



Play Training Module

This is a transcript of a narrated multimedia training module. You can view the online Multimedia training module by clicking the link above or at riskcentral.com.au

Introduction to Enterprise Risk Management

Tony Matthews, B.E., M.B.A
Managing Director - RiskCentral
Email: tony.matthews@riskcentral.com.au

2. Introduction

2.1.

Hello and Welcome. This is an “Introduction to Enterprise Risk Management” for managers and directors. The objective of this training is to help you understand the basics of Enterprise Risk Management Systems and how to design an ERM system that works or improve the effectiveness of an existing system. In the next 15 minutes we will discuss:

- The objectives of Enterprise Risk Management or ERM
- Common problems with ERM systems.
- Essential outputs of an ERM system and
- The critical elements in the design of an ERM system.

This is a basic guide only, designed for general awareness. It is not a comprehensive guide and does not ensure compliance with any standards, regulations or statutory obligations. Not all conditions or situations are discussed or contemplated. Rather the module targets the most important issues and concepts, in order to keep the training brief, practical and effective. Please note that effective ERM will reduce risks but will **not eliminate** them. Risk Management should be seen as a Continuous Improvement Process.

3. What is Enterprise Risk Management

3.1.

The term Enterprise Risk Management was conceived as a name for an overarching business management process designed to reduce the chance of a business experiencing major losses and increase the chance of businesses achieving their goals.

The objective of ERM is clear and generally agreed but that is where the agreement ends. There is no general agreement on what this process should look like and how it should work. There is no agreement between companies, regulators, countries, consultants or even standards.

Adding to this problem is that most of the ERM processes used do not produce the desired outcomes or stand up to critical analysis. Most major companies which have failed in recent times had an ERM system in place. You have probably been exposed to some of these ineffective risk management systems yourself.

So we have a problem, how do we design an effective ERM system if there is no agreement on how to do it and most are poorly designed? Well, let's start by identifying what doesn't work. In the following sections we will discuss some of the major reasons why ERM systems fail.

4. Why Systems Don't Work

4.1. Ad hoc and Unsystematic Risk Management

A lot of traditional risk management has been based on Ad hoc or Unsystematic methods or approaches. You have experienced these before and they include:

- Relying on personal experience to determine how important individual risks are – in other words - Making sure you don't make the same mistake twice.
- Relying on personal experience to determine appropriate controls and appropriate risk levels – famous last words - I have been doing it this way for 10 years and nothing has ever gone wrong.
- Relying on intuition or subjective uneducated opinions to determine how important risks are.
- Thinking that Insurance = Risk Management.

- Having an Emergency Response Plan - that is - relying on re-active rather than pro-active controls.
- Complying with statutory requirements – that is - relying on government to tell you how to manage your risks.
- Relying on prescriptive controls rather than performance based controls. It does not matter how well you comply with prescriptive controls if they do not effectively control the risk. Audits traditionally focus on if the rules are followed rather than if they are the right rules. And finally
- Industry norms – that is - doing what everyone else is doing. Thinking that you can't get into too much trouble if you are doing what every one else is doing'.

The reliance on these approaches lead to ad hoc, fragmented and ineffective risk management processes that underestimate some of the biggest risks to business and overestimate others. This leads to uncontrolled risks and unnecessary costs.

4.2.

These traditional unsystematic approaches to risk management have lead to many failures of businesses. As an example - The world's banks and financial institutions relied heavily on 'industry norms' and 'regulation', as the primary methods of managing the risk of sub prime market before the world financial crisis of 2008. It turned out that the industry as a whole had failed to identify the very serious risk associated with the sub prime market. Mostly because they blindly followed what everyone else was doing without any significant analysis of possible risks.

Regulations, which are generally reactive rather than proactive, also did not anticipate this risk. Obviously relying on regulations and industry norms is not ideal.

In contrast, some organisations did identify and quantify these risks. They consequently had controls in place to reduce their losses.

4.3.

The previous individual approaches, themselves are not to blame. There is nothing inherently wrong with the listed traditional approaches and they all have their part to play in an ERM system. But they can not be relied upon by themselves to form an effective system because they lack an overarching high level systematic process to ensure that:

- All significant risks are systematically identified
- All identified risks are systematically quantified and ranked, and

- All risks are systematically and appropriately controlled

This high level systematic process, which identifies, quantifies and controls significant risks is therefore an essential part of every effective ERM system.

4.4.

Directors have a legal requirement to demand effective risk management systems that manage organisational risks and keep the directors informed. However, most large organisations could not accurately tell their Directors what their top 10 risks are, let alone demonstrate a systematic and logical process for managing each risk. This is allowed to happen because most directors are not aware of the flaws and unsystematic nature in the traditional approaches.

Company stockholders should also be demanding evidence of this high level process and independent reviews on how the ERM systems are performing.

4.5. Focus on Failure

The objective of an ERM system should be to maximise the chance of an organisation succeeding or reaching its objectives, not just, reducing the chance of it failing.

If the ERM system can be seen in this light, than Risk Management becomes an important part of everyone's job, not just something done by the accounting department or Health and Safety. It then becomes a valuable business management system.

4.6. Hidden Agenda's

Although there is a common agreement about what the objectives of ERM system should be, the stated objectives are often undermined by hidden alternative objectives. Some examples of alternative objectives are:

- To achieve compliance with a standard, requirement or rule – in other words - the risk management system only exists to get the tick in the box.
- A system to cover your back side, if something goes wrong.
- Obtain funds for a pet project, for a department or to increase the importance of someone's job. Or
- Validate or support someone's pre existing opinions.

Companies regularly waste millions of dollars, waste peoples time and stifle productivity because risk management systems have improper hidden objectives. There is no point in having a system which no one can trust or understand.

4.7. Financial ERM models

Some ERM models are only concerned with financial risks and financial controls. This overlooks major strategic and operational risks which may seriously reduce the success of the organisation. This is obviously a flawed approach. All risks to organisational objectives need to be managed by any ERM system.

4.8. Inaccurate Risk Assessments

As discussed earlier, an ERM system should:

- Systematically identify all significant risks to business objectives including strategic, operational and financial risks.
- Accurately quantify the size of risks. Then prioritise and allocate resources to manage them based on their size.
- Select and implement the best controls to cost effectively reduce risks to acceptable levels.

4.9.

One of the most important steps is accurate risk quantification. Unfortunately a lot of risk quantification methods, used by organisations and consultants, are frighteningly inaccurate and misleading. Most of these organisations and consultants are blissfully unaware of the problem.

If a risk quantification tool delivers inaccurate, deceptive or incorrect results, this will lead to a misallocation of resources and risks that are not appropriately prioritised or controlled. Exactly the same problem we were trying to avoid in the first place. A poor quantification method can reduce the effectiveness of the ERM system to the point where it is counterproductive.

The good news is, learning how to quantify risk with appropriate accuracy is not difficult but does need the right tools; a little instruction and practice.

4.10.

You have probably experienced risk quantification tools which don't make sense or don't help. Common poor outcomes include:

- Over estimating risks so that most risks are rated as extreme risks. This doesn't help prioritise the larger risks for attention because smaller risks have been over estimated, often by factors of 100s or 1000s of times. It doesn't allow scarce resources to be directed to the areas of most need.
- Results that don't resemble the reality of the situation. If the results aren't realistic they will not help direct resources to the areas where they will do the most good. This will lead to higher levels of risk, ineffective control and additional costs.
- Having too many risks in your risk register. If you have hundreds or thousands of risks in your risk register, then it is likely that most of the risks have been over estimated in size, are not significant, are broken down into too much detail or have been repeated. The document is too big to be useful and is not accurate. This doesn't help prioritise or manage risk. The ERM system should be a high level system that relies on other lower level systems to manage smaller risks.

4.11.

Correct and incorrect methods of quantification are discussed in detail in the online training module "How to do a Risk Assessment" and the discussion paper "Advanced Risk Assessment". Both are available at riskcentral.com.au. But to start with, your system should use the correct equation to calculate risk. Risk equals Consequences times likelihood. Or, the Risk of a possible loss scenario equals the consequences of the scenario times the likelihood of the scenario.

This is a natural mathematic equation and can be very easily proven. Be very sceptical of any system which does not use a form of this equation as the basis for risk quantification.

5. What Will Work

There are models or processes that will achieve ERM objectives and they can be uncomplicated, understandable and practical. In the next few sections we will explain what the tangible outputs of an ERM system should be and how systems can be designed to achieve these outputs.

5.1. The tangible outputs of an ERM system

As stated earlier, the objective of a risk management system should be, to ensure that:

- All significant risks to business objectives are identified including strategic risks, operational risks and financial risks.
- Risks are prioritised based on size, and resources are allocated to manage them appropriately.
- The best controls are selected and implemented to cost effectively reduce risks to acceptable levels.

5.2.

If a risk management system is to achieve these objectives, the system needs to produce some specific tangible outcomes. These tangible outcomes need to include:

1. An up to date Risk Register

A Risk Register is a concise list of the largest identified risks along with some important risk details such as the risk scenarios considered and the estimated size of risk. The Risk Register is one of the primary documents of an ERM system. It is vital to continuously update the document as conditions change, to accurately reflect changes in the risk profile. The system should ensure that all significant risks to organisational objectives are identified and quantified, in a systemic way and recorded in an up to date risk register.

The management of each identified risk should be allocated to an appropriate person. This person should be responsible for managing, maintaining accurate information and reporting on this risk to management, at appropriate intervals.

5.3.

2. Up to date Risk Action Plans

‘Risk Action Plans’ document the plans put in place to manage significant risks. The person responsible for each significant risk should be responsible for the production and maintenance of a Risk Action Plan for that risk. The Risk Action Plan for larger risks should include business cases or a cost benefit analysis to select the most appropriate controls. This may also include an analysis to determine appropriate residual risk levels. An appropriate risk level may be based on balancing risk and return.

5.4.**3. An effective Risk Management Culture**

An effective risk management culture may be defined as - The pervasive and effective use of appropriate risk management tools through out the organisation to help in decision making. The ERM system should promote the use of appropriate risk management tools and methods in all significant decisions.

5.5.**4. Appropriate Management and Board Reports**

The accumulation of all the previous outcomes should be accurate, concise and informative reports to help decision makers make the best decisions. Regular management and board reports should include up to date risk registers and risk action plans for high level risks. This will help ensure the directors and management are appropriately informed of larger risks, planed controls, the business cases for these controls and other important details.

The effectiveness of an ERM system can be largely measured by how effectively it produces these 4 outcomes. As such, it is also vitally important that performance reviews of the ERM system be conducted to regularly measure the quality of these outcomes. This should include both internal and external reviews.

6. The elements of an ERM system**6.1.**

As with all business systems, an ERM system requires a number of elements to perform effectively.

6.2.

ERM system elements can be broken into three parts.

The Hard elements provide information on what managers are expected to do, and when and how they should do it. These hard elements are primarily documents.

Policy - Documenting vision, objectives, strategy, roles and responsibilities

Methods and Tools – Documenting Risk Assessment and Risk Action Plan methods and tools

Rules and Guidelines - How are managers expected to manage risk? What are they expected to do and when they are expected to do it.

Information Management - Access and maintenance of information such as Risk Registers, Risk Action Plans, ERM Policy and rules.

Hard Elements

System Element	Description
Policy	Documenting vision, objectives, strategy, roles and responsibilities
Methods and Tools	Risk Assessment and Risk Action Plan methods and tools
Rules and Guidelines	How are managers expected to manage risk? What are they expected to do and when they are expected to do it.
Information Management	Access and maintenance of information such as Risk Registers, Risk Action Plans, ERM Policy, rules, etc

6.3.

The Motivational elements help ensure that people follow the rules and guidelines.

Reporting Structures - Reporting structures, management meetings & reporting requirements.

KPIs - Setting Risk Management KPIs for senior management

Performance Reviews - Individual performance reviews & external ERM system performance reviews

Value Perception - Do people think the ERM system is valuable

Motivational Elements

System Element	Description
Reporting Structures	Reporting structures, management meetings & reporting requirements.
KPIs	Setting Risk Management KPIs for senior management
Performance Reviews	Individual performance reviews & external performance reviews of the system
Value Perception	Do people think the ERM system is valuable

6.4.

Training Elements

Training may be required to ensure managers understand the ERM system and their responsibilities under the system.

6.5.

These elements can be brought together in many ways to produce acceptable risk management systems and outcomes. That is to say, there is no “one best” mix of system elements to achieve desired outcomes. Decisions as to which elements to adopt should be made by experienced persons with consideration of the organisation’s particular culture, structures, personalities, political circumstances and what systems are already working well in the business. Some part of the system may be just extensions of existing systems. For example, the risk management KPI element may just be an extension of your existing KPI system for management. The Reporting structures for the ERM system may be included in existing management structures and normal management meetings.

6.6. Important Parts of the ERM System

Some parts of an ERM system are more important than others. In most cases the 4 most essential parts to an ERM system are:

- Accurate and effective risk assessment methods. This is part of the ‘Methods and Tools’ system elements.
- A simple set of requirements for managers. This is part of Rules and Guidelines system elements. – Requirements may be something like:
 - Each manager is to identify and quantify the top 5 risks they are responsible for
 - Each manager is to maintain an up to date risk register and risk action plan for each risk.
 - Nominate someone to combine the risks from all managers into one risk register and order by size

6.7.

- Scheduled and systematic reviews of how well each manager is managing the risks they are responsible for. This is part of Reporting Structures system elements. This could be done by placing risk management reviews as a permanent agenda item in management meetings. Managers could then take turns at presenting their risks for group discussion. Attention should be allocated to risks based on their size.
- Each manager is assigned Key Performance Indicators (KPIs) related to risk management responsibilities, which are seriously considered in Performance Reviews.

7. Conclusion

You should now better understand the objectives, outcomes and design of ERM systems. This knowledge should allow you to:

- Improve the effectiveness of your existing system
- Design and implement an ERM system or
- More effectively participate in your organisation's ERM system

As a director or manager, if your organisations' ERM system is not producing these outcomes or does not have these elements or objectives then you should be asking why not.

As a share holder of a company you can look for the existence of these system outcomes, elements and objectives as indication of how well your investment company manages risk. A company can not make the content of its risk registers public because it will contain commercially sensitive information but it can report its existence and document the ERM system elements and objectives. The performance of ERM systems should also be reviewed by third party experts, much like accounting systems are review by auditors. Review Reports should be made available.

An effective ERM system will help your organisation reach its goals and remain successful. It does not need to be complicated but it does need to have the right objectives, the right methods, the right elements and the right outcomes.