

# A SHORT GUIDE TO ENTERPRISE RISK MANAGEMENT



LIZ TAYLOR RISK CONSULTING



## EXECUTIVE SUMMARY

This “Short Guide to Enterprise Risk Management” is intended to be a basic introduction to Enterprise Risk Management, particularly aimed at Senior Management, Board Members and Chief Officers. We hope that this “Short Guide” will help to dispel some of the myths surrounding Enterprise Risk Management. It should give some idea of the benefits there are in embracing it as part of the good management processes and provide a little insight into what it’s all about and the phasings involved.

## INTRODUCTION

Our main aim is to highlight Enterprise Risk Management as an enabler in management systems. Managed risk taking is at the heart of innovation, thus Enterprise Risk Management can be used to unlock the potential for innovation so that more risk can be taken in a managed and knowing way. But Enterprise Risk Management must not be a stand alone discipline; it should be a part of everything else that happens from strategic planning to managing projects and delivering your business.

**Checklist or real cultural change** – If your advisers are only concentrating on getting you better scores on the checklists for Enterprise Risk Management, you may be missing out on a big opportunity to make cultural improvements, get rid of the blame culture and unlock the potential of your staff to innovate.

**You are already doing it** - It should also help you to understand that much of what you do already is good Enterprise Risk Management, but in another guise and in different words. For example, if you are properly using the “Prince 2” methodology for project management, then you are already doing Enterprise Risk Management as part of your project management – but with different terminology. If you already have great management systems and are successful in your enterprises, you are already doing Enterprise Risk Management.

**Only you can do Enterprise Risk Management** – Enterprise Risk Management is not something that someone can come in and implement for you or give you a simple checklist to comply with. Checklists are important when it comes to auditing that what you are doing is right, but the practice of Enterprise Risk Management comes from those in your organisation who are making decisions, taking action, and delivering goods and service.

**Everyone’s job** – You cannot appoint one person as a risk manager, risk champion, or chief risk officer and then leave them to take responsibility for Enterprise Risk Management within your whole organisation; wherever there is a decision or an action being taken, there lies risk potential. The person taking that decision or action has also to take responsibility for managing the risk of that action or decision. Your risk manager or chief risk officer should be the focus for good practice, an enabling person, a trainer, facilitator and a guide.



**Every minute of every day but with balance** – Enterprise Risk Management is like a good safety system for a toddler; it's got to be constant, engaging and thorough. If you try to manage the safety of a toddler once every so often, like auditing safety once a week, accidents are certain to happen. Everyone around the toddler has to take some part in ensuring that hot cups aren't on the edge of the table, cords aren't hanging down, breakables are not within reach and there's nothing small enough to push into the DVD slot. Imagining the hot cups as new projects, cords as existing systems, breakables as policies; now you can see that everyone has to take responsibility for all the hot cups, cords and breakables in their area.

However, you have to exercise balance in managing the risk. If the toddler has a habit of taking objects and banging them against his head, what do you do? Your choices are a) deny him access to all objects, b) tie his hands down, or c) just let him get on with it, having removed the most dangerous objects (too small, too sharp, too hard), and hope that he doesn't come to too much harm before he understands the link between hitting himself and it hurting.

The choice is yours, but if you choose anything other than c), what kind of risk taker will the child grow up to be if given no managed exposure?

Similarly, in a work environment, people have to be stretched in their decision making and "doing" role. If there is no allowance for taking managed risks in an appropriate control environment, you stifle the whole process, prevent innovation and breed poor morale. So a balanced approach to Enterprise Risk Management should allow for risk taking in a managed environment.

**Layered approach** – we encourage our clients to manage risk on a layered approach based on the risk in hand. The ultimate protection is to do a risk assessment on everything (every step, every plan, every piece of new kit etc) but that is hugely time consuming and counter productive. This would leave no time for running the business. To do this "micro risk assessment"<sup>1</sup> only approach prevents spontaneity and ownership by the decision makers. The layers of controls are for you to work out in your management process and will depend on the risk presented and the environment. A "micro risk assessment" approach must be carried out for critical risks, and a "macro risk assessment"<sup>2</sup> for all critical and non-critical risks updated on an "exceptions" basis when any of the controls or environmental influences change.

For example consider a frequent activity such as BACS transfer of funds to a supplier for a regular order. A macro risk assessment is carried out on that activity once every so often. Included in this is consideration to those things that would highlight an anomaly such as a variance in amount in excess of 15% or the frequency of payment changes. These are your exceptions and if either of those triggers is encountered the system should call for a micro risk assessment.

---

<sup>1</sup> "Micro risk assessment" done frequently at operational level on the activity itself

<sup>2</sup> "Macro risk assessment" done periodically on the systems or on the control environment. Updated on an "exceptions" basis when any of the controls or environmental influences change



## BENEFITS OF ENTERPRISE RISK MANAGEMENT

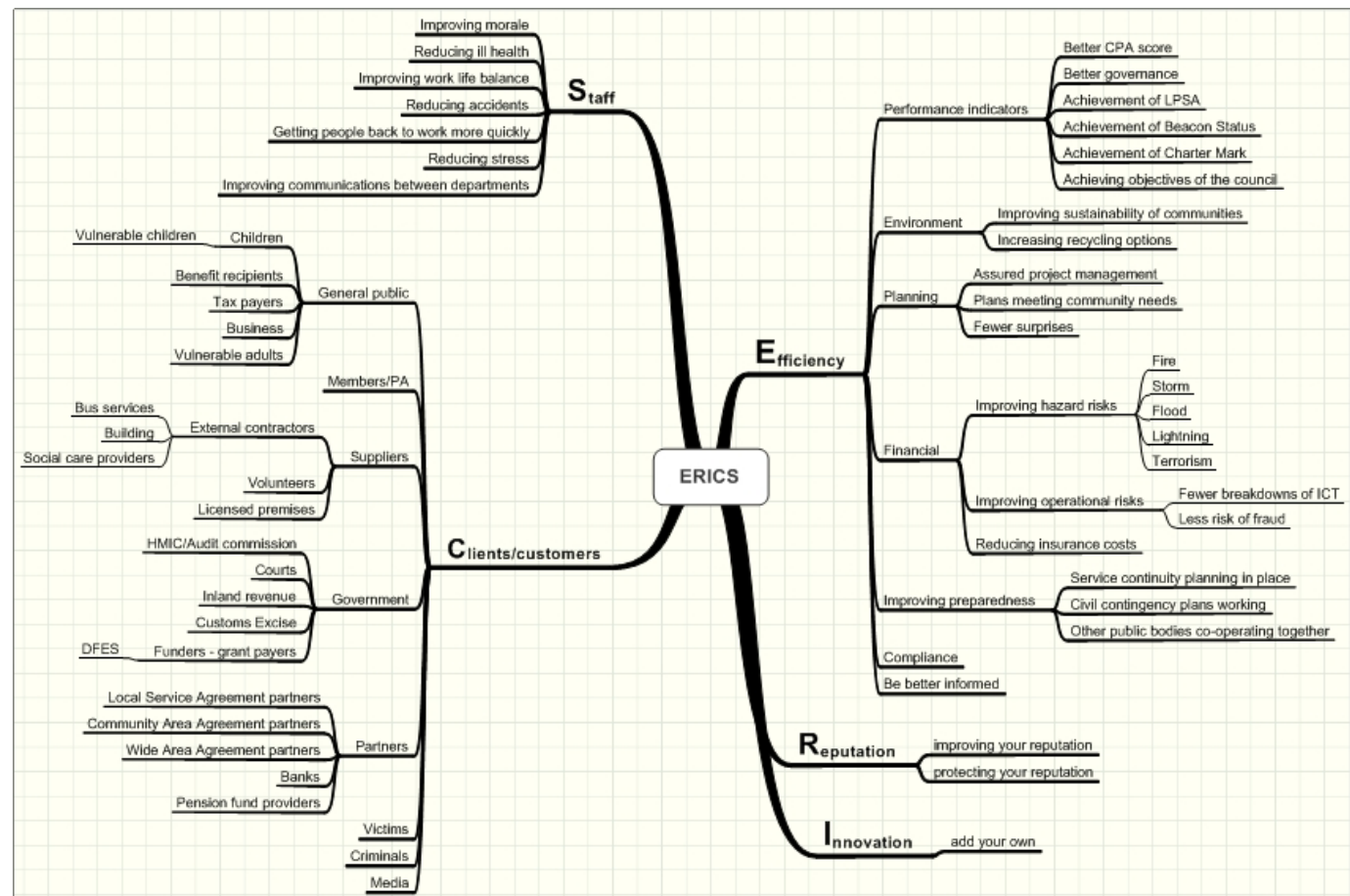
Rather than start with what it is and how to do it, it's worth having a look at what the **benefits** are of doing Enterprise Risk Management properly. We are not just talking here of getting a good Governance Report, or a good internal/external audit. We are talking about where Enterprise Risk Management is consumed into the core culture of the organisation where all decision makers are also safe risk takers.

## STAKEHOLDER BENEFITS

We use the acronym ERICS to summarise the key benefits to stakeholders – **E**fficiency, **R**eputation, **I**nnovation, **C**ustomer, **C**lient or **C**ommunity satisfaction and **S**taff.

This chart sets out some of the subdivisions of ERICS that you can analyse for your organisation to see where you want to see most improvement through the use of Enterprise Risk Management.

This type of approach also enables you to set performance indicators for the Enterprise Risk Management programme so you can track the benefits and measure them against the costs and investment in time.





## BASICS OF ENTERPRISE RISK MANAGEMENT

**What is risk?** Risk is something that crops up to stop you doing something you want to do, or changes the dynamics of a situation. It's not always a bad thing, as there is no activity without risk; it's in the very nature of things. Risk can present a threat, or an opportunity. Sometimes it can present both a threat and an opportunity.

What is bad is when it's a surprise, and it rocks the whole enterprise or where there is an event that seriously affects a stakeholder. Some people confuse risk and hazard. Think of a swimming pool full of sharks. That's a hazard. It's only when someone selects to jump in that it becomes a risk. You can have as many hazards around as you like, but the moment people, systems, property etc are exposed to them, they become risky.

Risk is a combination of the impact on the organisation, the likelihood of it occurring and the proximity of the event – ie how soon might it happen. There's more about this in the section on risk assessment below.

**What is uncertainty?** This is when there are unknowns that may prevent decisions being made. Sometimes we have to make assumptions based on the unknowns. Risk and uncertainty share a commonality in that you can use the same methodologies for both.

**Who does it and what do they do?** You need to work out what Enterprise Risk Management structure you propose to put in place, working out who's going to lead the process, who sets the policies, who implements the programme, the resources and support put into it, and the allocation of responsibilities.

**What is embedding Enterprise Risk Management?** This is where you get everyone in the organisation to take responsibility for managing the risks that they have an impact on. It requires the same cultural shift that you made when you had everyone take responsibility for Health and Safety. In an organisation that has embedded Enterprise Risk Management, no business plan is presented to management without consideration to the risks and the control environment; no strategic decision is made without an analysis of the uncertainties, threats and opportunities.

**How do you identify risk?** The first thing to do is to set out your goals or vision, or the goals/vision of the department or business activity that you want to do the risk analysis for.

Then you work out the things that can stop you from achieving those goals/vision, involving as many of the decision makers and front line staff as you can. It's also worth involving your clients or customers in this stage of the process. You can use any one of a number of models to provoke the ideas, like a PESTLE



(political, economic, social, technological, legal, environmental) model, such as mentioned in *Enterprise Risk Management – a Key to Success*<sup>3</sup>, or divide them into the sections hazard, operational, financial and strategic as set out in the *Risk Management Code of Practice BS31100*.<sup>4</sup> Don't worry if you have a long list of risks and some seem irrelevant.

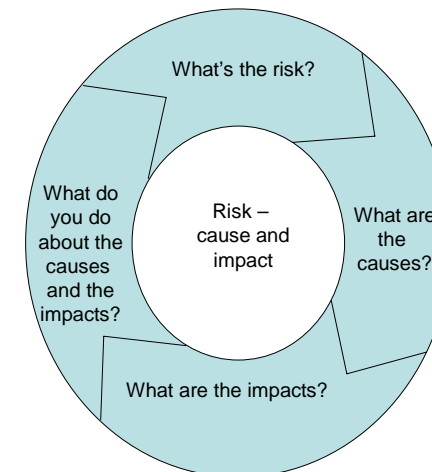
**How do we define risks?** Sometimes working out a definition for risk can be tricky. It's worth thinking about the causes and effects of a risk so that you get a list of risks that are not causes or effects. For example, brand or reputation damage often appears as a risk on a risk list or risk register. Brand damage is actually the result or effect of a risk. So what can cause brand damage? A major product failure? A professional failure? So you might list the risk as being a major public event caused by a number of professional and operational failures resulting in damage to our brand, image and reputation. So the risk is the major public event. See figure 1 – the Cause and Effect diagram.

**What is risk assessment?** This is where you prioritise the risks identified, based on likelihood (probability) and impact (magnitude) (see figure 2 below). It is also important to consider the proximity of the risk in terms of time. Again it is advised that you do this in a collective way, as people's perceptions will vary on the likelihood and impact based on their own experience and exposure. For example you must know people who are afraid of flying. Their internal risk evaluation process has got stuck on magnitude – "...if it crashes I'm sure to die..." and on the fact that the risk is out of their control. They cannot rationalise "probability", even though on a mile for mile basis flying is the safest form of travel.

**Visualising the risks** – your first prioritisation process is to look at the **impact** of the risk on the whole organisation (or the bit of the organisation you want to concentrate on). Now you might think that impact can only be measured on the basis of financial impact. But for example in the public sector reputation and community health are more important. Maybe brand or image are critical to your business? You might also want to have achievement of performance indicators as your key measurement of impact or even some other measurement, and don't forget health and safety risks.

Figure 1

## RISK – CAUSE AND EFFECT DIAGRAM



<sup>3</sup> See "Risk Management – a Key to Success" from ALARM on page 10 for further information

<sup>4</sup> See <http://www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/All-Standards/BS/BS-31100-Draft-for-Public-Comment-DPC/>



The next area to consider is the probability or likelihood of the risk occurring. Is it a question of when, rather than if? For example, an aeroplane crash is very low probability (with high impact) but a flood might be very likely (with a medium impact).

The Risk Matrix at Figure 2 shows how you might plot the risks on a chart with scoring for each risk.

This matrix has two axes, one for impact and one for likelihood. Bottom left hand corner is where the risk has negligible impact and improbable likelihood. The top right hand side of the matrix is where the risk has a catastrophic impact and a very likely likelihood. So you can use this to plot the risks that you have identified so you have an immediate visual understanding of which ones need to be tackled first. For this purpose we've used the scores 1 – 5 so our very like risk which is catastrophic appearing in the top right hand box scores 5 x 5 = 25. It is useful to use a numeric scoring like this as it makes it easier to prioritise risks.

### Prioritisation

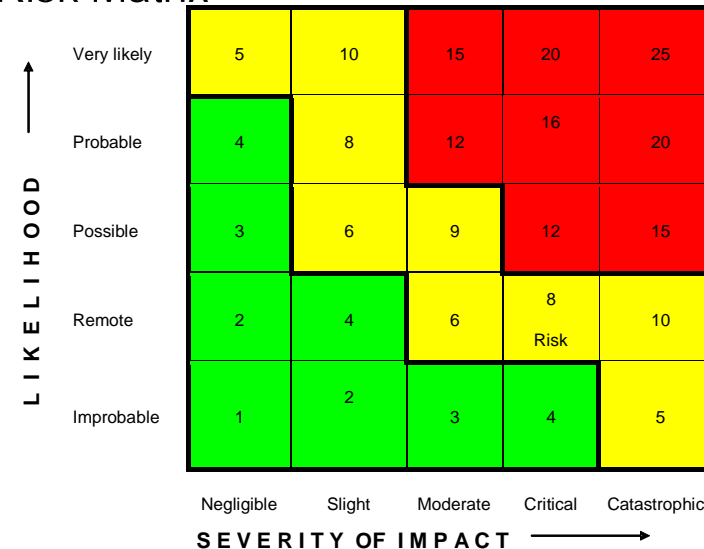
We would recommend that the risk assessment process goes further than just analysing impact and likelihood. There may be risks over which you have no control or that would take years of change and investment to alter and might affect very few people or make very little impact on the business. So we would recommend that you reassess all of your risks, on the basis of opportunity to improve, speed and ease of improvement, cost of improvement and breadth of business or community affected.

**How do you work out your risk appetite?** You know that you cannot reduce all risks. There has to be some risk left after you've done what you can to reduce the risks within your organisation. Maybe you can tolerate a delay of two days to your latest IT project, but a four month delay would have a serious impact on other plans. Perhaps a £15m fire in one property would be disastrous for the depot budget, but a loss of £500k at the call centre would not. Your risk appetite should be analysed carefully as this will help you to redefine the prioritised risks after the risk assessment process. In the chart at figure 2 the red risks cannot be tolerated, and would be prioritised for action first, and then the yellow risks, and finally you might decree that green risks are tolerated but monitored carefully.



Figure 2

### Risk Matrix





**What do you do about the risks?** The commonly held view is that you can only implement an action plan for a limited number of risks. So you take the top twenty or so risks from your risk assessment process, work out their “proximity” or how soon they might happen. Then you work out a plan to reduce the magnitude and/or impact of those biggest and most proximate risks that you have control over. Working out the causes and effects of the risk is really helpful here, as being very specific about what they are, can lead to a really good list of things that you can do and help you work out simple elegant solutions.

You allocate responsibility for each risk to one person and the risk action plan to all those that own the risk making activity. You then track performance over a period of time with specified performance indicators to ensure that real progress is being taken. When you’ve made the expected progress then you re-challenge the previous process and then start on the next twenty risks. This doesn’t mean that you should relax the controls on areas that are not in your top twenty risks, there is never any excuse for poor health and safety, and compliance is always a top priority.

It’s worth thinking about the things that you can do about risk in terms of;

- Terminate – stop doing that business activity where the risk is. If the risk outweighs the benefits, why are you doing it?
- Transfer – maybe you can transfer the risk to someone else either by contracting with them to take on the business activity, or perhaps to buy insurance.
- Tolerate – put up with the risk. Maybe doing something about it is far too expensive and risky in itself.
- Treat – do something about the risk. Choices might include stopping the risk from happening in the first place, tracking that it’s happening and do something then (a stitch in time saves nine), minimise the risk while it’s happening, or respond to the risk after it’s happened (business continuity, disaster recovery etc).

**What communication programme do we use?** Communication is vital to the success of many management strategies so that all involved feel some sense of ownership in the process, understand what’s going on, why it’s happening, and what’s in it for them. We work particularly closely with our clients in developing the communication programmes.

**What next?** The programme of training, monitoring, reporting, auditing and incentivising will be dependent on your own culture and existing management programmes. Further papers from Liz Taylor Risk Consulting are available for these areas. Do contact us if you wish to receive more information.



## THE ENTERPRISE RISK MANAGEMENT PROCESS SUMMARISED

1. What do you want to achieve – set out your goals clearly
2. What can stop you achieving it – identify the risks (whether they are threats or opportunities), their causes and their effects
3. How big is the risk – work out the impact of the risk and the likelihood. Also consider how soon the risk will happen
4. What do you do about it – based on the priority of the risk, work out if you can terminate the business activity, transfer the risk to someone else, tolerate the risk, and if all those fail, treat the risk by stopping it happening in the first place if you can
5. Then what – track and monitor that you are actually taking managed risks well



LIZ TAYLOR RISK CONSULTING

### Further reading

"Risk Management – a Key to Success" from ALARM at [www.alarm-uk.com](http://www.alarm-uk.com)

HM Treasury (2000) *Management of Risk: A Strategic Overview 'The Orange Book'*, HM Treasury.

BS 31100 – The British Standard for Risk Management, contact British Standards

### About Liz Taylor Risk Consulting

We are a consulting organisation dedicated to improving risk management for our clients. Our consultants are highly experienced in helping to implement risk management programmes.

Contact us on [info@liztaylorryskconsulting.co.uk](mailto:info@liztaylorryskconsulting.co.uk)

Tel 01626 337626

Fax 01626 330592

[www.liztaylorryskconsulting.co.uk](http://www.liztaylorryskconsulting.co.uk)