

GPG RISK MANAGEMENT FORUM

23 March 2018

Integration of Governance, Risk and Compliance

Jonathan Crisp –Director

www.barnowl.co.za

jonathan@barnowl.co.za

+27 83 260 1653 (mobile)

+27 11 540 9100 (office)

Why the need for GRC

King IV: 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

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.

Gerry Grimstone, keynote speaker at an IIA's 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.

Michael Judin, partner in the Johannesburg based law firm, JUDIN COMBRINCK INC speaking on business judgement said you cannot act if you are not properly informed; you need to stress test and check your info. How did you come to your decision? You need to know enough and question with an understanding mind. Michael also spoke about business (and country) leaders' misconceptions that the power lies within the board room. The power really lies with the new millennials and the power of social media and the smart phone.

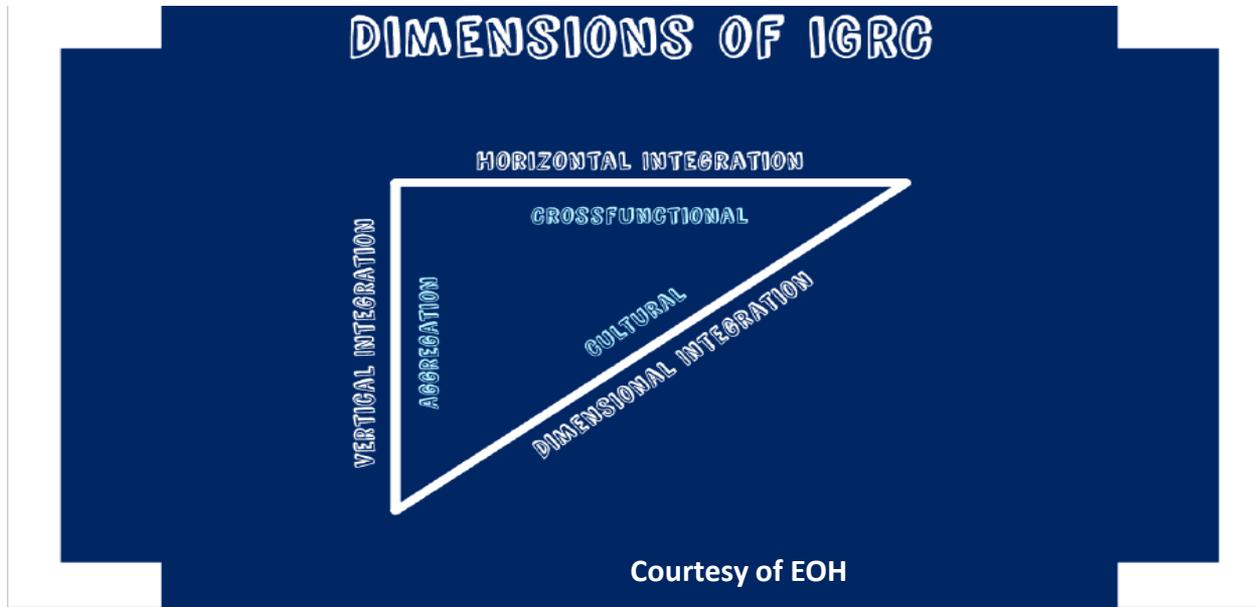
Cyril Ramaphosa said: "The architecture of the state-owned sector would be worked on to achieve better co-ordination, oversight and sustainability. Business Day 16 Feb 2018

The Value of GRC

- Focus on providing assurance on achievement of business objectives
- Focus on the top value creation and potential value erosion objectives
- Optimise the level of risk being taken to best achieve the organisation's objectives whilst still operating within the risk appetite of the organisation
- Identify key processes and risks that are inadequately controlled and / or over-controlled.
- The achievement of business objectives isn't just about managing what might go wrong (risks), but is actually about making things go right
- **Trusted advisor: key strategic value creation objectives and potential value erosion objectives (video clip):**
 - Reputational risk (Salomon Brothers, VW, Bell Pottinger, KPMG, Steinhoff, Brand SA...)
 - Technology disrupter risk/s (trusted advisor, bigger picture, thinking out the box)
 - People risk (leadership, accountability, performance, consequences)
 - Political risk (downgrades, Brand SA)
 - Decision making (in time (predictive), early warning, taking action)
 - Integrated Approach

www.barnowl.co.za/videos/

The need for an integrated and embedded approach



- **Horizontal Integration (Cross Functional):** Governance, Risk, Compliance, Assurance, Fraud, IT Security. Incorporate Risk Management in Strategy (and Vice Versa) and establish a healthy Risk Appetite (combined assurance)
- **Vertical Integration (Aggregation):** Top down, bottom up embedding of risk and coordinate and aggregate disparate risk information for Decision Makers
- **Dimensional Integration (Cultural):** Tone at the Top, manage Human Behaviour / Change Management as part of the Risk Management and the Audit Process (buy-in, embed, ownership, KPIs, consequences)

Cyril Ramaphosa said: “The architecture of the state-owned sector would be worked on to achieve better co-ordination, oversight and sustainability”.

Business Day 16 Feb 2018

<http://www.barnowl.co.za/event/9849/>

PFMA

38. General responsibilities of accounting officers.—(1) The accounting officer for a department, trading entity or constitutional institution—

- (a) must ensure that that department, trading entity or constitutional institution has and maintains—
 - (i) effective, efficient and transparent systems of financial and risk management and internal control;
 - (ii) a system of internal audit under the control and direction of an audit committee complying with and operating in accordance with regulations and instructions prescribed in terms of **sections 76 and 77**;
 - (iii) an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective;
 - (iv) a system for properly evaluating all major capital projects prior to a final decision on the project;

51. General responsibilities of accounting authorities.—(1) An accounting authority for a public entity—

- (a) must ensure that that public entity has and maintains—
 - (i) effective, efficient and transparent systems of financial and risk management and internal control;
 - (ii) a system of internal audit under the control and direction of an audit committee complying with and operating in accordance with regulations and instructions prescribed in terms of sections 76 and 77; and
 - (iii) an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective;
 - (iv) a system for properly evaluating all major capital projects prior to a final decision on the project;

MFMA

62. General financial management functions.—(1) The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure—

- (c) that the municipality has and maintains effective, efficient and transparent systems—
 - (i) of financial and risk management and internal control; and
 - (ii) of internal audit operating in accordance with any prescribed norms and standards;

165. Internal audit unit.—

- (1) Each municipality and each municipal entity must have an internal audit unit, subject to [subsection \(3\)](#).
- (2) The internal audit unit of a municipality or municipal entity must:
 - (a) prepare a risk based audit plan and an internal audit program for each financial year;
 - (b) advise the accounting officer and report to the audit committee on the implementation of the internal audit plan and matters relating to—
 - (i) internal audit;
 - (ii) internal controls;
 - (iii) accounting procedures and practices;
 - (iv) risk and risk management;
 - (v) performance management;
 - (vi) loss control; and
 - (vii) compliance with this Act, the annual Division of Revenue Act and any other applicable legislation; and

MFMA (continued)

166. Audit committees.—

- (1) Each municipality and each municipal entity must have an audit committee, subject to subsection (6).
- (2) An audit committee is an independent advisory body which must—
 - (a) advise the municipal council, the political office bearers, the accounting officer and the management staff of the municipality, or the board of directors, the accounting officer and the management staff of the municipal entity, on matters relating to—
 - (i) internal financial control and internal audits;
 - (ii) risk management;
 - (iii) accounting policies;
 - (iv) the adequacy, reliability and accuracy of financial reporting and information;
 - (v) performance management;
 - (vi) effective governance;
 - (vii) compliance with this Act, the annual Division of Revenue Act and any other applicable legislation;
 - (viii) performance evaluation; and
 - (ix) any other issues referred to it by the municipality or municipal entity;

King IV

(copyrighted to The Institute of Directors Southern Africa).

- **The definition of corporate governance for the purposes of King IV**, is defined as the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes:
 - Ethical culture
 - Good performance
 - Effective control
 - Legitimacy

- **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.

- **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 good corporate citizen.

King IV

(copyrighted to The Institute of Directors Southern Africa).

- **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.

- **Internal Audit:**
 - 48. The governing body should assume responsibility for internal audit by setting the direction for the internal audit arrangements needed to provide objective, relevant assurance that contributes to the effectiveness of governance, risk management and control processes.
 - 58. The governing body should monitor on an ongoing basis that internal audit:
 - Follows an approved risk-based internal audit plan; and
 - Reviews the organisational risk profile regularly, and proposes adaptations to the internal audit plan accordingly.
 - 59. The governing body should ensure that internal audit provides an overall statement annually as to the effectiveness of the organisation's governance, risk management and control processes.

<http://www.barnowl.co.za/insights/king-iv-report-risk-compliance-and-assurance/>

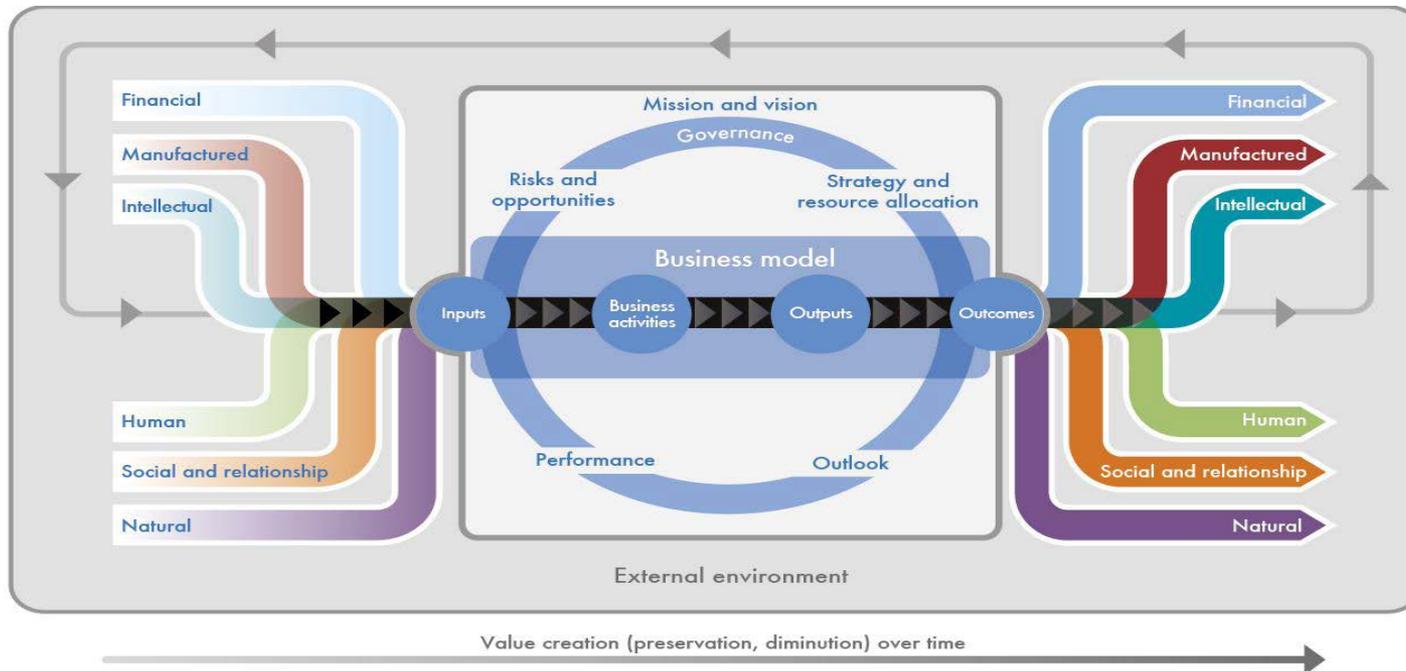
King IV

(copyrighted to The Institute of Directors Southern Africa).

Michael Judin, partner in the Johannesburg based law firm, JUDIN COMBRINCK INC on 'Why King IV is not another layer of regulation but creates add-on value', spoke about business (and country) leaders' misconceptions that the power lies within the board room. The power really lies with the new millennials and the power of social media and the smart phone.

<http://www.barnowl.co.za/info-sharing/information-sharing-23-february-2017/>

<http://www.barnowl.co.za/insights/good-corporate-governance-alive-and-kicking/>

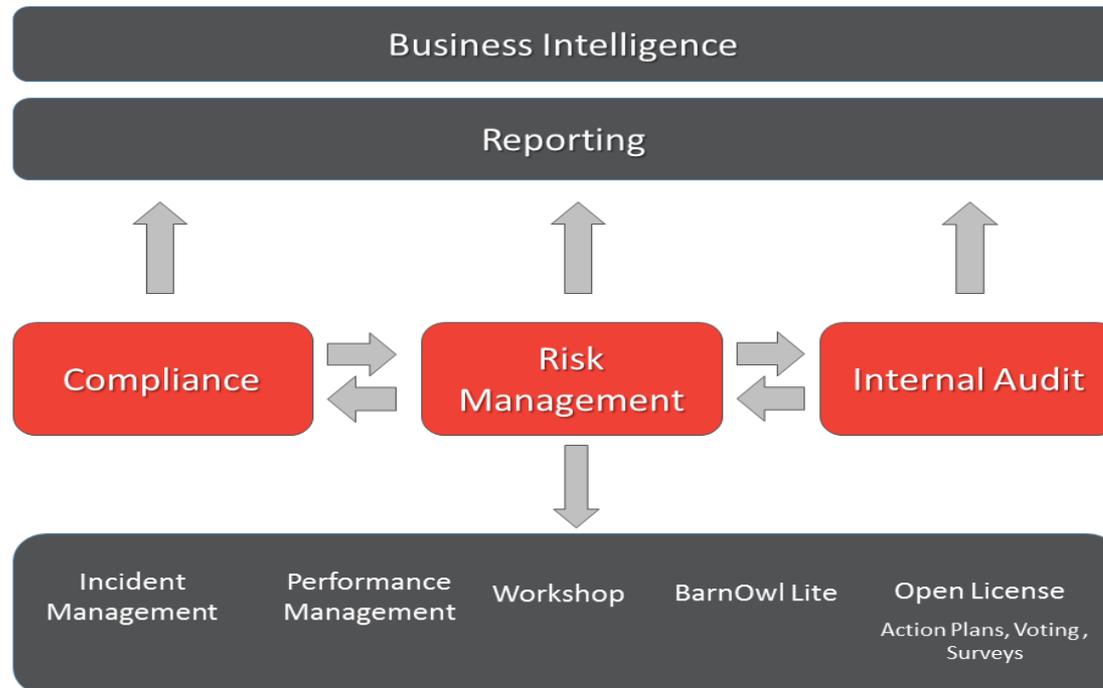


<http://www.barnowl.co.za/info-sharing/barnowl-information-sharing-session-29th-july-2016-on-the-integrated-report-and-integrated-thinking-in-the-reign-of-king-iv-by-leigh-roberts/>

By Leigh Roberts CA(SA), IRC of SA -CEO

Why the need for integrated GRC software

- Facilitates and embeds integrated GRC providing enterprise-wide visibility of risk with combined assurance reporting
- Incorporates built-in best practices and supports the adoption of the standards (COSO, ISO31000, National Treasury, IPPF, GACP, PFMA, MFMA, King IV)
- Provides an up to date dashboard of your risk universe (drill down bar, pie, trend, heat maps...) in support of informed decision making
- Enables the monitoring of risk appetite at all levels of your organisation with aggregation
- Enables real time updating of Risks, KRIs, Controls, Incidents, Findings, Follow-up, Action Plans
- Facilitates a culture of risk and control within your organisation (CSAs, online action plans etc.)
- Reduces admin / reporting time
- Enhanced integrity of data, standards, common risk language, transversal risks
- Reputation / Director / Accounting officer protection (formalised approach to risk management / compliance)



Why the need for integrated GRC software

- Advanced business intelligence reporting in support of decision making:
 - Top risk trends by business unit
 - Top risks and their root causes
 - Root cause analysis by business unit and process
 - Key performance linked to business objectives and risk management
 - Key Risk indicators – leading indicators (predictive)
 - Combined assurance reporting

<http://www.barnowl.co.za/insights/still-using-excel-for-risk-management-and-or-audit/>

<http://www.barnowl.co.za/insights/6-ways-risk-based-auditing-adds-value-to-your-organisation/>

‘The risks of risk management’ written by C. Burt, Halex Consulting Limited UK: http://www.slideshare.net/cjburt/the-risks-of-risk-management-61986579?qid=f9eaaf9d-9168-4096-81f1-976e0f6cddcf&v=&b=&from_search=1

In summary...

- Ensures senior management and the board / governing body are aware of the current residual risk status linked to key strategic value creation objectives and potential value erosion objectives
- Enables an organisation to optimise the level of risk being taken to best achieve the organisation's objectives whilst still operating within the risk appetite of the organisation
- The achievement of business objectives isn't just about managing what might go wrong (risks), but is actually about making things go right

<http://www.barnowl.co.za/insights/6-ways-risk-based-auditing-adds-value-to-your-organisation/>

'The risks of risk management' written by C. Burt, Halex Consulting Limited UK: http://www.slideshare.net/cjburt/the-risks-of-risk-management-61986579?qid=f9eaaf9d-9168-4096-81f1-976e0f6cddcf&v=&b=&from_search=1

Thank You

Jonathan Crisp –Director

www.barnowl.co.za

jonathan@barnowl.co.za

+27 83 260 1653 (mobile)

+27 11 540 9100 (office)



BARNOWL