

USING A BUSINESS RISK MODEL

PRESENTED BY BARRY S LEITHHEAD FCPA CIA
LEITHHEAD & ASSOCIATES, SYDNEY, AUSTRALIA

OVERVIEW

A Business Risk model helps practitioners when they start risk-based internal auditing. The model describes the risk management process and extends into the key areas of risk management policy and resources. This paper covers:

- How a business risk model works;
- Basic methodology for using a business risk model;
- Examples of a business risk model in practice;
- Tips for getting the best results with a business risk model.

This paper describes two business risk management models, from:

- The Australian Standard on Risk Management AS/NZS 4360; and
- The IIA's global Competency Framework for Internal Auditing (CFIA).

Internal auditing provides assurance that risk exposures are understood and managed appropriately in dynamic changing contexts.

THE BUSINESS RISK MANAGEMENT MODEL

The generic risk management model contains a number of levels and components:

- 1 The organization's external and internal *dynamic contexts*;
- 2 The organization's risk management context;
- 3 The organization elements that are *at risk*;
- 4 The likelihood of a risk occurring;
- 5 The immediate *consequences* of the risk occurrence;
- 6 The ultimate *effects* of the risk occurrence;
- 7 The *criteria* by which risks are assessed and prioritised;
- 8 The risk *treatment* options and processes;
- 9 Consulting, communicating, monitoring and reporting.

AUSTRALIAN RISK MANAGEMENT STANDARD (AS/NZS 4360)

The Australian/New Zealand Standard is the only one of its type and an International Standard (ISO) is being developed from this base. The Standard was developed by a group of people representing a variety of professions – internal auditing, risk management, insurance, IT, engineering and academics. The result was a document that all of them could use across a

variety of applications.

The Standard describes the risk management process as a number of steps:

Source: Risk Management Standard AS/NZS 4360:1999

This model recognises that to ‘*treat*’ risks, i.e. *control* risks, requires identification, analysis and assessment against agreed criteria. First though, the organizational and risk management contexts have to be recognised. That is, what is the operating environment of the organization, covering the external and internal contexts, of current conditions and changing circumstances? As well, what is the organization’s attitude to risk taking – what is the pain threshold?

Internal auditors can easily see themselves in this process. The key issue is to consider the contexts and identify the exposures to risk and assess the risks, before considering the control options. Risk analysis comes before control evaluation.

DYNAMIC CONTEXTS ARE THE SOURCE OF RISK

It is important to understand where risks come from – what is the source of risks. There are two ways to look at the source of risks:

- The *place* where risks start or develop;
- The *conditions* which give rise to the risk.

Dynamic Contexts are the variety of ‘environments’ (*places*), which are made up of the *Conditions* at a point in time and the changing *Circumstances* that create new conditions.

- Organizations need to be in tune with contextual *conditions* or they are at risk.
- Organizations need to be alert to changing *circumstances* or they are at risk.

The Dynamic Contexts which usually relate to organizations include:

UNIVERSAL CONTEXTS

Global, Economic, Political, Regulatory, Technology, Society, Knowledge

SECTORAL CONTEXTS

Public, Private, Not-For-Profit, Co-operative, Cross-sectoral.

INDUSTRY CONTEXTS

Types of industry, Product/Process, Markets, Customer, Supplier, Contractors, Manufacturers, Service, and Distributors.

ORGANIZATIONAL CONTEXTS

Power, Size, Culture, History, Geography, Sociology.

Dynamic contexts provide opportunities (positive risk) and threats (negative risk) to organizations. The conditions and changing circumstances of some of the contexts are shown in the following table:

CONTEXTS	INHERENT SOURCES OF BUSINESS RISK	
	CONDITIONS	CHANGING CIRCUMSTANCES
Globalization	Different languages, customs, currency standards of living and development, time zones, political systems.	Opportunities for investment; political climate; economic growth/decline; Tariff barriers reduction; New regional alliances.
Institutional	Governments regulate the conduct of organizations, e.g. in environmental management or fiscal responsibility.	The range and complexity of regulation increases; Political pressure is applied.
Sectoral	Government departments provide services and conduct related business activities as a public service;	Government businesses are corporatised and privatised or compete with the private sector.

CONTEXTS	INHERENT SOURCES OF BUSINESS RISK	
	CONDITIONS	CHANGING CIRCUMSTANCES
Industry	Products, services and processes are well defined. Industry participants are known. Markets are competitive.	Emerging and converging products, services and processes introduce new participants and new alliances with those from other industries.
Technology	Technologies provide advanced processes and facilities to improve products and services.	Research and development rapidly increases the array of available technology; People are attracted to/repelled by new technology.
Work	People are employed in organizations to contribute to achieving common goals.	Unemployment is a source of social unease; Skilled employees are hard to recruit; Part-time work becomes customary; People work in teams, making decisions and changes.

This is a sample of the contexts, conditions and circumstances, which inherently expose organizations to risk.

Assessing contextual risk is the highest level of strategic risk analysis. Many internal auditors may not be involved at this level, although it is the proper role of internal auditing. This contextual risk analysis also applies at the functional level, where the marketing, manufacturing and customer service departments and others, face contextual risks. Internal auditors are active at the functional level and their evaluation of control systems must consider contextual risk at that level.

Risk Profiling is a search and discovery process, which considers the potential impact on an organization, from the variety of *sources* in the variety of *contexts*. The sources include:

- Complexity, volatility and uncertainty;
- Hazardous conditions, products and processes;
- Ignorance, incompetence and negligence;
- Inequity, injustice and inconsistency;
- Criminality and corruption.

The table below provides examples of Business Risks:

GENERIC RISK SOURCES	INHERENT RISKS IN BUSINESS OPERATIONS
Complexity, volatility, uncertainty;	Participation in a joint venture in offshore countries involves <i>complex conditions</i> that are difficult to fully understand and manage.
	Commodity markets are volatile and forecasting price movements and taking positions in commodities is difficult to manage.
	Investing in new technology is important, but rapid developments create uncertainty about the best timing for investment.

ORGANIZATION ELEMENTS	INHERENT RISKS IN BUSINESS OPERATIONS
<p>Hazardous conditions, products, processes;</p>	<p>Industries are exposed to hazards such as:</p> <ul style="list-style-type: none"> ➤ Gaseous, poisonous and corrosive substances; ➤ Inflammable sources and combustible materials; ➤ Confined spaces or extreme heights; ➤ Climatic, underground and at-sea conditions; ➤ Parallel operations using shared resources.
<p>Ignorance, incompetence, negligence;</p>	<p>Organisation staff may be exposed to conditions for which they are untrained and unprepared and may not possess the appropriate knowledge and capability</p> <p>The need to develop the organization's culture, to meet new and emerging trends, may not be recognised and is neglected, allowing attitudes of indifference and negligence to occur.</p>
<p>Inequity, injustice; inconsistency;</p>	<p>Suppliers gain a position of influence of procurement decisions and cause their competitors to be excluded from opportunities;</p> <p>Development in the organisation over time may result in a situation where successful functions are rewarded. This is resented by others, creating a two tiered staff structure and discontent and disharmony in the organization;</p>
<p>Criminality, corruption</p>	<p>Managers in responsible positions realise opportunities for criminal and corrupt conduct and defraud the organization;</p> <p>Segments of the organization's client base lacks ethical standards and consistently attempts to take deceitful advantage of the organization</p>

WHAT IS 'AT RISK'?

Risks have their source in dynamic contexts and their effect in the *elements* of the organization. The table below provides examples of organization elements *At Risk* in Outsourcing:

ORGANIZATION ELEMENTS	INHERENT RISKS IN BUSINESS OPERATIONS
<p>Strategies;</p>	<p>The developments in customer attitudes and preferences is unexpected and makes obsolete the latest developments in the product range.</p> <p>A change in government in the country of a major joint-venture radically downgrades the prospects for business growth.</p>
<p>Outcomes, objectives, goals;</p>	<p>Productivity improvement and cost saving targets of a major investment are not achieved, because of unexpected and excessive learning curves;</p> <p>The benefits of new technology are not gained because of the failure to realise the size and significance of the required education and training program.</p> <p>Customers are dissatisfied with delivery service – organization functions cannot integrate their activities to achieve on-time delivery.</p>

ORGANIZATION ELEMENTS	INHERENT RISKS IN BUSINESS OPERATIONS
Resources, relationships;	Talented staff in the organization see limited prospects of career development into operations now outsourced and leave the organization. Tension between management and staff impacts on communication and on functional effectiveness. A long-time practice of procurement based on price, leaves the organisation without reliable, long-term supply relationships.
Events, activities, processes;	The organization is unaware of the latest changes to environmental regulations and its facilities and work practices cause unacceptable breaches; Excessive dependence on key processes, without adequate back-up, causes undue interruption in the event of breakdown.
Control systems.	Information systems cannot be adapted readily to meet the changing needs of the organization; Functional managers and staff are not sufficiently aware of the contexts, risks and control systems, to anticipate the effects of future business conditions.

These scenarios of the *sources* of risks and what is *at risk*, describe some inherent risks. Compare these examples with a generic list of consequences and effects, to consider whether other exposures can be identified. What sources and 'at risks' would be involved in these new scenarios? Generic consequences and effects of risk include:

- 1 Death, injury, ill-health;
- 2 Loss, destruction, damage, impairment.
- 3 Failure, interruption, delay;
- 4 Opportunity loss, Reputation loss, Heritage loss;
- 5 Financial loss; Non financial loss.

RISK ASSESSMENT CRITERIA

Risk is assessed at the *inherent* level, that is, the exposure to risk without considering the presence or effectiveness of any control system or process. The *inherent* risk influences what form and what degree of control is needed, given the organization's stance on and tolerance for risk. The risk *effect* may be assessed for one or more different criteria, including:

- Revenue;
- Cost;
- Investment;
- Time;
- Quality;
- Reputation;
- Health and Safety; and
- Damage/Impairment.

For example, it is possible to assess risks against the criteria:

- impact on revenue, cost or investment;
- time to recover from a loss;
- impact on quality and reputation;
- effect on health, safety;
- cost of damage or impairment.

The following table provides *indicative* criteria to describe Consequences. Each organization needs to establish assessment criteria, which are relevant for its size and stance on risk:

Risk Criteria	HIGH RISK	MEDIUM RISK	LOW RISK
Revenue	Loss >\$1 million	Loss >\$250K	Loss >\$50K
Cost	Loss >\$1 million	Loss >\$250K	Loss >\$50K
Investment	Loss >\$10 million	Loss >\$1 million	Loss >\$250K
Time	Delay to Customers >24 hrs	Delay to Customers >48 hrs	Delay to some Customers
Quality	Customer Rejects >2%	Customer Rejects >1%	Customer Rejects >0.5%
Reputation	Severely adverse media	A critical community	Some critical media
Health & Safety	Death or serious injuries	Serious injury	Serious injury
Damage	Loss >\$10 million	Loss >\$1 million	Loss >\$250K
Impairment	Clean-up >\$1 million	Clean-up >\$250K	Clean-up >\$50K

Likelihood is considered in risk assessment and the High, Medium and Low scales can be used. Cross-referencing Likelihood and Consequence, the following risk profiling table results:

L
I
K
E
L
I
H
O
O
D

<u>High</u>	Medium	High	High
<u>Medium</u>	Low	Medium	High
<u>Low</u>	Low	Low	High
	<u>Low</u>	<u>Medium</u>	<u>High</u>
	C O N S E Q U E N C E		

NOTE:

Cell content names relate to overall Risk ratings not just Consequence or Likelihood

A STRUCTURED APPROACH TO BUSINESS RISK ANALYSIS

The purpose of risk analysis is to identify the elements-at-risk, the sources of risk and to assess the consequence of the risk. For example, contextual risks to organisational elements can be shown as opportunities (positive) and threats (negative), together with weaknesses in achieving objectives and control systems. Each type of risk to each organisational element could be assessed as High, Medium and Low and the results displayed on a table.

Aggregate assessments for each element and each risk are shown in the shaded total columns:

ORGANISATION RISK ANALYSIS					
ORGANISATION ELEMENTS	CONTEXTUAL DYNAMICS		CAPABILITY WEAKNESS		OVERALL RISK
	OPPORTUNITIES	THREATS	OBJECTIVES	CONTROLS	
Products and Services	<i>High</i>	<i>High</i>	<i>Low</i>	<i>High</i>	<i>High</i>
Functions and Departments	<i>Low</i>	<i>Medium</i>	<i>Medium</i>	<i>Medium</i>	<i>Medium</i>
Management	<i>Low</i>	<i>Medium</i>	<i>Medium</i>	<i>Medium</i>	<i>Medium</i>
Stakeholder relationships	<i>Medium</i>	<i>High</i>	<i>Medium</i>	<i>High</i>	<i>High</i>
The Total Organisation	<i>Medium</i>	<i>High</i>	<i>Medium</i>	<i>Medium</i>	<i>Medium</i>

The assessments in each cell of this matrix may be the judgments of those people in positions to know. Alternatively, each cell is the summary of a more detailed assessment. For example, the *High* score for products and Services Opportunities could be the result of considering the major Products and Services against opportunity risk sources, such as:

RISK SOURCE	POTENTIAL BENEFIT
<i>Alliance</i>	<i>Alliance with other products or services or suppliers, enhances volume and/or price.</i>
<i>Growth</i>	<i>Improved marketing/selling increases market size or market share</i>
<i>Innovation</i>	<i>Redesign/development of features provides new applications, markets, volume.</i>
<i>Advantage</i>	<i>Promotion of features improves market position over competitive products</i>
<i>\$ Reward</i>	<i>Manufacturing/distribution costs reduction or price increase improves contribution</i>
<i>Reputation</i>	<i>Quality and reliability provide vehicle for promotion, price increase, increased contribution.</i>

This group of potential benefits (or a more relevant group, depending on the organisation) can be assessed for each major product or service and the results entered in a matrix. The aggregate assessment for all products and services (*High*) is transferred to the summary matrix (above):

PRODUCTS and SERVICES	ORGANISATION RISK ANALYSIS - CONTEXTUAL OPPORTUNITIES						TOTAL
	<i>Alliance</i>	<i>Growth</i>	<i>Innovation</i>	<i>Advantage</i>	<i>\$ Reward</i>	<i>Reputation</i>	
P & S 1							
P & S 2							
P & S 3							
TOTAL							<i>High</i>

The table below describes examples of the sources of risk that need to be assessed:

- opportunities and threats for Contexts; and
- the capabilities for Objectives and Internal Controls.

<u>CONTEXTUAL DYNAMICS</u>		<u>CAPABILITIES</u>	
OPPORTUNITIES	THREATS	OBJECTIVES	INTERNAL CONTROLS
<i>Alliance</i>	<i>Uncertainty</i>	<i>Leadership</i>	<i>Control components</i>
<i>Growth</i>	<i>Complexity, volatility</i>	<i>Market position</i>	<i>Adequate understanding</i>
<i>Innovation</i>	<i>Inequity, injustice</i>	<i>Value creation</i>	<i>Adequate design</i>
<i>Advantage</i>	<i>Competition</i>	<i>Resource custody/use</i>	<i>Efficient application</i>
<i>Financial Reward</i>	<i>Ignorance</i>	<i>Research & development</i>	<i>Effective application</i>
<i>Reputation</i>	<i>Criminality, fraud</i>	<i>Results</i>	<i>Adequate documentation</i>

THE IIA’S GLOBAL COMPETENCY FRAMEWORK FOR INTERNAL AUDITING (CFIA)

CFIA provides a risk-based perspective for internal auditing. At the core of CFIA is the functional definition and the tasks and sub-tasks. IIA’s global Competency Framework (CFIA) describes internal auditing as:

“A process by which an organization gains assurance that the risk exposures it faces are understood and managed appropriately in dynamically changing contexts”.

CFIA provides a Focus/Process/Outcomes matrix, which re-positions internal auditing.

Internal Audit Processes/Outcomes	Internal Audit Focus		
	Dynamic Contexts	Risk Exposure	Control Systems
Developing <i>Understanding</i>	✓	✓	✓
Contributing to <i>Improvement</i>	✓	✓	✓
Providing <i>Assurance</i>	✓	✓	✓
Management of the Function	✓	✓	✓

The focus of the Internal Auditing Function is on organizational *risk exposures* and related *control systems*, and the *contextual dynamics* that may make these control systems inappropriate or ineffective. The audit processes utilised by the Function involve - developing *understanding*, facilitating *improvement*, providing *assurance*. The organizational *outcomes* from those processes are assurance, improvement and understanding. *Managing* the Function itself and the contexts it faces is the final process.

The risk perspective is detailed in the first task of CFIA’s Competency Standards:

Task 1. Develop understanding within an organization about the risks associated with its functioning and contexts.

Sub-Task 1.1 Understand an organization's objectives/strategies, processes, capabilities, and the contextual dynamics affecting its functioning

- 1.1.1 Identify/clarify the organization's objectives and strategies
- 1.1.2 Identify the key processes used to support strategies
- 1.1.2 Identify the patterns of resource use associated with key processes
- 1.1.4 Identify the core capabilities supporting the organization's strategies
- 1.1.5 Identify the contextual dynamics (competitive, institutional, environmental) affecting the organization's strategic success and its future.

Element 1.2 Profile the organization's philosophy (attitude/stance) on risk

- 1.2.1 Identify/develop/select a framework for structuring enquiry and communication about risk
- 1.2.2 Negotiate acceptance of this framework within the organization
- 1.2.3 Conduct relevant enquiries and communications about risk in relation to the organization with key personnel
- 1.2.4 Confirm with management the profile developed of the organization's philosophy (attitude/stance) on risk.

Element 1.3 Understand the risk management strategies of the organization

- 1.3.1 Identify the key 'risk drivers' facing the organization, through appropriate forms of analysis, interaction and involvement
- 1.3.2 Identify the policies/practices used to manage risk with respect to each key driver
- 1.3.3 Identify responsibilities for risk management in relation to each key driver
- 1.3.4 Consolidate/express the organization's policies/practices for risk management as strategies.

Element 1.4 Provide advice/recommendations relating to the organization's risk management philosophies, strategies, and their implementation.

- 1.4.1 Review/assess the risk management strategies of the organization from the perspective of best practice
- 1.4.2 Review/assess the risk management strategies of the organization relative to their degree of organizational implementation/understanding
- 1.4.3 Review/assess the level of integration between the organization's philosophies on risk and its risk management strategies
- 1.4.4 Assess the vulnerability of the organization's risk management strategies to contextual shifts
- 1.4.5 Develop advice/recommendations on risk management within the organization, and negotiate these in relevant settings.

TIPS FOR BEST USE OF A RISK MODEL

1. Negotiate your involvement in business risk management and position your function and yourself to contribute and add value.
2. Remember, the model is *just the tool*, not the end result of the risk analysis. Don't get carried away with the analysis and the use of the model. Use simple tools.
3. Recognise and respect the risk-taking responsibilities of managers.
4. Focus on the key risks that (properly) concern managers and don't get caught up on detailed analysis of risks that may not mean much.
5. Develop *sensitivity and awareness* about your organization's exposure to risk.
6. Watch newspaper and business magazine articles, and learn how to *migrate and adapt* other organizations' experiences to your organization.
7. Assess *inherent risks* before considering the application of control systems, don't just assess the residual risks.
8. Develop *future scenarios* as the way to explain and justify your concern about *future risks* and the application of *current control systems*.
9. In risk assessment, *forget likelihood and remember 'Murphy's experience'*:
"If something can go wrong, it will, at the worst possible moment!!"
10. Talk and work with others in your organization involved in business risk management. Get their perspective on risk and develop your own perspective.

SUMMARY

Internal auditors can contribute to business risks management at three levels:

1. Developing the organization's strategies;
2. Making the investment decisions;
3. Managing operations.

This involvement by the internal auditor has substantial support from authoritative references and risk models, which guide the auditor's approach and methods:

- Dynamic contexts need to be understood as the *source of risk*;
- Identified risks need to be assessed against relevant criteria;
- Risk treatment options need to be considered for adequacy and effectiveness;
- Effective business risk management improves business results.