Risk Management Seminar – June 2017
Compiled by:
Raaghielb Najjaar, Yaeesh Yasseen & Rashied Small
Defining Risk

- Risk reflects the chance that the actual event may be different than the planned/expected event.

- The effect of an uncertainty that could have a negative impact on achieving the business objectives.

- Upside risk – the uncertainty of the possibility of making gains (potential opportunities)

- Downside risk - the probability that losses or negative outcomes will occur (mitigate negative outcomes)
Brain Teaser #1

Discuss whether the following represents a risk to the organisation:

1. The organisation budgeted an annual amount of R 3.7 million for salaries and wages. The actual expenses incurred amounted to R 4 million.

2. The organisation budgeted an amount of R 26 million for revenue. The accounting recorded reflected an annual revenue of R 31.2 million.

3. The business owner is prepared to take any income generating opportunity irrespective of the potential losses.

4. The business organisation strategic objectives is to maximise profit.
Hierarchy of Risk

Strategic decisions
Decisions transferring strategy into action
Decisions required for implementation

Strategic
Programme
Project and operational

Uncertainty
Brain Teaser #2

Discuss whether the following statements are True / False:

1. An organisation with no strategic objective or goal seldom encounters risk in its business activities.

2. An organisation with a clearly defined strategic objective is more likely to manage potential risk.

3. The potential for risk occurring at operational level is often attributed that managers do not take accountability.
Understanding Risk

What road do I take?

Well where are you going?

I don’t know.

Then it doesn’t matter. If you don’t know where you are going, any road will get you there.

If you can’t explain it *simply*, you don’t understand it well enough.

– Albert Einstein
Brain Teaser #3

Discuss whether the potential risks and/or challenges encountered in:

1. An accounting practice

2. An organisation conducting business locally and internationally
# Types of Risks

<table>
<thead>
<tr>
<th>Business/Operational Risk:</th>
<th>Financial Risk:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Strategy risk</td>
<td>- Cash flow risk</td>
</tr>
<tr>
<td>- Product risk</td>
<td>- Credit risk</td>
</tr>
<tr>
<td>- Operating risk</td>
<td>- Liquidity risk</td>
</tr>
<tr>
<td></td>
<td>- Interest rate risk</td>
</tr>
<tr>
<td></td>
<td>- Currency risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environmental Risk:</th>
<th>Reputational Risk:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Political risk</td>
<td></td>
</tr>
<tr>
<td>- Economical risk</td>
<td></td>
</tr>
<tr>
<td>- Social risk</td>
<td></td>
</tr>
<tr>
<td>- Technological risk</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Risk

Financial Risk
- Market
- Interest, FX, Commodity
- Credit & counter-party
- Liquidity
- COMPLIANCE
- Dodd-Frank
- IASB

Business Risk
- Industry
- Location
- Business strategy
- Environmental
- COMPLIANCE
- Companies Act
- Sarbanes Oxley
- Tax

Operational Risk
- Business continuity
- System
- Supplier
- COMPLIANCE
- Sarbanes Oxley
- Health & Safety

Enterprise Risk
Types of Business Risks

Figure 2: Risks to business

- **Strategic**
  - Demand shortfall
  - Customer retention
  - Integration problems
  - Pricing pressure
  - Regulation
  - R&D
  - Industry or sector downturn
  - JV or partner losses

- **Operational**
  - Cost overrun
  - Operating controls
  - Poor capacity management
  - Supply chain issues
  - Employee issues, including fraud
  - Bribery and corruption
  - Regulation
  - Commodity prices

- **Hazard**
  - Macroeconomic
  - Political issues
  - Legal issues
  - Terrorism
  - Natural disasters

- **Financial**
  - Debt and interest rates
  - Poor financial management
  - Asset losses
  - Goodwill and amortisation
  - Accounting problems
Business Risks

Four Quadrants of Business Risk

- Operational Risk
  - Bid Process
  - Information Transfer
  - Construction Management
  - Accounting Process

- Financial Risk
  - Cost of Capital
  - Growth Capitalization
  - Market Risk
  - Bank & Surety Support

- Strategic Risk
  - Customer/Industry Changes
  - Growth Strategy
  - Branding/Image
  - Competition

- Hazard Risk
  - Employee Injury/Illness/Theft
  - Third-party Liability
  - Natural Hazards
  - Property Loss
Internal Operational Risks

Operational Risk

People
- Skills / Competence
- Training
- Absenteeism

Processes
- Qualitative risk
  - CRM - satisfaction

Technology
- Quantitative risks
- Changes / outdated
- Efficiency risk
- Functionality
External Risks

- Reputation
- Competition
- Regulatory environment
- Stakeholders
- Financing
- Natural disaster
Brain Teaser #4

Discuss and rate (scale of 1 – 10) the external risks encountered by the Professional Accountant:

- Reputation
- Competition
- Regulatory environment
- Stakeholders
- Financing
- Natural disaster
Risk Management

• Risk management refers to the process designed to reduce or eliminate the risk of certain kinds of events happening or having an impact on the business - process for identifying, assessing and prioritizing risks.

• Enterprise Risk Management is defined as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” - COSO
These are the high level goals that are aligned with and support the institution’s mission.
ERM – Operations Level

Relate to the ongoing management process and daily activities of the organization.
ERM – Reporting Level

Relates to the organization’s adherence to applicable laws and regulations.
ERM – Compliance Level

Relates to the protection of the organization’s assets and quality of financial reporting.
ERM – Operations Level

The Internal Environment relates to the general culture, values and environment in which an organization or entity operates (e.g. tone at the top).
Risk Management Model
Risk Management Process
Establishing the Risk Context

• Establish the context by identifying the objectives of the project, event or relationship and then consider the internal and external parameters within which the risk must be managed.

• Establishing the context sets the framework within which the risk assessment should be undertaken, ensures the reasons for carrying out the risk assessment are clearly known, and provides the backdrop of circumstances against which risks can be identified and assessed.
Establishing the Risk Context

• Set the scope for the risk assessment by identifying what you are assessing

• Define the broad objectives and identify the reason for the risk assessment

• Identify the relevant stakeholders, the areas that might be impacted and seek their input - inclusive process

• Gather background information by ask the right people and identify the information that is available as well as information that is not available (immediately) but may be necessary
Establishing the Risk Context

When gathering information consider:

• Strategic & business plans
• Reports such as financial statement, inspections, site visit
• Personal experience of staff
• Corporate knowledge & ‘institutional memory’
• Previous event investigations or reports
• Surveys, questionnaires and checklists
• Insurance claim reports
• Business experience (local or international)
• Structured interviews or Focus group discussion
• Historical records
Context of Risk - Business Model

- **Growth Strategy**: How we plan to grow and what we hope our organization will be in 5 years. Do we plan to sell and if so to, who and where?

- **Partners**: Who will we need to partner with or the input we are dependent on in order to develop/deliver the value proposition. How does well the gap?

- **Cost Base**: €
  - How much will it cost to initially develop the value proposition and how much it will cost to subsequently market and deliver it?

- **Value Proposition**: The offer to the consumer including how and why it addresses their need/fulfills their job to be done. How consumers themselves would describe the benefit.

- **Channel**: How the value proposition is delivered to the customer (distribution, channel), and how it is communicated to them (marketing channel).

- **Market Segments**: What group(s) of people benefit from value proposition. How many there are rewarded in the future.

- **Pricing Model**: How we will price the proposition, whether it be fixed, variable or subscription pricing. Includes alternative sources of revenue, particularly important if the consumer is not expected to pay.

- **Competitive Strategy**: Who the existing competitors are and how we will react to them and likely new entrants into this space. Why will we win?

- **Fixed BM**

---

**Context of Risk**

- **Business Model**

---

**Risk Management - June 2017**
Brain Teaser #5

Identify possible risks associated with each of the segments in the business model:

- Market segment
- Channels of delivery
- Resources/capacity
- Operational segment
Risk Assessment – Business Model

- Do current applications meet business needs?
  - Can service vendor applications meet the need?

- What technologies can support the business needs?
  - Are service vendor technologies appropriate to business needs?

- What process elements require company ownership?
  - What processes are high volume / repeatable transactions?

- Can more resources improve data quality by applying simple business rules?
  - Consistent business rules for data management?

- Do company resources have the necessary skills to fulfill business needs?
  - Do service vendor resources have the necessary skills?

- Are process turnaround times sensitive to location of resources?
Porter’s 5 Forces

Threat of New Entry
- Time and cost of entry
- Specialist knowledge
- Economies of scale
- Cost advantages
- Technology protection
- Barriers to entry

Competitive Rivalry
- Number of competitors
- Quality differences
- Other differences
- Switching costs
- Customer loyalty

Supplier Power
- Number of suppliers
- Size of suppliers
- Uniqueness of service
- Your ability to substitute
- Cost of changing

Threat of Substitution
- Substitute performance
- Cost of change

Buyer Power
- Number of customers
- Size of each order
- Differences between competitors
- Price sensitivity
- Ability to substitute
- Cost of changing
Establishing the Risk Context

Establishing context for a Supply Risk evaluation...

- Supplier Performance
  - Delivery performance
  - Product performance
  - Agility - Response to changes
- Buyer exposure to Supplier
- Supplier market share in buyer’s industry
- Supplier exposure to other Value Chains
- Market reputation
- Brand recognition
Identification of Risk

• Risk identification involves identifying sources of risk, areas of impact, events and their causes and consequences - risk of doing nothing and missing an opportunity

• Identify sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences

• Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of your objectives.
Identification of Risk

Questions to identify risk

- What could go wrong?
- What caused the risk?
- Where did it happen?
- Why did it happen?
- What is the impact?
- Who owned the risk?
Identification of Risks

- Collaborative discussions
  - Interviews
  - Patterns/common lists
  - Expert judgement
  - SWOT analysis

- Assess probability
- Assess impact
- Assess urgency
- Qualitative analysis

- Architectural
  - Security
  - Quality
  - Team and organizational
  - Schedule
  - Financial

- Light-weight description
  - Detailed description

- Risk backlog
  - Risk list
  - Risk register/database

- Information radiators
  - Informal reviews
  - Audit/formal reviews
Identification of Risk

• Identify risks early in the process or project

• Identify risks in an iterative and holistic manner

• Identify risks with a consistent frequency – ongoing and regularly

• Identify risks when change control is performed

• Identify risks when major milestones are achieved
Identifying Risks

Methods used to Identify Project Risks

- Documentation Reviews
- Information Gathering
- Checklist Analysis
- Assumptions Analysis
- Diagramming
- SWOT Analysis
- Expert Judgment
Identification of Risk

- SWOT
- Interview
- Brainstorming
- Delphi Technique
- Assumptions
- Checklist
- Documentation
SWOT Analysis

Favourable

Internal

- What are your strengths?
- What do you do better than others?
- What unique capabilities and resources do you possess?
- What do others perceive as your strengths?

External

- What trends or conditions may positively impact you?
- What opportunities are available to you?

Unfavourable

Weaknesses

- What are your weaknesses?
- What do your competitors do better than you?
- What can you improve given the current situation?
- What do others perceive as your weaknesses?

Threats

- What trends or conditions may negatively impact you?
- What are your competitors doing that may impact you?
- Do you have solid financial support?
- What impact do you weaknesses have on the threats to you?
PEST Analysis

Political
- Political Stability
- Proper laws and legal framework
- Proper IPR protection
- Government policies
- Favorable tax policies
- Favorable labor laws
- Favorable policies for foreign investment
- Proper Security

Technological
- Technological Development
- Innovation
- R&D
- Skilled resources
- Easier acceptance of new technologies
- Information and Communication

Economical
- Economic Industrial Growth
- GDP Per Capita
- Purchasing Power Parity
- Number of Consumers
- Interest and Inflation rate
- Exchange rate and currency stability
- Unemployment rate
- Investment Opportunity
- Trade Balance

Social
- Demographic including growth rate, sex ratio, age distribution, population density etc.
- Social culture and lifestyle
- Basic and Higher Education
- Human Development Index
- Social safety and benefits
Delphi Method

**Step 1:** Facilitator seeks individual assessments from a pool of experts.

**Step 2:** Experts respond to the request, receive feedback and revise their responses.

**Step 3:** Facilitator compiles the responses and sends a revised set of questions to each expert. Several cycles of feedback may be needed.

**Step 4:** Experts respond to the revised set of questions.

**Step 5:** Facilitator compiles the responses from the experts.

**Step 6:** Experts respond to the compiled responses.

**Step 7:** Final report

Facilitator produces report on experts’ responses, noting key outliers.
Brain Teaser #6

Professional Accountants performing the compilation, review or audit of financial statements use the following statement extracted from the relevant report included in the financial statements to limit their risks when business faces financial and business risk:

“The preparation of the financial statements set out on pages 3 to 13 are the responsibility of the member. We have ascertained that the financial statements are in agreement with the accounting records, summarized in the manner required by section 58(2)(d) of the Act, and have done so by adopting such procedures and conducting such enquiries in relation to the books of accounts and records as considered necessary in the circumstances.”

Discuss the possible reasons why the Professional Accountants may be held liable for the financial and business risks faced by organisation.
Identification of Risk - Pitfalls

• Risks are not identified early when it is less expensive to address

• Risks are not identified in an iterative manner

• Risk are not identified with appropriate stakeholders

• Risk are not identified using a combination of risk identification techniques

• Risks are not captured in one location

• Risks are not visible and easily accessible.

• Risks are not captured in a consistent format (e.g., Cause -> Risk -> Impact).
Analysis of Risk

• Risk analysis is the systematic study of uncertainties and risks encountered in business and many other areas. Risk analysts seek to identify the risks, understand how and when they arise, and estimate the impact (financial or otherwise) of adverse outcomes.

• This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the company.
Analysis of Risk

Assess the likelihood of the risk occurring – measuring the probability of occurrence

Assess the consequence/impact if the risk occurred – measuring the frequency or severity

The risk matrix then determines whether the risk rating is low, medium, high or extreme
Types of Risks

Inherent Risk
The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)

Control Risk
Risk of loss arising from internal control systems to lose their effectiveness and thus expose or fail to prevent exposure of the objective they were to protect.

Detection Risk
Risk to detect a material misstatement in the financial statements.

Residual Risk
The risk that remains after controls are taken into account (the net risk or risk after controls).
Residual Risk

Residual risk is the risk that remains after risk treatment has been applied to reduce the potential consequences.

Inherent Risk

Residual Risk

Controls
Analysing Risks - Methods

- **Risk Analysis**
  - **Qualitative Risk Analysis**
    - Risk Register
    - Probability-Impact (PI) Matrix
    - Risk Categorization
    - Expert Judgement
  - **Quantitative Risk Analysis**
    - Sensitivity Analysis
    - Decision Tree Analysis
    - Scenario Analysis
    - Latin Hyper Cube Simulation
    - Monte Carlo Simulation
Risk Impact Assessment

• Risk impact assessment is the process of assessing the probability (likelihood) and consequences of the events if they are realised.

• The results of the assessment are used to prioritise risks to establish a most-to-least critical importance ranking.
Risk Impact Analysis

1. Risk Identification
- Risk events and their relationships are defined
- Assess Probability & Consequence
- Watch-listed Risks
- Assess Risk Criticality
- Decision-analytic rules applied to rank-order identified risk events from "most to least" critical

2. Risk Impact Assessment
- Probabilities and consequences of risk events are assessed
- Consequences may include cost, schedule, technical performance impacts, as well as capability or functionality impacts

3. Risk Prioritization Analysis
- Risk events assessed as medium or high criticality might go into risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

4. Risk Mitigation Planning, Implementation, and Progress Monitoring
- Reassess existing risk events and identify new risk events

Identify Risks
Risk Analysis Matrix
## Risk Management - June 2017

### Brain Teaser #7

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Description</th>
<th>Likelihood occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Certain</td>
<td></td>
</tr>
</tbody>
</table>
## Risk Likelihood Descriptor

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Description</th>
<th>Likelihood occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare</td>
<td>Highly unlikely, but it may occur in exceptional circumstances, but probably never will</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>Not expected, but there is a slight possibility it may occur at some time</td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td>The risk might occur at some time as there is a history of casual occurrence in the business or similar businesses (industry)</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>There is a strong possibility the risk will occur as there is a history of frequent occurrence in the business or similar businesses (industry)</td>
</tr>
<tr>
<td>5</td>
<td>Certain</td>
<td>Very likely as the risk is expected to occur in most circumstances as there is a history of regular occurrence in the business or similar businesses (industry)</td>
</tr>
<tr>
<td>Risk Rating</td>
<td>Description</td>
<td>Financial impact</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td></td>
</tr>
</tbody>
</table>
## Risk Likelihood Descriptor

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Description</th>
<th>Financial impact</th>
<th>Business interruption</th>
<th>Reputational impact</th>
<th>Business objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Minimal financial loss</td>
<td>Negligible as risk does not affect operations</td>
<td>Negligible impact externally</td>
<td>Resolved as part of day-to-day management activities</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Limited loss exposure</td>
<td>Inconvenient to function of operations</td>
<td>Adverse effect which may impact on customers</td>
<td>Minor impact which require investigation</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Acceptable loss exposure</td>
<td>Limited disruption to the operations</td>
<td>Directly affecting customer relationships</td>
<td>Significant impact which require management intervention</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Negative impact of performance</td>
<td>Systems failure which causes temporary disclosure</td>
<td>Negatively affect the reputation of the business</td>
<td>Major impact which require senior management intervention</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Financial disaster</td>
<td>Systems failure which require major interventions</td>
<td>Result in regulatory investigations and threaten business closure</td>
<td>Disastrous impact which require strategic decision</td>
</tr>
</tbody>
</table>
## Risk Classification

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Consequence</th>
<th>Risk Class</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
<td>Critical</td>
<td>Marginal</td>
</tr>
<tr>
<td>Frequent</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Probable</td>
<td>I</td>
<td>I</td>
<td>II</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>Remote</td>
<td>II</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Improbable</td>
<td>III</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Incredible</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
</tr>
</tbody>
</table>
## Risk Ranking

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>ACTIONS</th>
<th>LIKELIHOOD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIGNIFICANT</strong></td>
<td>Considerable Management Required</td>
<td>Must Manage and Monitor Risks</td>
</tr>
<tr>
<td>MODERATE</td>
<td>Risk are bearable to certain extent</td>
<td>Management effort worthwhile</td>
</tr>
<tr>
<td>MINOR</td>
<td>Accept Risks</td>
<td>Accept but monitor Risks</td>
</tr>
<tr>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Risk Management - June 2017
Risk Classification

Intolerable Region

ALARP or tolerability region
(Risk is undertaken only if the benefit is desired)

Broadly acceptable region
(No need for detailed working to demonstrate ALARP)

Risk cannot be justified except in extra-ordinary circumstances

Tolerable only if further risk reduction is impracticable or if the cost is grossly disproportionate to the improvement gained

As the risk is reduced, the less proportionate it is necessary to spend to reduce it further to satisfy APARP. The concept of diminishing proportion is shown by the triangle

It is necessary to maintain assurance that the risk remains at this level

ALARP = As Low As is Reasonably Practical
Evaluation of risk

• Risk evaluation is a process conducted to decide whether the risk is acceptable or unacceptable with the specific purposes of making decisions about future actions.

• Decisions about future actions may include:
  • not to undertake or proceed with the event, activity, project or initiative
  • actively treat the risk
  • prioritising the actions needed, if the risk is complex and treatment is required
  • accepting the risk
Risk Appetite & Risk Tolerance

- **Risk Appetite**: "The amount and type of risk an organization is willing to accept in pursuit of its business objective".

- **Risk Tolerance**: "The maximum amount and type of risk an organization is willing to tolerate".

- **Risk Capacity**: "The maximum level of risk an organisation may run given its capital and liquidity position and other restrictions".

- **Risk Universe**: "All potential risks of the organization".
Risk Appetite & Risk Tolerance

- Risk appetite is a broad-based description of the desired level of risk that the organisation is willing to take in pursuit of its strategy objective.

- Risk Tolerance reflects the acceptable variance in the outcomes related to the strategic action taken – ability to tolerate downside risk.
Risk Appetite & Risk Tolerance

Risk appetite/tolerance/target example

- Risk tolerance
- Actual risk position
- Risk limit (high end)
- Risk limit (low end)

Risk exposure

- Actual risk exceeds risk tolerance, must reduce net risk position
- Actual risk exceeds risk limit, manage down unless returns justify risk position
- Actual is less than risk limit, add more risk unless return is not adequate

Risk target
### Risk Register

<table>
<thead>
<tr>
<th>Risk ID #</th>
<th>Risk Statement (Description)</th>
<th>Probability of Occurrence</th>
<th>Impact</th>
<th>Score (Probability \times Impact)</th>
<th>Risk Trigger</th>
<th>Risk Owner</th>
<th>Planned Response(s) (Description)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Register - Content

When documenting a risk assessment record the following information within the risk register:

• A description of the risk (setting the context)
• Causes or contributing factors
• Consequences of the risk – actual or potential
• Current controls in place that help manage the risk
• An assessment of the likelihood and consequence based on current or existing controls to rate each risk
• Actions or treatments needed to address the risk
• Progress updates as the treatments are implemented
• Results from monitoring and review, including effectiveness of controls
Risk Register - Value

By formally recording risks the benefits to the organisation are:

• commit to continuous learning;

• obtain benefits for reusing information for management purposes;

• minimise costs & efforts of creating & maintaining records;

• maximise access & retrieval of information; and

• comply with retention periods; and recognise the sensitivity of the information.
Treatment of Risk

Risk treatment takes place in two distinctive contexts:

• Proactive context - where an organisation has successfully integrated risk management into a system of management. Risk treatment is integral to and effectively indistinguishable from decision-making. Therefore, at the time a decision is finalised the risk created by the decision will be within the organisation’s risk criteria.

• Reactive context - the organisation is looking retrospectively at the risk created by decisions taken and implemented previously, and so any risk treatments found necessary will be remedial in nature.
Treatment of Risk

• Treatment of risk ensures that effective strategies are in place to minimise the frequency and severity of the identified risk - develop actions and implement treatments that aim to manage, control or mitigate the risk.

• Treatment options not applied to the source or root cause of a risk are likely to be ineffective and promote a false belief within the organisation that the risk is controlled.
Treatment of Risks

Risk treatment options:

• Avoid the risk by not starting or continuing an activity
• Take or increase risk in order to pursue an opportunity
• Remove the risk source
• Change the likelihood
• Change the consequence
• Share the risk e.g. through Insurance, contracts, financing
• Retain the risk by informed decision
Treatment of Risk
Brain Teaser #9

SME owners usually conclude that it is often to cost to mitigate risks and are therefore willing to accept risks and deal with the consequences.

Discuss the circumstances under which risks may be accepted.
Treatment of Risks

A risk may be acceptable or tolerable in the following circumstances:

• No treatment is available

• Treatment costs are prohibitive (particularly relevant with lower ranked risks)

• The level of risk is low and does not warrant using resources to treat it

• The opportunities involved significantly outweigh the threats

A risk is regarded as acceptable or tolerable if the decision has been made not to treat - does not imply that the risk is insignificant.

-- Mark Twain

Throw off the bowlines,
Sail away from the safe harbor,
Catch the tradewinds in your sails.

Treatment of Risks

Opportunity
- Exploit
- Share
- Enhance
- Ignore

Strategy
- Eliminate Uncertainty
- Re-Allocate Ownership
- Modify Exposure
- Communicate & Monitor

Threat
- Avoid
- Transfer
- Reduce
- Accept
Treatment of Risks

Acceptance/Retention
If, after controls are put in place, the residual risk is deemed acceptable. However, plans should be put in place to manage/fund the consequences of the risk should it occur.

Reduction
Implement a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense.

Share/Transfer
Implement a strategy that shares or transfers the risk to another party, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk.

Avoidance
Deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process.
Treatment of Risk – Developing a Plan

Determine the level of treatment plans required for each risk level that have improvement opportunities. Effective risk treatment relies on attaining commitment from key stakeholders and developing realistic objectives and timelines for implementation.

For each risk identified in the risk assessment, detail the following:

• Specify the treatment option agreed - avoid, reduce, share/transfer or accept.

• Document the treatment plan - outline the approach to treat the risk. Any relationships or interdependencies with other risks should also be highlighted.

• Assign an appropriate owner - who is accountable for monitoring and reporting on progress of the treatment plan. Where the plan owner and the risk owner are different, the risk owner has ultimate accountability for implementing the plan.

• Specify a target resolution date - where risk treatments have long lead times, consider the development of interim measures.
Treatment of Risk - Implementation

The treatment plan owner is responsible for coordinating activities that ensure risk treatments are implemented. The owner may not be directly responsible for implementing the risk treatment plans, however, they are responsible for ensuring that plans are completed within the expected timeframe.

When implementing a treatment plan, consider how the initiatives will be supported:

• Firm structure – Is there a need for any change to structure or delegations of responsibilities to support the risk treatment plan?

• Financing - If the budget for control improvement is constrained, should there be a process to prioritise controls with the greatest need or cost benefit?

• Resource availability - Does the firm have sufficient physical, human or financial resources to implement the risk treatment plan?

• Communication with stakeholders - Does the firm need to commence briefing sessions to inform stakeholders as to what changes are required and why?
Treatment of Risk - Implementation

For each risk identified in the risk assessment, detail the following:

• Monitoring mechanisms and review points - The treatment plan owner should specify the mechanisms by which implementation will be monitored. This may include indicators to determine if the risk is increasing or decreasing. Successful implementation will usually be linked to business planning activities and will be reviewed regularly at meetings.

• Status of the treatment plan - the status of the treatment plan is either ‘open' for in progress or ‘closed' when implementation has been completed. If the status is closed and the risk has been eliminated, it may be removed from the current risk register into a closed items register. Where a risk is not eliminated, it should be retained in the current register and if another treatment plan is required this should be agreed or, if no other action is possible, the treatment agreed could be to accept and monitor the risk.
<table>
<thead>
<tr>
<th>RISK IDENTIFICATION</th>
<th>RISK TREATMENT</th>
<th>Risk Owner</th>
<th>Resolve by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to meet compliance obligations</td>
<td>Implement formal compliance monitoring process:</td>
<td>Practitioner</td>
<td>30-Sep-12</td>
</tr>
<tr>
<td></td>
<td>1. Identification of compliance requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Identification of system or tool to manage compliance requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Monthly review of compliance requirements to ensure there have been no material compliance breaches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of Risk Practitioner</td>
<td>Implement succession plan:</td>
<td>Practitioner</td>
<td>31-Oct-12</td>
</tr>
<tr>
<td></td>
<td>1. Put in place power of attorney arrangements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Document key processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Put in place a key client management system to ensure adequate documentation is maintained for key clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Adequately train a secondary level of management and/or identify a potential candidate for partner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure to collect receivables in a timely manner</td>
<td>Implement receivables tracking and debtor follow-up process:</td>
<td>Office Manager</td>
<td>15-Sep-12</td>
</tr>
<tr>
<td></td>
<td>1. Identify requirements to track receivables, consider such things as payment terms and conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Develop process to track aged debtors/receivables and supporting requirements including system reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Consider monitoring requirements including frequency.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring & Evaluation of Risks

• Monitor changes to the source and context of risks, the tolerance for certain risks and the adequacy of controls. Ensure processes are in place to review and report on risks regularly.

• To ensure structured reviews and regular reporting occurs and each area is encouraged to identify a process that allows key risks within their area to be monitored.

• Given the diverse and dynamic nature of the business environment, it is important to be alert to emerging risks as well as monitoring known risks.
Monitoring & Evaluation of Risks

Continuous monitoring:

Once risks have been identified, recorded, analysed, and the agreed treatments have been implemented, an appropriate monitoring and reporting regime needs to be established to provide assurance that the treatment has been effective and now helps to control the risk. Some risk treatments will of course become embedded into daily practices and methods of work. The frequency of review will depend on the risk rating, the strength of controls and the ability to effectively treat the risk.
Monitoring & Evaluation of Risks

Departmental / Entity Management review:
Managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. Wherever possible, risk management should become an agenda item on management meetings or committees and avoid the need for separate processes. The aim of regular review is to identify when new risks arise, and to monitor existing risks to ensure that treatments or controls are still effective and appropriate. How frequently a review process and reporting cycle occurs will depend on the risk appetite and level of risk tolerance but local management review is required.
Monitoring & Evaluation of Risks

Internal audit:
The organisation’s internal audit program provides for a review of systems, policies and process assurance and compliance. The auditors apply a risk-based approach to the audit program and help bring a measure of independence and external perspective to the organisation Risk Management Framework.

External audit:
That external audit covers financial, governance, contracting, IT and risk management systems and processes. Management and staff may be required to respond to the risk management activities involved with these audits. Other audits occur from time to time and are imposed through contracts, compacts, and regulation.
Corruption & Fraud Risk Management

Brainstorming

Risk Assessment Team

IT on fraud risks

Incentives

Regulatory and legal misconduct and reputation risk

Pressures

The population of fraud risks relevant to the organization

Opportunities to commit fraud

Risks of management override of controls

Fraud Risk Identification
Corruption & Fraud Risk Management

Fraud Risk Management

1. Identity Potential Inherent Risk
2. Assess Likelihood of the Identified Fraud Risk
3. Evaluate Potential Suspects
4. Evaluate whether the identifier controls are operating effectively & efficiently
5. Identify & map out the existing prevention and detective controls to reduce fraud risks
6. Evaluate their possible methods
7. Identify & evaluate fraud risks regarding ineffective or non-existent controls
8. Respond to residual fraud risks

Source: Managing the business risk of fraud 2008 ACFE
Corruption & Fraud Risk Management

An Approach to Fraud Risk Management – The Anti-fraud Roadmap

<table>
<thead>
<tr>
<th>Evaluate</th>
<th>Identify</th>
<th>Action Plan</th>
<th>Mitigate</th>
<th>Monitor</th>
<th>Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate current status and effectiveness of an organization’s approach to implementing antifraud programs and controls</td>
<td>Assess, define, and document fraud risks and control effectiveness. Establish fraud risk profile by analysis of risk against controls</td>
<td>Develop a fraud action plan based on findings and identify activities that define next steps to address an organization’s antifraud program activities</td>
<td>Enhance, implement, and maintain preventative and detective control activities, which mitigate fraud risks identified during assessment</td>
<td>Enable continuous monitoring activities through technology and ongoing review activities to alert management of potential fraud. Incorporate findings into annual fraud risk assessment process</td>
<td>Assist in responding to potential occurrences of fraud</td>
</tr>
</tbody>
</table>

- Internal Survey
- Fraud Risk Assessment
- Fraud Risk Action Plan
- Fraud Awareness Training
- Continuous Monitoring Tools
- Fraud Case Management Tools
- Diagnosis of Current Position
- Mitigate Deficiencies
- Data Analytics
- Fraud Response
Corruption & Fraud Risk Management

PREVENT
- Mitigate fraud through strong internal controls procedures.
- Preventive fraud controls/mechanisms includes Code of Conduct and Ethical Standards, Training, Employee and 3rd Party Due-Diligence

RE-ASSESS
- Based on fraud trends re-assess the fraud related preventive and detective controls

RESPOND
- Investigate
- Take Remedial Action
- Disclosure Protocol

DETECT
- Detection mean identification of frauds after it has occurred
- Mechanisms include Hotlines and Whistle Blower complaints, auditing & monitoring and proactive forensic data analytics
Financial Risk
Financial Risk

![Financial Risk Diagram]

- **Market Risk**
  - Absolute Risk
  - Relative Risk
  - Directional
  - Non-directional
  - Basis Risk
  - Volatility Risk

- **Credit Risk**
  - Credit event
  - Sovereign Risk
  - Settlement Risk

- **Liquidity Risk**
  - Asset liquidity
  - Funding liquidity

- **Operational Risk**
  - Fraud Risk
  - People Risk
  - Model Risk
  - Legal Risk
Types of Risks

Inherent Risk
The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls).

Control Risk
Risk of loss arising from internal control systems to lose their effectiveness and thus expose or fail to prevent exposure of the objective they were to protect.

Detection Risk
Risk to detect a material misstatement in the financial statements.

Residual Risk
The risk that remains after controls are taken into account (the net risk or risk after controls).
Financial Statement - Risk

• Financial statement risk is defined as the risk that financial statements may be materially misstated and thus does not satisfy the qualitative characteristics of financial statements as per the Accounting Framework standard.

• Financial statement risk implies that the financial statements may not in whole or part fairly represent the financial performance and position of the business and therefore may not be considered to be reliable.
Some Advice on Risk

Entrepreneurs’ risk taking behavior

- Risk taking is a **skill** need to be learned
- Do not fear to take **calculated** or **moderate** risks
- Do not take risks **unnecessarily**
- Perceive risk as **opportunity** rather than as **threat**
- Perceive risk as **challenge** that triggers them to behave entrepreneurially
Summary – Risk Management

- **Risk Assessment**
  - Identification
  - Measurement
  - Prioritization

- **Risk Management**
  - Control It
  - Share or Transfer It
  - Diversify or Avoid It

- **Risk Monitoring**
  - Process Level
  - Activity Level
  - Entity Level
time for questions
Risk Management- References

1. The University of Adelaide RISK MANAGEMENT HANDBOOK
docplayer.net/4489777-The-university-of-adelaide-risk-management...


3. Eurojuris Risk management Manual | EUROJURIS International
www.eurojuris.net/en/node/41583

www.dot.ca.gov/hq/projmgmt/documents/prmhb/archive/caltrans...