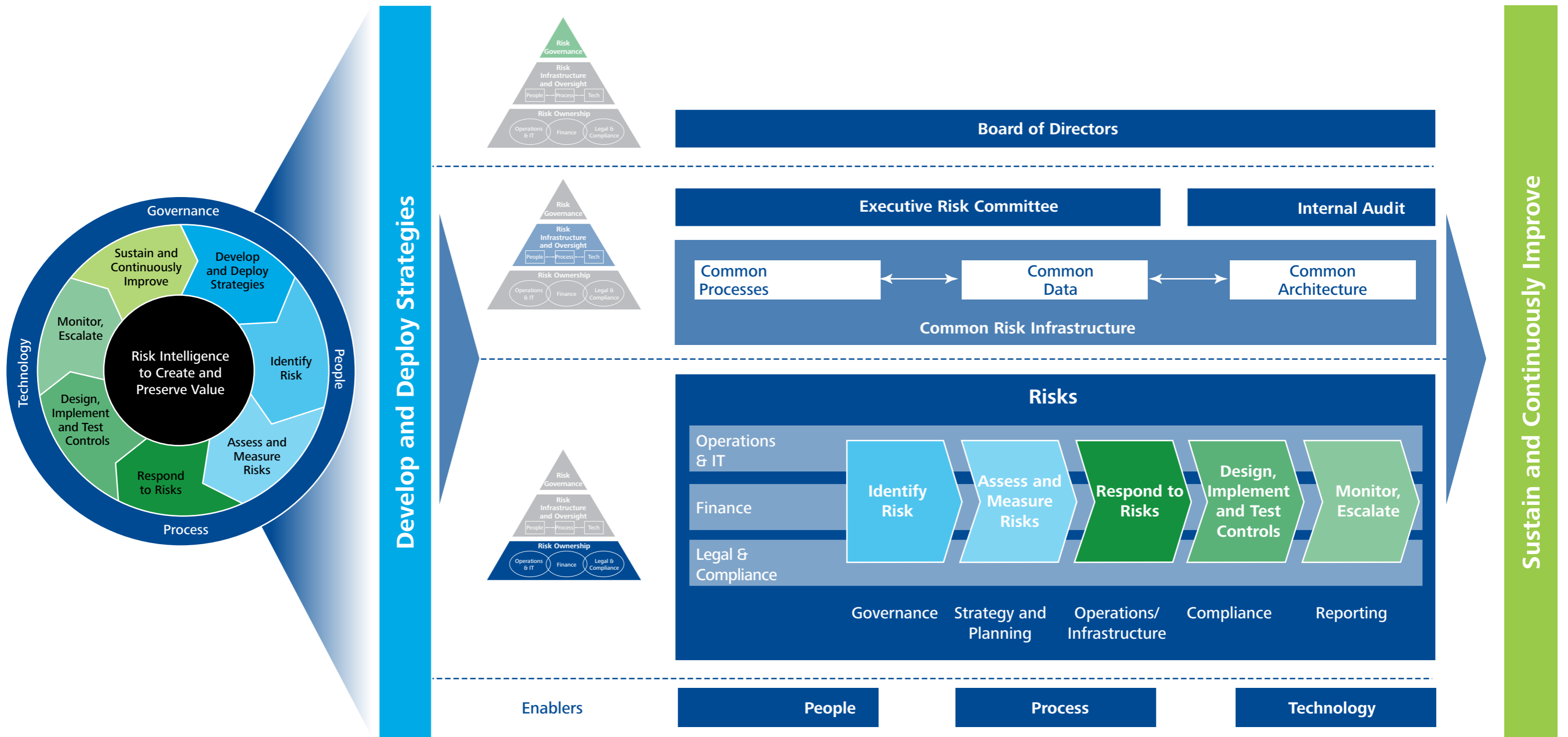
**#9** – Certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organisation's risk programme to governing bodies and executive management

### Risk Ownership

**#7** – Business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management

**#8** – Certain functions (e.g., finance, legal, HR, etc.) have a widespread impact on the business and provide support to the business units as it relates to the organisation's risk programme

## The Risk Intelligent Framework



# Is risk a threat or opportunity?

---

Principle #1: In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organisation.

Risk is often a topic of conversation that many businesses avoid. This is understandable because many people think of risk in terms of threats — bad things happening to the business.

But the discussion can flow freely if you consider the other side of risk, the one that applies to value creation — risk taking for reward.

Introducing new products, entering foreign markets, and acquiring competitors — all these are challenging ventures. If you do not manage the associated risks properly, you may not reap the potential rewards.

So consider adopting a more comprehensive definition of risk, one that gives equal weight to managing the risks related to growth and profitability.



# A risk framework that meets your needs

Risk management in many organisations is fragmented and does not have a centralised view. This fragmented approach leads to duplicated risk management efforts and risk technology implementation, which also results in multiple sources of risk information.

For an enterprise risk management programme to be effective, it must be built around a framework. A risk framework — such as COSO ERM and ISO 31000 — allows for efficient risk-based decision making and provides a streamlined process for evaluating opportunities for your organisation. It provides a structured guidance that helps you decide which opportunities to pursue and which threats to avoid.

The framework must therefore be robust to support your risk management objectives. It must accommodate your unique strategies, initiatives, and organisational structure. And it must be adaptable to your industry and regulatory requirements.

There is no need to over evaluate which risk framework to use. Just make sure it is something that is able to meet your organisation's needs.

---

**Principle #2: In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organisation to manage risks.**



# Coordinated, communicated risk management

---

Principle #3: In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined within the organisation.

Done right, risk management is a coordinated effort, where multiple roles are involved simultaneously in an integrated manner.

Of course, there may be people in your organisation who do not realize they have a role to play in risk management. Your product development manager, IT supervisor, or deputy vice president responsible for mergers and acquisitions probably considers risk management as somebody else's responsibility.

To promote Risk Intelligence in your organisation, it is essential to change that mindset. You will need clear communication at the individual level to convey what Risk Intelligence means, why it is important to the organisation collectively and to employees individually, and what your people need to do on a daily basis.

This effort requires clear communications, a strong risk-focused culture, reward programmes that incorporate risk-related objectives, and learning programmes to promote intelligent risk management.

In brief, risk management needs to be a harmonious collaboration where:

- the board sets the direction
- the executive leads the risk programme
- the business units work as a team for a successful implementation
- certain functions (HR, finance, IT, legal, tax) support the risk programme
- other functions (internal audit, risk, and compliance) monitor the results.



# A common language for all

Risk specialists tend to behave like any social groups: They stick together. They share similar beliefs and habits. They develop their own set of rules.

However, it is essential for risk specialists to break away from their groups. Risk does not exist in isolation, so risk managers cannot do so either.

To effectively and efficiently manage risks and reap the rewards, organisational silos must be bridged. In particular, a common risk infrastructure needs to be created. All the business units and functions should also use the same supporting risk technologies and processes where it is practical to do so.

The bridging process involves synchronising — coordinating across boundaries within the organisation, harmonising — ensuring that risk managers all speak the same language and have a common definition for risk, and rationalising — eliminating duplication of efforts.

The bridging process also involves the use of tools like The Risk Intelligence Map™ to facilitate your internal discussions. It may get you thinking and talking about risk in ways you have never envisioned. In addition, you should also draw upon your risk framework to help standardise your approach.

Common risk technology, measurement, processes, and terminology will provide the link to bridge all the business units and functions within the organisation.

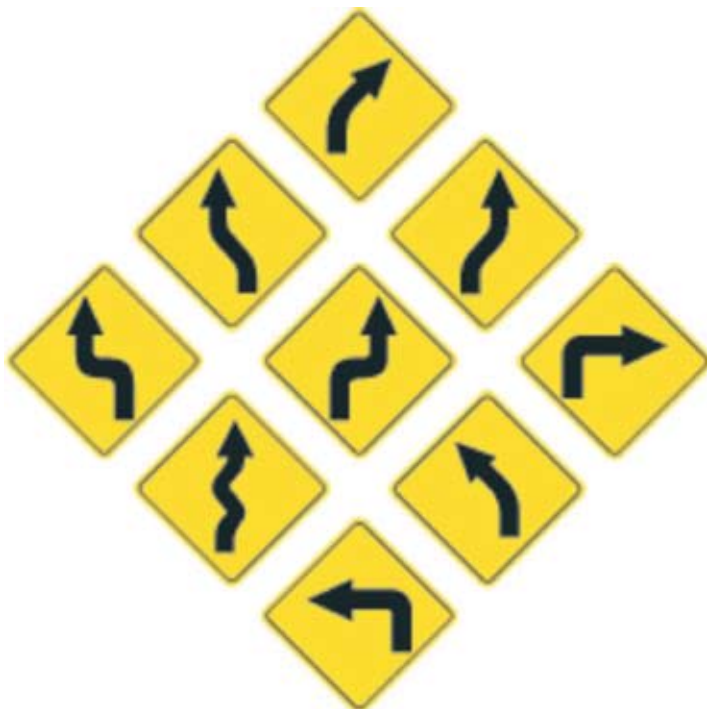
---

Principle #4: In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.



# Know your risk

**Principle #5: In a Risk Intelligent Enterprise, governing bodies (e.g., boards, audit committees, etc.) have appropriate transparency and visibility into the organisation's risk management practices to discharge their responsibilities.**



Some boards of directors are not kept informed on how risk is being managed within the organisation. This should obviously be avoided as board members have a fiduciary responsibility to ensure that management has appropriate processes in place to manage risk. This duty cannot be executed without the right knowledge.

To fulfill their responsibilities and to provide value, board members should:

- put risk on the agenda. Make time for risk before risk demands it. Discussing risk at every board meeting is not too often
- examine the current risk structure. How are risks managed? Are risk silos being bridged?
- review risk periodically with the management team. Identify risks that will prevent the organisation from executing its key strategies
- discuss risk scenarios. Where do the greatest opportunities lie? What could put a stop to the organisation's ability to meet its strategic objectives?
- check the organisation's risk appetite. Determine how much risk the organisation is able to take on. How much is it willing to take on? And how much is it actually taking on? Are these in line?
- get reasonable assurance. Ask the management team: How confident are you? Why?
- get independent reassurance. Conduct an internal audit or engage an external consultant to evaluate the effectiveness of your risk management programme.

# Risk begins from the top

Everyone has a responsibility for risk. But if you are a member of the executive team, this responsibility is even greater.

As an executive, you have the benefit of leadership and authority. You need to exercise them to get people thinking about risk taking for reward, to push risk management through all the layers of the organisation, to set expectations, to ensure accountability, to engage the board, to drive change, and to establish a Risk Intelligent culture.

This is an ambitious agenda. How can you get it all done? Form a Risk Intelligence group — an executive-level risk committee — to bring better risk insights to your management team and help create a Risk Intelligence programme.

In some organisations, a key member of this executive-level Risk Intelligence group is the Chief Risk Officer (CRO). Sitting at the table with other top executives, the CRO helps develop policy and common approaches that are rolled out to business units, communicates and monitors the organisation's risk appetite, and reports risk information to the management and board-level oversight functions.

The role of the CRO varies considerably and needs to match the requirements and risk philosophy of the organisation. Some may choose to take on the role of a business partner, a facilitator, or even a traffic police. Whatever the role, you can be sure the risk programme is their primary responsibility.

---

Principle #6: In a Risk Intelligent Enterprise, executive management is assigned with primary responsibility for designing, implementing, and maintaining an effective risk programme.



# Risk ownership

---

**Principle #7: In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.**

So everyone is responsible for risk. But who “owns” it?

The ownership question causes plenty of confusion throughout organisations, so it might be helpful to state it in simple terms: If you own the business unit, you own the risk.

In other words, if you are accountable for the success of a business unit, you have primary responsibility for the day-to-day management of the risks associated with that unit. But this does not mean the other members of the business unit do not need to carry out their risk-related responsibilities.

What does risk ownership involve? Among other things, risk owners have the responsibility to identify, measure, monitor, control, and report on risks to executive management, promote risk awareness, and reprioritise activities as dictated by effective risk analyses.

Needless to say, risk owners must also abide by the rules and operate under certain constraints. For example, they do not choose the framework — they live within it. They do not determine the organisation’s risk appetite — they stay within the level determined by the organisation.



# The risk support team

Certain functions, including finance, legal, human resource (HR), tax, and IT, differ from the business units in that they do not just own risk management — they also help support it.

Like the business units, these functions bear primary responsibility for the risk that originates within their operations. At the same time, they also have risk responsibilities that go beyond their functions.

For example, finance who takes the lead on internal control audit related risk may have an extensive risk assessment capability that can be leveraged by other functions. Other than taking the lead for technology related risk, IT can help other parts of the business monitor and mitigate risks. While HR's primary responsibility is talent and staff risk, they can also identify risk areas of emerging concern through employee engagement surveys, and exit interview results.

As these functions are present throughout the organisation, they are usually tasked to develop and enforce company-wide policies, procedures, and controls that help mitigate risks. They support each business unit and help them understand their requirements for intelligent risk taking for reward. They collect key information for management and perform risk mitigation analyses.

It is important that these key functions join the risk team with defined roles in the risk framework and by participating in risk committees and other key risk forums.

---

**Principle #8: In a Risk Intelligent Enterprise, certain functions (e.g., finance, legal, IT, HR, etc.) have a widespread impact on the business and provide support to the business units as it relates to the organisation's risk programme.**



# The risk observer

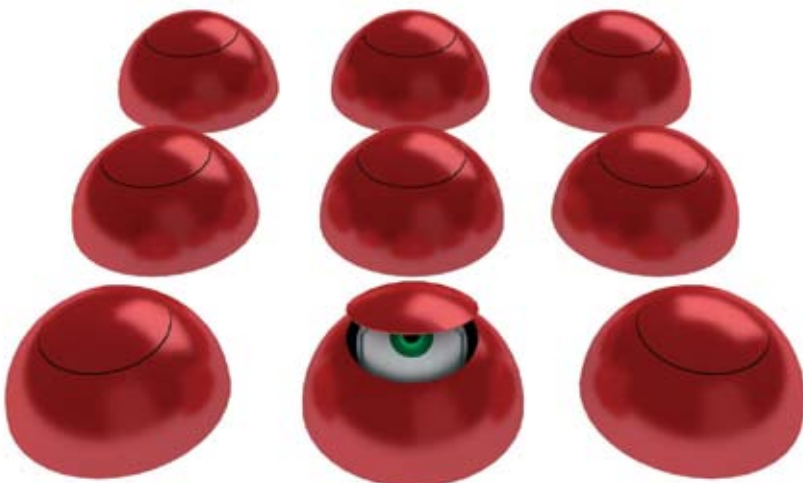
**Principle #9: In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organisation's risk programme to governing bodies and executive management.**

When it comes to risk management, certain groups within the organisations carry a unique role — namely, the internal audit, compliance, and risk management functions. Their key responsibility is to provide assurance that the internal control and risk structure operates effectively.

This role sets them apart from every other entity within the organisation. They have no responsibility for setting and directing the operations of the business. Their role is to monitor and enhance the effectiveness of the organisation's risk management activities.

Specific roles and responsibilities of these groups vary from one organisation to another. Some groups do far more than provide reassurance, while others are more restricted in their activities. The roles they can play include:

- assessing the current state of risk management, while providing the vision to help management identify future risks and opportunities
- determining whether the organisation is taking on risk at a level that it is able to manage
- verifying if the organisation is ensuring that risk is interacting and descending at an appropriate level
- investigating ways to eliminate inefficiencies in risk management
- gathering support for resources related to risk-taking for reward, addressing risks associated with increasing profitability, and increasing shareholder value
- drawing attention to and getting support for resources to address risk areas deemed insufficiently covered
- providing deep knowledge and expertise in key risk areas such as fraud
- getting involved in control rectification and design, and helping to conduct and interpret risk assessments.



# Key contacts in Australia

## Sydney

Ron Loborec

Partner

[rloborec@deloitte.com.au](mailto:rloborec@deloitte.com.au)

+61 (0) 2 9322 7163

## Mark Young

Partner

[mayoung@deloitte.com.au](mailto:mayoung@deloitte.com.au)

+61 (0) 2 9322 3533

## Melbourne

Matthew Fraser

Partner

[matfraser@deloitte.com.au](mailto:matfraser@deloitte.com.au)

+61 (0) 3 9671 7261

## Brisbane

Matt Thomson

Partner

[matthomson@deloitte.com.au](mailto:matthomson@deloitte.com.au)

+61 (0) 7 3308 7153

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.