BARNOWL

Risk Management (RM) Software Buyer's Guide

BARNOWL

The need for Risk Management (RM)

As a result of organisational failures in the past, stakeholders do not want to be caught unawares by risk events. Stakeholders require assurance that management has taken the necessary steps to protect their interests. Corporate governance thus places the accountability for risk management in the hands of the Accounting Authority / Officer and the Board. Stakeholders expect internal control and other risk mitigation mechanisms to be based on a thorough assessment of institutional wide risks.

Some of the benefits derived from the risk management activities include:

- More effective strategic and operational planning with alignment of objectives and risks across the organisation
- Greater confidence in decision making and achievement of operational and strategic objectives
- Greater stakeholder confidence by demonstrating transparency and sustainable capability
- Early warning system and visibility and reporting of significant risks to avoid surprises
- Proactive management of risk rather than reactive after the event which costs time, money and reputation
- Cost effective internal controls and control strategy
- Evidence of a structured / formalised approach in decision making
- Regulatory compliance and director protection

What do the standards say?

According to ISO 31000, risk is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected. Risk management refers to a “coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.”

The COSO “Risk Management-Integrated Framework” published in 2004 defines RM 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.”

Legislation such as PFMA and the MFMA together with corporate governance codes such as King IV expect an institution to implement a risk management plan. The King IV code on corporate governance (copyright Institute of Directors Southern Africa) applies to all entities, regardless of their nature, size or form of incorporation. The Code is implemented on an “apply and explain” basis. The following principles relating to risk governance are embodied in the Code:

- Strategy, Performance and Reporting: Principle 4: The governing body should appreciate that the organisation’s core purpose, its risk and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process.

- Risk Governance: Principle 11: The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives.

Recommended Practices

1. The governing body should assume responsibility for the governance of risk by setting the direction for how risk should be approached and addressed in the organisation. Risk governance should encompass both:
    a. the opportunities and associated risks to be considered when developing strategy; and
    b. the potential positive and negative effects of the same risks on the achievement of organisational objectives.

2. The governing body should treat risk as integral to the way it makes decisions and executes its duties.

3. The governing body should approve policy that articulates and gives effect to its set direction on risk.

What do the standards say?

4. The governing body should evaluate and agree the nature and extent of the risks that the organisation should be willing to take in pursuit of its strategic objectives. It should approve in particular:
   a. the organisation’s risk appetite, namely its propensity to take appropriate levels of risk; and
   b. the limit of the potential loss that the organisation has the capacity to tolerate

5. The governing body should delegate to management the responsibility to implement and execute effective risk management.

6. The governing body should exercise ongoing oversight of risk management and, in particular, oversee that it results in the following:
   a. An assessment of risks and opportunities emanating from the triple context in which the organisation operates and the capitals that the organisation uses and affects
   b. An assessment of the potential upside, or opportunity, presented by risks with potentially negative effects on achieving organisational objectives
   c. An assessment of the organisation’s dependence on resources and relationships as represented by the various forms of capital
   d. The design and implementation of appropriate risk responses
   e. The establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility, and to withstand and recover from acute shocks.
   f. The integration and embedding of risk management in the business activities and culture of the organisation

7. The governing body should consider the need to receive periodic independent assurance on the effectiveness of risk management.

8. The nature and extent of the risks and opportunities the organisation is willing to take should be disclosed without compromising sensitive information.

9. In addition, the following be disclosed in relation to risk:
   a. An overview of the arrangement for governing and managing risk
   b. Key areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks taken outside of the risk tolerance levels
   c. Actions taken to monitor the effectiveness of risk management and how the outcomes were addressed
   d. Planned areas of future focus

Why implement risk management software

An organisation cannot management risk effectively without the use of specialised risk software which drives accountability and ownership for risk in a coordinated manner across the organisation. Therefore, if your organisation is serious about risk management you need specialised risk management software which will:

- Facilitate and embed RM in your organisation turning RM into a ‘living’ activity which is integrated within the business and its operations

- Facilitate a culture of risk and control within your organisation driving accountability for risk management at all levels of the organisation enabled by the ‘live’ updating and monitoring of action plans

- Facilitate an integrated approach rather than a silo-driven approach to risk management by linking related risks across the organisation and monitoring the knock-on effect of risks, key risk indicators, incidents, controls, causes etc.

- Improve the quality and consistency of data captured giving you one version of the truth, audit trails etc.

- Provide an up to date dashboard of your risk universe including consolidated and trend reporting at any level of the organisation all at the click of a button

- Ensure Director / Accounting officer protection through a formalised system-driven ap-

Why implement risk management software

Why can't we just use Excel?

- Multiple 'versions of the truth' with little or no version control with 100s of spreadsheets floating around the organisation,
- Data is not well structured (inconsistent columns and naming conventions, free text versus drop-downs etc.) limiting the ability to report on data,
- Limited data validation (free text versus drop down boxes),
- The quality and completeness of data is compromised,
- Information is not consolidated into a single repository,
- Security access to data is non-existent in most cases,
- Excel is silo based and ignores interdependencies of risk across business units and users etc.,
- Excel spreadsheets can't easily be shared / worked on at the same time,
- It's not possible to perform aggregated reporting without exhaustive manual intervention,
- It's almost impossible to generate trend reporting,
- Excel is a static system as opposed to a 'living' system which provides the ability to send out automated email notifications, reminders, escalations etc. based on system triggers,
- Complex spreadsheets are 'lost' when the owner leaves the organisation and are re-invented again by the new person, wasting time, money and effort.

Steps to the successful implementation of risk management software

Software implementation:

1. Ensure you have an existing risk management policy, risk framework an methodology
2. Identify the risk champions and risk owners at the various levels of your organisation. Limit the number of users to start with
3. Sanitise and import your existing Excel-based risk registers into the system
4. Confirm the kinds of risk management reports you would like out of the system: heat maps, trend analysis etc.
5. Get buy-in from the top and educate your users as to the value of RM and the reason for a system

Now you are ready to use the software:

6. Inform users that whilst the system is non-intrusive there will be automated follow-up of action plans and automated risk & control self-assessments
7. Embed and expand the usage of the system over time
8. Add value to the organisation with insightful reporting
9. Demonstrate the effective mitigation of risks and monitoring of controls
10. Follow up on remedial action plans

Considerations and key questions when buying risk management software

- Does the software support best practice standards (COSO, ISO31000) and is there seamless integration with compliance and audit if required

- Does the solution provide a simple, cost effective, user friendly and non-intrusive interface for the normal business user? E.g. action plans, checklists, risk& control self-assessments etc.

- Is the system flexible, configurable and parameter driven in order to support your risk methodology

- Ensure that the software offers flexible reporting capability without any programmer intervention

- Apart from the standard features, what differentiators / value add does the software offer

- What is the setup process and estimated timelines; it should be easy to get up and and going with the software

- Is the system fully documented, user manuals, online help, FAQs (Frequently Asked Questions)

- Is there local support and how responsive are the software owners and developers to your changing requirements

- Are there any hidden fees or costs (e.g. hosting, support, additional implementation, other required 3rd party software licenses, online action plan users etc?)

- Ensure that there are regular upgrades to the software ensuring that it is aligned with best practice risk management standards as well as kept up to date with the latest technology platforms and that the upgrade process is simple and never overwrites existing custom fields / custom settings.

- Request client references / testimonials

Don’t:

- just buy basic software which may meet your current requirements today but won’t meet your future requirements

Key feature comparison checklist

Use this comparison checklist to compare important feature sets from competing software solutions:

Important features	BarnOwl	Software B	Software C
Is the system a fully integrated GRC software solution offering additional modules such as compliance, incident management and audit	✓		
Full system functionality supporting the COSO, ISO31000 standards including functionality to maintain objectives, risks, controls (including multi-rating of controls per assurance provider), contributing factors, KRIs, incident management, action plans, voting, risk & control self-assessments, surveys, questionnaires	✓		
Simple and flexible take-on / import functionality	✓		
Flexible and parameter-driven to ensure configuration for your risk methodology (ratings etc.)	✓		
Ability to maintain a central library of common objectives, risks, controls, KRIs etc.	✓		
User-defined fields available anywhere in the system and ability to report on user-defined fields	✓		
Linking of objectives to risks and risks to other risks, KRIs etc. enabling dynamic re-assessment and automated notifications to ‘risk owners’ of a changing risk environment	✓		
Highly flexible and customisable report generation without any programmer intervention	✓		
Combined assurance reporting	✓		

Key feature comparison checklist

Important features	BarnOwl	Software B	Software C
Graphical slice and dice reporting: e.g. risk heat map, heat map movement, trends, risk ranking, causal analysis, etc.	✓		
Automated risk & control self-assessments without any licensing or cost implications			
Online questionnaires and surveys without any licensing or cost implications	✓		
Online action plans with email notifications to all auditees without any licensing or cost implications	✓		
Offline and online synchronisation enabling workshops to be conducted offline	✓		
Ease of use including a ‘Lite’ offering allowing easy adoption and buy-in for the system by the business users.	✓		
User / Group security restricting unit and risk owner access	✓		
Ability and willingness of the vendor to respond to software enhancement requests	✓		
Online help, FAQs, up-to-date system documentation	✓		

Key feature comparison checklist

Important features	BarnOwl	Software B	Software C
End user support process, support portal	✓		
Regular and seamless software upgrades	✓		
Regular user groups, refresher training etc.	✓		
Client references and track record of the vendor	✓		

About BarnOwl

BarnOwl is a fully integrated governance, risk management, compliance and audit software solution used by over 200 organisations in Africa, Europe and the UK. BarnOwl supports best practice risk management, compliance and audit frameworks (e.g. COSO, ISO31000, Compliance Institute’s handbook, International Professional Practice Framework), whilst offering a highly flexible and configurable parameter-driven system allowing you to configure BarnOwl to meet your specific requirements.

www.barnowl.co.za