Risk Management White Paper

Managing Risks in Councils

Table of Contents

Introduction

1. Over the past seven years, Paladin Risk Management Services has taught in excess of 100 people for Councils across Australia. In addition, the company has been engaged by a number of individual Councils to provide a variety of risk management services.

2. What has become apparent in undertaking this work is that almost all Councils struggle with the management of risk. Don't get me wrong, the majority of Councils have risk management policies, risk management plans and risk registers – after all, that is a requirement under the various Local Government Acts. What I am referring to is the difference between '***doing risk management***' and ***managing risk*** – the latter of those being the one where the struggle occurs.

3. In my career I have reviewed at least 50 risk registers from Councils and the one thing that has struck me is how different they are, not only in format, but, more importantly, in content. The key issues I have observed are as follows:

   a. Strategic and operational risks captured in the one register;

   b. Multiple risk registers across Council (often with exactly the same risks captured but with different owners);

   c. Ownership vested to inappropriate levels of Council;

   d. The determination of likelihood based on time frequency and probability; and

   e. **The *wrong* risks in the risk register**.

4. Given the significant similarities in the activities undertaken by Councils, risk registers should also reflect this – but this is not the case.

5. This White Paper will provide some insight to Councils of these issues and provide some advice in how they might be addressed.

Strategic and Operational Risks

Identifying Strategic Risks

6. I have now worked with multiple Councils across Australia and when reviewing their strategic risk registers, almost universally, what is contained within are neither strategic nor are they risks. Many Councils have been significantly impacted by China's decision to stop importing recycling waste and most, if not all, have struggled to cope in the aftermath of the decision. **This was a foreseeable strategic risk**.

7. So, what is the difference between a strategic and an operational risk?

> ***Strategic Risks***. *Risks **external** to Council that, if they were to eventuate, may require a **change in strategic direction**. Essentially, these risks are the Threats identified in the Council SWOT Analysis.*
>
> ***Operational Risks***. *Risks external or internal to Council that impact on the achievement of the **current** strategy.*

8. Given these definitions, the sources of strategic risk that I use when conducting a strategic risk workshop for Councils are:

a. Regulatory environment;

b. Political environment;

c. Technological environment;

d. Natural environment

e. Economic environment; and

f. Social environment.

9. I then ask: "which piece/s of legislation and/or regulation that, if they changed, could have a significantly negative impact on the organisation? Then I ask: what technology is likely to emerge in the future that we may need to adopt or adapt to? And so on.

10. A good cross section of strategic risks from the Councils I have advised are shown below:

a. Reduction in external government funding
b. Externally imposed organisational changes (including amalgamation)
c. Increased number and/or severity of major disaster events
d. Changes in demographics across the local government area
e. Changes to state government land use planning requirements
f. Increase in state government levies/charges collected by council
g. Technology advances more rapidly than council is able to adapt
h. Changes to regulations and legislation that impact Council operations
i. Rate capping imposed/extended by Government
j. Cost shedding/transfer by state/federal government

11. What should be evident from this list is the fact that these same strategic risks will apply to the majority, if not **all** Councils.

Assessing Strategic Risk

General

12. It is my belief that, based on the difference between the strategic and operational risk, we also need a different approach to the analysis of the risks.

13. Following a bit of trial and error, I have developed a separate set of criteria for strategic risks, as described below.

Likelihood Criteria

14. The level of control surrounding strategic risks is extremely limited (if there is any at all), so the likelihood needs to be based on the level of visibility/discussion of the issue in the public domain and/or the government policy considerations. To that end, the following is an example of the spectrum of likelihood criteria for strategic risks within a university:

Rating	Descriptor
Likely	• Currently the issue is being discussed on an almost daily basis in the mainstream media (national and/or international); *and/or* • Currently it is a policy issue that is being discussed by one or both sides of Federal politics and has become an **election issue**; *and/or* • One major review is currently in progress (national or international); *and/or* • External environmental scans undertaken by the university are showing significant evidence of the emergence of the issue.
Possible	• Currently the issue is being discussed in the mainstream media (national or international), but not on a regular basis; *and/or* • May be some fringe media or policy advocacy groups discussing the issue, and their influence is significant; *and/or* • Currently it is a policy issue that is being discussed by either or both sides of Federal politics, however, it has yet to be announced as a policy; *and/or* • Multiple smaller reviews are currently in progress (national or international); *and/or* • External environmental scans undertaken by the university are showing some changes to the current environment that warrant closer observation or some preliminary planning.
Unlikely	• Currently it is not being discussed as an issue in the mainstream media national or international; *and/or* • May be some fringe media or policy advocacy groups discussing the issue, but their influence is low; *and/or* • Currently it is not a policy issue that is being discussed by either side of Federal politics; *and/or* • No reviews are currently in progress (national or international); *and/or* • External environmental scans undertaken by the university are showing no changes to the current environment.

15. As an illustration:

a. Currently the issue of amalgamation has not been raised for some considerable time in many States and Territories. The current likelihood could, therefore, be assessed as **Unlikely**.

b. Let's move forward two years and the State government of the time commissions a report to fully investigate the current structure of local Government across the state, including in the terms of reference possible recommendations for amalgamation. On the basis of this report, and the fact that the media is reporting it, the likelihood has increased to **Possible**.

c. The report is delivered to the Government and it recommends some amalgamations. There will, obviously, be some further consultation with the impacted Councils to determine potential impacts, however, at this stage, the likelihood would need to change to **Likely**.

16. The majority of strategic risks will emerge over a period of time, which should provide the opportunity for Councils to put strategies in place. China's decision to stop importing recycling waste, despite being a foreseeable risk, and one that, if managed appropriately, may have resulted in a reduction in the consequences to the Australian recycling market, took all Councils by surprise.

Consequence Criteria

17. The consequence level for each strategic risk needs to be assessed on the level of change/disruption that arises as a result.

18. To that end, the following is an example matrix that may be applicable in a Council context:

Rating	Descriptor
Significant	• Complete change to strategic plan for the Council – full reissue; *and/or* • May involve consideration of significant restructuring of Council; and/or • May result in a significant reduction of staff levels; *and/or* • May result in several discretionary services (more than 5) not being offered by the Council.
Moderate	• Amendments to the current strategic plan for the Council but not reissue; *and/or* • May involve consideration of some restructuring of Council; and/or • May result in a moderate reduction of staff levels; *and/or* • May result in some discretionary services (less than 5) not being offered by the University.
Minor	• No amendment to the strategic plan but adjustment to extent and/or timing of current strategies; *and/or* • No restructuring required; and/or • May result in a minor reduction of staff levels; *and/or* • No impact on discretionary services being offered currently but may impact introduction of new services or expansion of current services.

Risk Matrix

19. As we have three consequence ratings and three likelihood ratings, we obviously require a 3 x 3 risk matrix. The following is the risk matrix used to determine the level of strategic risk for a Council:

	Minor	Moderate	Significant
Likely	**Medium**	**High**	**Extreme**
Possible	**Low**	**Medium**	**High**
Unlikely	**Low**	**Low**	**Medium**

20. The risk level, therefore, for our identified risk is **Medium** then **High** and then **Extreme**. There will be different actions that need to occur as the risk level rises, as shown in the table in the next section.

Actions to be taken

21. The table below identifies the actions required for each of the squares in the risk matrix:

	Minor	Moderate	Significant
Likely	No action required	Development of preliminary strategic impact document with scenario analysis and modelling	• Immediate emergency meeting of Council • CEO/deputy Mayor to enact planning conducted previously • Change management/ transition plan enacted • Communications strategy for all stakeholders to be enacted
Possible	No action required	Development of preliminary strategic impact document with scenario analysis and modelling	• CEO/Deputy Mayor to establish planning 'tiger team' to identify implications of the change • Tiger team to develop alternate strategies • Tiger team to develop change management/ transition plan to be enacted if risk is realised • Communications strategy for all stakeholders to be developed
Unlikely	No action required	No action required	• Development of preliminary strategic impact document with scenario analysis and modelling

22. As can be seen, the linking of the actions to the risk level allows for forward, proactive planning, rather than reactive planning if the risk does materialise.

Summary

23. The simple fact is that strategic and operational risks are different, and, therefore, it follows that they must be analysed in a different manner.

24. Recently, in the risk management frameworks developed for organisations, I have included criteria for the management of strategic risk and the management of operational risks.

Managing Strategic Risk

25. The management of strategic risk is problematic in that in all but the rarest of cases it is not possible to reduce the **likelihood** of the risk other than perhaps through lobbying.

26. To that end, the management of strategic risk is more focussed on “what happens if” and developing strategies to be prepared if the risk eventuates.

27. When managing these risks, Councils should be identifying two levels of strategy.

a. Strategies we can implement **now** that could reduce the consequence if the risk eventuates; and

b. Reactive strategies to be implemented if the risk materialises.

28. Of course, developing strategies that may protect us from these potential risks is much more prudent than reacting when it happens. These need to be planned sometimes years in advance.

29. Waiting for it to happen and then dealing with it is not a plan for the management of strategic risk.

Multiple Risk Registers

General

30. If you are like most organisations that I have engaged with, you will most likely have multiple risk registers. Separate risk registers will likely be maintained for two or more of the following categories of risks:

a. Operational risks

b. Financial risks

c. Security risks

d. Safety risks

e. Compliance risks

f. Reputational risks

g. Environmental risks

h. IT risks

31. Whole industries have been built around the management of risk by category. In my previous blog I highlighted that cyber-attack was not the risk – it was just a cause – and yet billions of dollars have been spent on "cyber risk". Billions of dollars are spent on safety risks and security risks and the like, but here in lies the controversy in this blog:

> ***There is no such thing as a safety risk, or a security risk, or a reputation risk – they are just risks***

32. Here's the thing, a risk is a risk – there are just multiple consequences every time a risk materialises.

Where are we now?

33. As previously stated, organisations, for the most part, maintain multiple risk registers. How have we ended up here?

a. 'Patch protection';

b. Organisations not structured to manage risk holistically; and

c. Belief that all risk types are different.

34. In my observation, this has led to:

a. Risks that are not actually being managed;

b. Significant duplication;

c. Significant control 'gaps'; and

d. Additional controls being introduced in one area that increase risk/s in another area.

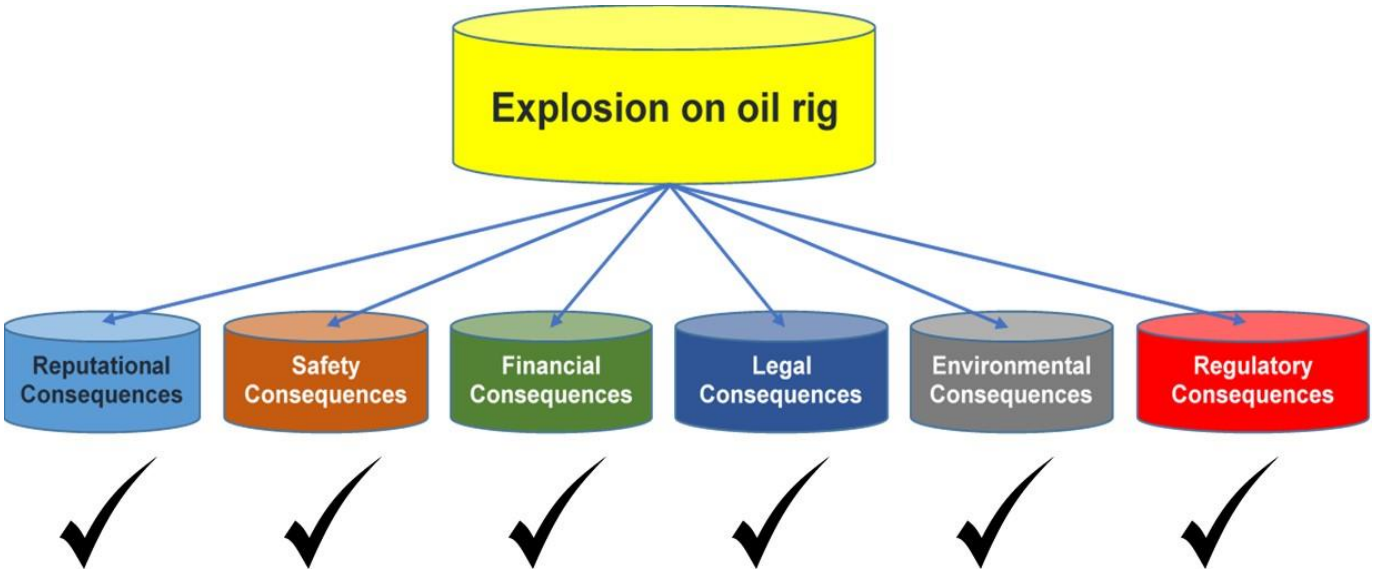
What is the reality?

One event – multiple consequences

35. The reality is that, when an incident occurs (i.e. a risk materialises), there are consequences, but these consequences do not mean that the risk can be categorised. The reason? **There is no such thing as a one consequence risk**.

36. Let's use a real-life example - the Deepwater Horizon tragedy. The risk in the risk register would (or should) have been: ***Explosion on the oil rig***.

37. Fast forward to 20th April 2010 when the risk exploded. Let's have a look at the consequences:



38. So here is my question. What category of risk was it and, therefore, what risk register would this risk have been captured in?

All Risks are Shared Risks

39. There would be very few organisations where the ownership of the risk, the ownership of the controls and those affected by the consequences would reside in one functional area.

40. Even risks that would be considered "safety risks" have controls that cross organisational boundaries and have consequences other than death or injury. That is why it is critical that risks are described in such a way that consequences are not captured in the risk statement.

41. As an illustration, a risk captured in the following way does not take into consideration that there are more than one potential cause and consequences: ***A faulty harness leads to a worker falling from heights resulting in death or injury***.

42. If the risk is described in the following way, it becomes apparent that the consequences are more far-reaching than just potential death or injury:

Risk Name:	**Worker falls from heights**
Causes:	1. No safety equipment provided 2. Failure of safety equipment 3. Worker fails to wear safety equipment 4. Lack of/ineffective training/induction 5. Lack of/ineffective supervision
Consequences:	1. Death/injury to worker 2. Negative impact on reputation 3. Shut down of site 4. Prosecution by regulator 5. Compensation

43. So, the question, even for a simple risk like this, is: is it a safety risk, or a reputation risk, or a compliance risk, or a financial risk? The answer is that is none of them – it is just a risk that, if it occurred would have multiple consequences.

44. I am currently working in a range of organisations where risks have been consolidated into just one risk register and are being treated as risks to the enterprise and not as safety or security or reputation risks.

45. So, the key messages?

a. Remove causes and consequences from your risk descriptions;

b. Consolidate risks into one risk register at the enterprise level and avoid categorising them.

46. Describing and managing risks in this manner provides for a more holistic approach and improves effectiveness significantly.

Risk Ownership

Introduction

47. For the longest time, risk ownership has been pushed down to the lower levels of the organisation in the belief that ownership of the risks should reside with managers that own the functions.

48. On the surface, that may seem reasonable and appropriate, however, over the last few months I have taken a differing view that may just turn risk ownership within organisations on its head. My view is that risks are being allocated ownership at inappropriate levels of the organisation (i.e. too low).

49. There are two reasons for this view.

a. Firstly, it leads to significant duplication and confusion and, secondly, the ownership of the controls reducing the risk levels are owned at the higher levels of the organisation.

b. The purpose of this blog, therefore, is to make a case for raising the level of risk ownership.

Duplication doesn't mean the risk is managed

50. I have recently been reviewing risk registers for a number of organisations and, in doing so, a number of patterns have emerged:

a. All functional areas had their own risk register;

b. The same risk, or variations of the same risk, were evident in each of the risk registers;

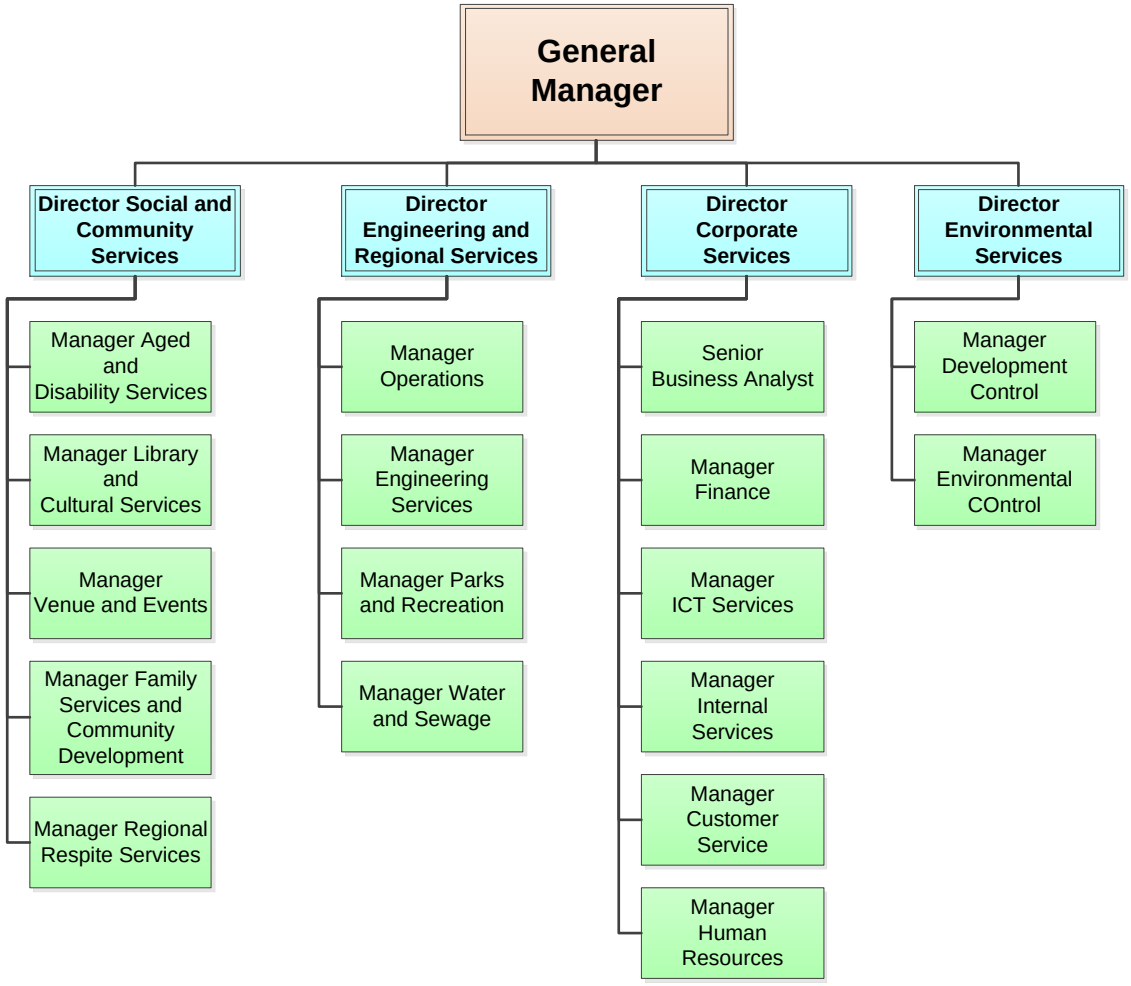
c. All these similar risks were given different owners within each functional area;

d. Each of the registers had their own unique treatment actions for the risk; and

e. **There was no coordination of any of the actions in relation to the management of the risk**.

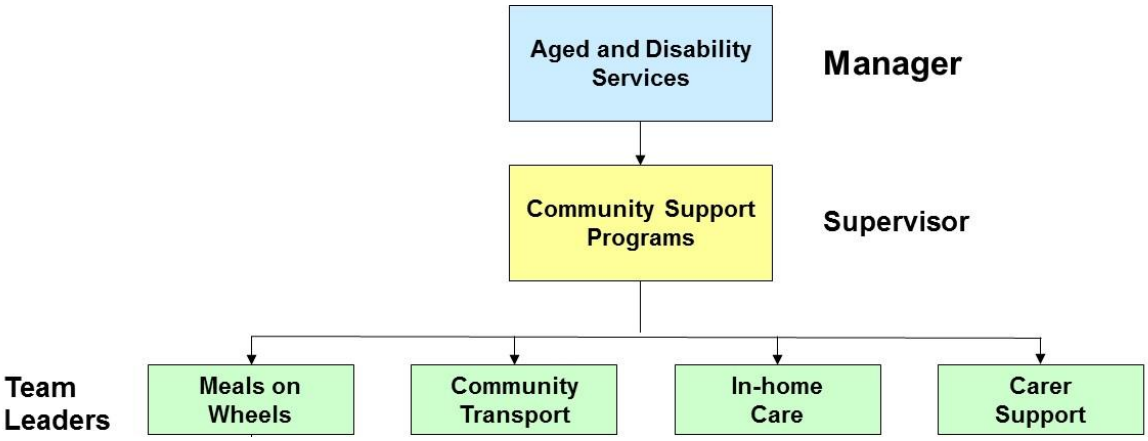
51. I previously supplied consultancy support to a Council that involved a review of their risk register. A not so quick scan showed they had 330 risks contained in the risk register. I was exhausted just at the thought of that number! Upon further analysis though it was clear why: there were a number of risks that appeared multiple times in the register, with one of them **appearing**, with the same wording, **25 times**! What was also interesting was that those 25 risks had – you guessed it – **25 different owners!!!!** The letters F-T-W came to mind, in a slightly different order!

52. Let's use the example of a Council with the following structure to illustrate my point:



53. In this example, we will focus on the Aged and Disability Services section within Social and Community Services.

54. Aged and Disability Services has the following organisational structure:



55. If we focus on the Meals on Wheels Operation, they will have the following risks:

a. Contaminated food delivered to meals on wheels recipients

b. Assault of meals on wheels client by delivery driver

c. Assault of a meals on wheels driver by a client

d. Theft of meals on wheels client property by delivery driver

e. Vehicle accident during delivery

56. If we look at this list of risks, we can make a case that there are other sections of Community Support Programs that would have similar risks. We could also make a case that there are other parts of Council where staff members interact with the public and other parts of Council where staff operate vehicles. If we push ownership of the risks to the lower levels of Council, it is conceivable that the same/similar risks will appear in multiple risk registers. This will result in:

57. The potential for different functional areas within the same organisation to either duplicate treatments being undertaken in other functional areas;

58. The potential for assumptions to be made that controls/treatments are being undertaken in another part of the organisation; and/or

59. The introduction of new treatments that result in additional risks or impact the risk level of an existing risk.

60. What needs to be recognised is that the causes and consequences are going to be the same no matter where they occur within Council. If we look at our Meals on Wheels example, we can see that these causes and consequences are likely to be the same for a similar risk in other functional areas of Council as shown below:

Risk Name:	**Assault of meals on wheels client by delivery driver**
Causes:	1. Lack of/ineffective background checking of staff at time of recruitment 2. Lack of/ineffective training in conflict de-escalation 3. Driver under the influence of drugs/alcohol 4. Lack of/ineffective supervision 5. Lack of/ineffective understanding of pre-existing conditions of client
Consequences:	1. Death/injury to client 2. Negative impact on reputation 3. Potential legal action 4. Action by regulators leading to potential fines/prosecution

61. So, what does this mean?

62. Quite simply, it means that we can capture these risks as an Enterprise level risk, i.e. one that exists in multiple areas of the organisation. This means that we can now capture our risks as follows:

a. Contaminated food served at Council location or to Council client

b. Assault of in-home client by Council staff member, volunteer or contractor

c. Assault of Council staff member, volunteer or contractor whilst conducting operations

d. Theft of client property by Council staff member, volunteer or contractor

e. Council staff member, volunteer or contractor involved in vehicle accident whilst conducting operations

63. There may be causes specific to certain functional areas and these can be notated in the risk register, however, this does not mean that the functional area requires a separate risk. By taking this approach, we will, in all likelihood, reduce the number of risks within the organisation considerably.

64. That, in itself, is a good enough reason to adopt this approach, but, surprisingly, it is not the most compelling reason.

Authority

65. My biggest issue in relation to driving risk ownership to the lower levels of the organisation is the fact that the controls that are controlling the risk are owned, for the most part, at the corporate level. This means that those given responsibility for the ownership of the risk do not own any of the controls that are reducing the likelihood and/or the consequence of the risk and, more importantly, they have no visibility of the effectiveness of those controls.

66. If we go back to our: *Assault of meals on wheels client by delivery driver*, risk:

Risk Name:	**Assault of meals on wheels client by delivery driver**
Causes:	1. Lack of/ineffective background checking of staff at time of recruitment 2. Lack of/ineffective training in conflict de-escalation 3. Driver under the influence of drugs/alcohol 4. Lack of/ineffective supervision 5. Lack of/ineffective understanding of pre-existing conditions of client
Consequences:	1. Death/injury to client 2. Negative impact on reputation 3. Potential legal action 4. Action by regulators leading to potential fines/prosecution

67. If we then look at the controls associated with this risk, an interesting pattern begins to emerge:

Assault of meals on wheels client by delivery driver		
Causes	**Controls**	**Control Owner**
Lack of/ineffective background checking of staff at time of recruitment	Recruitment Policy includes requirement for background checking	HR Manager
	Policy requiring personnel within Council working with children and/or vulnerable people to hold a current certificate	HR Manager
	Certificate register	HR Manager
Lack of/ineffective training in conflict de-escalation	Conflict Resolution training for all personnel working with the public	HR Manager
	Training register	HR Manager
	Annual refresher training as part of mandatory induction program	HR Manager
Driver under the influence of drugs/alcohol	Substance Abuse Policy	HR Manager
	Substance Testing Policy	HR Manager
	Training for managers in recognising the signs of personnel under the influence	HR Manager
Lack of/ineffective supervision	Policy relating to visitation of clients by supervisors	Director Social and Community Services
	Register of visitation	Director Social and Community Services
Lack of/ineffective understanding of pre-existing conditions of client	Policy relating to health and wellbeing assessment of clients	Director Social and Community Services
	Procedure relating to health and wellbeing assessment of clients	Director Social and Community Services
	Register of health and wellbeing assessments	Director Social and Community Services

68. What we can see from this table is that the ownership of the controls associated with the risks rests with executives at the corporate levels of the organisation. So how can we push ownership down when the “owner” of the risk – in this case the Team Leader Meals on Wheels has absolutely no visibility on the effectiveness of the controls and, in most organisations will not have the authority to even ask the question?

69. This then leads me to my rule of thumb when it comes to risk ownership within an organisation: Ownership of the risk must be allocated at a level *at or above* the highest level of ownership of the controls controlling the risk.

70. In the case of the risk: *assault of in-home client by Council staff member, volunteer or contractor* – ownership could sit with either the Director of Corporate Services or the Director Social and Community Services. If there were other parts of Council outside of Social and Community Services where staff were entering client's homes my call would be that the owner of the risk would be Director of Corporate Services.

Summary

71. If we take this approach within our organisations, we would achieve the following:

a. Significant reduction in the number of risks;

b. Improved coordination;

c. Significant reduction in duplication;

d. Ownership at the appropriate level of authority;

e. A greater capacity to actually **manage** the risk.

72. In taking this approach, I have reduced risk register numbers by up to 97% and the number of risks within an organisation by an equivalent amount, but at the same time achieved a greater understanding of the risk profile for the organisation.

73. This approach may not satisfy the conventional wisdom surrounding risk management, but would you rather **do risk management** or **manage risk**?

Likelihood is not based on Time, Frequency or Probability

General

74. Assessing the level of likelihood for risk is something I have been questioning for some considerable time. I have followed the conventional wisdom up until this point and used the 'traditional' criteria to express likelihood. You may have criteria similar to the following:

Likelihood score	Descriptor	Frequency How often might it/does it happen
1	Rare	This will probably never happen/recur
2	Unlikely	Do not expect it to happen/recur but it is possible it may do so
3	Possible	Might happen or recur occasionally
4	Likely	Will probably happen/recur, but it is not a persisting issue/circumstances
5	Almost certain	Will undoubtedly happen/recur, possibly frequently

Probability	Uncertainty Statement	Evaluation
➢ 80%	Almost certainly	5
61-80%	Probable	4
41-60%	Improbable	3
21-40%	Unlikely	2
1-20%	Highly unlikely	1

LIKELIHOOD	QUANTIFICATION	% PROBABILITY	DESCRIPTION
Almost Certain	0 - 12 months	95% - 100%	The event is expected to occur
Likely	1 - 3 years	65% - 95%	The event will probably occur
Possible	3 - 6 years	35% - 65%	The event might occur at some time
Unlikely	6 - 10 years	5% - 35%	The event could occur at some time but is improbable
Rare	Beyond 10 years	< 5%	The event may occur only in exceptional circumstances

75. These descriptors, whilst standard across the industry, have not sat well with me for some time, but I was unsure why. That was until recently when it hit me like the proverbial ton of bricks. It makes absolutely no sense to assess the likelihood of events that are not time or frequency dependent using time or frequency as the measure.

76. I started to ask – is this an appropriate measure to determine the likelihood of risks such of these that ?

a. Contaminated food served to restaurant patrons

b. Worker exposed to unbonded/friable asbestos

c. Wrong medication administered to a patient

d. Explosion at fuel storage depot

e. Legionnaires outbreak in the hospital

f. Unauthorised release of, or alteration to client confidential information

77. The likelihood of these risks occurring is in no way going to be based on frequency or probability. The likelihood of these risks is going to be based on the **effectiveness of the current control environment**.

78. So, let's take one of these - *contaminated food served to restaurant patrons* as a case study and apply it to two restaurants, neither of which has had a contaminated food incident in the past seven years.

79. What would be the likelihood of this risk if we used this criteria?

Qualitative Rating	General Description
Almost Certain	Likely to occur more than once a year
Likely	Likely to occur approximately once a year
Possible	Likely to occur approximately once every 5 years
Unlikely	Likely to occur approximately once every 5-10 years
Rare	Likely to occur with less frequency than once every 10 years

80. To my way of thinking, it is impossible to estimate the likelihood of this risk based on frequency. What will make this risk unlikely to rare is the effectiveness of the controls established within the restaurant.

81. So what if we were to use a likelihood matrix such as this?

Qualitative	Descriptors
Almost Certain	All of the controls associated with the risk are extremely weak and/or non-existent. Without control improvement there is almost no doubt whatsoever that the risk will eventuate
Likely	The majority of the controls associated with the risk are weak. Without control improvement it is more likely than not that the risk will eventuate.
Possible	There are some controls that need improvement, however, if there is no improvement there is no guarantee the risk will eventuate.
Unlikely	The majority of controls are strong with few control gaps. The strength of this control environment means that it is likely that the risk eventuating would be caused by external factors not known to the organisation.
Rare	All controls are strong with no control gaps. The strength of this control environment means that, if this risk eventuates, it is most likely as a result of external circumstances outside of our control.

82. We then assess the likelihood based on the following observations of the effectiveness of the controls. So let's apply this likelihood matrix to two different restaurants:

Restaurant 1

Current Controls and their Effectiveness	Food handling policy	**Effective**
	Food handling training for staff	**Effective**
	Food storage policies and procedures	**Effective**
	Maintenance of refrigeration	**Effective**
	Strict purchase policies in relation to supplies	**Effective**
	Monitoring of cooking temperatures	**Effective**

Restaurant 2

Current Controls and their Effectiveness	Food handling policy	**Effective**
	Food handling training for staff	**Partially Effective**
	Food storage policies and procedures	**Effective**
	Maintenance of refrigeration	**Ineffective**
	Strict purchase policies in relation to supplies	**Partially Effective**
	Monitoring of cooking temperatures	**Ineffective**

83. Based on the effectiveness of the controls the likelihood of *contaminated food being served to restaurant patrons* would be **significantly** higher at restaurant 2.

84. If we continue to try and estimate likelihood based on frequency for risks where the likelihood is actually dependent on the effectiveness of the controls, the decisions we take may be flawed.

85. So how likely is likely? Understand the effectiveness of your controls to truly understand how likely it is that the risk will materialise as an issue.

Getting the Right Risks in the Risk Register

General

86. Earlier this year, all Councils were asked to rank the following risks in order of their importance from 1-10:

a. Financial Sustainability.
b. Reputation Risks.
c. Ineffective governance.
d. Cyber incidents/IT infrastructure.
e. Business continuity and community disruption.
f. Natural catastrophes/Climate change.
g. Increased statutory and/or regulatory requirements.
h. Effective HR and/or WHS management.
i. Errors, omissions or civil liability exposures.
j. Theft, fraud, and/or crime threats.
k. Property & Infrastructure management or damage.
l. Environment management.
m. Terrorism.

87. The problem with this survey is that, for the most part, as shown below, these are not risks:

"Risk"	Commentary
Financial Sustainability	Financial stability is a measure of performance. It is also a category of consequence, **but it is not a risk**.
Reputation Risks	Reputation is a consequence of a risk eventuating **but is not a risk**
Ineffective governance	Is a cause (of many things), **but it is not a risk**
Cyber incidents/IT infrastructure	This is a mix mash of a number of things. Cyber incidents is a cause of: • Unauthorized access to, unauthorized disclosure of, or loss of personal and sensitive information held by Council; and/or • Disruption to xyz critical business function for a period in excess of abc. IT infrastructure is, once again, a cause for the above risks. **Neither are risks**.
"Business continuity and community disruption"	Once again – mix mash. Business continuity is a function/program to prevent/reduce the effects of disruption. Community disruption is a broad consequence but does not specify what within the community is disrupted. A disruption to the collection and disposal of waste has very different outcomes to disruption to library services. **Once again, neither are risks**.
Natural catastrophes/ Climate change	Natural catastrophes are a cause for many risks – including risks relating to disruption to services. Climate change is a source/cause of emerging risks into the future – but, in and of itself, is not a risk

"Risk"	Commentary
Increased statutory and/or regulatory requirements	This is a strategic risk. The risk is the change – not the increase.
Effective HR and/or WHS management	Effective HR and/or WHS management are tasks **but are not risks**.
Errors, omissions and/or civil liability exposures	Errors, omissions are causes. Civil liability exposures are consequences. **Neither, however, are risks**.
Theft, fraud, and/or crime threats	Theft and fraud are risks. Crime threats is not a risk – it is a source of risk.
"Property & Infrastructure management or damage" –	Property & Infrastructure Management is a task. Property & Infrastructure Damage could be a risk – but may be better expressed as: *Structural failure and/or loss of access to, infrastructure/facilities used by residents*.
Environment management	This is a task – **not a risk**
Terrorism	Terrorism is a potential cause of a range of risks (disruption to; loss of access to; contamination of …. **It is not a risk**

88. If the "wrong" risks are in the risk register, it is simply not possible for Councils to adequately manage their risks.

What is a Risk?

89. It may seem obvious but, fundamental to the effective management of risk, it is essential that we actually understand what a risk is.

90. From the outset let me be frank, I consider the definition of risk management in ISO 31000 (***the effects of uncertainty on objectives***[1]) to be confusing, and, utterly ineffectual as a definition. I make this quite clear in my blogs and my eBook *Risk is not a Four-Letter Word*.

91. **Effect** is defined as "a change which is a result or consequence of an action or other cause[2]". In essence, an effect is an outcome or consequence, so if we substitute that into the definition it becomes: the ***consequence of uncertainty on objectives***.

92. In this definition, the focus is on identifying the consequences of the uncertainty, rather than what the actual uncertainty is. Confusing, I know, and so the now superseded AS/NZS 4360 defined risk management as:

the chance of something happening that will have an impact on objectives

93. Whilst this definition was certainly more focussed on events (something happening), it was more geared towards the chance of something happening (i.e. the likelihood). So, this definition can be expressed as: ***the likelihood of something happening that will have an impact on objectives***.

94. Neither of these definitions, in my view though captures the essence of what the risk is: the **event that we are trying to prevent from happening**.

[1] AS/NZS ISO 31000:2009: Risk management — Principles and Guidelines
[2] AS/NZS 4360:2004, Risk management

95. To that end, I have developed a definition that I think more meaningfully describes what a risk is. To me there needs to be a real focus on the actual thing we are trying to stop: in other words, seeing a risk as a potential event, as shown in the definition below:

> ***"A possible event/incident/issue that, if it occurs, will have an impact on the organisation's objectives"***

96. This definition focusses on the event, not the consequence or the likelihood.

97. When you hear people say: *they obviously didn't manage the risk very well*, it is, **always**, after an incident, issue or disaster, so, this definition makes much more sense.

98. So, what does this mean for us?

99. It means that we need to focus more on identifying **the thing we are trying to stop from happening**.

A more Granular Approach

100. One of the areas I have been working on in relation to the management of risk is the parent/child relationship. The parent risk can also be described as the "headline risk". This is the risk that, using the risk levels of the child risks will be reported to the Executive.

101. The following would be the parent risks for a Council:

a. Unauthorised release of/amendment to/use of and/or loss of corporate/confidential information

b. Incorrect, incomplete or untimely information provided to a critical stakeholder

c. Disruption to critical business function for a period in excess of specified Maximum Acceptable Outage

d. Fraudulent/corrupt behaviour by a member of staff and/or 3rd party

e. Incident/s of inappropriate behaviour by a member of staff

f. Council delivers a project/program that is not fit for purpose or of poor quality

g. Incident occurs that threatens the health and/or safety of stakeholders

h. Council is unable to meet financial obligations

i. Incident occurs that impacts the environment

102. Like the strategic risks previously identified, these would be common to every Council. Where the differences in risk would occur would be in the child risks as some Councils do activities that others don't.

103. To illustrate, let's look at a parent risk with the child risks where there would be **no difference** in the risks from Council to Council:

Parent Risk	PR X	Fraudulent/corrupt behaviour by a member of staff and/or 3rd party
Child Risks	X-1	Fraudulent/corrupt behaviour by a member of staff involved in procurement activities
	X-2	Fraudulent/corrupt behaviour by a member of staff involved in accounts payable/receivable/payroll/cash
	X-3	Theft of council supplies/equipment
	X-4	Member of council staff or counsellor accept benefits for approvals
	X-5	Council contractor paid for services not provided
	X-6	Fraudulent/corrupt behaviour by a member of staff involved in management of contracts
	X-7	Member of staff receives benefits to which they are not entitled

104. Now let's look at a risk where there will be differences between Councils based on the activities they conduct (although some will be the same across all Councils):

Parent Risk	PR Y	Disruption to critical business function for a period in excess of specified Maximum Acceptable Outage (MAO)
Child Risks	Y-1	Disruption to sewage treatment operations
	Y-2	Disruption to rubbish collection and disposal operations
	Y-3	Disruption to water treatment operations
	Y-4	Disruption to in-home support for high dependency clients
	Y-5	Disruption to provision of access to records

105. I have developed child risks for all of the parent risks and truly believe the risk landscape in Councils would change exponentially if all Councils adopted them.

About Paladin Risk Management Services

Paladin Risk Management Services has been in business since May 2007 and since commencing operations has been engaged by organisations in both the public and private sector for a range of risk management activities including:

- Assessment of organisational risk management capabilities;
- Development of risk management frameworks;
- Development/review of risk management documentation (including fraud control);
- Facilitation of risk management workshops;
- Risk identification, analysis and development of treatment options;
- Development and delivery of risk management training; and
- Development of Business Continuity Management Frameworks and Plans.

To date Paladin Risk Management Services has built an enviable reputation as a provider of quality risk training and consultancy services to its clients.

Paladin Risk Management Services has provided similar services to:

- Horsham Regional City Council;
- Bunbury Council;
- Tweed Heads Council;
- Broken Hill Council;
- Ballarat Council;
- Indigo Shire Council; and
- Yarra Council.

In addition, personnel from over 80 Councils have attended Paladin Risk Management Services training courses.

Rod Farrar is the Principal of Paladin Risk Management Services.

Rod 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 Risk Management expertise is highly sought after as is the insight he provides in his risk management training and workshop facilitation.

Rod was recognised by the Risk Management Institution of Australia as the **2016 Risk Consultant of the Year** and one of the first five **Certified Chief Risk Officers** in Australasia.

For information please contact:

Rod Farrar | Director |
PO Box 359, MITCHELL ACT 2911 Australia
T +61 400 666 142 | **F** +61 2 8208 7398 | **E** rod@paladinrisk.com.au
W: www.paladinrisk.com.au

We are also on social media:

@paladinrisk

Facebook: Paladin Risk Management Services

Linkedin: Rod Farrar

PALADIN
RISK MANAGEMENT SERVICES