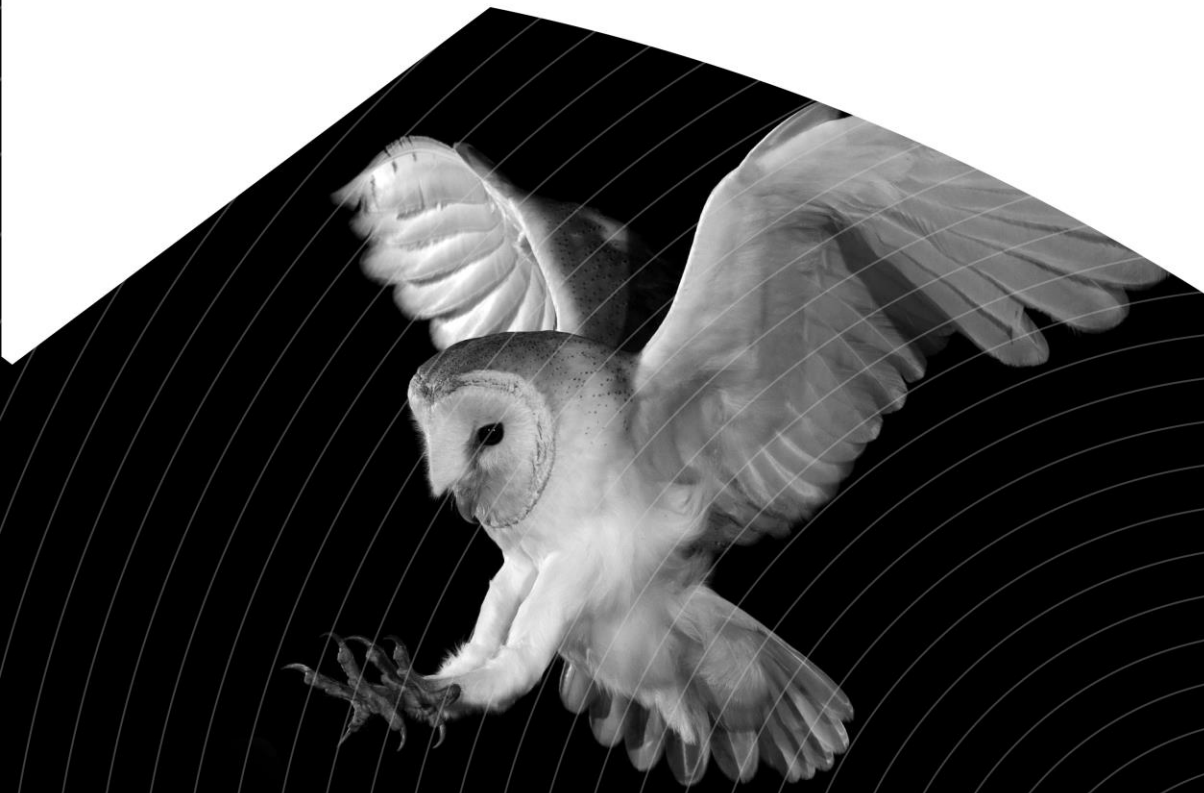


BARNOWL

IDI Technology Solutions (Pty) Ltd
Jonathan Crisp – Director

Western Cape Risk & Audit Forum

24 July 2018

RISK APPETITE AND TOLERANCE

ISO theory

Risk Appetite - *"Amount and type of risk an organisation is prepared to take in order to achieve its objectives"*

- Difficult to define – especially for non-tangible consequences (safety, environmental etc.)
- Changes over time as it is linked to context (external and internal)
- Changes with experience/capabilities built by the organisation
- A complex and sophisticated concept that is often over-used – be careful … ensure it is practical and will aid decision making!
- Risk criteria combined with an organisation's consequence table is a good start – a recognised vehicle to achieve the above

Risk Tolerance - *"Organisation's readiness to bear risk after risk treatment, in order to achieve its objectives*

- It forms part of the evaluation of risk and involves cost benefit analysis when considering risk treatment

COSO and ISO Definitions (Norman Marks)

https://normanmarks.wordpress.com/2011/04/14/just-what-is-risk-appetite-and-how-does-it-differ-from-risk-tolerance/

Let's look first at the **COSO ERM Framework**. It defines risk appetite as "the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value." In their Strengthening Enterprise Risk Management for Strategic Advantage, COSO says:
"An entity should also consider its risk tolerances, which are levels of variation the entity is willing to accept around specific objectives. Frequently, the terms risk appetite and risk tolerance are used interchangeably, although they represent related, but different concepts.

Risk appetite is a broadbased description of the desired level of risk that an entity will take in pursuit of its mission. Risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.

So, to ISO. Here are a few definitions from **ISO Guide 73, *Risk Management – Vocabulary***.
•**Risk attitude:** organization's approach to assess and eventually pursue, retain, take or turn away from risk
•**Level of risk**: magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood
•**Risk criteria:** terms of reference against which the significance of a risk is evaluated
•**Risk evaluation:** process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
•**Risk appetite**: amount and type of risk that an organization is willing to pursue or retain
•**Risk tolerance**: organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

It is worth noting that the ISO 31000:2009 standard doesn't use all these terms. Rather than getting into a detailed discussion around risk appetite and tolerance, the standard says you should establish risk criteria and then evaluate risks against those criteria to determine which risks need treatment.

BARNOWL

E&Y definition (Norman Marks)

Ernst & Young has an interesting perspective, which they explain in Risk Appetite: the strategic balancing act. In the referenced PDF version, they include definitions of multiple terms:

- **Risk capacity:** the amount and type of risk an organization is able to support in pursuit of its business objectives.
- **Risk appetite:** the amount and type of risk an organization is willing to accept in pursuit of its business objectives.
- **Risk tolerance:** the specific maximum risk that an organization is willing to take regarding each relevant risk.
- **Risk target:** the optimal level of risk that an organization wants to take in pursuit of a specific business goal.
- **Risk limit:** thresholds to monitor that actual risk exposure does not deviate too much from the risk target and stays within an organization's risk tolerance/risk appetite. Exceeding risk limits will typically act as a trigger for management action.

There are similarities to the COSO ERM definitions, with both using *appetite* for the organization's overall acceptable level of risk, and *tolerance* to describe risk at a lower, more granular level.

A colleague with IIA Canada, Eric Lavoie, shared with me a model he has used with one of his financial services clients. My representation is shown below.

Risk appetite is represented by a range. When risk levels fall outside that range, performance is sub-optimal. When risk levels exceed the organization's risk tolerance, it becomes more critical to take action.

BARNOWL

Definitions Continued (Norman Marks)

Companies have to take risk to make a profit, or deliver value to their stakeholders. The level of risk they pursue is their *appetite* for risk. But they may be able to tolerate, or absorb, a different level of risk without significant pain and impact on achieving their strategic objectives. This is their *tolerance*.

Frankly, I would prefer more detailed guidance on this, as the decision on how much risk to take is the key to effective risk management. But, we will have to wait for more practical guidance from ISO and its national organizations.
Here's my view. I like and use the ISO definitions (from Publication 73) I listed above.

https://normanmarks.wordpress.com/2011/04/14/just-what-is-risk-appetite-and-how-does-it-differ-from-risk-tolerance/

BARNOWL

Definitions Continued

https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance.aspx

Risk appetite and tolerance
Risk appetite can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.
Risk appetite and tolerance need to be high on any board's agenda and is a core consideration of an entreprise risk management approach. IRM's guidance provides practical direction, advice and information to support boardroom debate.

While risk appetite will always mean different things to different people, a properly communicated, appropriate risk appetite statement can actively help organisations achieve goals and support sustainability.

While risk appetite is about the pursuit of risk, risk tolerance is about what an organisation can actually cope with.
Organisations have to take some risks and avoid others. To do so, they need to be clear about what successful performance looks like. This question may be easier to answer for a commercial organisation than for a government department, but can usefully be asked by boards in all sectors.

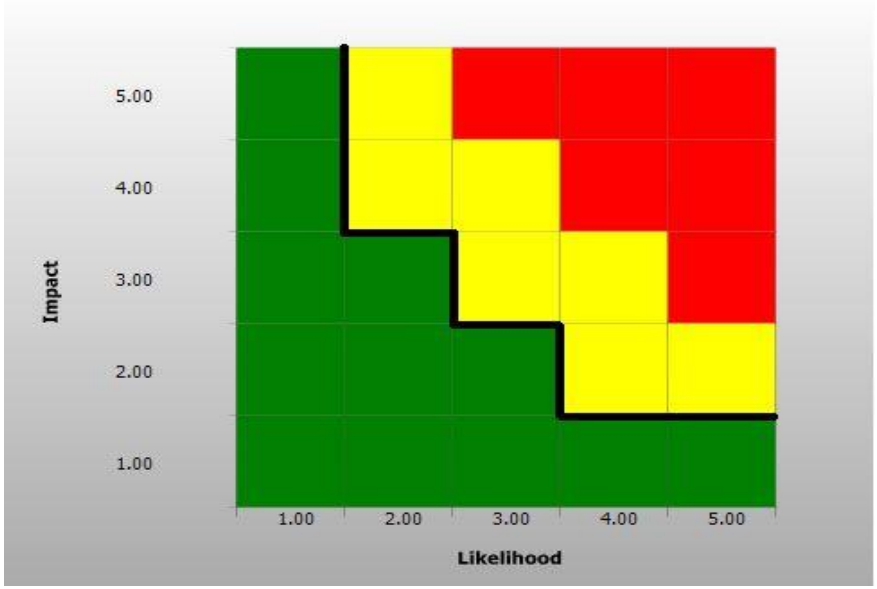
Risk Appetite vs. Risk Tolerance
According to the IIA, both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept. A risk appetite statement is a higher level statement that considers broadly the levels of risks that management deems acceptable, while risk tolerances are narrower and set the acceptable level of variation around objectives.

BARNOWL

Step 1: Understanding Risk Appetite and Tolerance

Whilst **Risk Appetite** deals with the level of risk that the organisation will pursue to meet their organisational objectives,
Risk Tolerance defines the upper and lower levels that an organisation is able to deal with / absorb, without significantly impacting the achievement of the strategic objectives.

Tolerance levels can be graphically represented alongside the appetite levels on what is referred to as a risk matrix or heat map taking into account the Impact (Consequence) x Likelihood of the risk. The example below shows the appetite line, above and to the right of which performance is deemed to be sub-optimal and action should be taken.



BARNOWL

Step 2a: Setting the Risk Appetite Scale

2a: Qualitative Risk Appetite

Most organisations use risk impact and likelihood rating scales / models similar to the table below which gives guidance to risk owners on how to rate the impact and likelihood of their risk/s:

Figure 2: Impact Rating Scale

Risk Impact Model by Rating Category						
Rating	**Financial Impact**	**Health and Safety**	**Natural Environment**	**Social & Cultural**	**Reputation**	**Legal**
1	Insignificant >0% T/O	Minor medical treatment	Limited damage	Low level repairable	Public concern restricted	Low level legal issue
2	Minor > 1% T/O	Moderate irreversible	Minor effects	Minor social impacts on local population	Minor / local public or media attention	Minor legal issue
3	Moderate >2% T/O	Significant irreversible disability	Moderate short term effects	Ongoing social issues	Serious adverse national media	Serious breach of regulation
4	Major >4% T/0	Very serious irreversible injury	Very serious long term effects	Permanent social issues	International media coverage	Significant prosecution and fines
5	Critical >5% T/O	>50 fatalities	Very significant impact on highly valued ecosystem	Very serious wide-spread social impact	Prolonged international condemnation	High fines and potential jail terms

BARNOWL

Step 2b: Setting the Quantitative Risk Appetite

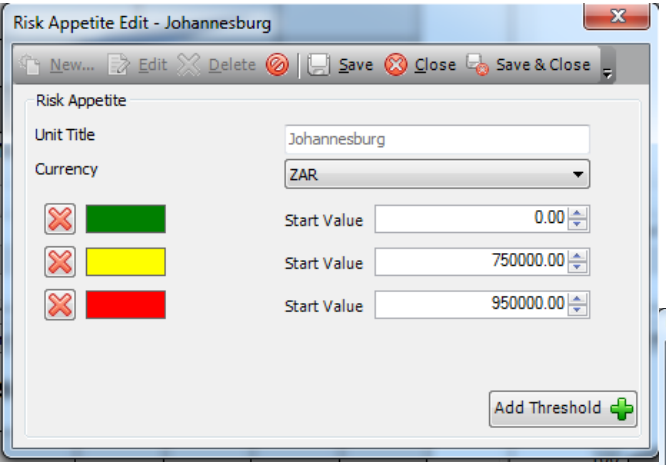
2b: Quantitative Risk Appetite

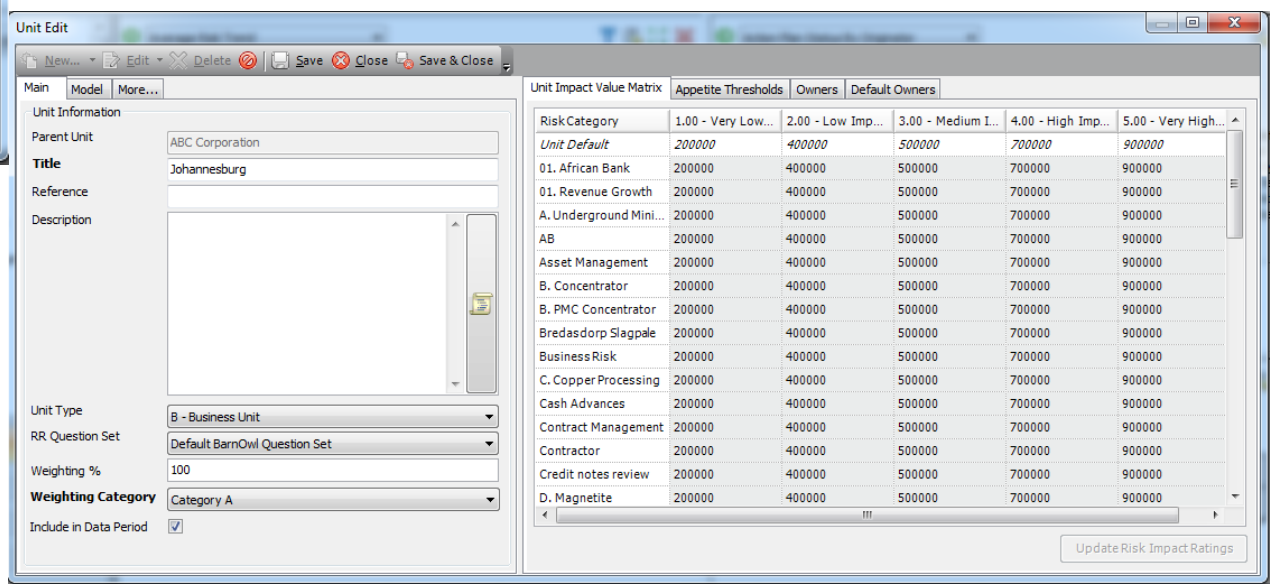
Where possible, we should also rate our risks quantitatively, albeit that some risks such as ‘reputational risks’ may be difficult to quantify. The nice thing about quantifying risks is that it make aggregation across business units relatively simple.

You can define quantitative thresholds at each level (unit) of your organisation in terms of:

(a) aggregated risk appetite thresholds (at the unit level)

(b) risk impact values applicable to each risk within the specific business unit per risk category

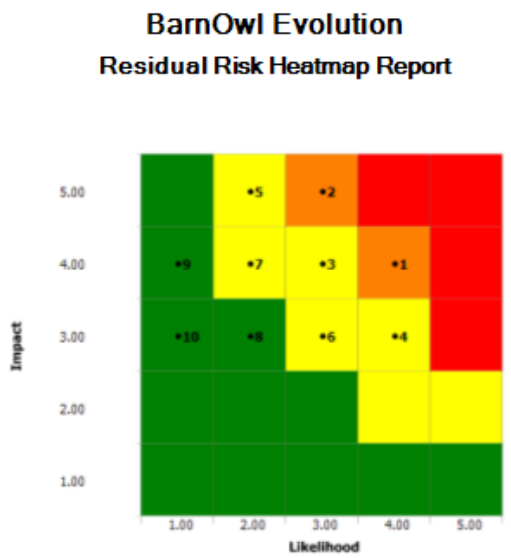




Step 3a: Reporting - Qualitative Risk Heat Map

3a: Qualitative Risk Heat Map

Impact and Likelihood plotted on a heat map as per risk appetite thresholds.



Point	Title	Unit Title	Description	RI	RL	IR	RR
1	02. Incorrect goods or quantities may be dispatched which may lead to unnecessary additional operational costs.	Finance	Incorrect goods or quantities may be dispatched which may lead to unnecessary additional operational costs.	4.0	4.0	16.00	16.00
1	03. Labour control and efficiency	The Mall of Africa		4.0	4.0	20.00	16.00
1	11. Weather	The Mall of Africa		4.0	4.0	20.00	16.00
1	Noncompliance - 0013.Qualifications of representatives and duties of authorised financial services provider	JHB Compliance		4.0	4.0	20.00	16.00
2	01. Assets may be misappropriated for personal use or sale	Assets		5.0	3.0	20.00	15.00
2	02. Formwork turn around	The Mall of Africa	02. Water ingress	5.0	3.0	20.00	15.00
2	04. Water ingress from the bulk	The Mall of Africa		5.0	3.0	20.00	15.00

Step 3b: Reporting - Weighted Qualitative Risk Heat Map

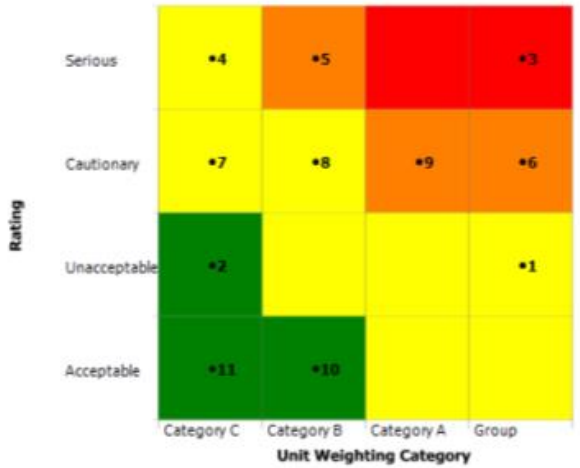
3b: Weighted Qualitative Risk Heat Map

Impact and Likelihood plotted on a heat map as per risk appetite thresholds taking into account importance (weighting) of business units.

BARNOWL

BarnOwl Evolution

Unit Weighting Residual Heatmap Report



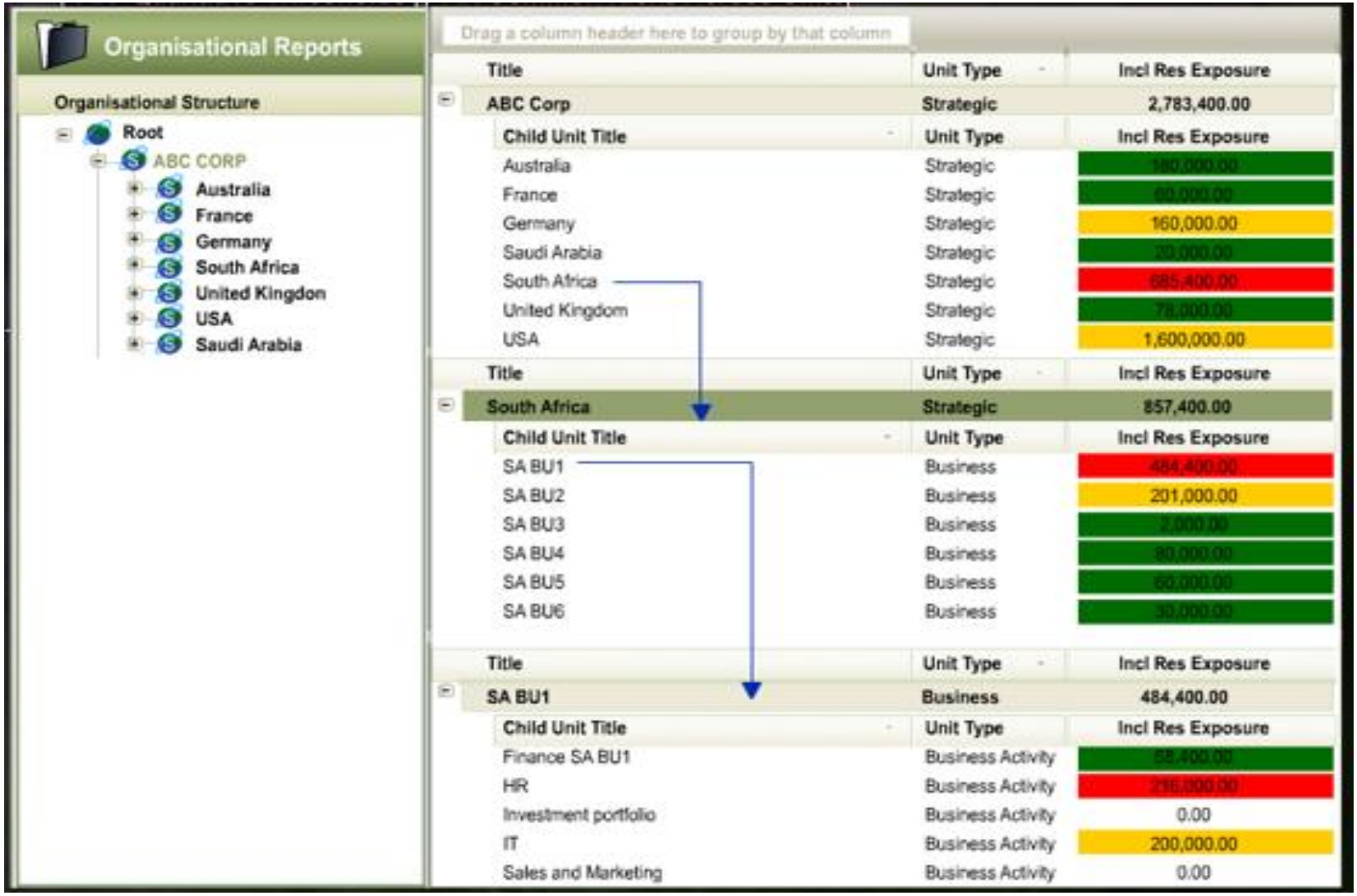
Point	Title	Unit Title	Parent Unit Title	IR	RR
1	03. Skills Shortage	ABC Corporation	Root	20.00	
2	Noncompliance - 0015.Publication of codes of conduct	Compliance	Durban	20.00	
3	01. Regulatory risk	ABC Corporation	Root	16.00	
3	02. Exchange Rate	ABC Corporation	Root	16.00	
3	05. Political Unrest / Strike Action	ABC Corporation	Root	15.00	
3	07. Interest Rates / Bad Debts	ABC Corporation	Root	16.00	
4	Noncompliance - GNR 0924 of 3 August 2004 Facilities	Compliance	Durban	16.00	

BARNOWL

Step 3c: Reporting - Quantitative Exposure

3c: Quantitative Risk Exposure

Aggregated Rand risk exposure plotted against appetitive thresholds per unit.



BARNOWL

In Summary

Step 1: Understand the definition of risk appetite and tolerance and how it relates to your organisation.

Step 2: (a) Formulate and rate risks based on your qualitative risk appetite model / statement. Define risk appetite model/s that take into account materiality at group, divisional and business unit level (b) set up your quantitative risk appetite thresholds at key levels (units) of your organsational.

Step 3: Report qualitatively as well as quantitatively on your risks, taking into account the significance (importance) of the different units within your organsational.

BARNOWL

Concluding Remarks (courtesy IRMSA)

- Very confusing and contradictory definitions – decide what is best for you!
- What does that mean:
  - Board must understand and be able to apply it
  - Exco must be able to manage by it including using it to make decisions … better decisions
  - It must resonate with both …
- Do not under estimate change management
- Appetite and tolerance may need a maturity curve … a roadmap to effectiveness
- Create the awareness, conversation and “fertile ground” before you slap it on them
- You may need to divide and concur

RMSA
The Institute of Risk Management
SOUTH AFRICA

Thank You

Jonathan Crisp –Director
jonathan@barnowl.co.za
+27 83 260 1653 (mobile)
+27 11 540 9100 (office)
2018

http://www.barnowl.co.za/insights/a-3-step-approach-to-implementing-risk-appetite-and-tolerance/

BARNOWL