OVERVIEW

Risk management is simply a process. The purpose of a risk management plan or register (they are one and the same) is to manage uncertainty and initiate actions to identify, assess, monitor and reduce the impact of risks to your business.

A good risk management plan (or risk register) with appropriate risk management strategies can minimise costly and stressful problems, and can in some circumstances reduce the need for excessive insurance claims and premiums.

DEVELOPING A RISK MANAGEMENT STRATEGY

Typically there are five core steps to developing a risk management strategy.

Step 1: Define the risk context of the business – General overarching risks

- Identify where or under what circumstances the risk occurs.
- Review the risk categories attached and determine, in general risk order (highest to lowest), how these apply to the business.

Step 2: Risk identification

Under each of the categories listed in general risk order, now identify specific risks that are likely to affect the achievement of your business goals.

For example, financial risks related to cash flow, information technology, taking on a particular project, a new or specialised data collection methodology, outsourcing critical stages of work, internationalisation and the fluctuating dollar, or the size of the business in relation to market research needs.

Describe the risk in terms of:

- What it is and what can happen?
- How and why it can happen.
- What happens if the risk eventuates (consequences)?

Systematically work through each function, activity or stage of your operations and identify what might happen for each function.

Review company history to identify things that have gone wrong in the past.

Analyse your systems and processes to identify critical points.

Step 3: Risk Assessment

This step involves analysing the likelihood and consequences of each identified risk using a typical risk matrix.

RISK MATRIX					
Likelihood	**1 Insignificant**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
A Almost Certain	H – 11	H - 16	E - 20	E – 23	E - 25
B Likely	M - 7	H - 12	H - 17	E - 21	E - 24
C Possible	L - 4	M - 8	H - 13	E - 18	E - 22
D Unlikely	L - 2	L - 5	M - 9	H - 14	E - 19
E Rare	L - 1	L - 3	M - 6	H - 10	H - 15

There are any number of Matrices – all do the same or similar job.

- Review the existing controls currently in place for each risk.
- Identify what your business does to control this risk.
- Rate the effectiveness of existing controls in preventing the risk from eventuating or minimising its impact should it occur.
- Decide whether existing controls are strong, just adequate or inadequate.

LIKELIHOOD is a qualitative description of probability and frequency. What is the likelihood of the risk occurring?

RISK MATRIX EXPLANATION		
Likelihood	**Probability**	**Frequency**
A Almost certain	>90%	Is expected to occur in most circumstances more than once during the year
B Likely	60% to 90%	Could easily occur and will probably occur once within a 1 to 2 year period.
C Possible	40% to 60%	Might occur at some time within a 2 to 5 year period.
D Unlikely	10% to 40%	Known to happen but not regularly. Could occur at some time within a 5 to 10 year period.
E Rare	<10%	Conceivable, but may only occur in exceptional circumstances. The event has not happened in the industry in the last 10-20 years.

CONSEQUENCE is the outcome of an event or situation, being a loss, litigation, disadvantage or failure to comply. What is the consequence of the risk event?

RISK MITIGATION		
	E 22 - 25	CATASTROPHIC - DO NOT PROCEED: Directors to determine strategic approach – legal risk pending. Strategies for due diligence measures to be undertaken. Seek expert advice as necessary before proceeding.
	E 18 - 21	MAJOR: Risk Management Strategy to be developed to determine whether to proceed. Incorporate strict risk controls if agreed to proceed. Performance monitoring in place to ensure long term preventive measures in place are effective.
	H 10 - 17	MODERATE: Review risk register and proceed with delegated authorities up the line – to ensure risk mitigation is being followed.
	M 6 - 9	MINOR: Proceed as per normal business.
	L 1 - 5	INSIGNIFICANT: Not considered a risk.

RISK RATING = Consequence Rating x Likelihood Rating.

On the Risk Analysis Matrix find the intersection of the likelihood and consequence ratings selected for the risk.

Risk Priority provides an indication of how soon you need to implement a strategy to treat the risk. Go to Attach 2# Risk Matrix and determine the risk rating.

RISK MATRIX					
Likelihood	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
A Almost Certain	H – 11	H - 16	E - 20	E – 23	E - 25
B Likely	M - 7	H - 12	H - 17	E - 21	E - 24
C Possible	L - 4	M - 8	H - 13	E - 18	E - 22
D Unlikely	L - 2	L - 5	M - 9	H - 14	E - 19
E Rare	L - 1	L - 3	M - 6	H - 10	H - 15

Step 4: Risk Strategies / Controls

The objective of this stage is to develop cost effective options for treating/controlling each risk. Determine the best treatment option from the five methods below.

a) Eliminate the risk by discontinuing the activity or removing the hazard i.e., not undertaking the activity that is likely to trigger the risk.

b) Consider the following factors when determining the validity of this option to avoid the risk:

- What will happen if the activity is not undertaken e.g. validation, client contract signed?
- Is the risk level too high to proceed or continue with the activity – e.g. what if you proceed without agreement from the client; is it s significant risk?
- Is the cost of the required controls higher than the benefit of the activity e.g. cost of validation makes the job non profitable?
- Will the failure of the activity have critical consequences for the business – loss of or corrupt data from an IT supplier?
- Consider the reasons for avoiding the risk. Is your business unnecessarily risk averse?
- Will the risk avoidance increase the significance of other risks or lead to the loss of opportunities for work e.g do not embrace new technologies due to risk of data integrity?
- Accept the risk; simply take the chance to incur the negative impact. You may already be doing all things reasonable to reduce the risk but it can't be completely eliminated e.g. make the decision whether to contract a reliable known source of online data provision or an untested, untried provider that is much cheaper.

c) Reduce the likelihood of the risk occurring in order to reduce the negative outcomes. Can the likelihood of the risk occurring be reduced? Through preventative measures, or quality assurance and management, change in business systems and processes e.g. make the decision to go with the known quality assured provider whilst still doing the project.

d) Reduce the consequences in the event that the risk occurs. Can the impact of the consequences be controlled or reduced if the risk occurs? Through contingency planning, minimising exposure to sources of risk or separation or relocation of a business activity and resources client e.g. keep the work in-house rather than contract to an insecure/untested source which may mean accepting a lesser profit for a more secure outcome.

e) Transfer the risk totally or in part may be achieved through moving the responsibility to another party or sharing the risk through a contract, insurance arrangements, or partnership/s and joint ventures – not all risks can be transferred. e.g. get the client to appoint/contract an online data collection provider of their choice thus taking the consequences of failure away from the company and giving it back to the xxxxxxx

Step 5: Monitoring and Review

Risk management is an ongoing process. Even if the existing control measures are adequate there is a need to regularly review whether anything has changed that may impact on the risk issues you have identified e.g. change could be technology based - with changes occurring rapidly in the current environment, IT risks could occur unnoticed that were not present 6 months ago (malware software and the like)

Another example of the need for continuous monitoring is the current change to the Privacy Legislation resulting in the need to review the risks associated with all forms of client and respondent data (data collection and handling methodologies, software systems, staff training, policies and procedures).

Once the proposed controls are completed reassess the risk by conducting regular risk reviews and reviewing the progress and effectiveness of your selected risk strategies.

Category	Examples
Commercial	Risks associated with market placement, business growth, diversification and commercial success. This relates to the commercial viability of the services the company provides.
Compliance / Legal	Compliance with legal requirements such as legislation, regulations, industry standards, privacy and other codes and contractual requirements. This also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.
Financial	Cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
Reputation	Entails the threat to the reputation of the business due to the conduct of the entity as a whole, the viability and reliability of service delivery, or the conduct of employees or other individuals associated with the business.
Strategic	Includes the planning, scoping and resourcing requirements for the establishment, sustaining and/or growth of the business.
Operational	Covers the planning, operational activities, resources (including people) and support required within the operations of a business that result in the successful development and delivery of a market research services.
Service delivery	Relates to the delivery of services, including the quality and appropriateness of service provided, or the manner in which a product is delivered, including customer interaction and after-sales service.
Project	Includes the management of venues, equipment, budget, resources, technology, timeframes and people associated with the management of projects.
Information Technology	Selection, implementation, management, maintenance and upgrades associated with information technology.
Security	Includes the overall security of the business premises, assets and people, and critically extends to security of information, intellectual property, and technology e.g. risks associated with client and respondent data security.
Stakeholder and Outsourcing Management	Relates to the management of stakeholders including subcontractors, and includes identifying, establishing and maintaining an appropriate risk managed relationship to ensure those risks identified as part of the overall business research management risk are also covered/managed by the outsourced providers.
Health & Safety	The safety of everyone associated with the business including any casual or contacted works. This extends from individual safety, to workplace safety, public safety and to the safety and appropriateness of services delivered by the business e.g fieldwork in a risk environment, product testing in focus groups etc.
Environmental	Loss or damage due to accidents or natural disasters such as fire, flood, hail or storms. Can extend to property damage causing loss of data, failure to deliver on time etc.

BUSINESS RISK CALCULATION TOOL

RISK MITIGATION		
	E 22 - 25	CATASTROPHIC - DO NOT PROCEED Directors to determine strategic approach – legal risk pending. Strategies for due diligence measures to be undertaken. Seek expert advice as necessary before proceeding.
	E 18 - 21	MAJOR Risk Management Strategy to be developed to determine whether to proceed. Incorporate strict risk controls if agreed to proceed. Performance monitoring in place to ensure long term preventive measures in place are effective.
	H 10 - 17	MODERATE Review risk register and proceed with delegated authorities up the line – to ensure risk mitigation is bing followed.
	M 6 - 9	MINOR Proceed as per normal business.
	L 1 - 5	INSIGNIFICANT Not considered a risk.

RISK MATRIX					
Likelihood	**1 Insignificant**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
A Almost Certain	**H – 11**	**H - 16**	**E - 20**	**E – 23**	**E - 25**
B Likely	**M - 7**	**H - 12**	**H - 17**	**E - 21**	**E - 24**
C Possible	**L - 4**	**M - 8**	**H - 13**	**E - 18**	**E - 22**
D Unlikely	**L - 2**	**L - 5**	**M - 9**	**H - 14**	**E - 19**
E Rare	**L - 1**	**L - 3**	**M - 6**	**H - 10**	**H - 15**

RISK MATRIX EXPLANATION		
Likelihood	**Probability**	**Frequency**
A Almost certain	>90%	Is expected to occur in most circumstances more than once during the year
B Likely	60% to 90%	Could easily occur and will probably occur once within a 1 to 2 year period.
C Possible	40% to 60%	Might occur at some time within a 2 to 5 year period.
D Unlikely	10% to 40%	Known to happen but not regularly. Could occur at some time within a 5 to 10 year period.
E Rare	<10%	Conceivable, but may only occur in exceptional circumstances. The event has not happened in the industry in the last 10-20 years.

Risk Management Additional Reading

- Financial Liquidity Risk
  http://cpaaustralia.com.au/~/media/Corporate/AllFiles/Document/professional-resources/business/managing-liquidity-risk.PDF
- Small Business Risk Management
  http://www.smallbusiness.wa.gov.au/risk-management\
- Business Risk
  http://www.business.qld.gov.au/business/running/risk-management/identifying-business-risk
- ISO 31000 Risk Management Standard