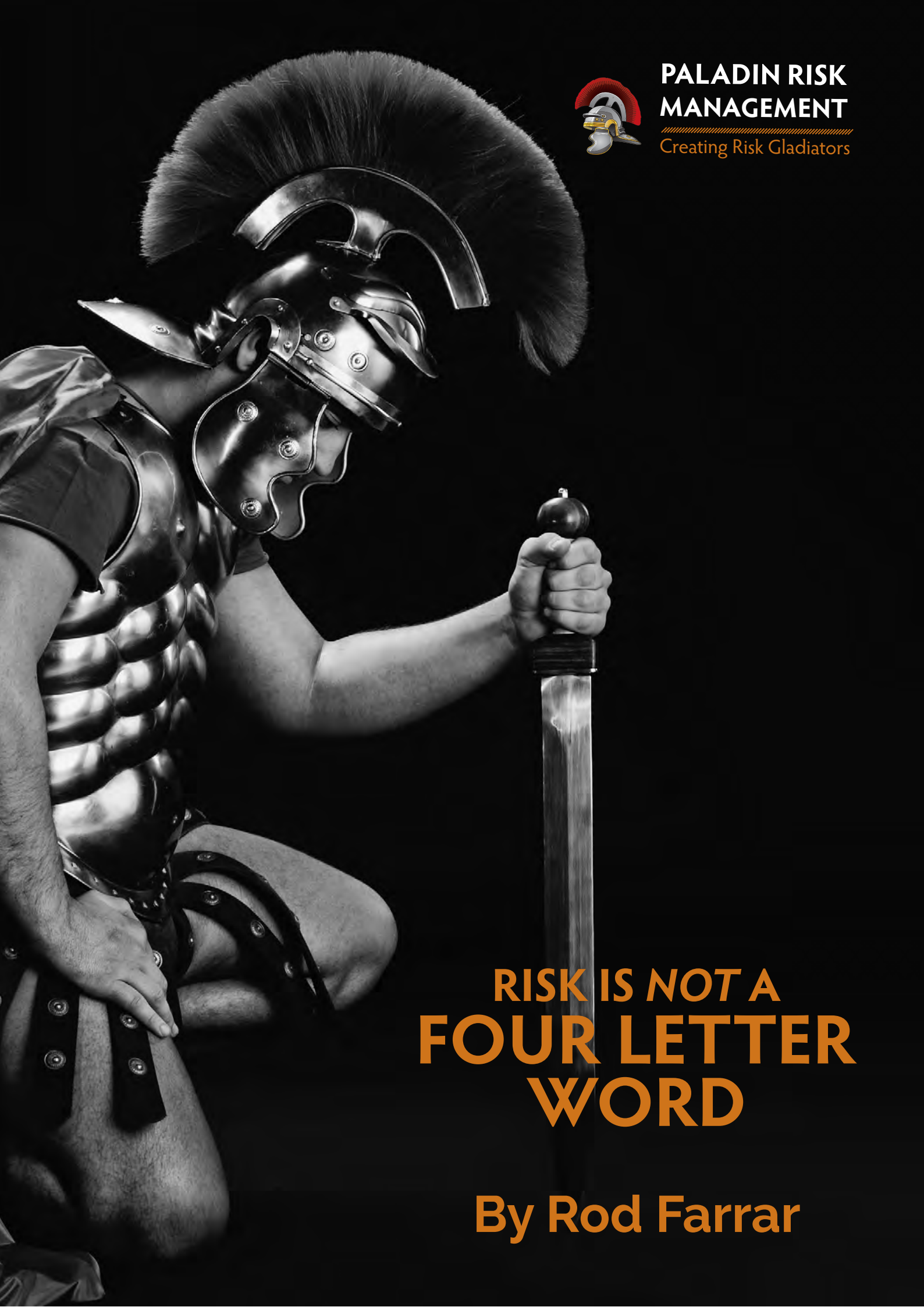


PALADIN RISK MANAGEMENT

Creating Risk Gladiators

RISK IS *NOT* A FOUR LETTER WORD

By Rod Farrar

Table of Contents

Welcome 3

CHAPTER 1: CONSEQUENCE IS KING 4

- Introduction to consequence 5
- Estimating Consequence 6
- Consequence based risk identification 9
- Consequence-based Internal Auditing 11
- Consequence-based Risk Reporting 13

CHAPTER 2: SOME THOUGHTS ON ISO 31000 16

- The Uncertainty Created by the Risk Management Definition 17
- The Likelihood Identity Crisis 19
- Describing a Risk 23
- Certification against ISO 31000 26

CHAPTER 3: MANAGING RISK IN OUTSOURCING 28

- The Risks of "Missing in Action" Contract Management 29
- Business Continuity in an Outsourced Environment 36

CHAPTER 4: RISKOLICE ALLSORTS 39

- Doing Risk Management or Managing Risk 40
- Downstream Risk – Is your Cure Worse than your Disease? 43
- Shared Risk 46

Welcome

Thank you for downloading my 2nd eBook – ***"Risk is not a Four Letter Word"***. Of course, risk is a four letter word, but not in the traditional vernacular of what constitutes a four letter word.

As I write this 2nd book, my 1st eBook – ***"Demystifying Risk Management"*** has been downloaded over 6,000 times in over half the countries of the World and has been reproduced in whole or in part by five international risk management organisations. The response has been overwhelming and somewhat humbling, and, as a result, I have squirreled myself away to produce this sequel.

Of course, these are my ideas and not all of you will agree with them but what I hope to achieve is to at least start a discussion in relation to risk management and the conventional wisdom around its application. The underlying message in this title is that risk is not something to be feared by organisations – but something to be embraced. If we do not embrace risk we cannot innovate. To quote John F Kennedy: *"There are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction"*.

In my role I see so many organisations "doing risk management" or, even worse, being seen to be "doing risk management" – rather than actually managing risk. In such cases, significant resources are being consumed for little or no improvement in the achievement of organisational objectives.

I truly hope you enjoy the eBook. If you would like to raise any points or vehemently disagree with anything I raise in the book, please do not hesitate to leave a post on my LinkedIn page or directly to me at rod@paladinrisk.com.au. Who knows, depending on the response to this book, it may indeed become a trilogy - ***50 Shades of Risk*** has a nice ring to it.

Rod

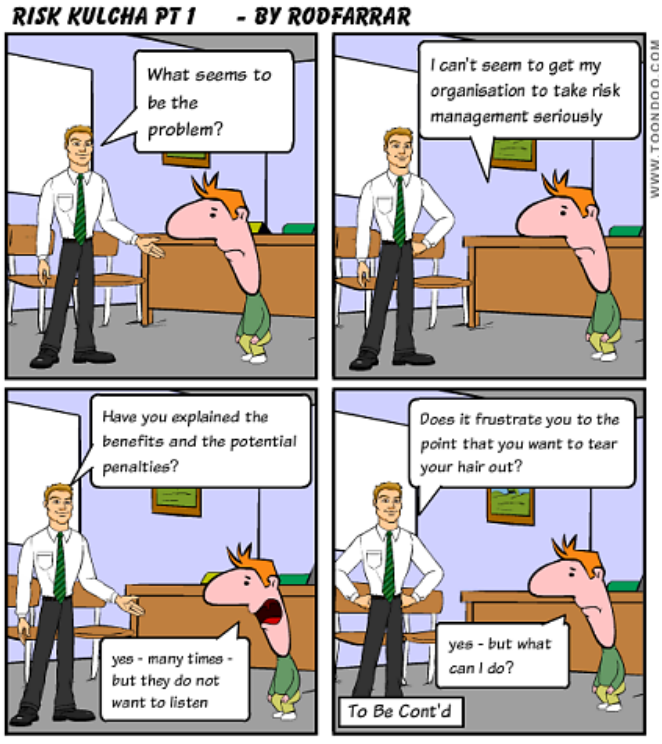

CONSEQUENCE
IS KING

INTRODUCTION TO CONSEQUENCE

In the risk management field we are taught that risk is a function of Likelihood and Consequence and that we need to identify both in order to determine the level of risk so we can make risk informed decisions.

In the truest sense of risk management, there is absolutely nothing wrong with that, however, I have been thinking long and hard in recent times about whether the focus on the level of risk (derived from both Likelihood and Consequence) is perhaps hindering our efforts in relation to using risk management as a tool to make those risk informed decisions.

This Chapter of the eBook explores a number of aspects relating to Consequence; how to determine consequence levels; how it can be used to assist in risk identification; how it may be used to drive our internal audit program; and how it may be used as the basis for risk reporting that can assist in the decision making process.



ESTIMATING CONSEQUENCE

One of the issues I have, and continue to encounter, is organisations who tend towards the worst case when assessing the consequence of the identified risk.

If you tend towards the worst case scenario with all of your assessments for consequence, what you may actually do is reduce the credibility of the risk management process and the risk management program within your organisation. If you do select the worst case scenario consequence for each of your identified risks, regardless of the likelihood, you are going to end up with a lot of risk in that top right hand corner of your matrix as shown below.

	CONSEQUENCE				
LIKELIHOOD	**INSIGNIFICANT**	**MINOR**	**MODERATE**	**MAJOR**	**MAJOR**
ALMOST CERTAIN	LOW	MEDIUM	HIGH	EXTREME	EXTREME
LIKELY	LOW	MEDIUM	HIGH	HIGH	EXTREME
POSSIBLE	LOW	MEDIUM	MEDIUM	HIGH	HIGH
UNLIKELY	LOW	LOW	MEDIUM	MEDIUM	HIGH
RARE	LOW	LOW	LOW	MEDIUM	MEDIUM

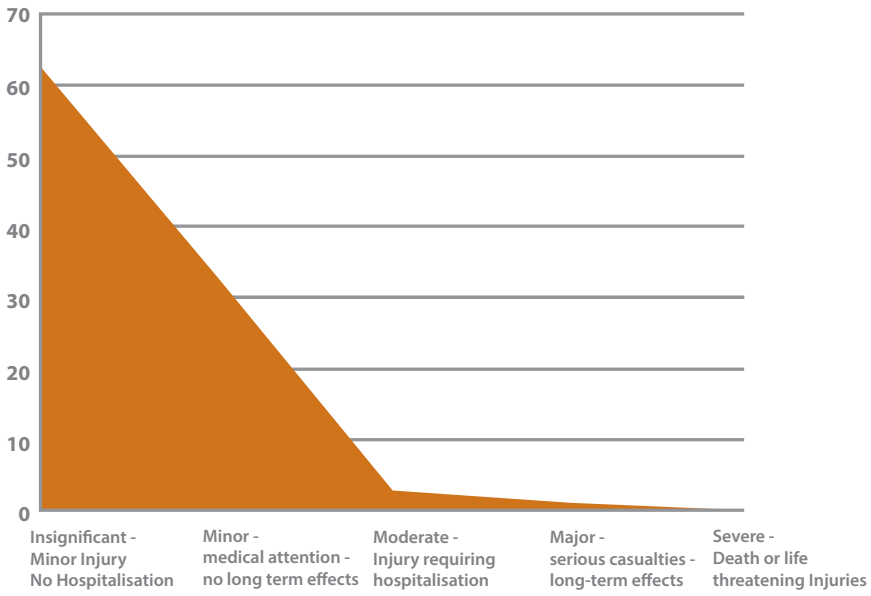
RISK BIT #1

There is no such thing as too many risks – we just need to make sure we identify and manage the right risks.

I believe that the way we should be assessing consequence is to determine the most **plausible** outcome against all of our impact areas.

To give you an illustration. If we had a hundred people that had a trip slip and fall in our workplace that resulted in an injury – about 90% of those are either going to have an insignificant consequence or a minor consequence (and many will have no injury at all). You might have one person break a wrist or something similar that requires hospitalisation. You might have one injury that is

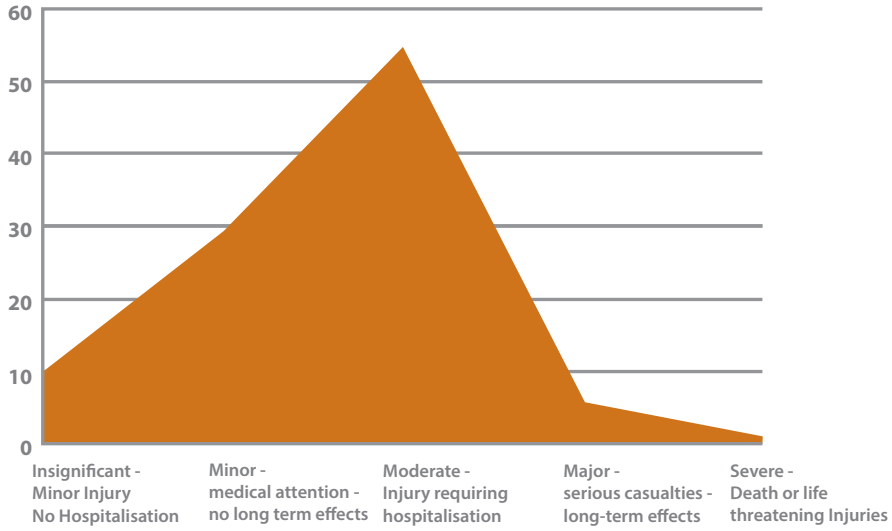
quite serious for which there will be long term effects. Out of that hundred, however, it is extremely unlikely that someone will die i.e. a severe consequence. The most **plausible** outcome here, however is somewhere in the insignificant/minor region as shown in the chart below:



In many organisations it is almost certain that we are going to have a trip slip or a fall over the next 12 months. If we were to take the worst case scenario and assess our consequence as severe (i.e. death) our risk would be rated as Extreme. In that case it is well above our target level of safety risk and one that requires urgent action. But what can you do? Short of laying pillows all over the floor or wrapping people in bubble wrap so they don't get hurt as they fall, it's not something you can really influence.

The way I determine consequence is to ask a simple question against each impact area I am assessing consequence against ….. if this event were to occur, what would be the most plausible consequence rating? What is the most plausible outcome from a reputation perspective - or from a compliance or regulatory perspective? Once we have done that, we have a much better understanding of the risk and whether it needs to be treated or not. If we tend towards the worst case on all of our consequences, we are going to treat a lot more risks than may be needed, which may consume unnecessary

resources and reduce the credibility of risk management in that organisation and probably render the framework unworkable. Another thing to consider here is the context in which the assessment of consequence is being made. If we use the same scenario of 100 people tripping, slipping or falling, however, this time it is in a nursing home, the chart would be somewhat different, because the context is different. The residents are older, may have existing conditions that make them more susceptible to injury .etc. In this case, when we assess the plausibility of the consequence the chart may look something like this:



So, the lesson out of this is, rather than determining the worst case consequence, ask; what is the most plausible consequence? If we do this for all of our risks, our assessed risk levels will be more credible and, the decisions based on these risk levels, more appropriate.

CONSEQUENCE BASED RISK IDENTIFICATION

Traditionally, when identifying risk we analyse an activity to determine what can go wrong then we assess the Likelihood and Consequence should that event occur. In doing so, we are likely to end up with a list of many risks – but are they the right risks?

One of the tools I have developed to assist organisations to determine their risks, particularly at the corporate level, is Consequence Based Risk Identification (CBRI). CBRI looks at risk identification from a completely different perspective, where we look at the Severe consequences in our organisational Consequence Matrix and ask ourselves: what would need to occur/what events would result in the organisation being subject to those consequences. This is a really effective way to identify those risks within the organisation that, if they were to materialise, would have the greatest impacts on the achievement of objectives.

To illustrate. Let's say that in our consequence matrix, the Severe consequence against Compliance is: *Would cause loss of licence to operate* – is rated as a Severe consequence. When conducting a risk workshop, we can then ask the question: what event or events would lead to us losing our licence? To determine that, we look to the Regulatory and Legislative framework within which we operate to identify what breaches (either singularly or cumulatively) would lead to a loss of licence and develop a risk statement related to that scenario.

I will give you another example. It's really interesting because people always talk about reputational damage. To me, (and I know there are differing schools of thought around this), reputation is a consequence. So, once again, at an Executive risk workshop we can look at the Severe Consequence against

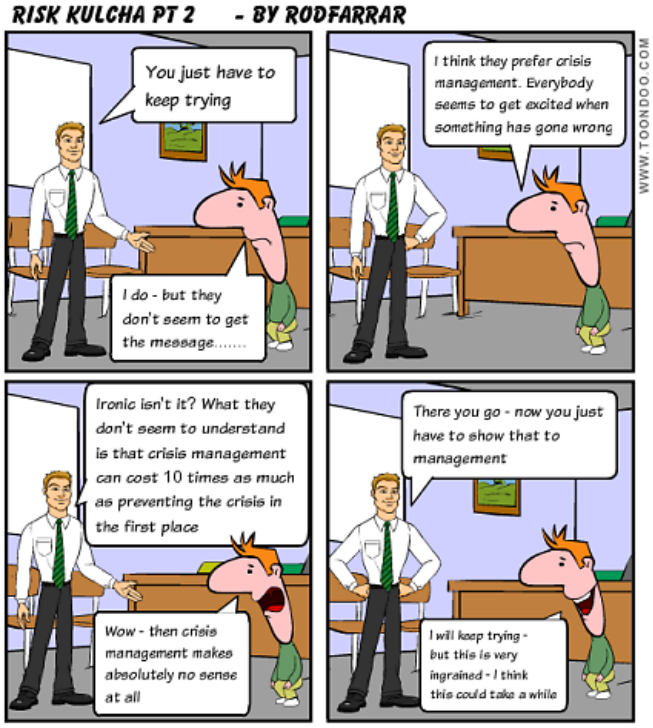
Reputation in the Consequence Matrix and ask the same question: what event/s may lead to us seeing those Reputation Consequences being realised.

Like any risk identification process, we cannot identify everything – there will always be unknown-unknowns. If you are able to identify a number of these Severe Consequence risks, however, we can ensure the controls that we have in place aimed at reducing the Likelihood of these event occurring are as effective as they can be.

Essentially, CBRI is just another tool in your tool box to help you identify risk. Try it and see what risks flow from it.

RISK BIT #2

Today's incident is yesterday's and tomorrow's risk.



CONSEQUENCE-BASED INTERNAL AUDITING

Okay – maybe I am about to open a can of worms here – but I think that Risk Based Internal Audit (RBIA) may be a misnomer.

Don't get me wrong, I am a firm believer in the internal audit program being aligned to the risk management program – in fact neither will be as effective if they are not intrinsically linked.

My argument here is not that it is not valid – but that the focus should be on Consequence Based Internal Auditing (CBIA) instead.

The Charted Institute of Internal Auditors defines RBIA as:

"a methodology that links internal auditing to an organisation's overall risk management framework. RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite".

This is all very true – particularly for those risks that don't fall within our target level of risk. But what about those risks that fall within our target – do we simply now accept that they have reached their target and become less vigilant?

My proposition is this ….. **regardless of the level of risk, internal controls linked to the risk events within the organisation that have the highest consequence must be the focus of the internal audit program**.

What is the purpose of an internal audit program? The internal audit program provides **assurance** that the controls that are currently in place are effective in order to reduce the likelihood that events will occur. Surely it follows then that the controls linked to the events with the highest level of consequence need to be the primary focus. Why? Well there

is a **direct correlation** between the effectiveness of the control environment and the Likelihood that the risk will be realised, so if these controls are not the focus then the chances of the risk eventuating becomes greater and nobody within the organisation may be aware that the event could be imminent!!!!

Is your organisation one where the primary focus of your internal audit program is around Cabcharge Cards or credit cards that have a limit of $2,000 on them or leave entitlements? I am not saying that these should not be done but they certainly should not be the **priority** for the program.

If we think about some major disasters such as the Longford Gas Explosion, the oil spill in the Gulf of Mexico, and many aircraft incidents the post event analysis that was conducted invariably shows that the breakdown of current internal controls was a **significant** contributory factor and that these controls were not being reviewed for effectiveness.

So what is the take home point of this section? Regardless of the overall risk level of the risks within your organisation, the primary focus of the internal audit program **must** be around those controls that are in place to keep the Likelihood of events with Severe or Major Consequences as low as possible.

RISK BIT #3

Organisations that don't manage their #risk will become very capable crisis managers because they will have lots of practice.

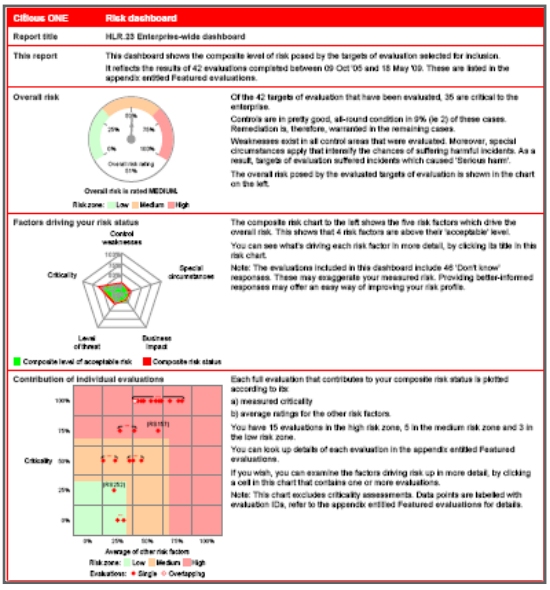
CONSEQUENCE-BASED RISK REPORTING

We have explored how we might use consequence to identify risk and then use it as the basis for our internal audit program. This section explores how we might use consequence as the basis for risk reporting.

One of the things I find most fascinating is the lengths that some software programs go in terms of ensuring that theirs is the most colourful report with as many dashboards, graphs, heatmaps and the like – but what are they actually telling us?

Reports such as this:

or this:



are used by management to assess the current status of the risks in the organisation – but are management asking the right questions when it comes to reporting? Simply receiving a report that lists the top risks to the organisation, or a graph that shows the categories of risk, or a heat map that shows us where the risks lie in the Risk Matrix are all well and good – but to what end? How do these graphs, in all honesty, assist management to make **Risk Informed Decisions**?

If I am a manager, what do I want to know?

First and foremost, I want to know which are the risks with the highest level of consequence to the organisation – **regardless** of Likelihood?

Secondly, I want to know that there are:

- Controls in place to reduce the Likelihood of these risks occurring; and (more importantly)
- **Assurance** that these controls are effective.

As I pointed out earlier, if we identify a risk with a significant consequence, we might assume that because we have controls in place (and we have assumed they are effective because nothing has happened in the past) that the Likelihood of the event is Unlikely, so the risk is assessed as Medium. It does not even get reported to management in the top level risks and it is unlikely to be included in the priorities for the Audit program as they are concentrating on the higher level risks.

RISK BIT #4

Risk management is not a barrier to innovation – it is an enabler.

Here is my question. If you are managing an organisation, do you want visibility and assurance around risks that have a higher Likelihood but Moderate Consequences or those with a lower Likelihood but with Severe Consequences? In my view, the estimate of Likelihood is just that – an

estimate - and even if we do have substantial amounts of data, past data is not an accurate indicator of future outcomes – otherwise the 1 in 100 year flood would happen on the same day every 100 years. Of the two, Likelihood is the most difficult (if not impossible) to estimate.

So my proposition is this: Identify those risks with the highest level consequence and provide regular reports in relation to the effectiveness of the controls surrounding those risks. That way you will not be blind-sided when the event does occur – all because you had assessed it as Unlikely or Rare.

I would much rather focus on those things that, if they happen can put teeth marks in my posterior – and, therefore, for me – Consequence will always be king.

SOME THOUGHTS ON ISO31000

(CONTROVERSY ALERT)

THE UNCERTAINTY CREATED BY THE RISK MANAGEMENT DEFINITION

Okay –this might be controversial – but as a risk management professional – I truly dislike the risk management definition.

There I said it!!!!!!!

I believe the ***effect of uncertainty of objectives*** has actually created uncertainty within the risk management fraternity since its release in 2009.

Let me take you back to the good old days of AS/NZS 4360:2004 which defined a risk as ***a chance of something happening that will have an impact on objectives***. This definition had it all – something happening (an event), a chance (Likelihood) and an impact (Consequence).

I am afraid, however, the current definition does not give us the same clarity.

Let's break it down: The **effect** of uncertainty on objectives.

Effect is defined as "a change which is a result or consequence of an action or other cause". In essence, an effect is an outcome or consequence. So if we substitute that into the definition: The **consequence** of uncertainty on objectives.

So what does this mean?

To my way of thinking the skewing of the definition towards being a consequence of uncertainty has taken away two of the most important aspects of risk management; the event itself and the Likelihood that event will actually occur…… but wait, there is more and this is where it gets really funky.

ISO Guide 73:2009 defines uncertainty as “state, even partial, of deficiency of information related to a future event, consequence or likelihood”.

So what do we have now?

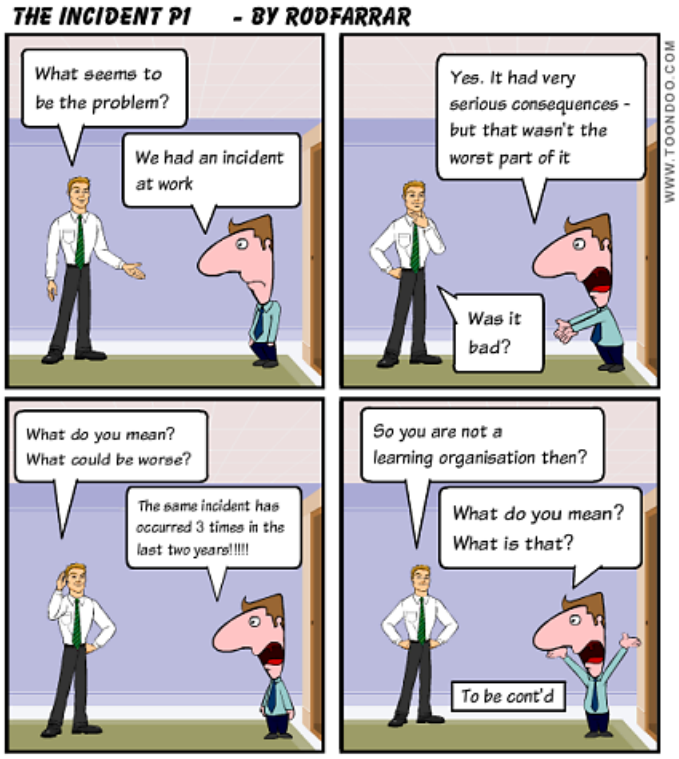
The ***consequence*** of a ***state of deficiency of information related to a future event, consequence or likelihood on objectives***.

I work in the risk management field and have done so for a number of years now and to be honest, I have absolutely no idea what this definition is trying to tell me. Even worse than that – I have no idea how I explain it to others and so I default to the previous definition because I know that it makes sense.

ISO 31000 is currently being reviewed. If any of the participants involved in that review happen to read this – please, please, please give us a definition we can work with – maybe the effect of uncertain events on objectives may be worth consideration.

RISK BIT #6

An absence of incident is not an indicator that a control is effective. The only way to know is to measure effectiveness.



THE LIKELIHOOD IDENTITY CRISIS

I am a simple man and, therefore, I like my definitions simple as well. From my earliest encounter with risk management, Likelihood was considered to be the Likelihood that the event being described would occur. We would then determine the Consequences should that event occur.

But then along came AS/NZS ISO 31000:2009 as well as Handbook SA/SNZ HB436:2013 (guidelines to AS/NZS ISO 31000:2009), which defined Likelihood in such a way that even Likelihood no longer knows what it is.

SA/SNZ HB436:2013 states:

*The level of risk is expressed as the **likelihood that particular consequences will be experienced**. Consequences relate directly to objectives and arise when something does or does not happen (i.e. there is an event or change in situation or circumstances that might occur at some point in the future). Therefore, the likelihood being referred to here is not just that of the event occurring, but also the overall likelihood of experiencing the consequences that flow from the event. (Page 8)*

I certainly agree with the notion that we need to assess the Likelihood of the event occurring in the first place, however, I do not believe that the statement that the level of risk is expressed as the likelihood that particular consequences will be experienced provides a true reflection on what a risk is and how we assess the risk level.

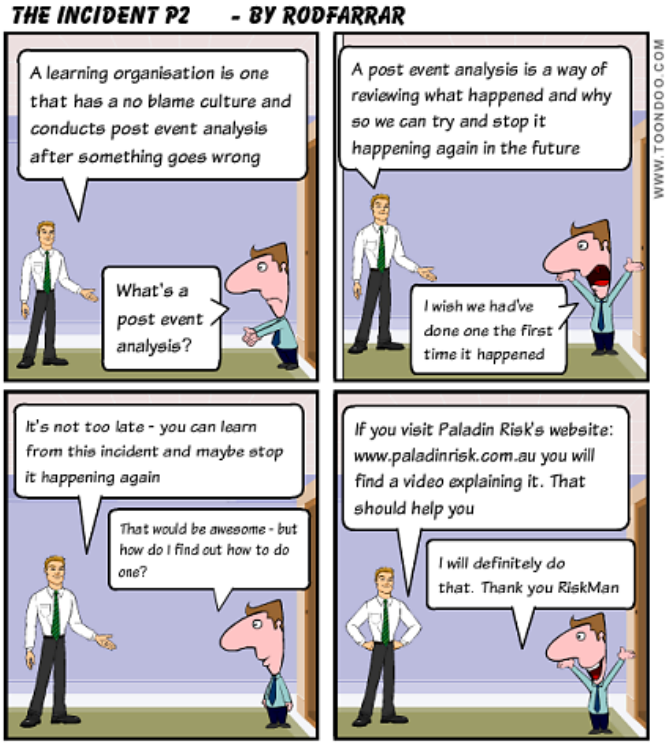
If we are to follow the guidelines outlined in the Standard, Risk Management becomes an absolute mess – why – because we have to assess our consequences against all of the impact areas, but rather than identifying the expected level of consequence against each impact area, we are now expected

to look at the likelihood that **each** of the consequences will arise.

Confused? Me too. So let's highlight an example to demonstrate.

The risk I am going to use is: *Food poisoning in a Kiosk at an aquatic centre*.

Using our assessment of our current controls we should be able to determine the Likelihood of the event occurring (i.e. the stronger/more effective the controls, the lesser the likelihood that the event will occur). We would then assess our consequence against all of our impact areas to determine a level of consequence. In this case we will simply use four impact areas: safety, compliance, revenue and reputation. In a traditional risk assessment we would identify which of these had the highest level of consequence and that would be entered into the table with the Likelihood to determine the risk score.



If we take the Standard literally then we end up with something like the following table for each risk:

EVENT	LIKELIHOOD OF EVENT	CONSEQUENCE CATEGORY	CONSEQUENCE LEVEL	LIKELIHOOD OF CONSEQUENCE
Food poisoning in a kiosk at an aquatic centre	Unlikely	SAFETY	SEVERE	RARE
			MAJOR	UNLIKELY
			MODERATE	UNLIKELY
			MINOR	POSSIBLE
			INSIGNIFICANT	LIKELY
		COMPLIANCE	SEVERE	RARE
			MAJOR	UNLIKELY
			MODERATE	UNLIKELY
			MINOR	LIKELY
			INSIGNIFICANT	POSSIBLE
		REVENUE	SEVERE	RARE
			MAJOR	UNLIKELY
			MODERATE	UNLIKELY
			MINOR	LIKELY
			INSIGNIFICANT	POSSIBLE
		REPUTATION	SEVERE	RARE
			MAJOR	UNLIKELY
			MODERATE	UNLIKELY
			MINOR	POSSIBLE
			INSIGNIFICANT	LIKELY

So my question is this …… how in goodness name do we determine a risk level for this risk?

As I outlined in Chapter 1, a more appropriate method for determining Consequence might be to highlight the most **plausible consequence** against each of the impact areas.

In the example above (and using a consequence table that I have), the most plausible consequence against each of the

Impact Areas would be:

- Safety – Minor;
- Compliance – Insignificant;
- Revenue – Minor; and
- Reputation – Insignificant.

Therefore, the highest level consequence is Minor. With a likelihood rating of Unlikely, in all probability the risk will be Low and will remain Low as long as the controls remain effective.

There are, of course, industries such as the insurance industry where this level of depth of analysis is appropriate, but what we need to recognise is that we are making a judgement (estimate) in terms of the Likelihood of the event occurring and then, a judgement (estimate) on the Likelihood of the Consequence. Data will assist accuracy, however, you just never know what is around the corner.

The more complex we make risk management, the fewer people within the organisation that will understand it and the less likely our risk framework will be effective.

RISK BIT #7

"What we learn from history is that we don't learn from history."

- Warren Buffett

DESCRIBING A RISK

Another area that I see many organisations struggle with is the manner in which a risk is described and captured in the risk register. In fact, I dedicated a full section in my 1st eBook to the subject. Once again, however, I believe that the Standard, and, in particular, the Handbook to the Standard have created confusion with respect to capturing risk information.

The Handbook to the Standard states that the risk description should also include the objective and the consequence against that objective. The example given is: *The margin on sales is reduced by more than 5% as a result of shoplifting*.

This description is making the assumption that there is shoplifting that is going on (so there is no real Likelihood of shoplifting here – it is 100% i.e. it is happening – so to me this is more of an issue statement). Margin on sales is **not** an objective – it is a measure of effectiveness. The reduction of 5% is expressing a **consequence** level and I would assume that it is being suggested that the Likelihood of that consequence is to be assessed.

So this poses a further question to me. Do we need to list more of these statements in the risk register to gain a better understanding of where the organisation sits in relation to this "risk"? i.e.:

- *The margin on sales is reduced by less than 2.5% as a result of shoplifting.*
- *The margin on sales is reduced by between 2.5% and 5% as a result of shoplifting.*
- *The margin on sales is reduced by between 5% and 7.5% as a result of shoplifting.*
- *The margin on sales is reduced by between 7.5% and 10%as a result of shoplifting.*
- *The margin on sales is reduced by more than 10% as a result of shoplifting*.

My next question is how is it treated? Are we treating the reduction in margin on sales or are we treating the shoplifting? What about the impact on other measures of effectiveness? We have only mentioned one here so do we need another risk that says: *Shareholder value is reduced by more than 5% as a result of shoplifting?*

And so it goes on.

I contend that it would be better, perhaps, to look at shoplifting as the event and then describe/capture the risk like so:

RISK NAME:	**SHOPLIFTING WITHIN STORE**
CAUSES	• lack of security presence • attractive items not stored securely • lack of electronic tagging • lack of/ineffective CCTV monitoring • lack of/ineffective screening of bags
CONSEQUENCES	• reduced margin on sales • reduction in shareholder value • additional costs for greater security • possible safety issues for security personnel who attempt to apprehend shoplifter
CURRENT CONTROLS AND EFFECTIVENESS	• security screening on entry and exit
	• CCTV cameras monitored constatnly during store opening times
	• all attractive items stored in cabinets
	• all attractive items contain electronic tagging
	• “Undercover” security personnel undertake regular patrols to identify suspicious behaviour

We then assess the effectiveness of the controls and determine the Likelihood and the most **plausible** Consequence of shoplifting based on the effectiveness of the controls. To my way of thinking, describing a risk in this manner allows a full assessment/analysis of not only the risk level but also the control environment, what would lead to it happening and the consequences if it did happen – without confining it to a single objective or consequence.

In my opinion: *The margin on sales is reduced by more than 5% as a result of shoplifting* is not actually a risk that can be treated as it is a **Consequence**. The risk we want to try and treat here is the risk of shoplifting.

The take home message from this section? Identify the event so that you can try and stop it happening. If you can't stop it (which would be the case for shoplifting in most businesses), we want to try and reduce the Consequences.

To quote a Meerkat appearing in commercials in Australia – *it's simples*.

RISK BIT #8

It is not practicable or practical to eliminate all hazards from a workplace otherwise nothing would get done at all.

CERTIFICATION AGAINST ISO 31000

I don't get it. Maybe I am reading a different Risk Management Standard to others – but I am at a complete loss to understand how there are organisations out there who are accrediting organisations and individuals to ISO 31000. Unlike Standards such as ISO 9001, ISO 31000 is not a prescriptive Standard but one that offers guidance.

If we consider the very first words of ISO 31000: *This International Standard provides* ***principles*** *and* ***generic*** *guidelines on risk management*. It then goes on to state:

RISK BIT #9

Risks without owners will never be managed.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

And here is the kicker ……..

This International Standard is not intended for the purpose of certification.

So how is it then, that there are organisations that are actively promoting that they will certify your organisation to ISO 31000 – or others where you can become a Certified ISO 31000 Risk Manager?

This to me is a blatant misrepresentation of the intent of the Standard and, worse still, may lead organisations to believe that because they are accredited or certified to ISO 31000 that

they are effectively managing risk when, indeed, all they have done is satisfy an organisation that itself may not understand risk management that it has a risk management program.

I explained in my previous eBook that to measure the effectiveness of risk management and the value it is adding to your organisation is a process which involves measuring compliance, maturity and the contribution risk management is having on the performance measures within the organisation.

You may have a piece of paper that says you are certified to ISO 31000 as an organisation or an individual, however, in my humble opinion (and based on the fact that the Standard itself states that it is not intended for the purpose of certification) there is only one use for such a piece of paper ……

CHAPTER SUMMARY

In summary, I continue to be somewhat baffled by the Standard (and now the Handbook) as I struggle to comprehend what they are trying to say.

Risk management is simple – what can go wrong? What would cause it to go wrong? What are the consequences if it does go wrong? What do we already have in place to stop it going wrong and how effective is it? What do I need to stop it going wrong?

The KISS Principle is one that resonates with risk management – because it needs to be understood by everyone in the organisation.

To me, the Standard and the Handbook have taken away that simplicity, created confusion and (in my opinion) made it less likely that organisations will take up the mantle and use risk management to create value to their organisation.

I truly hope the next iteration of the Standard will offer greater clarity.


MANAGING RISK
IN OUTSOURCING

THE RISKS OF "MISSING IN ACTION" CONTRACT MANAGEMENT

Many organisations use outsourcing for non-core functions. There is nothing wrong with that, in fact, for most organisations it is an efficient use of resources – provided you are getting the service you have paid for. In this section I want to discuss the risks arising from outsourcing, in particular the risks that arise from ineffective or non-existent contract management.

As we travel head long into our second budget under the Abbott Government, we continue to hear that Australia is experiencing a budget crisis - I watch on in despair as I witness (yes witness) money being unnecessarily wasted through, at best ineffective, in most cases, non-existent Contract Management. In the public sector, practices such as contractor self-assessment and supplier self-reporting have begun to gain prominence as resources in place to monitor and assure contract performance have been reduced. This significantly increases the risk of fraud and a reduction in service delivery.

Perhaps the lessons of the UK in 2013 might spur some similar action in Government organisations in this country.

RISK BIT #10

There is a direct correlation between the effectiveness of the control and the Likelihood and/or Consequence of a risk.

As reported in the February issue of the Prospect Magazine (UK):

Shortly before Christmas, Serco announced that it had agreed to return £68.5m (approximately AUD135m) to the taxpayer. An audit conducted by the Ministry of Justice (MoJ) - had uncovered ***systematic*** *overcharging on its contract for electronic monitoring of offenders.....As well as being forced to reach a settlement with the government, Serco was now the subject of an investigation by the Serious Fraud Office.*

It needs to be recognised here that the overcharging that was uncovered was for just one contract!!!!

The report by the MoJ released in December 2013 found significant shortcomings in contract management across a sample of contracts in the Department that I have observed first hand across Governments at all levels within Australia. Shortfalls in the following were observed across these contracts:

- Governance, process documentation, decision making and escalation;
- Definition of roles and responsibilities;
- Resource capability and capacity;
- Management information, reporting and contract data;
- Performance management, measurement and monitoring of service delivery; and
- Validation and assurance of supplier delivery and charges.

Let's cover each of these in terms of the findings and the implications for contract management in the Government sector in this country.

GOVERNANCE, PROCESS DOCUMENTATION, DECISION MAKING AND ESCALATION

The main elements relating to Contract Governance that need to be addressed are; the existence and following of contract management procedures; change management within the contract and the management of risk. These were found to be lacking in all of the MoJ contracts assessed in the report.

The report stated that:

- Contract management processes and procedures need to be readily available and actively implemented by the contract manager ensuring a consistent approach across the organisation.

- Processes need to be in place that clearly lay out the governance of contractual change with a focus on effective and prompt change implementation.
- Risks need to be formally identified and monitored regularly, with mitigating actions developed and implemented where possible, and 'obsolete' risks removed from consideration where appropriate. Escalation and reporting routes also need to be in place for effective risk governance.

Where these governance structures are not in place or are not followed, the management of contract changes and risk become problematic. What this means is that the contract, which is the very basis for the contract management relationship, may in itself be flawed.

DEFINITION OF ROLES AND RESPONSIBILITIES

Defined roles and responsibilities provide clarity of end-to-end management responsibilities, authority levels and interaction with other parties.

Where roles and responsibilities are not defined or understood, there are significant risks that the organisation's responsibilities in managing contract delivery may be missed.

The National Audit Office for the UK in their Good Practice Contract Management Framework highlights the need for:

- Contract managers to have accurate job descriptions, roles are positioned at an appropriate level and salary.
- Overall ownership of contract management across the organisation needs to be clear, with a 'contract management senior responsible owner' with responsibility for driving organisation-wide contract management performance. Contract managers have clear objectives and reporting lines and their performance is managed through reviews and appraisals.

My observation within a Government context is that Contract **Administration** is confused with Contract **Management**, resulting in a less than optimal approach to the management of the contract.

Let's explore the difference.

The table below shows the differing roles between Contract Administration and Contract Management:

CONTRACT ADMINISTRATION	CONTRACT MANAGEMENT
• Receive and pay invoices • Receive contractor reports • Process variations and changes to the contract • Maintain configuration of the contract (i.e. version control) • Organising contract meetings and distribution of documentation ***Contract Administration is essentially a post box function. There is no need for a relationship with the Contractor.***	• Relationship Management with the Contractor • Dispute resolution • Investigation and risk assessment of variations proposed by the Contractor • Proposal for variations initiated by the organisation • Assurance of performance against KPIs • Quality auditing • Escalation of issues to a higher authority • Contract reporting • Chair regular contract meetings ***The skills required by the person doing this function are significantly different from those of the administration function***

My observation is that many Government organisations have moved away from Contract Management in favour of Contract Administration and are simply believing the data that is provided by the Contractor and paying invoices accordingly. **Trust is not a contract assurance methodology.**

RESOURCE CAPABILITY AND CAPACITY

The report highlights that:

*Appropriate staff levels with the capacity and skills to manage work are **essential** for the success of any contract.*

Where resource is insufficient or lacks appropriate skills and experience, any aspect of contract management is at risk of being missed.

In my observation contract management is not a skill that is maintained effectively within many Government organisations. In fact, contract assurance positions have diminished over time in favour of a combination of Contract Administrators and blind faith in the fact that the performance data provided by the Contractor is accurate and that all deliverables have been provided. This did not work out well for the DoJ and I believe, without reservation, that similar audits on major contracts across Governments at all levels **would** find similar overcharging, and, in some cases, may uncover systematic contract fraud.

RISK BIT #12

A near miss can be considered as an event/ incident without consequence but we still need to learn from it and conduct a post event analysis.

MANAGEMENT INFORMATION, REPORTING AND CONTRACT DATA

We often hear the mantra - you can't manage what you can't measure. This is absolutely true of contract performance. High quality management information and underlying contract data is required to facilitate decision making, manage risk and give visibility of contract status and issues to management.

Where high quality management information is not readily available, there is a significant risk that management is unable to identify or address supplier performance issues or make decisions on end-to-end service delivery.

What does this mean? Well first and foremost, the contract needs measurable performance measures and key performance indicators. But these in and of themselves are of little benefit if they are not supported by the information management systems necessary to capture and record data.

It has been my experience that Government organisations do not maintain these systems to the level required and so verification of performance, once again, becomes problematic.

PERFORMANCE MANAGEMENT, MEASUREMENT AND MONITORING OF SERVICE DELIVERY

Appropriate measurement and monitoring of services delivered is one of the most important contract management activities to ensure requirements are met, management of risks and opportunities and to allow challenge and scrutiny of supplier charges. Where measuring and monitoring is ineffective, the organisation is exposed to risks that the intended end-to-end services are not being delivered, or the organisation is not carrying out essential activities for which it is responsible.

The MOJ Report found that:

- MOJ does not consistently measure end-to-end service delivery;
- KPIs are not always accurately reported and may not reflect actual service delivered or known service deficiencies;
- Examples exist where MOJ does not adequately define and monitor the KPIs to prevent interpretations by suppliers that adversely impact MOJ; and
- MOJ often relies on **supplier self-reporting of performance** and does not always validate services or assure supplier systems and processes.

This last point - contractor self-assessment is where I shake my head and lose all understanding. In our personal lives and dealings, we check the work by a contractor, and if we do not get what we paid for we make a complaint or seek recompense or withhold payment. So why is it so different for contracts where public monies are concerned?

Verification of services delivered against supplier charges is **the** most critical contract management responsibility in

managing an organisation's commercial risk. There are significant commercial and service management implications where verification of services and charges is not effective.

Contractor self-assessment does not and cannot work. Every organisation must assure itself that it is getting what it is paying for!!!!!!!

CONCLUSION

I believe the MoJ experience should be a wake-up call for all Government organisations in this country who manage contracts, particularly those related to service delivery. Why? The answer is simple - Government organisations and Contractors have different drivers. The organisation wants a service at a value for money price, whereas the company wants to maximise profits for their shareholders. Are we that naive that we believe that contractors won't take shortcuts when they can to reduce their costs for the provision of the service? If they do - how are we ever going to know unless we have a systematic contract assurance process tied to well defined, measurable KPIs for which data is available to verify performance claims?

For Serco, the overcharging was £62.5m for one contract. For those Government organisations within Australia that do not believe that systematic overcharging and overstating of performance is occurring - then have I got a bridge to sell to you. It is in Sydney - looks like a coat-hanger .....

BUSINESS CONTINUITY IN AN OUTSOURCED ENVIRONMENT

One of the issues I dealt with in my first eBook and one that I have observed for a long time now is the belief that some organisations have that by outsourcing they have transferred their risks to the contractor (the Risk Transfer Myth). Equally as troubling is the fact that by outsourcing, the organisation is no longer responsible for the business continuity of the function if it fails – that is the responsibility of the contractor.

Imagine my surprise/disbelief/horror when informed by a local Government representative that they had removed the risk relating to disruption to the removal of rubbish from the Risk Register as this was covered in the contract and was, therefore, no longer their risk!!!!!

Many organisations believe that because they have a business continuity clause in the contract all will be fines e.g. the Contractor is responsible for the uninterrupted provision of the service. That sounds all well and good in theory, however, in many cases the disruption will be caused due to issues arising with the Contractor. To use our rubbish removal example, there are a number of risks that come to mind:

- Industrial action by Contractor staff;
- Contractor forced into receivership; and/or
- Rubbish removal vehicles grounded by regulators.

Now we have a problem ……. **we** are responsible to the community for the collection of waste – but we no longer have the means to do it.

It is unacceptable to the community for the General Manager or CEO to stand in front of the cameras and say “this is a contractor issue” because the public doesn’t care who removes their rubbish – all they know is that they have paid the Council to provide the service and it is now not happening – and things are getting very smelly while you run around trying to rectify the situation.

If you have not planned and, more importantly, tested, for circumstances where contractor issues are the cause of the disruption, then you are likely to end up neck deep in something that doesn't smell particularly nice – literally.

You may recall in the last eBook I stated that if you own the consequence (or part of the consequence) **you own the risk**. It is similar with business continuity – **if you own the function you are responsible for the continuity of that function** – and this responsibility is not nullified if the function is outsourced.

In an outsourced function, the management of disruption related risk:

- Needs to be **owned** by the **contracting organisation**; and
- Is a **shared** risk.

What I mean by this type of risk being a shared risk is that it is one that must be managed by both parties. As an illustration, one of the strategies I have seen an organisation use in relation to this risk is to specify in the Contract that if there are issues with the Contractor, the Council can commandeer the vehicles and undertake the activity themselves. That sounds all well and good in theory, however, for this strategy to work: personnel within the Council who will undertake this role in those circumstances need to be identified; they need to be trained and have all of the appropriate licences; they need to know the routes and, ideally, have actually conducted the activity. If, for example, the Contractor staff do go on strike and the organisation has not prepared for that eventuality, can you imagine what would need to occur to commence removing rubbish in a manner that is safe to both Council staff and the community? It is not something that will happen within a day – or even a week.

So this is a shared risk – one that needs to involve both the Council and the Contractor in the detailed planning, training and testing of the plan.

Simply believing that a Contract clause will remove the responsibility of the organisation for the continued provision of the service is both naïve and potentially dangerous.

So the takeaway messages from this section are:

- Take a deep breath and accept that the continued provision of all functions within the organisation is the responsibility of the organisation – whether outsourced or not.
- For all of your outsourced functions, identify those events (including Contractor related issues) that could cause disruption to the ongoing provision of the service. Move away from saying – *this will never happen* and instead ask *what happens if*?
- For disruption risks that are Contractor related, involve the Contractor in the planning for the restoration of the service in the event that the disruption is caused by the Contractor.
- Conduct regular joint training and testing activities.
- If required, include appropriate contract clauses that identify the requirements of the Contractor, whether it be in planning, training, testing or execution of the business continuity plan as these need to be costed into the Contract.

If you adopt these processes, particularly around outsourced functions, you will be better prepared when things don't go your way (which will invariably happen).


RISKORICE
ALLSORTS

DOING RISK MANAGEMENT OR MANAGING RISK

You have probably heard it – in fact, you yourself may have said it "Our organisation does risk management" - but my question is – are you actually managing risk?

The reality is that there is a significant difference between doing risk management and managing risk. In my observation, an organisation that is doing risk management is doing what it needs to do to be compliant, whether that is with a regulation or whether that is with legislation or whether that is with policy.

At a Federal Government level in Australia we now have the Public Governance Performance and Accountabilities Act (PGPA) and the Commonwealth Risk Management Policy. My concern with the PGPA and the Policy is that agencies are now going to as much as they need to do to be compliant with the legislation as both are based on outputs rather than outcomes. Here's the thing – you can be compliant with the requirements of the Act and the Policy without risk management making any meaningful contribution to the achievement/improvement of operational outcomes.

RISK BIT #13

Organisations need to stop saying "this will never happen" and start asking – what happens if?

So what is the difference between doing risk management and managing risk? The table on the following page shows some of the differences between each (you may even want to do a quick analysis on where your organisation sits:

DOING RISK MANAGEMENT	MANAGING RISK
The organisation has documentation (e.g. Policy, Plan, Procedure) that it considers to be a framework.	The documentation is simply part of the wider framework (see previous eBook for an explanation of the elements of a Framework).
Risks are considered after planning has been completed as opposed to being a fundamental part of it.	Risk management is a fundamental part of the planning process, where goals, objectives, opportunities may be altered based on the risks of moving forward.
The organisation has a Risk Register/s that are reviewed once every 3, 6 or 12 months.	Reviews of risk registers occurs, but the risks in them are continually **monitored**.
Current control effectiveness is estimated but not measured	Current controls are measured for effectiveness.
Treatments are identified, but rarely undertaken.	All risk treatments are completed within specified timeframes.
Ownership is not assigned to risks or treatments or ownership is assigned to 'all' or 'XYZ Committee'.	All risks, controls and treatments have assigned owners.
The organisation seeks to assign individual responsibility after an incident has occurred and doesn't undertake post-event analysis to identify the root causes .i.e. a blame culture exists.	The organisation understand that every incident/event is a system failure and not the responsibility of one individual. Post event analysis is conducted so the organisation can continue to learn and grow.
Risk management is seen as a specialist skill that only certain personnel within the organisation are responsible for. Training is only provided to those in risk management roles.	All personnel understand that they have a role to play in the management of risk across the organisation and training has been provided accordingly.
Staff feel too intimidated to raise issues/risks for fear of reprisals.	Staff feel empowered to raise issues/ risks so that management have all of the information required to make risk informed decisions.
Risk reports are full of colour and charts but insufficient information to make risk informed decisions	Risk reports contain information that assists in the decision making process.

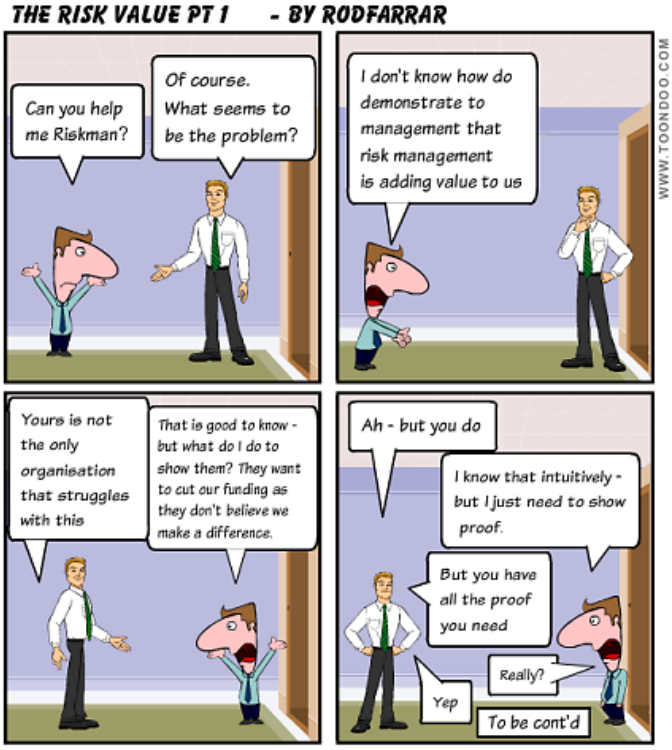
The organisation seeks to assign individual responsibility after an incident has occurred and doesn't undertake post-event analysis to identify the root causes .i.e. a blame culture exists. The organisation understand that every incident/event is a system failure and not the responsibility of one individual. Post event analysis is conducted so the organisation can continue to learn and grow.

You can only begin to imagine the difference in culture between these two types of organisation.

Those organisations that are managing risk as opposed to doing risk management, will find an improvement in performance, less crisis management, improved reputation within their stakeholder community including regulators and shareholders, and the attitudes of staff will be vastly different in relation to the raising of issues and risks.

The reality is that the transition from doing risk management to managing risk is not insurmountable in terms of resources, however the results are worlds apart.

You do risk management if you want to be compliant – you manage risk if you want to be successful!!!!!



DOWNSTREAM RISK – IS YOUR CURE WORSE THAN YOUR DISEASE?

An area of risk management that may not get as much attention as it possibly should is that of downstream risk.

Downstream risk is defined as the additional risk/s that arise from the implementation of an existing risk.

What we need to understand is that every treatment will create new risks, however, when the consequences of these downstream risks are greater than the consequences of the original risk then we could be confronted with a major issue.

To illustrate, let's use the example of the Wesley Hospital in Brisbane that suffered an outbreak of Legionnaires disease in 2013. In this case, the safety team identified that there is a risk to patients of being burned by hot water from a tap or in a shower. In fact, as the Health Minister of Queensland stated: *"Recently, Workplace Health and Safety considerations have required authorities across the world to lower the temperature in hot water systems to protect people from unintended scolds"*. Without a doubt scolding is possible, if not likely, however, the most **plausible** outcome (see previous discussion on estimating consequence) is, at worst, a first degree burn to someone's hand (bearing in mind we are talking about a normal tap here – not a hot water urn where the water is boiling).

So what are our options? We can accept the risk and understand that people have taps and showers in their homes and that it is unlikely that the hospital is their first encounter with hot water or, we can decide that this risk is not acceptable and treat it. Let's say we are very risk averse and choose option 2 – what can we do to lower the temperature in hot water systems?

The first option is to install tempering valves. A tempering valve mixes your hot and cold water to deliver hot tap water at a constant temperature. Tempering valves have a temperature sensitive element which adjusts the mix depending on the temperature of the incoming water flowing through the valve. The mechanism is a sliding valve that varies the ratio of hot and cold water that is allowed to pass. The valve is designed to maintain a constant outlet temperature, reducing the risk of accidental scalding. This is expensive, but very effective in reducing the risk of scalding.

The second option is to turn down the temperature of the stored hot water to 50oC. Sounds simple enough, however, to protect against the growth of Legionella bacteria, the cause of Legionnaires' disease, it is a **legal** requirement that any stored hot water be kept at a minimum temperature of 60°C. This requirement is as per Australian Standard AS3500 and applies to all hot water systems with tanks, including solar and heat pumps.

If we were to conduct a thorough assessment on the treatment options then option 1 is the only course of action that satisfies the workplace health and safety requirement to lower the temperature in hot water systems whilst at the same time remaining within the requirements of the Australian Standard (and the law).

Option 2, however, was the treatment that was chosen.
The result:

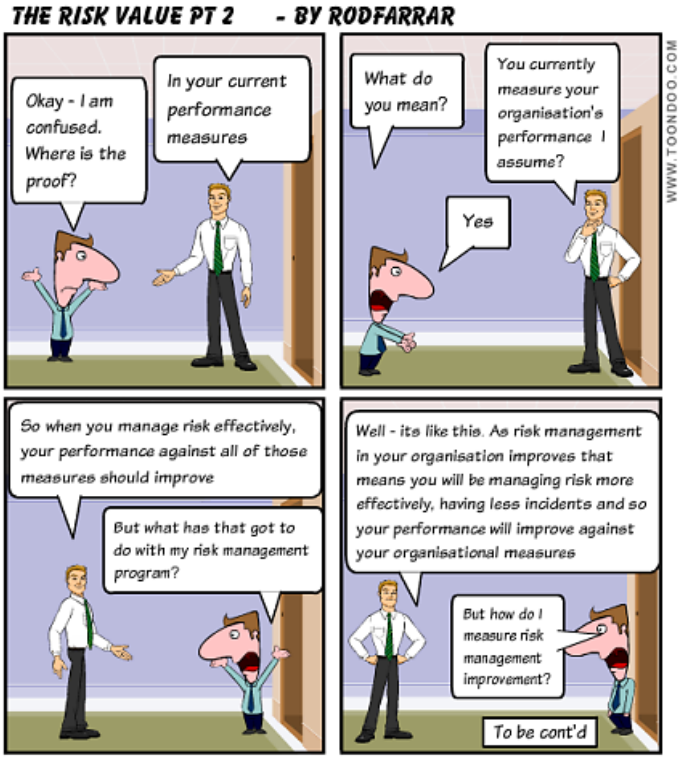
- A 60 year old man died from Legionnaires disease;
- Another person was stricken with the disease and needed to be treated in Intensive Care;
- A number of patients were transferred to other hospitals;
- Patients in the hospital were unable to shower for about a week;
- Admissions and elective surgery were refused until test results confirmed that there was no risk to patients;
- Over 1000 former patients had to be contacted and then tested;

- 2000 staff were potentially exposed to the bacteria;
- The hospital's hot water systems had to be flushed which involved turning up the water pressure and the temperature to 65oC, with the showers and taps run for 10 minutes – which had to be performed more than 500 times across the entire hospital;
- Significant time and resources in the investigation of the outbreak;
- Though not reported, it is likely that legal action would have been taken by those affected;
- The reputation of the hospital suffered significant damage as the outbreak was in the news for well over a month.

These consequences were **far worse** that the consequences of the original identified risk.

The lesson from this case study: when developing a treatment plan for an identified risk, ask yourself "if we implement this treatment, does it give rise to any further risks?" But don't just ask this question while sitting in a conference room conducting the risk assessment – **thoroughly** research the implications of the treatment.

In my opinion, had that research been conducted at the Wesley Hospital, this outbreak would not have occurred.



SHARED RISK

Element 7 of the *Commonwealth Risk Management Policy* states that: *each entity must implement arrangements to understand and contribute to the management of shared risks. It goes onto to define shared risks as: those risks extending beyond a single entity which require shared oversight and management. Accountability and responsibility for the management of shared risks must include any risks that extend across entities and may involve other sectors, community, industry or other jurisdictions*.

On the surface, it may appear simple, however, there are some significant challenges in managing shared risks.

The first challenge is to identify who owns the risk. The simple fact is that risks without owners will never be managed and even if an organisation has identified the shared risks, there may not be a willingness to take on responsibility or accountability for their management.

The second challenge is how do we measure control effectiveness when there are multiple entities involved and there is no appetite for sharing of information, let alone, assessing the effectiveness of another organisation's controls?

So let's look at an example.

The risk is 'An outbreak of foot and mouth disease within Australia'.

For this risk, the stakeholder community is significant, each of which manage certain preventative and/or detective controls aimed at stopping the disease from entering the country and corrective controls aimed at stopping its spread if it does enter. Obviously, the consequences to the country of such a risk eventuating would be absolutely devastating economically, from a reputation perspective and would leave the Government exposed to legal action if it was discovered that controls had failed.

The organisations that have a role to play in the management of this risk include (but are not limited to):

- Department of Agriculture, Fisheries and Forests (DAFF);
- Customs;
- Quarantine (AQIS);
- Airlines;
- Australia Post;
- Landowners;
- .etc.

Here are some questions to consider in relation to this risk:

- Which of these Agencies actually owns the risk?
- Do each of the Agencies understand the contribution their controls have to reducing the level of this risk?
- Who is making an assessment of the effectiveness of these controls in relation to the minimisation of the risk?
- Do these Agencies understand that when they make decisions relating to these controls that any reduction in funding (which may be due to Government cutbacks) may increase the Likelihood of the event occurring?
- Who is making the assessment of the impact of any policy decisions on the risk?

And the list goes on.

Of course, not all shared risks are going to have the same span in terms of the number of organisations involved. In this day and age, however, there will be a significant number of risks within an organisation that cross functional boundaries as a minimum and in some cases, will cross organisational boundaries.

So, how do we manage these risks?

For risks with significant consequences if the event occurs, I would suggest the following strategies:

- Ownership of the risk should sit with the organisation/

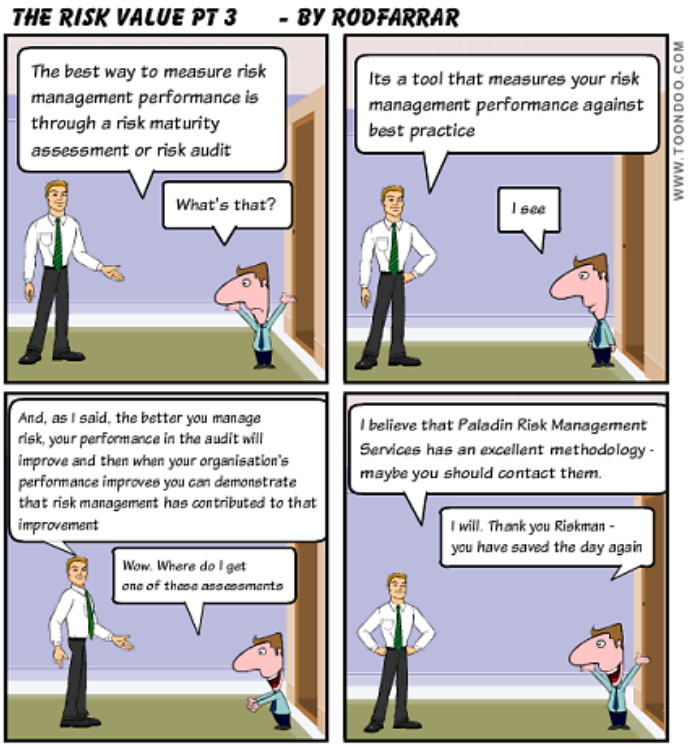
functional area subject to the highest level of consequence should the event occur.

- Form a stakeholder management group for the risk (with the risk owner being the Chair) and hold regular meetings as part of the monitor and review process (the higher the consequence, perhaps the more frequent the meetings).
- Ensure each functional area/organisation understand the controls they are responsible for and provide assurance at each meeting of the effectiveness of the controls so that a true assessment can be made on the level of that risk.

Without making a conscious effort to manage shared risks in this manner there will be a lot of assumption in terms of who is managing what controls; how effective these controls are; and who is reporting.

Assumption does not equal assurance and in shared risks where the consequences could be felt by multiple functional areas or organisations the prevalence of assumption is likely to be greater.

If the consequences are shared – so too should be the management of the risk.



ABOUT PALADIN

PALADIN RISK MANAGEMENT

Paladin Risk Management Services is the brainchild of Rod Farrar, who founded the company in 2007 as a result of his passion and skill for managing risk. Rod's extensive experience in assisting organisations to mitigate and eliminate professional risks they may encounter is at the core of Paladin Risk Management Services.The core service offering is risk management training workshops.

The Risk Management Diploma is a broad based program aimed at risk management and business continuity professionals or those aspiring to fill roles in these industries. After the four day course, attendants have six months to complete the assessment activities, at which point they will be awarded the Diploma.

The Paladin Risk Management Academy Advanced Diploma of Governance Risk and Compliance is fully accredited by the Australian Skills Quality Authority (ASQA). The four day course is the only offering in Australia which covers governance, risk, compliance and business resilience.

For those that cannot attend the courses in person, or want to learn at their own pace, Paladin Risk Management Services offers a Diploma of Risk Management and Business Continuity via distance education. This comprehensive course enables you to become accredited through the provision of education materials including an education kit and an accompanying chapterised DVD.

Since its foundation, Paladin Risk Management Services has provided a wide range of risk management services to a growing list of diverse clients, such as the Department of Defence, the Australian Federal Police, Reed Construction, Mont Adventure Equipment, contentgroup, National Health Call Centre Network, Victorian SES and Retirement Benefits Fund just to name a few.

Paladin Risk Management Services was selected as an ACT Finalist in the 2014 Telstra Business Awards.

With the understanding that no two organisations are alike, Paladin Risk Management Services has a range of flexible training, courses and consultancy options that can be specifically tailored to meet your organisation's needs.

ABOUT ROD

ROD FARRAR

Rod Farrar is an accomplished risk consultant with extensive experience in the delivery of professional consultancy services to Government, corporate and not-for-profit sectors.

Rod's knowledge of the risk management domain was initially informed through two decades as an Army Officer in varying Project, Security and Operational roles. Subsequent to that, Rod has spent nine years as a professional risk manager.

His risk management expertise is highly sought after, as is the insight he provides in his risk management training and workshop facilitation. Rod has been recognised by the Risk Management Institute of Australia, which has granted him Certified Practicing Risk Manager accreditation.

With an extensive list of qualifications, Rod has lectured at the University of Canberra, has been on the assessment panel for Certified Practicing Risk Managers as well as speaking at a range of conferences and forums. Rod's Diploma and Advanced Diploma have been attended by participants from all over Australia, as well as New Zealand, New Guinea, Solomon Islands, Indonesia, Bhutan and Ghana. The feedback from the course has been overwhelmingly positive.

Rod's passion for risk management is evident throughout all of his work. His ultimate goal is to help people become 'Risk Gladiators', by transferring the skills and knowledge of risk management so that every organisation is armed to mitigate and eliminate any risks they encounter.