Deloitte.

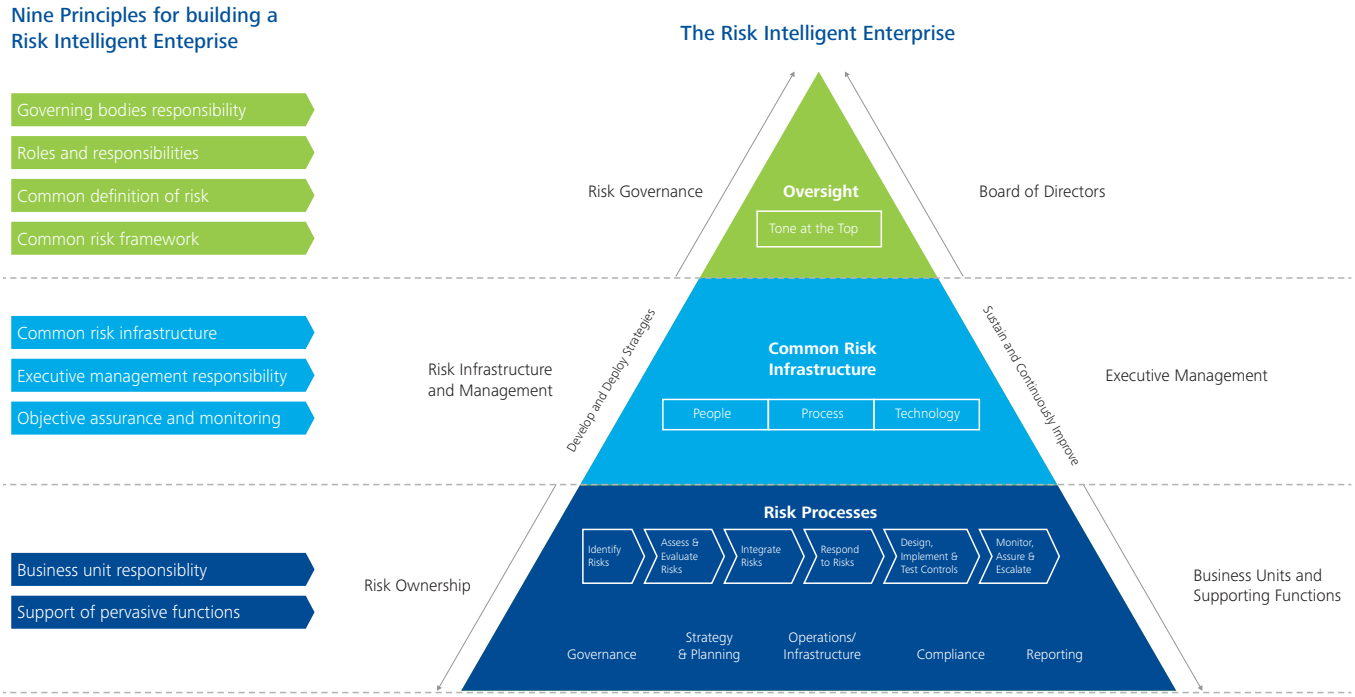
Risk intelligent enterprise

At many organisations, risk governance and value creation are viewed as opposed or even as mutually exclusive, when in fact they are inseparable. Every decision, activity, and initiative that aims to create or protect value involves some degree of risk. Hence, effective risk governance calls for Risk Intelligent governance - an approach that seeks not to discourage appropriate risk-taking, but to embed appropriate risk management procedures into all of an enterprise's business pursuits.

Deloitte's concept of the Risk Intelligent Enterprise integrates nine principles related to the responsibilities of the board, senior management, and business unit leaders into a cohesive risk management framework. Risk governance is at the apex of the framework: the unifying touchstone and guide to all of the organisation's risk management efforts. But on a more detailed level, what does effective Risk Intelligent governance entail?

Nine fundamental principles of a Risk Intelligence program

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.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organisation to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organisation.
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.
5. In a Risk Intelligent Enterprise, governing bodies (e.g., boards, risk committees, audit committees, etc.) have appropriate transparency and visibility into the organisation's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
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.
8. In a Risk Intelligent Enterprise, certain functions (e.g., Finance, Legal, Tax, IT, HR, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organisation's risk program.
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 program to governing bodies and executive management.



Based on our experience working with boards in their risk governance efforts, we have identified six distinct actions a board can take to help enable a Risk Intelligent governance approach:

1. Define the board's risk oversight role (delegated to the risk committee)
2. Foster a Risk Intelligent culture
3. Help management incorporate Risk Intelligence into strategy
4. Help define the risk appetite
5. Execute the Risk Intelligent governance process
6. Benchmark and evaluate the governance process

Collectively, these "areas of focus" reflect the view that risk-taking for reward and growth is as important as risk mitigation to protect existing assets. By treating risk as intrinsic to the conduct of business, Risk Intelligent governance elevates risk management from an exercise in risk avoidance to an essential consideration in every decision, activity, and initiative.

Area of focus 1: Define the board's risk oversight role

Effective risk oversight begins with a solid mutual understanding of the extent and nature of the board's responsibilities as compared to those of management and other stakeholders. Key board-level responsibilities include setting the expectations and tone, elevating risk as a priority, and initiating the communication and activities that constitute intelligent risk management. The ultimate goal is to assist management in creating a cohesive process in which risks and their impacts are routinely identified, evaluated, and addressed.

A board should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk.

Actions to consider in defining the board's risk oversight role:

- **Define the board's risk governance roles and responsibilities.** Although the entire board is accountable for overseeing risk management and should be involved in the risk oversight process, it may delegate responsibility for risk oversight to the risk committee. Having various committees play complementary roles in risk oversight (e.g. risk committee, audit committee, remuneration committee, etc.) - and share their findings and insights with each other and the entire board - can help set the tone that risk oversight is important to all board and committee members. Even in boards where the nominal responsibility for risk oversight rests with a single committee all board members should recognise that risk oversight is broader than that single committee. In any case, all such roles and responsibilities should be formally defined and clearly understood.
- **Consider board composition**. In our view, a board should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk. Consider performing a periodic evaluation, perhaps carried out by the nominations committee, of the board's overall composition as well as each member's experiences, knowledge, and special characteristics and qualities. Having the right mix of board members at the table will allow for discussions that are founded on Risk Intelligent knowledge and perspective.
- **Establish an enterprise-wide risk management framework**. Like any organisational process, risk management requires a framework that defines its goals, roles, activities, and desired results. Deloitte's concept of the Risk Intelligent Enterprise describes an approach to risk that can strengthen an existing framework or constitute a framework itself. Ideally, the chosen framework will help management establish goals, terms, methods, and measures, as well as gauge the need for specific programs (such as a contract risk and compliance program or training programs on risk awareness).
- **Perform site visits.** Consider touring the organisation's facilities to enhance your understanding of work processes and the risks associated with value creation and preservation. A number of boards today are indeed using site visits to broaden their knowledge of - and demonstrate their interest in – the work of the enterprise.

Questions to ask about risk oversight:

- How is risk overseen by our various board committees?
- Is there appropriate coordination and communication?
- Are we getting the information and insights we need for key decisions?
- Which framework has management selected for the risk management program? What criteria did they use to select it?
- What mechanisms does management use to monitor emerging risks? What early warning mechanisms exist, and how effective are they? How, and how often, are they calibrated?
- What is the role of technology in the risk management program? How was it chosen, and when was it last evaluated?
- What is the role of the tax function in the risk management program? Are we taking steps to demystify tax by gaining a high-level understanding of not only the downside consequences of tax risks, but also the upside potential that a robust tax risk management program can offer?

Area of focus 2: Foster a Risk Intelligent culture

In a Risk Intelligent culture, people at every level manage risk as an intrinsic part of their jobs. Rather than being risk averse, they understand the risks of any activity they undertake and manage them accordingly. Such a culture supports open discussion about uncertainties, encourages employees to express concerns, and maintains processes to elevate concerns to appropriate levels.

Actions to consider in fostering a Risk Intelligent culture:

- **Lead by example in communicating about risk.** The risk committee should ask management about the risks of specific decisions, activities, and initiatives. It should set expectations with senior executives and business unit leaders about what information the committee expects and how it will be conveyed. The committee should set the tone for an open and candid dialogue. Also, the risk committee has to work with management to develop appropriate messaging about the risk environment for the rest of the organisation.
- **Build cohesive teams with management.** Culture change occurs not by decree but through interactions with management. The committee should create opportunities to engage with management and to learn more about their risk management practices. These interactions can form the basis of a continual, interactive process of alignment that both allows the committee to refine its views and priorities, and enables management to adjust its practices to reflect your guidance.
- **Reward Risk Intelligent behaviour.** The risk committee should consider incorporating risk-related objectives into the company's executive remuneration structures. It may also wish to urge management to weave risk management practices into job descriptions, training, work processes, supervisory procedures, and performance appraisals.
- **Consider a third-party assessment.** In addition to self-assessment, commissioning an independent external review of the risk governance policies, procedures, and performance can yield useful benchmarking information and shed light on leading risk governance practices.

Questions to ask about the organisational culture:

- How are we communicating our Risk Intelligence messages and assessing the extent to which Risk Intelligence is understood throughout the enterprise?
- Are people comfortable in discussing risk, or are they afraid to raise difficult issues? How quickly do they raise issues?
- How might our remuneration programs encourage inappropriate short-term risk taking? How can we change these programs to encourage Risk Intelligent risk-taking instead? What mechanisms exist to recover remuneration when excessive risk-taking occurs?
- Has the organisation developed a common language around risk that defines risk-related terms and measures and that promotes risk awareness in all activities and at all levels?
- How have we demonstrated the significance of risk governance in our documentation and communications?
- What tools are we using to gauge our risk governance effectiveness, and with what results? What benefit might we derive from an independent evaluation?

Area of focus 3: Help management incorporate Risk Intelligence into strategy

Since one of a board's main responsibilities is to oversee the strategy-setting process, helping management incorporate Risk Intelligence into strategy is an inherent part of the risk committee's overall role. Drawing on a solid practical understanding of the enterprise's efforts around value creation and preservation, the committee can work with management to collaboratively move from a negative "incident" view of risk to a more positive "portfolio" view that considers risks and rewards in a broader strategic context.

Actions to consider in helping management incorporate Risk Intelligence into strategy:

- **Design processes for integrating risk management into strategic planning.** The committee may consider augmenting the overall strategic planning process with processes for considering risks across the organisation, prioritising the risks, and appropriately allocating risk management resources. It should consider the scenario-planning process and whether it incorporates both upside and downside risks, as well as a view into the overall risk exposures and opportunities. The committee may wish to develop processes that help verify that risk management incorporates value creation as well as preservation, that the risk appetite is defined and risk tolerances are identified, and that risk is handled accordingly. Also, the risk committee can include discussions about risk at retreats devoted to strategy.
- **Monitor strategic alignment.** Monitoring strategic alignment involves analysing the risk-return trade-off in setting the company's financial goals, the proposed means of reaching those goals, and likely constraints. To execute this monitoring, the risk committee will need to maintain visibility in strategic planning and risk-reward decisions. The committee must make it clear that any changes or events with potentially significant consequences for the organisation's reputation, as well as its financial position, are to be brought to its attention for consideration.
- **Establish accountability.** The risk committee should establish and reinforce executive accountability for risk management. One way to do this is to expect full disclosure by management of the risks associated with each aspect of the strategy. Give management on-going feedback about your satisfaction with their level of disclosure and the quality of risk-reward analyses. A formal evaluation process for specific executives, led by the chair of the risk committee may be considered.

Questions to ask when helping management incorporate Risk Intelligence into strategy:

- How can we build Risk Intelligence into decisions about capital allocation, acquisition, succession planning, and other strategic initiatives?
- How should risk-return trade-offs be weighed in strategic planning and review sessions? How can we generate more meaningful discussion of these trade-offs?
- What is the process for identifying and evaluating changes in the external environment? How are these findings considered in strategic planning?
- How realistic is the strategy? Under what scenarios would the strategy be achieved - or fail to be achieved – and what are the intended results or plans if it fails?
- What would it take - in resources, knowledge, alliances, or conditions - to increase the likelihood of achieving the desired results and to reduce the chances of failure?

Area of focus 4: Help define the risk appetite

Risk appetite defines the level of enterprise-wide risk that leaders are willing to take (or not take) with respect to specific actions, such as acquisitions, new product development, or market expansion. Where quantification is practical, risk appetite is usually expressed as a monetary figure or as a percentage of revenue, capital, or other financial measure (such as loan losses); however, we recommend that less quantifiable risk areas, such as reputational risk, also be considered when setting risk appetite levels. While the CEO proposes risk appetite levels, the risk committee on behalf of the board ought to approve them - or challenge them and send them back to the CEO for adjustments - based on an evaluation of their alignment with business strategy and stakeholders' expectations.

Risk appetites may vary according to the type of risk under consideration. Using a Risk Intelligent approach, companies ought to have an appetite for rewarded risks such as those associated with new product development or new market entry, and a much lower appetite for unrewarded risks such as non-compliance or operational failures. Some risks just come with the territory. If you are in the chemical business, there will inevitably be environmental spills and health and safety incidents. If you don't have the appetite for those types of risks, then you probably shouldn't be in that business. Once you have accepted this reality, you should do everything to prevent, rapidly detect, correct, respond to, and recover from any such incident.

Once the risk appetite is defined, management then should define specific risk tolerances, also known as risk targets or limits, that express the specific threshold level of risk by incident in terms that decision-makers can use (for instance, in completing an acquisition, the risk tolerance may be defined as a stop-loss threshold of a specified value). Management may have no tolerance for unethical business conduct or for environmental, health and safety incidents by adopting a zero incidents policy.

One important management responsibility is to continually monitor the company's risk exposures, evaluate actual risk exposure levels against the stated risk appetite, and adjust risk tolerances and policies as necessary to align actual risk exposure with the desired risk exposure as defined by the risk appetite. By having management report on this process to the risk committee, members can gain insight into whether there may be opportunities for further risk-for-reward strategies or, conversely, if the organisation is overly "stretched" in its risk levels.

Companies ought to have an appetite for rewarded risks...and a much lower appetite for unrewarded risks.

Actions to consider in helping to define the risk appetite:

- **Distinguish between risk appetite and risk tolerance.** Many business unit leaders and some senior executives fail to distinguish between risk appetite and risk tolerance. As a result, many organisations either set arbitrary risk tolerances that do not track back to an overall risk appetite, or wrongly assume that a general statement of risk appetite gives decision-makers enough operational guidance to stay within its parameters. The risk committee can help the organisation steer clear of these traps by assisting management in developing a cogent approach to defining the risk appetite, specifying risk tolerances, and communicating them across the enterprise.
- **Serve as a sounding board.** The committee should be available as a resource for helping senior executives understand and reconcile various views of risk within the organisation. One way to do this is to ascertain how management balances and aggregates the business units' risks as well as how management sets various risk tolerances, particularly in relatively risky businesses or markets.

Questions to ask regarding risk appetite:

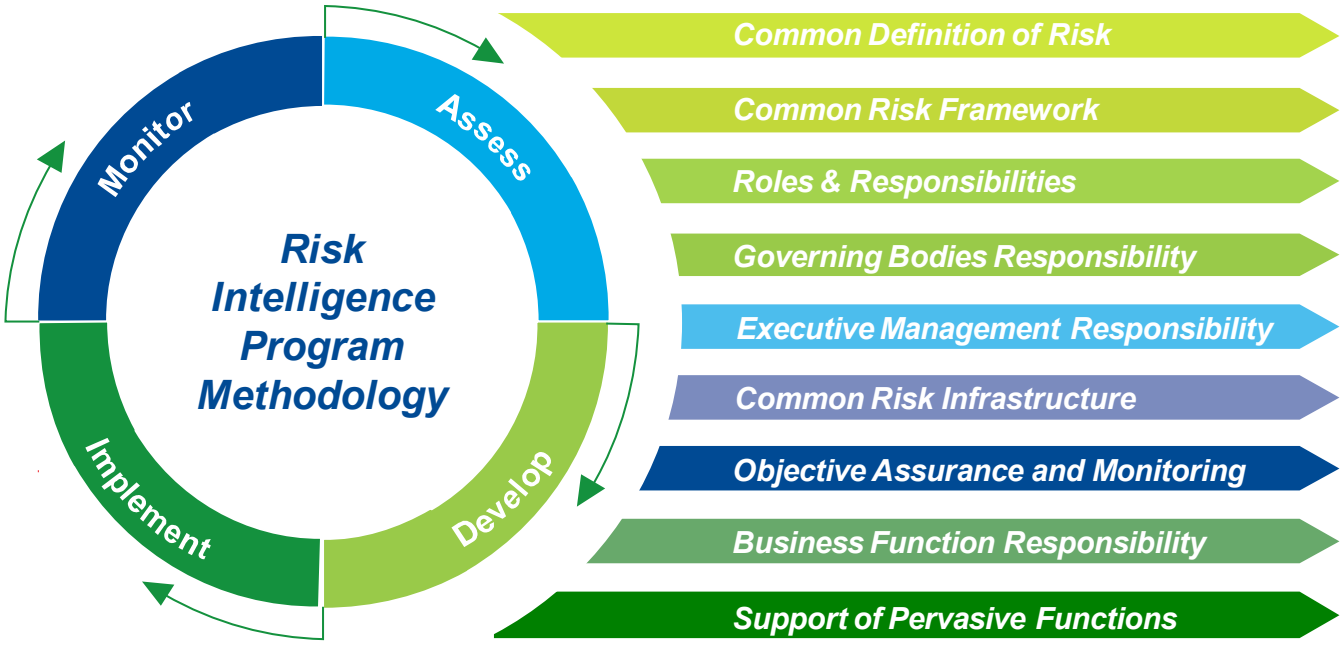
- What size risks or opportunities do we expect management to bring to our attention?
- How does management determine the organisation's risk appetite? Which risk categories are considered, and how do they relate to management's performance goals and compensation metrics?
- In developing the risk appetite, how did management incorporate the perspectives of shareholders, regulators, and analysts — and experiences of peer companies?
- How are risk tolerances set? How does that process account for risk appetite? How do risk tolerances relate to the risk appetite and to risk categories?
- What scenario-planning or other models are used in setting the risk appetite and tolerances? How do these tools account for changing circumstances and for the human factor?

Area of focus 5: Execute the Risk Intelligent governance process

A Risk Intelligent governance process should be strategic in design, promote awareness of the relationship between value and risk, and efficiently and effectively allocate the company's risk management resources. Effective execution of the process depends on maintaining a disciplined, collaborative approach focused on process design, process monitoring, and accountability.

Actions to consider in executing the Risk Intelligent governance process:

- Work with management on process design. A joint approach to process design can help establish processes that both the risk committee and management feel are effective, yet not overly burdensome. The committee can collaborate with executives to develop value creation and risk management objectives, board responsibilities, and mechanisms for elevating key risk issues. It's often useful to establish policies that detail the circumstances under which management must obtain board or committee approval for decisions, while noting that the board's role is risk governance rather than risk management.
- Monitor the overall risk management process. The risk committee should set up procedures for evaluating and overseeing the processes by which risks are systematically identified, reported, and managed. To execute effective monitoring, it's important that committee members keep abreast of the company's vulnerabilities, risk appetite, and risk tolerances; understand the risk management system; and bring an integrated view of the organisation's risk management methods to discussions with the executive team.
- Conduct formal risk management program assessments. A risk management program assessment can include questions about risk governance, risk infrastructure and management, and risk ownership. This provides a comprehensive view of the process and enables all stakeholders to see how they fit into both the basic process and any improvement efforts.
- Clarify accountability at the board and management levels. Complete, on-going disclosure of major risk exposures by the CEO to the committee and the board is fundamental to a Risk Intelligent governance process. We suggest that that committee works with the CEO to verify that responsibility for specific risks and related activities has been assigned to specific members of the management team. In doing this, it's important for the committee and the CEO to maintain a constructive, collaborative relationship — but that need not stop the risk committee from discussing difficult issues with management and questioning practices when doubts arise.



It's important for the risk committee and the CEO to maintain a constructive, collaborative relationship.

Questions to ask when executing the governance process:

- Are people at all levels — across silos — actively engaged in risk management? If so, how? If not, why not?
- What criteria does management use to prioritise enterprise risks? How well does the company's allocation of risk management resources align with those priorities?
- How is management addressing the major opportunities and risks facing the company? How do we know that these are, in fact, the major opportunities and risks, and that the steps management is taking to address them are appropriate?
- How do we know when risks are increasing, holding steady, or decreasing? What processes does management use to identify and monitor these trends over time?
- How often do we discuss risk with management? What issues have been brought to our attention in the past six to twelve months?

Area of focus 6: Benchmark and evaluate the governance process

Risk governance is a continual process, and systematic mechanisms for evaluating and improving risk governance proficiency can greatly benefit efforts to identify, prioritise, and implement improvements as well as give the risk committee visibility into the organisation's progress toward a Risk Intelligent governance approach. Such mechanisms allow the committee to gauge the institution's current stage of development relative to peers; they can also help track the progress of the governance program along a Risk Intelligence "maturity model." As it is good practice to obtain periodic independent assessment of the risk management process, King III requires that Internal Audit provide a written assessment of the risk management function to the Board.

Actions to consider in helping management iActions to consider in benchmarking and evaluating the governance process:

- **Use internal monitoring and feedback.** The risk committee should periodically ask for feedback from senior executives on how well the committee and other board members have played their risk oversight role. As part of this effort, the committee may consider the report from Internal Audit on the effectiveness of the risk management process. The committee may also wish to request relevant reports from the risk management team. The committee may also review the methods by which management assesses the risk management program.

Ask for feedback from senior executives on how well you and your fellow board members have played your risk oversight role.

- **Participate in continuing education and updates.** To keep individual committee members' knowledge up to date, it's helpful to receive on-going updates on approaches to risk management and on risks developing in the internal and external environment.
- **Solicit independent viewpoints.** An independent review of the risk governance program can help to identify what is working, locate any gaps, and prioritise areas for improvement. The committee should consider having management present the summary results along with a plan for any corrective actions.
- **Include risk as a topic in the annual board self-assessment.** The board's annual self-assessment process provides a broad view into how the full board feels that it is performing in its overall governing body role. Including questions in the assessment form focused specifically on risk governance effectiveness can be a valuable guide to measuring the committee and the individual members' effectiveness in providing Risk Intelligent governance. The nominations committee may wish to consider reviewing the assessment form to verify that it includes such language.

Questions to ask when benchmarking and evaluating the governance process:

- How have we gone about assessing our risk governance and management programs? What other tools might we use in this assessment?
- To what extent are our compliance, internal audit, and risk management teams employing Risk Intelligent approaches? How are risks aggregated across our businesses?
- What value might we derive by engaging a third party to assess our organisation against leading practices, industry peers, and other benchmarks?
- How can we improve our risk governance proficiency, stay current, and share knowledge about risk governance - both individually and collectively?
- What steps can we take to improve the quality of our risk governance and management processes?

Queries:

Dr Johan Erasmus – jerasmus@deloitte.co.za

Designed and produced by Creative Services at Deloitte, Johannesburg. (807474/dbn)

Previous