BARNOWL

SELLING **RISK MANAGEMENT (RM)** TO **THE BOARD** AND THE **EXECUTIVE**

TABLE OF CONTENTS

THE PURPOSE OF THIS GUIDE

This guide takes a critical look at the value of **Risk Management (RM) / Governance Risk & Compliance (GRC)** and what it means to each of the stakeholders (including the board and executive) and the organisation as a whole. The guide addresses some of the reasons why many senior executives are hesitant to implement **RM** in their organisation/s and suggests practical recommendations for the implementation of effective **RM**.

INTRODUCTION:

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 effective 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, 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 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 from the King IV code outline the responsibility of the board (governing body) and management in risk management:

THE PRINCIPLES:

1. 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.

3. Compliance Governance: Principle 13: The governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that supports the organisation being ethical and a good corporate citizen..

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

4. Assurance: Principle 15: The governing body should ensure that the assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision-making and of the organisation's external reports.

WHY THE NEED FOR EFFECTIVE RM?

A decade ago, lack of risk awareness might have satisfied litigators in the aftermath of a loss event. However, today's regulations have made board members and senior leadership teams accountable for risks, regardless of at what level the risk materialises. Mature Risk Management programs are more than a safety net. These programs are invaluable insurance policies against the surprises your business might face and assure achievement of corporate performance objectives.

Gerry Grimstone, keynote speaker at the IIA's recent conference in London, had a message for senior executives. "You can't easily blame a board member for not knowing something," Grimstone said. "But you can blame a board member for creating a culture where he doesn't know something." Grimstone also discussed the "tone from the top;" a need for an organisational culture where assumptions are challenged and ethical risk management practices are acclaimed, not neglected.

It's quite simple! Lack of disclosure and an ineffective RM information and reporting system equals negligence. Boards are explicitly given a choice between either having effective risk management in practice or disclosing their ineffectiveness in risk management to the public. If they do neither, it is considered fraud or negligence, as not knowing about a risk is no longer a defense.

> "You can't easily blame a board member for not knowing something," Grimstone said. "But you can blame a board member for creating a culture where he doesn't know something."

THE ROLE OF THE VARIOUS STAKEHOLDERS IN RM

RM is an important function in any organisation and affects the various stakeholders of an organisation in different ways.

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
BOARD MEMBER	• The board of directors plays a leading role in overall risk oversight. The board of directors is appointed to act on behalf of the shareholders to run the day-to-day affairs of the business. • Grow and protect the asset value of an organisation and maximise shareholder value. • Add value through a deep understanding of the business and the market in which it operates including the downside and upside risks that face the organisation. • Assist with strategic decision making based on a good understanding of the business, the market and the associated risks and trends. • Must be well informed and aware of the risks (leading and lagging) that may affect the sustainability of the organisation and how well they are being managed. • Play an active role in ensuring sound governance and ethical behaviour in order to protect the brand and minimise reputational risk. • Ask the difficult and sensitive questions of the exco / management to ensure that the 'real' risks are uncovered to ensure a balanced view point when making management decisions. • Review risk tolerance and appetite across the organisation ensuring that exco and management are operating within the boundaries and authority vested in them by the various stakeholders.

Note: some organisations make the mistake of inferring that only strategic and high level risks should be reported on however this is ineffective because of the gap between senior management and the front line activity level where risks first arise. The key to determining the effectiveness of a risk management program is the ability to collect risk information from the business level and process-level and aggregate this information, whilst preserving the effects of related upstream and downstream dependencies.

BOARD MEMBER	• Support the RM process which leads to greater transparency and better decision making.

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
EXCO MEMBER	• Set the tone from the top embedding a culture of ethical business behaviour, good governance and proactive risk management (culture of control and doing things the 'right' way). • Set and review risk tolerances and appetites across the organisation enabling activities to be assigned to management within the delegated authority. • Ensure that key insights and risks are captured and monitored via the RM processes. This includes strategic-level risk as well as operational and process-level risk and their interdependencies. • Review problem areas and root causes and ensure that process improvements are implemented. • Accountable for overall performance of the organisation which includes calculated risk taking based on informed and accurate risk management metrics. • Accountable for driving, measuring and monitoring key performance indicators. • Accountable for monitoring remedial actions. • Accountable for effective processes and communication between Exco and line management and vice versa.

> “Not considering or knowing about a risk is no longer a defense.”

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
LINE MANAGEMENT	• Proactive identification and monitoring of the risks in your business unit and understanding the consequence of these risks. • Being aware of risk interdependencies: i.e. other (internal and external) risks that affect your area of business and the knock-on effect of your risks on other areas of the business and /or the business as a whole. • Reporting on risk accurately and honestly. • Effective leadership and communication with the staff. • Analyse problem areas and root causes and implement process improvements. • Responsible for ensuring that remedial action takes place on time. • Monitoring of key risk indicators. • Responsible for achieving key performance targets.
STAFF	• Operating within the company's standards and operating procedures • Managing the risks in your area within the acceptable risk appetite and tolerance levels. • Performing remedial actions on time. • Monitoring and achieving your agreed upon key performance targets. • Whistle blowing and communicating problem areas to management.

> "Organisations have realised that their board level attestations on the effectiveness of risk identification and assessment can no longer just be a facilitated interview at the senior management level; instead, there needs to be a rigorous process at the activity level through the lens of what is material, not just in isolation of a single business silo, but overall as all the pieces come together at the top. The goal is to identify and objectively assess operational risks and ensure risk mitigation is in place at the activity level independently and then collectively. This integrity of this risk information needs to be preserved when aggregating and summarising by the strategic goals of the organisation."

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
RISK AND AUDIT COMMITTEE	• Management, the board, and the audit committee all play critical roles in an organisation’s tone at the top. Based on board expectations, executive management establishes the tone. It is the audit committee’s responsibility, though, to monitor that tone as well as oversee the organisation’s ethical environment and compliance with laws and regulations. • The King IV code on corporate governance (copyright Institute of Directors Southern Africa): o The role of the audit committee should be to provide independent oversight of, amongst others: the effectiveness of the organisation’s assurance functions and services, with particular focus on combined assurance arrangements, including external assurance service providers, internal audit and the finance function. o Whether or not the governance of risk is delegated to the audit committee, the audit committee should oversee the management of financial and other risks that affect the integrity of external reports issued by the organisation. o The governing body should consider allocating the oversight of risk governance to a dedicated committee, or adding it to the responsibilities of another committee as is appropriate for the organisation.

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
RISK PRACTITIONERS **(e.g. Chief Risk Officer, Chief Audit Executive, Compliance Officer)**	• The chief risk officer (CRO) of an organisation is the executive accountable for enabling the efficient and effective governance of risks and related opportunities, to a business and its various segments. The complexity of the business environment and rapid changes in the market place calls for stronger risk function. o Risk manager facilitates the risk management process across the organisation o Provides insight into the risk management process and assists with education and embedding a risk culture o Ensures that effective risk management, processes and reporting systems are in place. • The Institute of Internal Auditors (IIA) defines Internal Auditing as "An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes." The audit department executes an approved audit plan and will perform the following tasks in accordance with its overall strategy: o Verify the existence of assets and recommend proper safeguards for their protection; o Evaluate the adequacy of the system of internal controls; o Recommend improvements in controls; o Assess compliance with policies and procedures and sound business practices. o Assess compliance with state and federal laws and contractual obligations.

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
RISK PRACTITIONERS **(e.g. Chief Risk Officer, Chief Audit Executive, Compliance Officer)**	o Review operations/programs to ascertain whether results are consistent with established objectives and whether the operations/programs are being carried out as planned; o Investigate reported occurrences of fraud, embezzlement, theft, waste, etc. • The role of a compliance officer is to make sure that a company is conducting its business in full compliance with all national and international laws and regulations that pertain to its particular industry, as well as professional standards, accepted business practices, and internal standards. There is both an ethical component and a pragmatic component to compliance - a role that is crucial in helping organisations manage risk, maintain a positive reputation, and avoid lawsuits • A broad view of the firm and the interactions between areas, processes and risks is important to adequately measure impacts. This is also part of the training and experience.

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
SHAREHOLDERS	• Growth and protection of their investment • Transparency • Reputable and ethical company
CUSTOMERS	• Reputable brand • Trustworthy • Honest and reliable • Offers great service and products • Offers cost effective products and services

Role Player / Stakeholder	Role / Duty / Requirement / Expectation
SUPPLIERS	• Reputable with good corporate governance practices • Stable company • Pays on time • Ethical • Trust and win /win relationship • Operates according to best business practice and adheres to legislative requirements and rule of law. i.e. no back hander business
PUBLIC / SOCIAL RESPONSIBILITY / ENVIRONMENT RESPONSIBILITY	• Operating ethically and transparently • Reputable • Putting back and caring about the local community and exercising good corporate citizenship. • Caring and protecting the natural environment by exercising honest and transparent business dealings. • Contributing positively to the country as a whole; not all about profit, personal gain and corporate greed.

> “Focusing on strategic / high level risk alone is ineffective because of the gap between senior management and the front line activity level where risks first arise.”

SO WHY THE HESITANCY TO INVEST IN EFFECTIVE RM?

Despite evidence that mature RM programs add significant value, many organisations remain hesitant when it comes to adopting RM and embedding their RM processes. Below, are some of the typical queries / objections when it comes to investing in RM.

TYPICAL OBJECTIONS TO INVESTING IN RM

"We are not convinced of the value of GRC. It's a nice to have and not a necessity. As long as we can tick the box to say that we comply."

RESPONSE

Clem Sunter states in the IRMSA Risk report 2016: "Risk evaluation and management skills are now central to the long-term viability of any organisation". Clem further adds: "Moreover, risk management now constitutes a premier discipline that no organisation can do without. You only have to look at the high-profile and costly examples of companies that recently were devastated by some expensive flaw in their business model being exposed to public scrutiny. What they would have given to have perceived the full extent of the problem in advance and acted on it" You can download the full IRMSA 2016 risk report at http://www.barnowl.co.za/wp-content/uploads/2016/02/IRMSA_2016_Risk_Report_full.pdf as well as see some examples of recent corporate failures at http://www.barnowl.co.za/insights/6373/

The RIMS report 'Why a Mature RM Effort is Worth the Investment,' cites an independent study conducted by Queen's University Management School and University of Edinburgh Business School in an effort to answer the question many executives ask – "is improving our RM program worth the investment?" The answer?

Yes. Or as they wrote, there is “a highly significant premium of 25% for firms that had been classified as having ‘mature RM’ according to the RIMS Risk Maturity Model.” This fact – that an organization’s value can increase 25% through improving its RM program – is one that should catch the attention of executives, board members, and risk As Steven Minsky (Steven is a recognized thought leader in RM, and co-author of the RIMS Risk Maturity Model) says “A mature RM program is a safety net. It protects boards and senior leadership from accusations of negligence by demonstrating a clear dedication to uncovering risk. It also provides transparency and assurance of on-time and on-budget achievement of corporate performance objectives.”

> “Ensure that key insights and risks at all levels are captured and monitored via the RM processes.”

"We've been in business for a long time and know what our risks are. Why do we need a system to tell us what our risks are? We keep track of our risks in Excel."

RESPONSE

In a medium to large scale organisation, management may know what the top 10 strategic or top 10 operational risks are but with the best intentions in the world won't always be aware of what is going on 'below the surface' and the knock-on effects that exist between interconnected risks, controls, loss events, near misses, regulatory requirements, KPIs and resources which become serious risks to the organisation if not identified, managed and monitored.

It's impossible to see the warning lights or keep track of all risk related activities, and their inter-connectedness without a systematic approach supported by specialised RM software. See http://www.barnowl.co.za/insights/still-using-excel-for-risk-management-and-or-audit/ as to why Excel just won't cut it!

It's a mistake to base your decision making on the financial results (after the fact) and forecasts only and to ignore / minimise the importance a changing risk profile (be it internal or external). Ignoring or not being aware of the risks is a threat to the sustainability of your organisation and is considered negligent and is punishable by law.

> "Clem Sunter states in the IRMSA Risk report 2016: "Risk evaluation and management skills are now central to the long-term viability of any organisation".

“We have a business to run here and don’t have time for RM. It would add work to our day-to-day operations and our resources are already spread thin.”

RESPONSE

You may not have a business to run unless you find the time to identify and monitor your risks and make the relevant resources accountable for managing the risks within each of their areas of business.

In reality, everyone is performing risk management activities all the time in their daily lives be it at work or privately (e.g. crossing a street involves risk assessment and decision making). In a team environment however, if there is no formal risk management program, everyone does their own thing which is often counterproductive and creates duplicate effort and re-work.

A systematic approach to risk management supported by GRC software provides a centralised platform for all the risk activities you’re already doing. It acts as the centralised hub for your entire risk program. The risk assessments you send out, the mitigation activities you carry out and document, and the reports you’re creating are all housed in a single centralised database. GRC software isn’t simply a database where you document processes and store your data; it serves as a tool for you to make risk management processes easier, more efficient and enables you to gain insight into the data you’ve been collecting.

> “Institutional investors pay a premium of up to 25% for organisations that are classified as having ‘mature RM’ according to the RIMS Risk Maturity Model.”

“Exposing risk forces us to spend time and money on things we don’t have to worry about today.”

RESPONSE

There is still the idea in some organisations that “ignorance is bliss” and “what we don’t know can’t hurt us.” These sayings have no place in risk management, and regulatory agencies and stakeholders would agree.

Many executives only worry about the financial results, satisfying immediate demands of shareholders and getting their performance bonuses. This is often at the expense of the longer-term sustainability of the organisation. Claiming ignorance, ignoring or not knowing about a risk is now equally punishable (and as heavily penalised) as negligence.

Any member of exco and / or the board should insist on the implementation of robust RM processes to ensure that risks are identified, mitigated and continuously monitored in a transparent and effective way across the organisation; not only to protect the organisation but to protect themselves as well.

“We don’t want our stakeholders and competitors to know about our risks / vulnerabilities. It’s better to keep a tight lid on things.”

RESPONSE

Sooner or later the risks will materialise, which if covered up will result in a scandal and often serious reputational damage. It is far better to be transparent about the risks in your organisation and demonstrate your ability to manage the risks rather than sweep them under the carpet.

"How would having an RM / GRC system have prevented non-ethical behaviour, fraud, incidents, loss events etc. from happening?"

RESPONSE

No system will prevent someone from unethical behaviour or fraudulent activities especially those perpetrated at the highest levels of the organisation. However, if there are controls and cross-checks in place which are monitored and supported by systems, the chance of early detection and prevention is far greater thus minimising the impact as well as acting as a deterrent to would-be perpetrators.

"We don't have resources to adopt, administer and embed RM."

RESPONSE

This is exactly one of the reasons you should invest in GRC software. Effective GRC software is highly automated reducing the administrative burden of RM and facilitating and embedding risk management at all levels of the organisation whilst being non-intrusive. In addition, reports can be generated at the click of the button.

For example, intelligent GRC software will send out automated risk and control self-assessments to the relevant business unit owners based on a schedule, notify and enable owners to complete their action plans online, notify and enable owners to complete compliance checklists online as well as notify owners to re-assess their risks based on a changing risk environment.

With GRC software, these activities are all performed online and updated in real-time to a centralised database at the same time enforcing data integrity, recording audit trails (personal accountability) and tracking history and trends.

An intelligent GRC system allows the CRO and / or management to generate real-time reports at the click of a button transforming RM data into meaningful insights that support strategic planning and decision-making. (For example, a system such as BarnOwl provides a system-wide view of your risk, compliance and audit universe at a strategic group level as well as at each individual business unit level and / or process level. BarnOwl keeps risk managers / owners appraised of a changing risk environment improving their insight and oversight of issues and exposures of the business at a strategic level and operational level.)

> “ It's impossible to see the warning lights or keep track of all risk related activities, and their inter-connectedness without a systematic approach supported by specialised RM software. ”

“It looks like a lot of work to embed RM and populate a system.”

RESPONSE

Yes, the initial setup of your RM processes including risk identification at the various levels of your organisation does involve work. The good news is that the RM standards are well defined, logical and not based on ‘rocket science’. Risk workshops facilitate communication and provide a great opportunity to share ideas and get everyone ‘pulling’ in the same direction.

Once your RM process is in place, it is relatively easy to implement GRC software including the initial take-on by importing your existing Excel-based risk registers (including controls, KRIs, contributing factors, incidents, findings etc.) The end result is a standardised and centralised database of ‘living’ risks which are kept current through automated risk and control self-assessments, online action plans and online checklists. The ongoing management and reporting of risk is greatly simplified and made much more effective when using GRC software.

“We already have too many rules & regulations and systems and now another one?”

RESPONSE

The good news is that an integrated GRC system provides a single system, simplifying and enabling the risk management, compliance, audit and performance management processes.

> “Any member of exco and / or the board should insist on the implementation of robust RM processes not only to protect the organisation but to protect themselves as well.”

“Why should we spend more on a software solution when we are already paying a risk / compliance / audit officer/s to manage the risks and generate the relevant risk reports?”

RESPONSE

Did you know that on average, risk managers spend 62% of their time on tactical activities alone rather than strategic activities! Source: Future of Risk Management & Compliance: Global Trends and Perspectives. PRMIA. 2010. In a 40 hour week, that’s more than 24 hours spent manipulating spreadsheets, mining data, and building reports! How can GRC professionals be strategic if they are committing more than half their time to finding out which risks they need to manage? And how about the cost? How much does a senior resource cost per hour (CTC (Cost to Company)) to perform administrative and manual Excel work instead of giving strategic input into the organisation?

The benefits of a system far outweigh those of Excel both in terms of quality of data and reporting as well as reducing administrative workload significantly for all those involved in risk management activities. It’s hugely time consuming if not impossible to pull aggregated reports and trend reports out of Excel; not to mention the quality and consistency of data across disparate Excel sheets submitted by multiple respondents.

Note: Risk, Compliance and Audit officers do not manage or own the risks. They facilitate the RM process. Management and staff own their business unit specific / functional risks. GRC software enables a risk officer to allocate, automate and embed risk management at every level of the organisation ensuring that the relevant owner/s takes accountability for managing his / her risks.

In addition, a risk-based software taxonomy will link individual risks and activities to strategic goals (objectives) of the organisation. GRC platforms are dynamic, and enable your program to evolve as priorities change. GRC software creates all the reports you need at the click of a button based on the most recent 'real-time' data.

Risk-based GRC software is designed to work alongside your Audit and Compliance teams and link the work your Risk Management, Audit, and Compliance teams to a single centralised location, accelerating problem solving and reducing rework.

"Why would you need to or want to embed risk management down to low level staff?"

RESPONSE

The risks that pose the greatest impact may not be known by the senior executives that make governance decisions. But, the clues to those risks are often known at the front line, supervisory level of your employee base. In other words, what's unknown by the decision makers is typically well understood by the employees that face those risks on a day-to-day basis. Unfortunately, nearly all industries experience similar communication failures that result in risks not being elevated to the appropriate level.

GRC software embeds risk management at every level of the organisation ensuring that the relevant owner/s takes accountability for managing his / her risks. This includes linking operational and process-level risk to strategic-level risk.

"GRC software is a 'nice to have', not a need."

RESPONSE

The notion that RM software is more of a luxury than a necessity seems to be encompassed above. Board members may have the misconception that investing in risk management doesn't help a company financially. Executives often believe it would add work, and isn't absolutely necessary to their program. And CROs may recognise the range of software solutions already utilised by the company and ask "Why add one more?"

As outlined above, GRC software when implemented effectively serves a significant purpose. It reduces wasteful resource management by consolidating things like risk management, compliance, performance and audit into a single platform; it streamlines existing RM activities by adopting a universal, risk based methodology and it gives you great insight into your business at the click of a button.

Finally, GRC software is no longer a luxury item. Heavy fines for negligence continue being handed down to organisations with outdated processes.

> "No system will prevent someone from unethical behaviour or fraudulent activities however an effective RM process will improve the chance of early detection and act as a deterrent."

“We don’t have the funds for a system”

RESPONSE

The return on investment of a GRC system is soon realised not only by taking into account the time savings of your risk, compliance and audit officers, but the value of embedding RM within your organisation and reporting on an up-to-date risk universe at the click of a button.

“We already have a GRC software system but it isn’t working for us?”

RESPONSE

The two main reasons for this are:

- Any system and process needs to be owned and driven by a competent champion.
- Your existing system needs to be functionally rich / ‘fit for purpose’ and needs to be supported by a competent service provider committed to excellent after-sales support?

If you aren’t happy with your software or service provider consider a ‘cross-grade’ to a new system; it’s not as onerous as one would think! Please see http://www.barnowl.co.za/guides/ which documents a step-by-step approach to the implementation simple and effective GRC software.

CONCLUSION

Without a risk-based GRC solution, it's simply not realistic for any risk manager to gather all the necessary data, relate it across departments, and aggregate it into the actionable reports required by the board of directors and external regulators. At the very least, it's unrealistic to expect these steps to be accomplished before the information becomes outdated.

Boards cannot be scouring the front lines for unreported risk, so it's the job of risk management to be diligent in the risk assessment process and notify senior leadership if the program lacks the necessary maturity. A mature RM program is a safety net. It protects boards and senior leadership from accusations of negligence by demonstrating a clear dedication to uncovering risk. It also provides transparency and assurance of on-time and on-budget achievement of corporate performance objectives.

> “ GRC software reduces the administrative burden of RM and facilitates and embeds risk management at all levels of the organisation ”

Executive teams, boards and internal audit groups are obligated to know their company's' major risks and disclose these risks to their investors. Without an Risk Management software system to support an effective RM process, they risk being found negligent in risk management, and subsequently being exposed to maximum legal penalties.

Not being involved in the day-to-day running of the company where most operational risks actually occur means Boards of Directors must, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are effective at identifying all risks and demonstrating assurance over the most material ones.

Risk is viewed at its highest level by the board. Some people make the mistake of inferring that this risk information should then also be collected at only this high level, but this is ineffective because of the gap between senior management and the front line activity level where risks first arise. The key to determining the effectiveness of a risk management program is the ability to collect risk information from the business process-level and aggregate this information, while preserving the effects of related upstream and downstream dependencies.

Since the liability for error is so high, Internal Audit has now been tasked to do the fact-checking on the risk management information being presented to the board to ensure its integrity at the front line business process level. The Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF), requires auditors to validate the most timely and most significant risks, especially those that impact the achievement of the organisation's strategic objectives.

> “ A mature RM program is a safety net ”

The role of the risk manager has now finally become clear to close the gap between strategic level risk and all the operational risks at the activity level at the front line of organisations. The risk manager is responsible for setting the standards, practices and procedures for effective risk management and embedding them in all existing business processes. The risk manager is now accountable for risk metrics. This requires putting a mechanism in place to collect this risk information at level where most operational risks materialise and aggregate this risk information to a level the Board cares about, while preserving the links to the front line and the resources involved and then tie together the risks in related business processes—all at the activity level so an audit trail is clear for internal audit to follow.

Organisations have realised that their board level attestations on the effectiveness of risk identification and assessment can no longer just be a facilitated interview at the senior management level; instead, there needs to be a rigorous process at the activity level through the lens of what is material, not just in isolation of a single business silo, but overall as all the pieces come together at the top. The goal is to identify and objectively assess operational risks and ensure risk mitigation is in place at the activity level independently and then collectively. This integrity of this risk information needs to be preserved when aggregating and summarising by the strategic goals of the organisation.

> “ Organisations have realised that their board level attestations on the effectiveness of risk identification and assessment can no longer just be a facilitated interview at the senior management level ”

Business areas have a number of interdependencies and therefore overlap of activities that cannot be identified today because of the heavily silo’d nature of most organisation. RM solutions are all about getting cross-functional transparency across the organisation so the organisation can make more strategic risk/reward decisions by being able to see the complete picture, enabling better business performance and more efficient corporate governance. A structured RM framework, or a risk taxonomy, identifies the valuable information that is reusable across business areas and eliminates the unnecessary redundancies.

A GRC Software solution, supporting a risk based approach is the only way this process will work effectively.   Please see the ‘IRMSA / BarnOwl risk maturity survey (2015) (http://www.barnowl.co.za/surveys/) to see how your organisation matches up?

BARNOWL

About BarnOwl

BarnOwl is a fully integrated governance, enterprise 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 c onfigure BarnOwl to meet your specific requirements.

www.barnowl.co.za

PHYSICAL ADDRESS

WEDGEFIELD OFFICE PARK
17 MUSWELL ROAD SOUTH
BRYANSTON

TEL: +27 (0) 11 540 9100

WEBSITE

WWW.BARNOWL.CO.ZA