SWORD

ACTIVE RISK

Enterprise Risk Management Readiness Guide

The most successful businesses are the most successful risk managers. Is your business managing risk as effectively as it should?

The most successful businesses are the most successful risk managers. Is your business managing risk as effectively as it should?

Enterprise Risk Management Readiness Guide

INCLUDED IN THIS GUIDE FROM ACTIVE RISK:

Executive Summary

The idea in brief

You sense you are succeeding, but you are not breaking through. Compared to your peer competitors your EIBTDA is significantly lower, and despite your best efforts, you don't seem to be making the EIBTDA improvements you (and your board) think are critical for your business.

The answer might be your business' risk strategy.

EMBRACE RISK:

To succeed today, you must carefully expose your business to increasing level of risk, monitoring and managing risk as never before. Whether your objectives are improvement in steady state operations or expansion into new and emerging markets, aligning your risk management and internal control activities with your overall business strategy can transform your business practice.

CONSIDER ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management (ERM) is a scalable, holistic approach to risk management that combines risk information from across the organization and uses this to meet business objectives and drive business performance and growth through embedding and aligning risk management in business processes.

BENEFITS OF ERM:

Increased competitive advantage

Increased likelihood of achieving strategic objectives

Meeting increasing stakeholder expectations

Improved governance

Increased likelihood of adhering to evolving regulatory requirements

Increased likelihood of delivering projects on time

Fewer surprises

Improved decision making

Improved communication and reporting

The idea in practice

UNDERSTAND YOUR RISK MATURITY

If you are like most businesses, your risk management practice grew as a result of increasing regulations and compliance requirements (SOX, legal, etc…). You've created work roles, departments and business areas to monitor and manage compliance obligations.

Using a departmental approach, you are addressing compliance issues adequately, but your risk perspective is entirely threat-based. Risk management and control is fragmented and multiple parallel activities are putting increasing demands on your business, as different business units are asked for the same or similar information from different departments for different purposes. There is no clear organization-wide picture of business risks and appropriate reduction strategies.

DEVELOP A RISK-AWARE CULTURE

Don't require that your entire organization adopt risk management as an all encompassing initiative. In many organizations it may be more beneficial to develop a risk-measurement/management framework in 'bite-size' pieces. A phased approach will often encourage buy-in from stakeholders and provide the foundation for using risk data across your entire organization.

ADOPT RISK MANAGEMENT TECHNOLOGY

Modern ERM software will allow you to implement robust risk tracking and measurement, while providing visibility and transparency to risk data. The very best solutions: deliver a single automated solution to save time and ensure accuracy of data; support homogeneous risk management processes to promote a single risk language across the business; provide checklists, templates and easy access to historical data; facilitate consistent risk reporting; are easily integrated with other internal systems and provide clear audit trails, metrics and key performance indicators to increase overall business effectiveness.

FOCUS ON YOUR BUSINESS' RISK APPETITE

The business benefits of increasing the strategic application of business risk are well known. Specific data is starting to emerge that clearly proves a link between risk management and competitive Ernst & Young report that as *"Companies in the top 20% of risk maturity generated three times the level of EBITDA as those in the bottom 20%."*[1] Additionally, they state that *"Financial performance is highly correlated with the level of integration and coordination across risk, control and compliance functions."*[2]

ALIGN YOUR RISK AND BUSINESS STRATEGY

Business leaders who understand their organization's risk are better able to leverage it to create opportunity and competitive advantage. With superior Enterprise Risk Management, risk can be addressed thoughtfully and proactively – ensuring that strategic goals are met. As your organization's risk maturity grows, and you will Improve accountability and control, while improving your competitive edge.

Business leaders who understand their organization's risk are better able to leverage it to create opportunity and competitive advantage. With superior Enterprise Risk Management, risk can be addressed thoughtfully and proactively – ensuring that strategic goals are met.

1. Enterprise Risk Management Basics

WHAT IS ERM?

Enterprise Risk Management (ERM) is a scalable, holistic approach to risk management that combines risk information from across the organization and uses this to meet business objectives and drive business performance and growth through embedding risk management in business processes. In addition to focusing on process, ERM also takes account of the risk culture of the organization, or the behaviours, beliefs and values needed to underpin the actions required by the risk processes. ERM does not take a silo view of risk, but addresses all types of risk, and can be seen as the sum of Operational Risk, Project Risk, Governance & Compliance, Strategic Risk, Financial Risk and Opportunity Management. Importantly, ERM does not focus only on negative threats, but places as much importance on the exploitation and management of opportunities, or upside risk.

Prior to ERM, traditional risk management addressed risk in organizational silos (e.g. health and safety, insurance, internal audit) from a threat perspective. Arising in the main from increasing regulations and compliance requirements, additional functions, departments and business areas were created to manage the risks associated with compliance obligations (e.g. SOX, legal). With this increase in risk oversight came fragmented risk and control activities, resulting in increased demands on the business, and "risk fatigue" as business units were asked for the same or similar information from different departments for different purposes. Understanding and defining a clear organization wide risk picture became close to impossible, with duplication of effort and potential gaps in risk coverage. The resulting struggle of executives and boards to determine the adequacy of risk and control efforts led to the birth of ERM.

WHO NEEDS ERM?

The only thing certain in today's market is uncertainty. Organizations are under an unprecedented amount of pressure to improve performance, stay lean and manage shareholder value. In such a volatile business environment, the sensible approach appears to be to play it safe and avoid risk, but risk is inherent in business and success. Ignoring risk or managing it in a fragmented way leads to under-informed decisions that can ultimately affect profitability. All organizations - whether public or private – must take risk and as such, ERM is needed by all.

WHY ERM?

In recent turbulent times, ERM has become acknowledged as a key differentiator between business which are successful, and those which are less so. Data is starting to emerge that clearly proves a link between risk management and competitive advantage as *"Companies in the top 20% of risk maturity generated three times the level of EBITDA as those in the bottom 20%."*[3] Additionally, Ernst & Young state that *"Financial performance is highly correlated with the level of integration and coordination across risk, control and compliance functions."*[4]

New risks that have not traditionally been considered such as social networking and emerging markets now need to be debated and addressed, and the increasing impact

and range of new external events is affecting an organization's need to respond quickly to emerging risks. In addition, regulatory and legislative requirements are increasing and changing, as are the penalties and both personal and company liabilities associated with failures to comply. Given the dramatic events of the last decade – terrorist attacks, natural disasters, the global financial crisis, political upheavals – together with increasing globalisation and technological developments, traditional risk management is no longer sufficient to manage such complexity.

Companies need to become more resilient to risk, and what is clear is that if they fail to address the effectiveness of risk management, stakeholders will respond. Increasingly stakeholders are better informed and more interested in how risks to the organization are being managed, with certain groups being prepared to take action if they feel that risk management is not appropriate: *"Investors [will] apply a penalty if they think risk management is insufficient: 61% of respondents said they had avoided investing in companies for this reason and 48% had deinvested."*[5] With a figure as high as almost one in two stakeholders deinvesting, organizations could be left with large brand and reputation issues to manage if high profile stakeholders withdraw support.

Companies are therefore exposed to an increasing level of risk, with board attention focused on monitoring and managing risk as never before. Boards are requiring insights on whether investments are properly focused and consistent with industry risk issues, and are looking to the risk teams to answer this question. In addition, many organizations are growing significantly in emerging markets which furthers their need to invest in risk management and internal control activities. As a result of this focus, boards are particularly interested in the risk/ reward trade-off, and are keen to understand the benefits of funding a formal ERM program.

WHAT ARE THE BUSINESS BENEFITS OF ERM?

Examples of quantifiable benefits arising from ERM initiatives include:

Increased access to capital and reduced cost of debt. Since 2008 rating agencies such as Standard & Poor's have been including a rating of ERM in their evaluations of both financial and non-financial organizations. In the case of S&P, it believes that an organization's ability to meet its financial obligations on time and in full is more likely to be enhanced by strong ERM, or diminished by weak or nonexistent ERM

Reduced insurance premiums. Insurers are increasingly looking to understand the controls in place to manage an organization's key risks. Through this understanding they are able to accurately assess the premiums imposed on a business. The more robust and embedded the controls are, the more likely it is that the premium charged will be reviewed or continue to remain the same

Reduced cost of assurance activities. ERM frameworks are designed to be embedded within existing business processes. This includes internal and external audit. Through an analysis of which groups are providing assurance over which key controls, and an understanding of whether these controls are linked to the organization's significant risks, there is the opportunity to reduce the cost of assurance activities by removing duplications and focusing activity on controls of strategic importance

Reduction in overlaps and inefficiencies. Total risk spend can be reduced by aligning the various risk functions and processes within the business so that overlaps and duplications are removed, and gaps identified and addressed. Removing the duplications (for example duplicate responsibilities and tasks) results in resource savings of both time and cost

Reduced fines and penalties. Through monitoring risks around non-compliance with various regulatory standards, and acting before breaches are made, the organization has the opportunity to avoid the payment of significant personal and organizational fines and penalties

Reduction in manual reporting time. Implementing a single or integrated ERM software system, or reducing the number of places where risk data is held, means that risk data can be consolidated, analysed and reported in a predominantly automated fashion, so reducing the number of manhours (and therefore cost) associated with the reporting process

Reduction in incident response costs. By tracking, analysing and understanding the drivers behind the incidents, organizations can address the root cause and so reduce the likelihood of the incident occurring and/ or reduce the impact if it should. This in turn results in cost savings

In addition to the more quantifiable elements of ERM, there are numerous other benefits that are less easily quantified. For example, a survey by Aon found that 79% of organizations with mature risk management systems are either moderately or very successful at protecting and enhancing shareholder value.[6] Aberdeen Group state that "Embedding ERM in all business processes ... reduces liabilities. Business partners, regardless of their role in the value chain, will always prefer to do business with companies possessing lower liabilities. Similarly, customers will choose to conduct business with companies possessing lower risks. These business opportunities combined enable revenue opportunities that justify the ERM initiatives."[7]

OTHER BENEFITS INCLUDE:

Increased competitive advantage arising from a sound understanding of the organization's key risks and its risk appetite and tolerance – contributing to improved opportunity exploitation, agility in responding to risks and market growth.

Increased likelihood of achieving strategic objectives through understanding the threats to their success and identifying appropriate mitigation and contingency plans.

Meeting increasing stakeholder expectations (both internal and external) of how risk should be managed. Stakeholders need to be reassured that risk is being managed effectively and in-line with regulatory requirements. ERM provides this visibility and demonstrates a strategic and considered approach to threat and opportunity management.

Improved governance as the risk roles and responsibilities of various groups, committees and key stakeholders (including the board) are defined and communicated.

Increased likelihood of adhering to evolving regulatory requirements (resulting in improved credit ratings) through identifying and managing the risks of non-compliance.

Increased likelihood of delivering projects on time, to cost and quality requirements.

Fewer surprises as the organization is able to identify non-manageable risks before they have a negative impact, and to initiate an appropriate contingency strategy.

Improved decision making and management skills as relevant risk information is available to inform decisions taken.

Improved communication and reporting through a holistic understanding of risk including risk factors in all parts of the business and risk interdependencies. Using ERM software to automate and support this process facilitates the delivery of real time risk data to the right people at the right time in the right format.

In summary, business leaders who understand their organization's risk are better able to leverage it to create opportunity and competitive advantage. With superior Enterprise Risk Management, risk can be addressed thoughtfully and proactively – ensuring that strategic goals are met.

A successful enterprise risk management program will:

Provide the foundation for all risk data across the organization;

Deliver visibility to all risk data;

Improve accountability and control; and

Support compliance, new regulations and frameworks.

2. Preparing Your Organization for ERM Implementation

In recent times there have been a number of research documents produced by firms such as PricewaterhouseCoopers, Ernst & Young, Accenture and Harvard Review Business Analytic Services that have identified trends in the market and provide guidance on where risk resources should be focused to gain the most reward. According to PWC *"...most organizations should look to build on their current ERM frameworks by making three changes to the way they frame and think about risk:*

1. Developing a risk-aware culture

2. Explicit focus on risk appetite

3. Alignment of risk and strategy[8]

The companies who address these trends most successfully are those that make incremental enhancements to their risk framework utilising existing infrastructure. In order to encourage buy-in from stakeholders, it is important to recognise that ERM does not always have to be addressed as an all encompassing holistic approach which requires significant investment in terms of both time and money. In some, perhaps most, circumstances, it may be more beneficial to approach the framework in 'bite-size' pieces. For example:

1. Developing a phased approach to the framework deployment or improvement;
2. Identifying a part of the business or a specific project that would benefit from the principles and processes associated with ERM; and/or
3. Identifying part of the ERM process to focus on such as the risk appetite or a risk culture.

Once these specific improvement projects are demonstrating success and value, the next project/ process/ phase can be addressed.

It is important to remember that ERM is a scalable solution, and as such should be developed with the specifics of the organization in mind. Whilst any approach should be aligned with leading practice and standards, it should also be tailored to the organizational context and involve as little change as possible to current process and practice. In this way the ERM framework can be deployed more quickly and with less resistance from the business, meaning that less effort is expended in creating value.

Prior to beginning any initiative however, it is vital to define a clear business case using business language (as opposed to technical risk "speak") which includes: the reasons why ERM is needed; what benefits are expected to be achieved (both tangible and intangible); how key stakeholder concerns will be addressed; a clear approach and objectives; and what the risk/ reward trade-off will be. Once this is agreed, action can begin with the support and understanding of the stakeholders.

COMPONENTS OF AN ERM FRAMEWORK

One way of breaking down and making the ERM framework more manageable is by considering it in terms of five key components: governance, people, process, systems and culture.

GOVERNANCE...

Governance is often overlooked when considering the ERM framework, but plays a vital role in ensuring that the right risk culture is in place, and that the right people and groups of people have oversight of relevant risk data. Risk governance helps ensure the correct flow of risk information around the business – to the right people at the right time in the right format – and ensures that risk information supports the decision making process at strategic levels.

Key features to consider when defining risk governance procedures include:

Tone from the top – the board and executive need to support the ERM framework, and talk and act in a way that promotes the consideration of risk in all business activity.

Strategies and objectives – a clear strategy for the ERM framework needs to be articulated, whether purely to meet compliance requirements, and/ or to recognise competitive advantage and exploit opportunities. This must be agreed and understood by the board in conjunction with its risk appetite.

Alignment to business objectives – core risk activity should be focused around managing the risks that may have an impact on organizational objectives. As such, there is a need to embed risk management within the strategy setting process so that it can be used as a driver of business performance.

Organizational structure – the accountability and responsibility for ERM needs to be clearly defined across the organization, including establishing clear charters and mandates for the board and its committees that address ERM. In some instances, it may be beneficial for the organization to consider the appointment of a Chief Risk Officer (CRO) or equivalent, who can act as the key ERM sponsor and drive risk activity throughout the business.

Reporting – risk reporting requirements need to be defined and reports tailored dependent on the audience. This may vary from high level dashboard style outputs, to detailed risk register reports. Frequency and ease of understanding should also be considered.

PEOPLE...

Without the right people in the risk team and in key risk positions, whose skills and experience align with the objectives of the ERM initiatives, embedding ERM within the business is a difficult task. The following considerations are key examples of what should be defined when addressing the people aspect of ERM:

Competence and capabilities – individuals appointed into risk positions or those with significant risk responsibilities should have as a minimum a basic understanding of the key ERM principles and practices the organization has defined. Where this is not the case, tailored education and training should be utilised, and/ or external recruitment considered to fill any skills gaps.

Roles and responsibilities – should be clearly defined and communicated. Measuring and monitoring metrics should also be considered to ensure individual understanding of expectations, and to ensure effectiveness/ value of the roles defined.

Ownership & accountability – should be clearly defined, communicated and understood, including ownership and accountability for components of the ERM process, individual risks, controls, mitigation and contingency actions.

Identification of key business supporters – in addition to specific risk roles, it may be valuable for the organization to develop a risk "champions" network of individuals who sit within the business but who are able to act as the "go to" person within the function or business unit for risk queries. In this way limited resources within the central risk function can be subsidised, and there is a direct information flow and feedback channel from the business to the risk team and vice versa.

Alignment and coordination – risk roles should be considered from a holistic process across the organization so that there are no unexpected overlaps and duplications in responsibilities, or gaps in accountability. This avoids unnecessary inefficiencies, and allows resource to be allocated in the most effective manner.

PROCESS...

Having ERM processes and procedures defined is a key element of the framework. Many standards and leading practice guides exist to help with the definition of risk process. It is however important to remember that the process should be customised to the organizational context, be as simple as possible, and leverage existing processes and practice to make it as familiar as possible to the business.

Rewards & sanctions – to emphasise the importance of ERM initiatives and drive home the message regarding expected risk behaviours, the organization may consider implementing a system of sanctions and rewards. For example, personal KPIs (Key performance indicators) may be developed regarding risk activities such as the timely management of risks, and linked to remuneration to encourage certain behaviour. Alternatively, approaches such as "name and shame" may be deployed if certain parts of the business are not acting in accordance with expectations. By shaping behaviour, rewards and sanctions are another means to influence the ERM culture, and to demonstrate the commitment of senior management to the importance of ERM.

Executive sponsorship – as mentioned previously, the "tone from the top" is vital in highlighting the importance of ERM to the organization, particularly if the executive "walk the talk" and lead by example. Appointing an executive level sponsor is another indicator of the level of importance given to ERM, and provides a means of raising and influencing the visibility of and discussions on ERM as part of the board agenda.

POTENTIAL DIFFICULTIES

Implementing or improving an ERM framework is not always straight forward. In order to be prepared and address potential blockers before they arise, below are some of the most common problems encountered when attempting to implement an ERM framework:

Unrealistic expectations – ERM is a journey not an overnight solution. Increasing and developing risk management maturity as an organization takes time, effort, money and necessarily involves a significant process of change management which is not always considered or handled well.

Failure to consider the risk culture – a successful ERM framework must also consider the behaviour, beliefs and values required to support the defined ERM processes. It is unrealistic to expect that all key stakeholders will follow the risk process purely because it has been written down – time and effort has to be invested in communicating the changes, validating understanding and buy-in, and measuring compliance if the framework is to be fully embedded.

Failure to define risk appetite – *"There [is] a failure to properly understand, define, articulate, communicate and monitor risk tolerances, with the mistaken assumption that everyone understands how much risk the organization is willing to take."*[12] Most usually, risk appetite and tolerance levels are poorly defined in an organization as those responsible for defining what these boundaries should be, are unable to clearly articulate these levels and gain agreement from all key stakeholders on a value. In particular, placing quantitative rather than qualitative values on these boundaries creates real difficulties, and is quite often placed in the "too hard" bucket. However without fully defined and communicated risk appetite and tolerance levels, there are no clear guidelines for individuals throughout the organization to understand when they should be exploiting, managing or escalating risks. The end result is that opportunities may be missed, or threats may be accepted that are actually beyond the capacity or willingness of the organization to manage.

Lack of alignment between risk strategy and business strategy – ensuring that risks are formally considered as part of the strategy definition process means that there is less chance of threats and opportunities being overlooked, and informs the debate as to whether achievement of the organization's strategic aims is in fact realistic and can be achieved within the organization's risk appetite. ERM can also be used to drive business performance through embedding risk management within other key business processes such as financial management, internal audit and procurement so that there is consideration and informed discussion across all parts of the organization about both the threats and opportunities that need to be managed.

Poor data management – according to Deloitte, one of *"The greatest challenges in implementing an effective ERM program ... [is] integrating data across the organization."*[13] Many organizations struggle with the holistic nature of ERM as they lack the supporting technology to enable data capture, sharing, analysis and presentation on an enterprise-wide basis, and in formats suitable for a varying audience. Failure to tell the audience anything they do not already know, or conversely, drowning meeting with pages of detailed risk information does not encourage participation in or understanding of the threats the organization may be facing or opportunities they may be missing.

"Failure to use enterprise risk management to inform management's decision making for both risk-taking and risk-avoiding decisions."[14] – despite being a holistic discipline that pulls together risk information from across the organization, risk information is rarely used to inform and drive the decision making process, mainly due to the way the data is accessed and presented to management and the executive. Providing the right information to the right people in the right format at the right time is a critical element in proving the value that ERM can bring to the organization.

Failure to identify executive sponsorship – an executive level sponsor is needed to communicate the importance of the ERM framework at the senior levels of the organization, and to hold peer discussions at the board level. In addition, the sponsor should "act as the face" of ERM to the business, and promote the importance and benefits for the entire organization. Without a focal person who can champion the risk agenda at a senior level, it may be difficult to raise risk up the board agenda and gain the visibility needed to create action.

ERM is viewed as synonymous with Governance, Risk and Compliance – another view of ERM is that it is synonymous with GRC (Governance, Risk and Compliance), and is therefore overhead intensive. ERM is however different from GRC, as ERM is a driver of strategic value, competitive advantage, and business growth. Unfortunately, due to the corporate and accounting scandals of the late 1990s, "risk management" has become synonymous with Sarbanes-Oxley, which had the unintended consequence of adding tremendous complexity. Rather than adding complexity and "ticking the box" in terms of complying with relevant legislation, ERM is about business performance, profitability and growth; and it is this message that is sometimes misunderstood by key stakeholders.

The risk management team contains the wrong people – based on a number of studies conducted by Active Risk, it has become clear that "Senior management should build a risk team with the range of skills needed to meet current business objectives. This blend of skills may need to change over time as the organization becomes more risk mature and starts to roll out an enterprise-wide programe."[15] Risk management roles are generally held by individuals with a range of personality types, and these differences, strengths and weaknesses, needed to be exploited in the most effective possible manner for the organization. Failure to do so may result in the skill set of the risk team unsuccessfully meeting the needs of the business, particularly as the organization's risk management maturity increases. In addition there is frequently a failure *"...to develop and reward internal risk management competencies"*[16] so that the right behaviours are encouraged or a clear risk career path to encourage individuals to invest their time and effort into the role.

Failure to identify "quick wins" – the intangible nature of a discipline that deals with uncertainty means that it can sometimes be difficult to quantify the true return on investment of ERM. In addition, the long-term nature of the discipline means that without planning and consideration, it is not always possible to identify "quick wins" and prove the quantified value of ERM. Similarly, unless risk is embedded in business processes such as strategic planning, internal audit, performance management and finance, recognising improvements in business performance and growth cannot definitively be linked to ERM.

ASSESSING SUCCESS

Prior to launching an ERM initiative, it is important to have in mind what benefits are expected to be achieved, how these will be measured and what success will look like for the organization. This may be tangible or intangible benefits, or a mixture of both. In addition,
it is helpful to identify quick wins that demonstrate value at an early stage in the process, as these will facilitate buy-in to continued ERM activity. Examples of the types of benefits and successes that can be enjoyed as a result of ERM range from quantifiable cost savings and efficiencies, to the less tangible but vital benefits such as increasing competitive advantage and meeting stakeholder expectations.

From a measurement perspective, success can be measured through a combination of methods including:

FRAMEWORK ELEMENT	METRICS
OVERALL ERM FRAMEWORK	Audit reports which benchmark against leading practice frameworks. Risk maturity assessments benchmarked against an adopted model. Increased efficiency (reduced total risk spend).
RISK CULTURE	Outcome of a risk culture survey including an assessment against desired behaviours (requires an analysis process to develop criteria for measurement). % board agendas/reports including reference to risk. % management reports specifying risk areas. % of job descriptions containing risk KPIs. % projects defining risk in business cases and managing risk. % of risks, controls and actions with specified owners.
CONTROL EFFECTIVENESS	Change in risk profile over time (improved residual risk ratings). Ratings from internal audit reports over specific areas (process, controls) demonstrating improvements over time. Reduced cost of assurance activities through more efficient allocation of resources.
STRATEGIC APPROACH	Reduced cost of capital Reduced insurance premiums

This list of questions provides an example of the types of considerations that should be taken into account prior to implementing or improving an ERM framework or initiative.

3. Assess Your Organization's Readiness for ERM with our Questionnaire

1. What level of risk management competency do you want to achieve across the organization?
2. Where will enhanced risk management activities deliver the greatest value?
3. What impact will any change have on the business and how should this be managed?
4. How will risks and controls be identified, assessed, monitored and improved?
5. Have the risk appetite and tolerance boundaries been defined, agreed, communicated and understood?
6. Which existing business processes can be leveraged to embed ERM throughout the organization?
7. What level of oversight will there be on risk and control?
8. Are the risk functions effectively aligned and coordinated to manage risk?
9. Has an executive sponsor been identified?
10. Will the culture (behaviors, beliefs and values) encourage taking the appropriate risks?
11. How effectively will information technology be leveraged to support the organization's risk and control framework?
12. Do the relevant skills and experience exist within the organization to execute the ERM framework?
13. What communication will be needed for both internal and external stakeholders to encourage buy-in to the ERM framework?
14. Has consideration been given to continuous improvement of the framework?
15. How will the success and value of the ERM framework be measured and monitored?

The following questions comprise a brief, self-guided risk maturity assessment. Answer the questions as accurately as possible. Compute your maturity index by adding together the values at the end of each of your selected responses. Then use the matrix on the following page to gain a broad understanding of your risk maturity.

4. Understanding Your Risk Maturity

1. WHAT LEVEL OF RISK MATURITY HAS YOUR ORGANIZATION ATTAINED?

a. Optimized – Risk-adjusted corporate planning & performance is driven from a senior management level down throughout the business and is seen as a competitive advantage, strategic risks are identified and measured. (6)

b. Embedded – Risk management has become part of the business reporting and decision making processes across the whole business. (5)

c. Established – Consistent risk management processes with communication & accountability are being rolled out through the business. (3)

d. Formalized – Basic compliance. Risk awareness is growing. (2)

e. Undeveloped – Basic risk identification done in silos, with inconsistent adoption across the business. (0)

2. WHAT IS THE RISK CULTURE IN YOUR ORGANIZATION?

a. Employees have little awareness of risk management and its importance (0)

b. Employees have heard about risk management, but regard it as just another corporate initiative lost among many others (1)

c. Employees feel risk has some importance, but that it is someone else's responsibility (i.e. risk professionals) (2)

d. Employees want to participate in risk management, but feel that there is no easy way to share what they know about risks (4)

e. Employees feel risk management is an intrinsic part of their own role (6)

3. DOES YOUR ORGANIZATION HAVE A CLEAR UNDERSTANDING OF ITS RISK APPETITE?

a. Risk Appetite is neither identified, understood, or communicated. (0)

b. Risk Appetite is formally discussed and used for decision-making at the board and executive level only (1)

c. Executives understand their aggregated and interlinked level of risk so they can determine whether it is acceptable (2)

d. Managers understand the degree to which they are permitted to expose the organization to the consequences of an event or situation when making decisions (3)

e. Risk appetite and any changes to it are communicated to all levels of the organization in a timely and appropriate manner, with understanding confirmed at all levels. (5)

4. HOW WIDELY HAS YOUR ORGANIZATION DEPLOYED RISK MANAGEMENT PRINCIPLES AND PROCESSES?

a. Risk management is deployed right across the enterprise AND IS used in strategic decision making at board level (5)

b. Risk management is deployed right across the enterprise BUT NOT YET used in strategic decision making at board level (4)

c. Risk management is only deployed in specific divisions or departments (3)

d. Risk management is only used for a range of programs and projects (2)

e. Risk management is only used on isolated projects (1)

f. Our organization has not yet deployed risk management (0)

5. WHICH TOOLS DOES YOUR ORGANIZATION USE FOR RISK MANAGEMENT? (CHOOSE THE MOST PREVALENT TOOL THAT YOUR ORGANIZATION USES.)

a. Package from application software vendor (5)

b. In-house developed software (4)

c. Spreadsheets (2)

d. Paper-based solution (1)

e. No tool (0)

6. DOES YOUR ORGANIZATION HAVE A FORMALIZED RISK MANAGEMENT CAREER PATH?

a. There is no formalized risk career path and no plans to develop one (0)

b. We think a formalized risk career path would be a good idea, but haven't done anything yet (1)

c. We are in the process of developing a formalized risk career path (2)

d. Our organization already has a formalized risk career path (5)

Scoring: Total your risk maturity index using the values listed at the end of each possible response. Use the matrix below to gain a broad understanding of your risk maturity.

0–7	Immature. Consider a formal process to complete the ERM Readiness questionnaire. Involve all level of the organization in the self-assessment.
8–14	Implementing. You are building a risk practice and beginning to demonstrate the value of risk understanding across you organization. Your risk practice success is largely dependent upon a small set of risk "champions". Consider a larger investment in training to build the knowledge base of risk across you
15–24	Maturing. Congratulations, your risk practice is expanding. Where risk management is being practiced, it is driving business value and business success. It is likely that your record-keeping processes and communication procedures are bogging down your progress in extending risk to all parts of your organization . Your next step is to implement a formal ERM platform.
25–30	Mature. Your risk practice is informing your entire organization. Risk levels are measured, monitored and discussed throughout your organization. Your risk organization is becoming a full partner in strategic decision-making at every level of the company.
31+	Congratulations! You've successfully implemented a world class enterprise risk practice. Your risk strategy and your business strategy are aligned frequently. You are increasing your firm's competitiveness through the appropriate application of risk in all your business practices. Consider speaking at next year's World Risk Day Virtual Summit.

Each individual and each organization has different concerns when it comes to ERM readiness. However, here is a compiled list of the questions most commonly asked of Active Risk when customers are considering implementing or expanding their risk practice.

5. Enterprise Risk Management FAQs

HOW DO I KNOW IF MY ORGANIZATION IS READY FOR AN ERM INITIATIVE?

Here are the key signs that the organization is ready for an ERM initiative include:

Requests for ERM activity and/ or data from the board or executive;

Requests for ERM activity and/ or data from the business;

A threat has occurred or an opportunity has been missed that would have been better managed or exploited through a formal ERM framework;

Risk data is not being appropriately captured, analysed or escalated;

There is little or no understanding of what risks are within the organization's tolerance;

There are multiple 'risk' functions with overlapping mandates and approaches to risk; and/ or

Elements of the ERM framework are already in place.

In addition, see the ERM Readiness Questionnaire on page 12 which provides examples of the types of questions to be taken into consideration prior to an ERM implementation.

HOW CAN I ENCOURAGE BUY-IN TO AN ERM IMPLEMENTATION?

To encourage buy-in, it is important to bring about the minimal amount of change to existing processes and practices. In other words, if it is possible to leverage existing processes and embed ERM within these, there is likely to be less resistance than there would be to wholesale change. In addition, any changes made should be incremental and supported by a strong business case that not only clearly identifies and quantifies the anticipated benefits of ERM, but which also addresses personal benefits and value for those involved in the change.

Other key points to consider when encouraging buy-in are to use business language rather than technical risk terms, and to be as practical as possible when developing new processes and practices. The timing and format of the implementation of any changes should take into account whether there have been other recent process changes within the business, and use lessons learned from previous change initiatives to avoid any pitfalls.

HOW QUICKLY WILL I SEE RESULTS?

The timeliness of the recognition of benefits will vary between organizations, and depends on how the ERM initiative has been rolled-out. For example, benefits are likely to be seen sooner if the ERM project has initially focused on a specific part of the framework rather than on an immediate enterprise wide deployment. The amount of resources dedicated to the initiative will also impact how quickly benefits will be realised, as – for example – the greater the number of resources dedicated to implementing and embedding the change, the quicker it is likely to happen and results be generated. It is also important to be clear prior to commencing the ERM activity what the anticipated benefits will be, and what measurements will be put in place to demonstrate that they have been achieved.

HOW CAN I INFLUENCE OUR RISK CULTURE?

To influence the culture it is first necessary to understand what the current risk culture is, and then understand whether this is sufficient or what changes need to be made to facilitate the desired culture. Understanding the current state can occur through the use of a risk culture survey which can be drafted in-house or outsourced to consultants. The types of areas such surveys may look at include: how senior management react to bad news, whether risk is associated with blame; and how useful risk management is perceived to be. Once this is determined, actions should be defined and implemented to change any of the results which are felt to be inappropriate, and the impact of these changes should be measured and monitored (e.g. by repeating the survey at agreed intervals) to ensure the required culture shift is occurring.

6. Glossary of Enterprise Risk Management Terms

ANALYTIC METHODS	Models whose solutions can be determined "in closed form" by solving a set of equations. These methods usually require a restrictive set of assumptions and mathematically tractable assumed probability distributions. The principal advantage over simulation methods is ease and speed of calculation.
CANDIDATE ANALYSIS	A restricted form of optimization analysis in which only a finite number of pre-specified decision options are considered, and the best set among those options is determined through the analysis.
COMPLIANCE RISK	Exposure to uncertainty resulting from external regulations and government statutes.
CREDIT RISK	Exposure to loss due to the default or downgrade of a bond-issuer, reinsurer or similar party.
DFA OPTIMIZATION	The formal process by which decisions are made under conditions of uncertainty. Components of an optimization exercise include a statement of the range of decision options, a representation of the uncertain conditions (usually in the form of probability distributions), a statement of constraints (usually in the form of limitations on the range of decision options), and a statement of the objective to be maximized (or minimized). An example of an optimization exercise is an asset allocation study (see below under Risk Management Applications).
EARNINGS BEFORE INTEREST, DIVIDENDS, DEPRECIATION, AND AMORTIZATION (EBITDA)	A form of cash flow measure, useful for evaluating the operating performance of companies with high levels of debt (when the debt service costs may overwhelm other measures such as net income).
ECONOMIC VALUE ADDED (EVA)	A corporate performance measure that stresses the ability to achieve returns above the firm's cost of capital. It is often stated as net operating profits after tax less the product of required capital times the firm's weighted average cost of capital.
ERM, ENTERPRISE RISK MANAGEMENT	A scalable, holistic approach to risk management that combines risk information from across the organization and uses this to meet business objectives and drive business performance and growth through embedding risk management in business processes and culture.
GOVERNANCE RISK	Exposure to uncertainty resulting from corporate or project leadership, and internal reporting requirements.
HAZARD RISK	Exposure to loss arising from damage to property or from malicious usually also includes the perils covered by property/casualty insurance.
LIQUIDITY RISK	Exposure to adverse cost or return variation stemming form the lack of marketability of a financial instrument at prices in line with recent sales.
MARKET RISK	Exposure to uncertainty due to changes in rate or market price of an invested asset (e.g., interest rates, equity values).
MEAN/VARIANCE/COVARIANCE (MVC) METHODS	A special class of statistical methods that rely on only three parameters: mean, variance, and covariance matrix.

OPERATIONAL RISK	Exposure to uncertainty arising from daily tactical business activities.
OPPORTUNITY RISK	Probability of loss arising when resources are irreversibly committed for one opportunity and a better opportunity presents itself.
PROBABILITY OF RUIN	The percentile of the probability distribution corresponding to the point at which capital is exhausted. Typically, a minimum acceptable probability of ruin is specified, and economic capital is derived.
PROJECT RISK	Exposure to uncertainty within a specific project, including, for example, schedule, technology or implementation issues.
RISK APPETITE	The amount of risk that an organization is willing to seek or accept in the pursuit of its long term objectives.17
RISK CULTURE	The behaviours, beliefs and values as exhibited by the organization in relation to risk management.
RISK DASHBOARD	The graphical presentation of the organization's key risk measures (often against their respective tolerance levels); typically used in reports to senior management.
RISK GOVERNANCE	Oversight of the ERM framework encompassing risk roles, committees and reporting.
RISK IDENTIFICATION	The qualitative determination of risks that are material, i.e., that potentially can impact the organization's achievement of its financial and/or strategic objectives. This is often done through structured interviews of key personnel by internal (e.g., internal audit) or external experts. In some cases, the organization's business process maps are used to guide the risk assessment.
RISK MAPPING	The visual representation of risks (which have been identified through a risk assessment exercise) in a way that easily allows priority-ranking them. This representation often takes the form of a two-dimensional grid with frequency (or likelihood of occurrence) on one axis, and severity (or degree of financial impact) on the other axis; the risks that fall in the high-frequency/high-severity quadrant are given priority risk management attention.
RISK MATURITY	The level of skills, knowledge and attitudes displayed by people in the organization, combined with the level of sophistication of risk management processes and systems in managing risk within the organization.18
RISK PRIORITIZATION	The ranking of material risks on an appropriate scale, such as frequency and/or severity (see also "risk mapping," below).
RISK PROFILE	Represents the entire portfolio of risks that constitute the enterprise. Some companies represent this portfolio in terms of a cumulative probability distribution (e.g., of cumulative earnings) and use it as a base from which to determine the incremental impact (e.g., on required capital) of alternative strategies or decisions.
RISK TOLERANCE	The boundaries of risk taking outside of which the organization is not prepared to venture in the pursuit of its long term objectives.19
SHORTFALL RISK	The probability that a random variable falls below some specified threshold level. (Probability of ruin is a special case of shortfall risk in which the threshold level is the point at which capital is exhausted.)

SIMULATION METHODS (OFTEN CALLED MONTE CARLO METHODS)	Models that require a large number of computer-generated "trials" to approximate an answer. These methods are relatively robust and flexible, can accommodate complex relationships (e.g., so-called path dependent relationships commonly found in options pricing), and depend less on simplifying assumptions and standardized probability distributions. The principal advantage over analytic methods is the ability to model virtually any real-world situation to a desired degree of precision.
STATISTICAL METHODS	Models that are based on observed statistical qualities of (and among) random variables without regard to cause-and-effect relationships. The principal advantage over structural models is ease of model parameterization from available (often public) data.
STRATEGIC RISK	Exposure to uncertainty arising from long-term policy decisions.
STRUCTURAL METHODS	Models that are based on explicit cause-and-effect relationships, not simply statistical relationships such as correlations. The cause/effect linkages are typically derived from both data and expert opinion. The principal advantages over statistical methods include the ability to examine the causes driving certain outcomes (e.g., ruin scenarios) and the ability to directly model the effect of different decisions on the outcome.
TAIL VALUE AT RISK (TAIL VAR) OR TAIL CONDITIONAL EXPECTATION (TCE)	An ECOR-like measure in the sense that both the probability and the cost of "tail events" are considered; the calculation differs from ECOR in such a way that it has a desirable statistical property (i.e., coherence) that is beyond the scope of this document to describe.
VALUE AT RISK (VAR)	The maximum loss an organization can suffer, under normal market conditions, over a given period of time at a given probability level (technically, the inverse of the shortfall risk concept, in which the shortfall risk is specified, and the threshold level is derived therefrom). VaR is a common measure of risk in the banking sector, where it is typically calculated daily and is used to monitor trading activity.

Adapted from The Language of Enterprise Risk Management: A Practical Glossary and Discussion of Relevant Terms, Concepts, Models, and Measures, Jerry Miccolis, Tillinghast-Towers Perrin. May 2002. Certain of these definitions were adapted from *The Dictionary of Financial Risk Management*, by Gastineau and Kritzman, 1996, Frank J. Fabozzi Associates.

7. Resources

WWW.WORLDRISKDAY.COM
Proceedings from the first annual World Risk Day Global Virtual Summit. Includes one-demand webcasts from global risk leaders, discussion groups, Q&A sessions, white papers and downloadable presentations

WWW.ACTIVERISK.COM
Active Risk is the first Enterprise Risk Management (ERM) solution provider to drive business performance by allowing organizations to manage risk more effectively. Active Risk Manager (ARM) helps organizations meet Operational Risk, Project Risk, Opportunity Management and Governance & Compliance challenges with advanced software which can be implemented across businesses in a range of industry sectors. Active Risk has offices in the UK, USA and Australia, servicing customers worldwide through a growing network of partners.

WWW.RIMS.ORG
RIMS (The Risk and Insurance Management Society, Inc.) is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Founded in 1950, RIMS brings networking, professional development and education opportunities to its membership of more than 10,000 risk management professionals who operate in more than 120 countries.

WWW.THEIRM.ORG
IRM are independent, well-respected advocates of the risk profession, owned by practising risk professionals. IRM passionately believes in the importance of risk management and that investment in education and continual professional development leads to more effective risk management. They provide qualifications, short courses and events at a range of levels from introductory to expert.

WWW.PMI.ORG
The Project Management Institute (PMI) is the world's leading not-for-profit membership association for the project management profession, with more than 600,000 members and credential holders in more than 185 countries. PMI's worldwide advocacy for project management is supported by its globally-recognized standards and credentials, our extensive research program, and its professional development opportunities.

WWW.RMIA.ORG.AU
The Risk Management Institution of Australasia Limited (RMIA) is the largest professional association and peak body for risk management in the Asia-Pacific region. Members of RMIA cover every sector of the economy and all levels of government. RMIA's members are located predominantly in Australasia, but there is a growing membership internationally.

WWW.PRIMACENTRAL.ORG
For three decades, the Public Risk Management Association (PRIMA) has been the one-stop resource for educational programming, risk resources and networking opportunities for public sector risk managers. PRIMA's mission and goals are guided by its core competencies for public sector risk managers. Headquartered in Alexandria, VA, PRIMA is the largest risk management association dedicated solely to the practice of risk management in the public sector. PRIMA's membership is made up of more than 2,000 entities in over 1,800 jurisdictions.

WWW.FERMA.EU
FERMA provides the means of co-ordinating risk management and optimising the impact of these Associations outside of their national boundaries on a European level. Since 1974, FERMA has been the leading organization for risk management in Europe. FERMA promotes communication among its members and also within IFRIMA (International Federation of Risk and Insurance Management Associations) of which FERMA is a member.

WWW.AFERM.ORG
AFERM is a professional organization dedicated to the advancement of federal Enterprise Risk Management (ERM). The Association serves its members by providing a forum for discussion of issues relevant to participants in the federal risk management profession, sponsoring appropriate educational programs, encouraging professional development, influencing governmental risk management policies and practices and serving as an advocate for the profession.

[1-2] *Ernst & Young, Turning Risk into Results. 2012, p3*

[3-5] *Ernst & Young, Investors on Risk. The Need for Transparency. 2006, p3*

[6] *Aon, Global Enterprise Risk Management Survey. 2010, p11.*

[7] *Aberdeen Group, Managing Enterprise Risks. An Executive's Guide to Reducing Corporate Liabilities and Costs. 2011, p3*

[8] *PWC, Black Swans Turn Grey, the Transformation of the Risk Landscape. 2012, p7*

[9] *Turning Risk into Results, Ernst & Young, 2012, p3*

[10] *Aberdeen Group, Managing Enterprise Risks. An Executive's Guide to Reducing Corporate Liabilities and Costs. 2011, p10*

[11] *PWC, Risk in Review: Rethinking Risk Management for New Market Realities. 2012, p1*

[12] *RMIS, The 2008 Financial Crisis. A wake-up call for ERM. 2009, p6*

[13] *Deloitte, Global Risk Management Survey Seventh Edition. Navigating in a Changed World. 2012, p2*

[14] *RMIS, The 2008 Financial Crisis. A wake-up call for ERM. 2009, p4*

[15] *Active Risk, What Makes a Great Risk Manager? Survey Summary Report. 2012, p1*

[16] *RMIS, The 2008 Financial Crisis. A wake-up call for ERM. 2009, p4*

[17-19] *IRM, Risk Appetite & Tolerance Guidance Paper. 2011, p15*

About Active Risk

Active Risk™ wants to change the way organizations look at risk management.

At Active Risk, we help our customers win in their businesses by making risk management valuable. We listen, innovate and provide the world's most amazing Enterprise Risk Management solutions that give our customers tools to expand their risk taking ability, uncover new opportunities and out-manoeuvre their competition. We build these solutions so our customers can focus on achieving their goals, beating their competition and leading their industries. At Active Risk, we believe that *Risk Management Success = Business Success.*℠

Active Risk is the first Enterprise Risk Management (ERM) solution provider to drive business performance by allowing organizations to manage risk more effectively. Active Risk Manager™ (ARM™) is the first dedicated web-based risk management tool built specifically for today's enterprises. ARM helps organizations meet Operational Risk, Project Risk, Opportunity Management and Governance & Compliance challenges with advanced software which can be implemented across businesses in a range of industry sectors. ARM provides a true risk management system of record for the business, so users can stay ahead of the risks with real-time data, instantly available throughout an organization via executive dashboards, alerts and reports.

We continuously deliver value to our customers, employees and shareholders by providing the most proven, innovative Enterprise Risk Management software available anywhere.

EMEA Headquarters

Sword Active Risk
1 Grenfell Road Maidenhead
Berks SL6 1HN
UNITED KINGDOM

Tel: +44 (0)1628 582500
Learn more at www.sword-activerisk.com

US Headquarters

Sword Active Risk, Inc.
13221 Woodland Park Road Suite 440
Herndon, VA 20171
UNITED STATES

Tel: +1 (703) 673 9580
Email us at info@sword-activerisk.com

Australia

Sword Active Risk Pty Ltd 40/140 William
Street Melbourne
VIC 3000
AUSTRALIA

Tel: +61 3 9229 3850
Follow us on Twitter @ActiveRisk