Deloitte.

Enterprise Risk Management
A 'risk-intelligent' approach

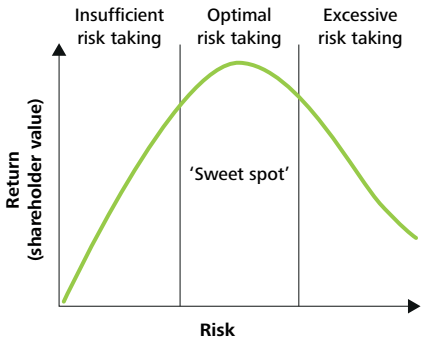
Deloitte Risk Advisory
August 2015

Why Enterprise Risk Management?

Effective governance is a critical aspect of a successful business: it supports management in delivery of the strategy, managing costs, attracting investment, making better decisions and responding to risk. There has never been more focus on how organisations identify and manage risk. From regulators to investors to senior executive management, companies are under pressure to be able to clearly articulate how they identify the principal risks to their business and how they ensure these are being managed within their risk appetite.

Balancing risk and return

Companies need to take risks to create value, and manage risks to protect value. There is a range of 'optimal risk taking' which supports maximum return – 'the Sweet Spot' – and effective risk management is about ensuring that the risks an organisation takes are the right ones and that they are appropriately managed. Top-quartile companies are focused on operating in the Sweet Spot by 'risk-intelligent' decision-making – i.e. by measuring and managing key risks effectively and efficiently in the context of decisions both taken and not taken.



Changes to the corporate governance code

In September 2014 the Financial Reporting Council issued a new iteration of the Corporate Governance Code. The amended code is aimed at strengthening the focus of companies and investors on long term sustainable value creation. The key changes are as follows:

- **Risk identification** – organisations will have to ensure that they have a robust process in place to identify 'principal' risks. For many companies this will involve a significant evolution of their risk management processes, and how these risks are identified and managed;
- **On-going monitoring** – an increased focus on monitoring an organisation's system of risk management and internal control will encourage companies to challenge themselves as to how effective their current monitoring processes are; and
- **Long-term viability statement** – the directors should explain in the annual report how they have assessed the prospects of the company, over what period they have done so and why they consider that period to be appropriate.

Management should consider a number of aspects of their internal control monitoring processes: from the management information they collate, to the effectiveness and co-ordination of the various assurance functions within their business, to the opportunities improved technology can bring in real time understanding of the control environment. To effectively and efficiently identify and manage risk, we believe it is critical that organisations consider and challenge how integrated their governance framework is.

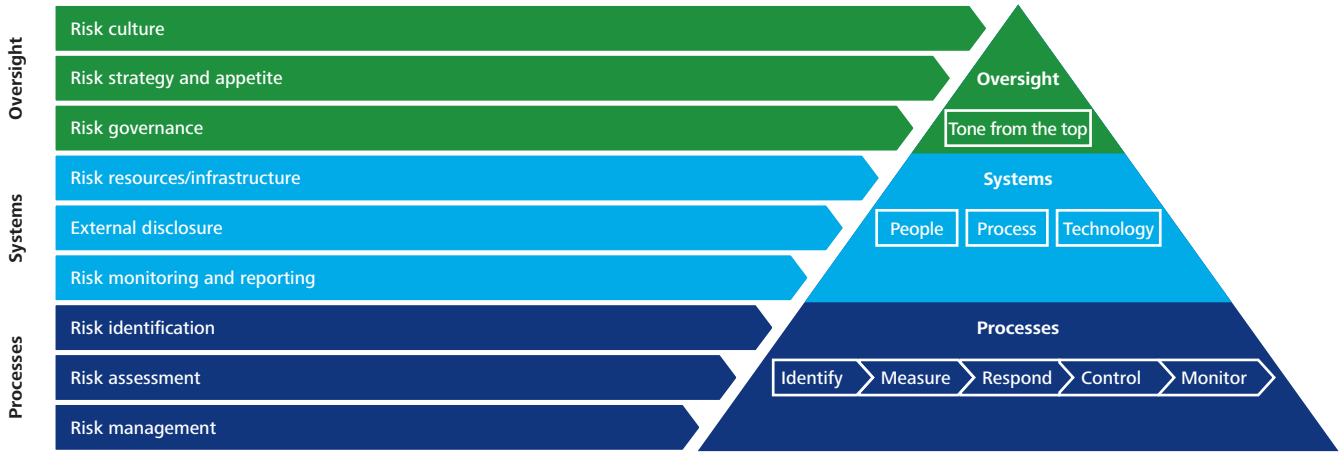
Key challenges

Most organisations, in our experience, will have a view on what their principal risks are; many of these will be strategic in nature and will form a regular part of senior managements' meetings. However, many do not yet have a risk process in place that goes sufficiently beyond the identification of principal risks. The detailed work required to really understand these risks, how they are being mitigated and monitored and whether the risk profile is changing, is often either absent, or currently happening in an uncoordinated way with limited transparency to senior management. In addition, there is also limited integration of the risk management process into key business planning and decision making processes.

A Risk Intelligent Enterprise

Risk Intelligence (RI) is Deloitte's risk management philosophy that is focused on maintaining the right balance between risk and reward. Simply put, organisations create value by taking risks and lose value by failing to manage them. An effective risk management programme focuses simultaneously on value protection and value creation. A 'Risk Intelligent Enterprise™' is an organisation with an advanced state of risk management capability balancing value preservation with value creation.

Deloitte's Enterprise Risk Management Model



There are three levels of responsibility with respect to risk management, as depicted in the figure above. At the apex lies the responsibility for risk governance, including strategic guidance and risk oversight, which rests with the board of directors. In the middle lies the responsibility for risk infrastructure and management, including designing, implementing and maintaining an effective risk programme, led by executive management. At the base lies the responsibility for risk ownership, including identifying, measuring, monitoring and reporting on specific risks, led by the business units and functions.

Typical groups involved in Risk Intelligent Enterprise Management

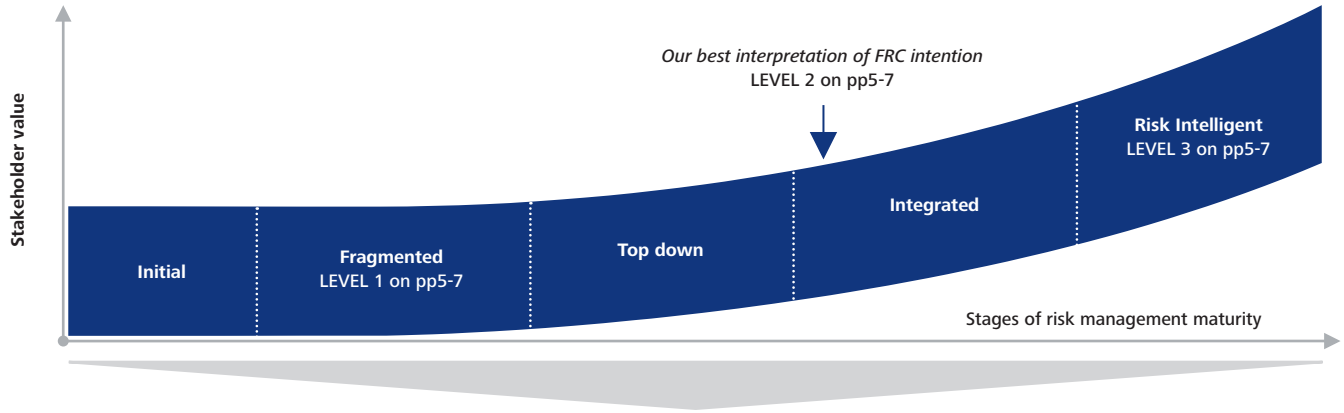
Boards and management use a top-down approach to understand risk at a strategic level, while risk owners in the business units and functions use a bottom-up approach to identify and monitor specific risks, escalate concerns and generate the risk-related data to inform leadership's strategic view.

<table>
<tr><td>Risk Governance</td><td colspan="4">Board of Directors (and the Audit Committee)
• Foster a risk Intelligent culture
• Approve risk appetite
• Ratify key components of the Enterprise Risk Management (ERM) programme
• Discuss enterprise risks with executive management</td><td rowspan="3">Technology (all pervasive):
• Provide periodic/ real-time dashboards to oversee risks
• Make monitoring and reporting easier
• Support timely maintenance and pre-empt problems
• Facilitate risk escalations</td></tr>
<tr><td>Risk Infrastructure and Management</td><td>Executive management:
• Define the risk appetite
• Evaluate proposed strategies against risk appetite
• Provide timely risk-related information</td><td>Enterprise risk group:
• Aggregate risk information
• Identify and assess enterprise risks
• Monitor risks and risk response plans</td><td>Internal Audit:
• Provide assurance on effectiveness of the ERM programme, and the controls and risk response plans for significant risks</td><td>Risk Management:
• Create a common risk framework
• Provide direction on applying framework
• Implement and manage technology systems
• Provide guidance and training</td></tr>
<tr><td>Risk Ownership</td><td colspan="2">Business units:
• Take intelligent risks
• Identify and assess risks
• Respond to risks
• Monitor risks and report to enterprise risk group</td><td colspan="2">Support functions:
• Provide guidance/support to the enterprise risk group and business units</td></tr>
</table>

Build on what you already have

The good news for most organisations is that they're likely to already have many of the elements of Risk Intelligent Enterprise Management in place. The path forward should be much more a matter of building on what currently exists than of starting from scratch. For this reason, we think it's important for organisations to take stock of their current risk management capabilities before making major changes or investments in risk management.

Deloitte's Risk Maturity Model

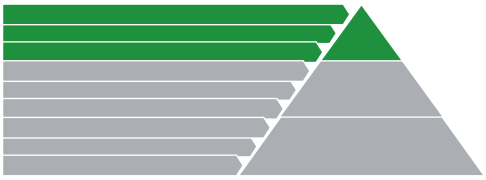


Typical attributes				
• Ad hoc/chaotic • Depends primarily on individual heroics, capabilities, and verbal wisdom	• Independent risk management activities • Limited focus on the linkage between risks • Limited alignment of risk to strategies • Disparate monitoring and reporting functions	• Common framework, programme statement, policy • Routine risk assessments • Communication of top strategic risks to the Board • Executive/Steering Committee • Knowledge sharing across risk functions • Awareness activities • Formal risk consulting • Dedicated team	• Coordinated risk management activities across silos • Risk appetite is fully defined • Enterprise-wide risk monitoring, measuring, and reporting • Technology implementation • Contingency plans and escalation procedures • Risk management training • Clear input into Internal Audit and other assurance activity plans	• Risk discussion is embedded in strategic planning, capital allocation and product development • Early warning risk indicators used • Linkage to performance measures and incentives • Risk modeling/ scenarios • Industry benchmarking used regularly

When performing such an assessment, it's vital to understand not just where your enterprise currently stands, but where you want and need it to be from a risk management perspective – which, importantly, may not always be at the very top. Various areas of risk differ in importance from industry to industry, and even from company to company within the same industry. Hence, it's not always necessary to maintain leading risk management capabilities with respect to every possible aspect of risk. The challenge is to understand in which areas 'good enough' really is good enough – and in which areas the enterprise truly needs top-notch capabilities to meet stakeholders' risk management expectations.

One way to better understand both where you are and where you 'should' be is to evaluate your organisation's risk management capabilities against a maturity model such as Deloitte's Risk Intelligence maturity model (above). For leaders, an assessment against such a maturity model can be a useful way to frame the discussion of what types of initiatives to pursue in various risk areas, as well as how much of the organisation's limited resources to invest in each initiative.

Details – Oversight



The key driver of a company's risk management maturity is the attitude that the board and senior management take towards the role and priority of risk management, because this then cascades down throughout all levels of the organisation.

Risk Culture	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Awareness of risks	**Fragmented** Beyond a common understanding of health and safety risks, individual functions only understand their own specific risks	**Knowing where to find information** There is a central risk register which compiles all principal risks across the company and which is updated at least once a year	**Front-of-mind** The concept of risk-return tradeoffs is front-of-mind for employees on key decision points throughout the company
Willingness to raise risks	**'See no evil, hear no evil'** Apart from the use of a whistleblower policy for extreme examples, there is an ingrained cultural resistance against recognising risks	**Procedures in place** There are procedures in place as part of the day-to-day work for reporting individuals or procedures for improvement	**Incentive mechanisms** Employees are rewarded for making suggestions for improvement which are implemented, and failure to report breaches are penalised
Ownership of risks	**'Someone else's problem'** Beyond a common understanding that health and safety is everybody's personal responsibility, risk is assumed to be dealt with by the business	**Knowing who to go to** Employees understand whom to go to within their division to report on risks and how to escalate issues if unresolved	**Personal responsibility** Employees have a sense of personal responsibility for the consequences of their actions which are built into their performance contracts
Inclusion of risks in decision-making	**Only if asked** Risk management is generally seen as a separate activity from commercial decision-making and to be dealt with after decisions are taken	**Periodic planning cycles** Risks are taken into account as part of the business planning and budget forecasting cycle which is done at least once per year	**Risk-informed decision-making** Risk is taken into account in key decision points including day-to-day operational decisions as well as more occasional strategic decisions

Risk Strategy & Appetite	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Risk appetite statements	**Not fit-for-purpose** Apart from health and safety, any guidance on risks, to the extent that it exists, tends to be so general that it is of little practical use	**Qualitative** Qualitative risk appetite statements exist for each principal risk category for practical use at key decision points	**Key Risk Indicators** Risk appetite statements based on risk-return trade-offs supported by robust KRIs around impacts and exposure limits are used for risk-informed decision-making
Awareness of risk appetite	**Fragmented** Beyond a common understanding of zero accidents, there is no common understanding of acceptable limits for other types of risk	**Knowing where to find information** Employees understand whom to consult or where to look to understand how much risk they can expose the company to during their work	**Front-of-mind** An understanding of the risk-reward tradeoffs incurred as part of their work and acceptable limits is front-of-mind for employees
Inclusion of risk appetite in decision-making	**Only if asked** Decision-making is generally seen as a binary activity ('go'/'no go') with any risks to be addressed afterwards	**Periodic planning cycles** Risk appetite is taken into account as part of the business planning and budget forecasting cycle which is done at least once per year	**Risk-informed decision-making** Risk appetite is taken into account in key decision points including day-to-day operational decisions as well as strategic decisions

Risk Governance	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Delegations of authority	**Incomplete/not followed** The delegations of authority for decisions relating to risk is not followed because it is inefficient, incomplete or even non-existent	**In place and adhered to** There is a formal delegations of authority structure for decisions relating to risk which must be followed, with sanctions for non-compliance	**In place and optimised** Delegations of authority have been aligned with the commercial demands of the business without compromising on risk
Risk monitoring and mitigation	**Needs escalation** Issues encountered relating to risk routinely have to be escalated to management on an individual and ad-hoc basis	**As part of standing agenda** Issues relating to risk are reported and resolved during regular Risk Committee meetings with the option of ad-hoc referrals if urgent	**Principle of subsidiarity** Issues relating to risk are resolved at the lowest possible level in the organisation to maximise efficiency without compromising on safety

* Our best interpretation of the FRC's intention at the time of writing (August 2015)

Details – Systems

Within the 'middle band' of the ERM framework, there is generally a high level of correlation between the maturity of a company's risk infrastructure, external disclosure and ongoing monitoring and reporting capabilities.

Resource/Infrastructure	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Risk Champion	**Too junior/part-time** The nominated 'risk champion' is too junior to be taken seriously and/or too busy to devote sufficient time to the role	**Appropriate level and support** There is a nominated senior risk champion with appropriate time and resources reporting to the Head of Risk as well as the business	**Senior stakeholder** The risk champion is supported by the Head of Risk/CRO or other member of the C-suite to highlight the importance of the role across the company
Data quality (format, completeness, accuracy)	**Errors and omissions** Information on risk is frequently incomplete, inaccurate, inconsistent in terms of detail, contradictory and/or out-of-date	**Mix of qualitative/quantitative** There is sufficient and reliable data to monitor and report on key risk indicators which are a mix of qualitative and quantitative	**Aligned with decision-making** KRIs are aligned with KPIs so that risk management is seen as part of strategy management and not just a compliance activity
Reporting process	**Manual** Compiling data on risks is a manual and labour-intensive activity which eats into people's time to do their actual day-job	**Fit-for-purpose** There is a standard risk reporting pack which must still be compiled manually but is done as quickly as possible with minimal time loss	**Automated** There is a standard risk reporting pack which can be updated with the latest data and pulled off the system as and when required
IT systems	**Multiple systems** There are multiple IT systems which are incompatible with each other, and reporting generally has to be done via spreadsheets	**Fit-for-purpose** The risk reporting pack is generated by a single and fit-for-purpose system which can be used by more than just a few key individuals for use	**Integrated** The risk reporting pack is generated by a single IT system which is used across the firm for all data and reports

External Disclosure	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Disclosure of risks	**Generic** Risks disclosed are generic to the sector and do not help to distinguish the company's prospects from those of its competitors	**Specific** Risks disclosed are specific to the company's strategy and add additional information in line with the spirit of the FRC's guidance	**Stratified** Risks are stratified by confidence internal and correlated to root drivers corresponding with different outlook scenarios for the sector
Long-term viability statement	**Misnomer** The long-term viability statement is so heavily caveated that it effectively provides no additional information beyond a 12-month horizon	**Insightful** The statement provides additional insight into the company's potential long-term prospects in line with the spirit of the FRC's guidance	**Shift in perceptions** The statement and supporting analysis provides clear evidence that the company is genuinely focused on long-term strategic objectives

Monitoring & Reporting	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Frequency	**On demand** The monitoring and reporting of risks is an activity that is generally avoided and only done when demanded by the board	**Included in reporting packs** Risk monitoring and reporting is done for the ExCo and board reporting pack, and also on an ad hoc basis as requested between meetings	**Included in all key decisions** Risk monitoring is largely automated and therefore done on a continuous basis, and reports can therefore be compiled as required
Link to KPIs	**Limited linkage** Risks are reported on a bottom-up basis, with large and unwieldy risk registers, and therefore have little direct link to business KPIs	**Risks aligned with KPIs** Risks are reported on a bottom-up basis, and grouped according to their impact on top-down business KPIs for more meaningful reporting	**Quantified risks and KPIs** Risks are reported on a bottom-up basis, and then quantified with respect to business KPIs, in terms of probabilities, impacts and correlations
Link to strategic objectives	**Bottom-up only** Risks are reported on a bottom-up basis, with large and unwieldy risk registers, and therefore have no link to wider strategic objectives	**Aligned with strategic objectives** Risks are reported on a bottom-up basis, and grouped according to their impact on the firm's wider strategic objectives	**Quantified strategic impacts** Risks are reported and quantified with respect to strategic objectives, in terms of probabilities, impacts and correlations

* Our best interpretation of the FRC's intention at the time of writing (August 2015)

Details – Processes

How risks are managed is where the link between risk management and actual decision making is most visibly made – the 'so what' of risk management – and risk-intelligent decision-making most valuable.

Risk Identification	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Approach	**Limited – bottom-up only** The only risks that are reported tend to be those that are captured as part of a bottom-up process and added to a risk register	**Mix of bottom-up and top-down** Bottom-up operating risks are complemented by management's top-down view of principal risks, as well as any additional company-wide risks	**Horizon-scanning** The focus of effort is on anticipating those risks that can have a material adverse impact on the business and/or its strategy well in advance
Types of risks	**Focus on financial risks** The nature of risk registers means that only easily identifiable/ financial risks tend to be reported, with other risks taken as assumptions	**Key business risks** The focus is on risks that can have a material impact on the business, including less tangible categories such as reputation risk	**Key business and strategy risks** In addition to risks that can disrupt BAU, there is equal focus on risks to the company's strategy, which has a higher impact in the long-term

Risk Assessment	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Measurement	**RAG** Risks are measured using a traditional RAG matrix ('red/amber/green')	**RAG with qualitative ranking** Risks are measured using a RAG-rating and ranked according to a consistent metric (e.g. probability x impact x vulnerability)	**Quantitative prioritisation** Quantitative probabilities and impacts are estimated, using uncertainty ranges, for more robust risk-informed decision-making
Aggregation	**None** Risks are added to the risk register with an aggregate exposure at the bottom if all risks were to materialise i.e. the worst possible scenario	**Portfolio perspective** An effort is taken to aggregate total risk exposure i.e. recognising that simply adding them all up corresponds to a very unlikely downside scenario	**Quantitative incl. correlations** Quantified probabilities and impacts allows for easy aggregation of risks across different dimensions and at any level of confidence using statistics

Risk Management	LEVEL 1: Fragmented	LEVEL 2: FRC expectation*	LEVEL 3: Risk-Intelligent
Approach (accept/ transfer/ avoid/ mitigate)	**'Gut feel'** The decision on how to respond to a risk is made on 'gut feel' and often because a decision needs to be taken quickly and/ or there is no data	**Cost-benefit analysis of options** Different options are identified and a cost-benefit analysis is carried out on a shortlist, qualitatively and also quantitatively where possible	**Cost-benefit-uncertainty analysis** Quantitative cost-benefit analysis is carried out, including the uncertainty around both cost and benefit and residual risk exposures
Subsequent monitoring	**Added to risk register** The risk is added to the risk register, which is reviewed and updated either as part of a periodic sweep or on demand	**As part of management meetings** Key risks are discussed as part of management meetings until they have been resolved to management's satisfaction	**Tracked against risk appetite and revisit response options** Risk exposures continue to be tracked and monitored against risk appetite, with the option to change the original response if required

* Our best interpretation of the FRC's intention at the time of writing (August 2015)

Hans-Kristian Bryn
Partner
+44 (0)20 7007 2054
hbryn@deloitte.co.uk

Hugo Sharp
Partner
+44 (0)20 7303 4897
hsharp@deloitte.co.uk

Tim Archer
Partner
+44 (0)20 7303 4484
tarcher@deloitte.co.uk

Pooya Alai
Senior Manager
+44 (0)20 7303 6919
poalai@deloitte.co.uk

Raj Cheema
Senior Manager
+44 (0)20 7007 5860
racheema@deloitte.co.uk

Matthew Davy
Manager
+44 (0)20 7007 0515
madavy@deloitte.co.uk

For further information, visit our website at **www.deloitte.com**

Designed and produced by The Creative Studio at Deloitte, London. J1470