IIA WESTERN CAPE
12 OCTOBER 2017

ELEVATING AUDIT THROUGH OBJECTIVE / RISK-BASED AUDITING

Jonathan Crisp –Director

www.barnowl.co.za

jonathan@barnowl.co.za

+27 83 260 1653 (mobile)

+27 11 540 9100 (office)

BARNOWL

Elevating audit through objective / risk-based auditing

- The Institute of Internal Auditors (IIA) framework defines internal auditing as: ‘An independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It 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’

- It is a common fallacy that the Internal Audit function exists to pick holes in management’s operations. This is not at all the case! Internal Audit must involve the organisation more in the audit process and produce recommendations that contribute to the organisation’s objectives. At the same time, the internal audit activity has to be careful not to lose its independence and objectivity because of moving closer to the operations

BARNOWL

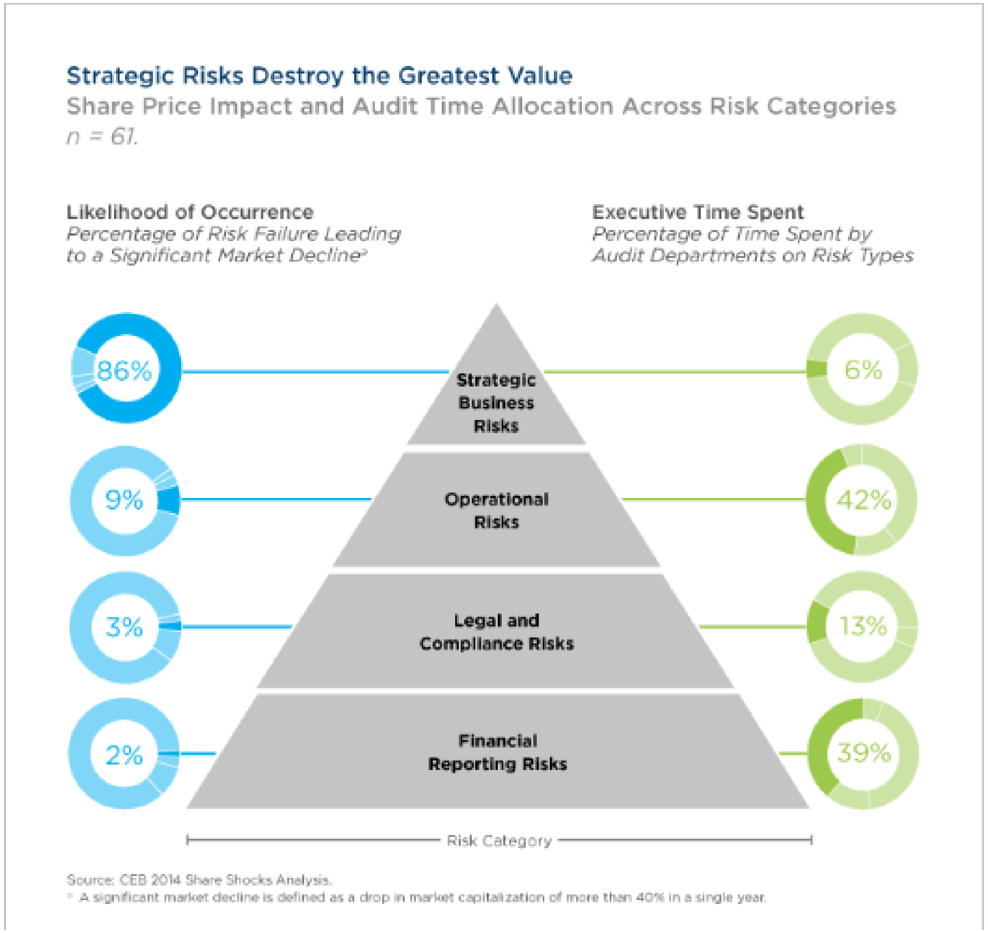
Elevating audit through objective / risk-based auditing

- **The consequences of poor risk management (Video clip)**:
  - Reputational risk
  - Technology disrupter risk/s
  - People risk
  - Political risk
  - Decision making

- **Effective Risk Management and Assurance:**
  - 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.
  - Internal Audit transitions from the business of providing subjective opinions on "control effectiveness" on a small fraction of the risk universe to ensuring senior management and the board are aware of the current residual risk status linked to key strategic value creation objectives and potential value erosion objectives.

BARNOWL

Elevating audit through objective / risk-based auditing



https://buff.ly/2x1NCnT: Among the more than 10,000 companies that make up CEB's global membership—including almost 2,000 general counsel, chief compliance executives, chief audit executives, chief information security officers, and heads of ERM—the best companies employ three standout risk management practices to avoid Organizational Drag:

1.Incorporate Risk Management in Strategy (and Vice Versa) and Establish a Healthy Risk Appetite

2.Coordinate Disparate Risk Information for Decision Makers

3.Manage Human Behavior as Part of the Risk Management Process

BARNOWL

6 ways objective / risk-based auditing adds value to your organisation

- **Business focussed approach assisting the organisation to achieve its objectives**: Audit focus on providing assurance on achievement of business objectives as opposed to standard audit programmes where it is not always clear how these impact the bigger picture.
- **Internal Audit focuses on the top value creation and potential value erosion objectives elevating IA's stature and value add**: Audit recommendations provide the greatest value added in terms of the optimising the level of risk being taken to best achieve the organisation's objectives whilst still operating within the risk appetite of the organisation.
- **Inclusive audit approach facilitating buy in and ownership from management**: Management is far more likely to support the audit work when they are involved in the process and can see how the audit's recommendations relate to the achievement of their business objectives. Embedded risk management down to all levels.
- **Optimal level of assurance supporting the achievement of business objectives**: Risk-based auditing is more efficient because it directs audits at the high-risk areas, as opposed to simple rotation of predominantly financial areas, which may not represent the greatest risk.
- **Improved operational efficiency**: Risk-based auditing should highlight key processes and risks that are inadequately controlled and / or over-controlled.
- **More effective use of audit resources**: The audit plan is based on clear instructions from senior management and the board on the level of risk assessment rigor and independent assurance they require related to strategic / business objectives. It differs from the alternative approach, whereby the resources available determine the audits that can be conducted.

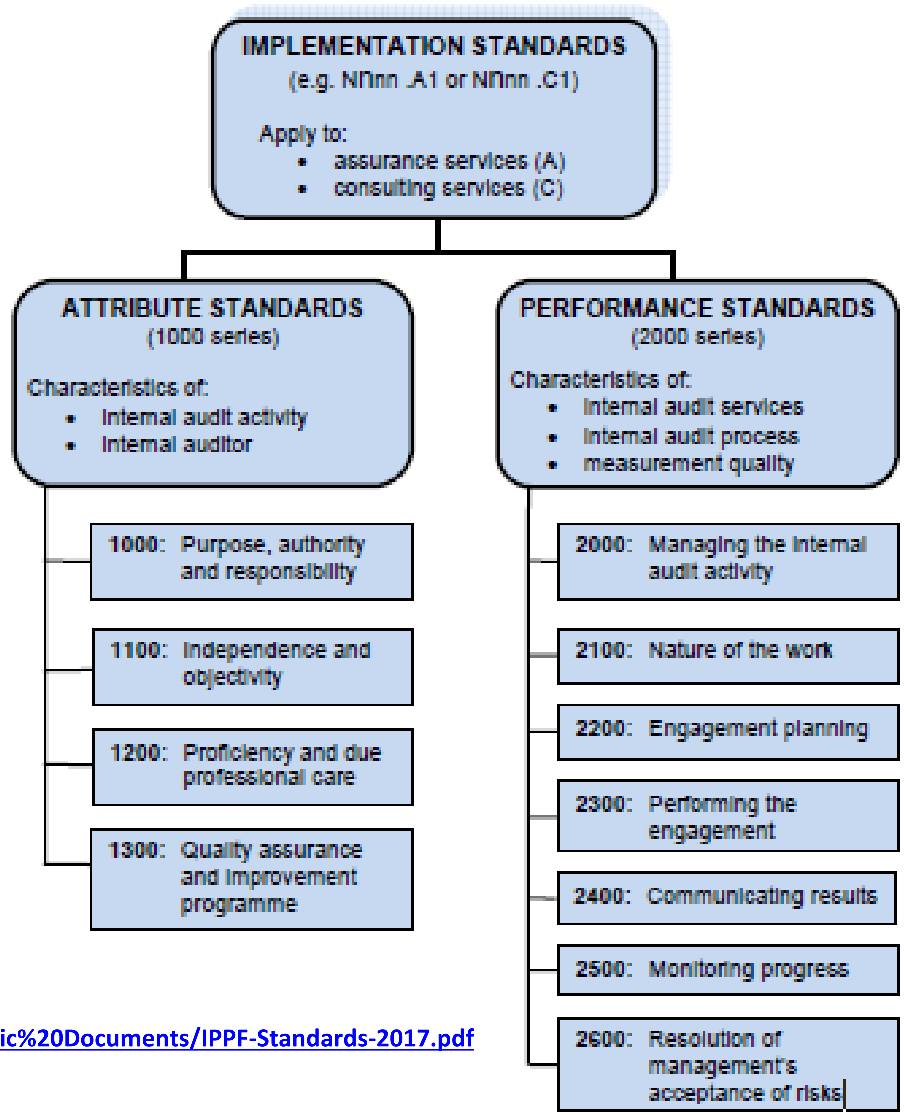
http://www.barnowl.co.za/insights/6-ways-risk-based-auditing-adds-value-to-your-organisation/

'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

BARNOWL

International Standards for the Professional Practice of Internal Auditing (IPPF)

Figure 1.2: Summary of the Standards



https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf

BARNOWL

International Standards for the Professional Practice of Internal Auditing (IPPF)

- **1220.A3** – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.
- **2010.A1 –** The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.
- **2010.C1 –** The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.
- **2100 – Nature of Work -** The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

BARNOWL

International Standards for the Professional Practice of Internal Auditing (IPPF)

- **2120 – Risk Management -** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes:
  - Organizational objectives support and align with the organization's mission.
  - Significant risks are identified and assessed.
  - Appropriate risk responses are selected that align risks with the organization's risk appetite.
  - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

- **2200 – Engagement Planning -** Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

- **2450 – Overall Opinions -** When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

- **2600 – Communicating the Acceptance of Risks -** When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

BARNOWL

Audit approach based on Risk Maturity

	Controls	Monitoring	Audit approach
Risk enabled	All risks identified and assessed. Regular reviews of risks. Responses are in place to manage risks	Management monitor that all types of response are operating properly. All managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	**Assurance**
Risk managed		Management monitor that all types of response are operating properly. Most managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	
Risk defined	Majority of risks identified and assessed. Regular reviews of risks. Responses are in place to manage most risks	Some management monitoring that all types of response are operating properly	**Consultancy**
Risk aware	Controls may be in place but are not linked to risks	Little monitoring	Cannot use RBIA. Adopt a consultancy approach to promote risk management and achieve 'risk defined' status. Carry out risk driven audits.
Risk naive	Controls, but some may be missing or incomplete	Very little, if any monitoring	

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.

BARNOWL

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 adaptions 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/

http://www.barnowl.co.za/event/information-sharing/ The journey from King I to King IV: Why King IV is not another layer of regulation but creates add-on value. presented by Michael Judin, partner in the Johannesburg based law firm, JUDIN COMBRINCK INC.

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

BARNOWL

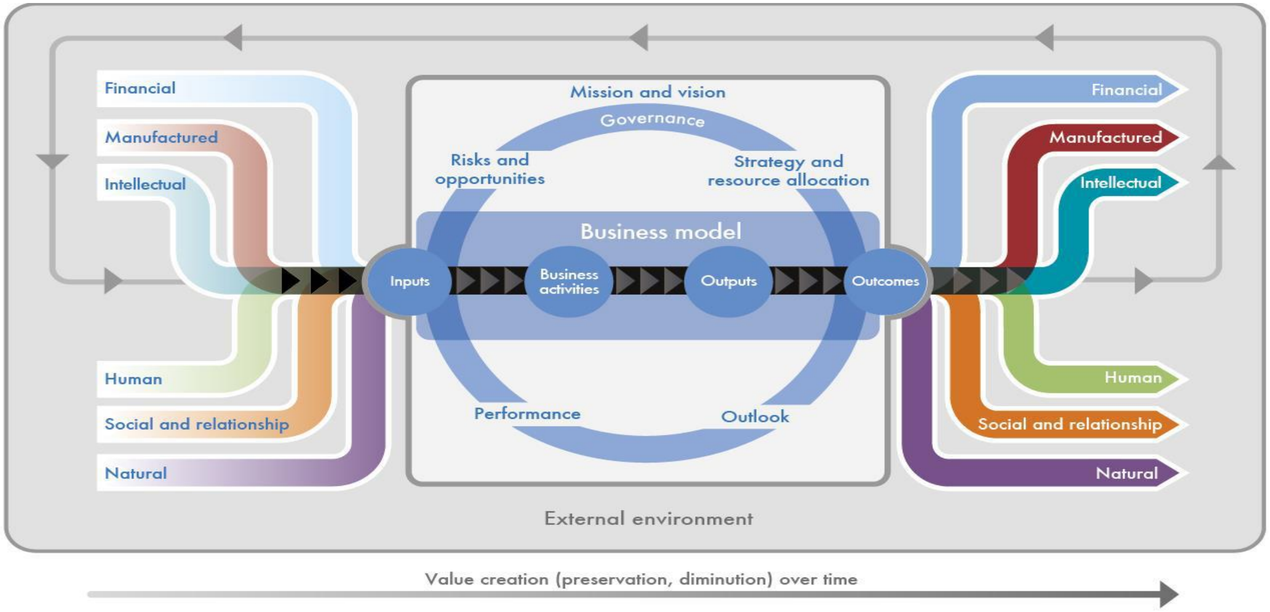
King IV

(copyrighted to The Institute of Directors Southern Africa).

In summary a few points worth noting about the King code:

- It's not just another layer of regulation but a real value add. It's here to help us
- The King code appeals to a way of life rather than just a way of doing business; Governance supported by King IV is an aspirational code
- People who understand King embrace it
- Don't ignore the millennials; understand the value of the 3 Ps (People, Planet and Profit)
- It's not only about risk but also the opportunity within the risk
- Corruption is at a tipping point
- It's you (your business) versus the people
- Appreciating the value of information and technology; business disrupters; artificial intelligence, millennial thinking.

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



http://www.barnowl.co.za/wp-content/uploads/2016/08/The-IR-and-IT-in-the-reign-of-KIng-IV-JUly-2016-R1-final.pdf

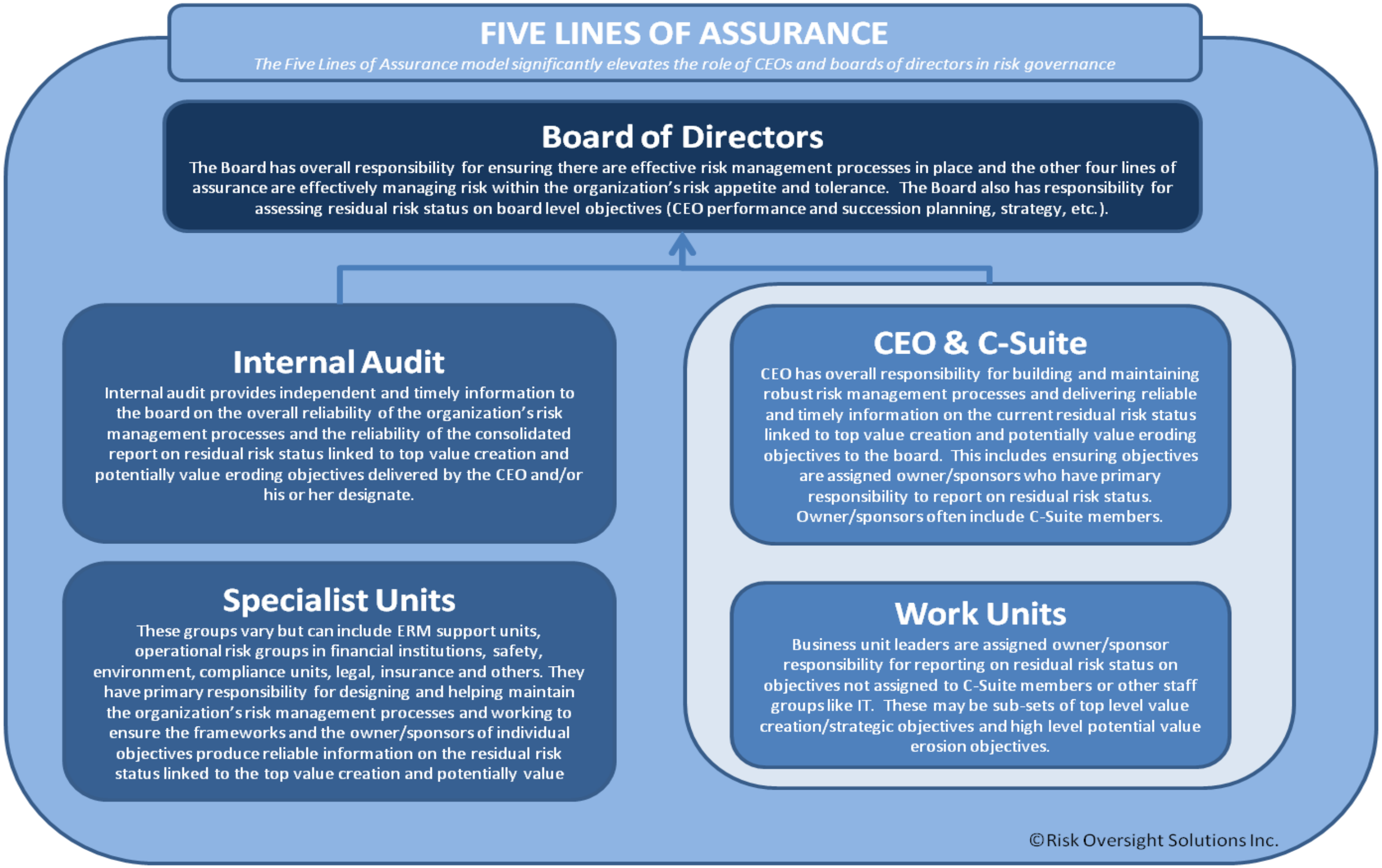
By Leigh Roberts CA(SA), IRC of SA -CEO

BARNOWL

Objective Centric Five Lines of Assurance

- Want more value from your ERM and internal audit spending? Objective centric ERM and internal audit is the answer.

  Tim Leech: Risk Oversight Solutions: http://riskoversightsolutions.com/ro-resources



BARNOWL

Objective Centric Five Lines of Assurance

- Boards are active participants, not bystanders
- Communicates and reinforces the key role the CEO and the Board must/should play in ERM going forward.
- Emphasis is on risk taking and risk treatment
- Senior management and boards are provided with a concise picture of the state of residual risk status linked to the organization's top value creation and erosion objectives to help them assess its acceptability
- Boards and senior management define the level of risk assessment rigor and independent assurance they want. This defines ERM staff and IA's scope and resources required
- Supports better resource allocation decisions
- The objective is not to minimize risk but rather to optimize the level of risk being accepted to best achieve the organization's objectives while still operating within an acceptable level of retained/residual risk.
- In addition to analysing "residual risk status" the process focuses on "optimising risk treatments" – i.e. the lowest possible cost combination of risk treatments necessary to operate within risk appetite/tolerance
- IA focuses on the top value creation and potential value erosion objectives elevating IA's stature and value add

BARNOWL

Objective Centric Five Lines of Assurance

- IA staff must learn to consider and assess the full range of “risk treatments” not just “internal controls”.
- IA actively participates in the process of generating the information necessary for management and boards to assess if the current residual risk status is, or is not, within their risk appetite and tolerance (i.e per the FSB the “Risk Appetite Framework”)
- IA transitions from the business of providing subjective opinions on “control effectiveness” on a small fraction of the risk universe to ensuring senior management and the board are aware of the current residual risk status linked to key strategic value creation objectives and potential value erosion objectives. Conflict and non-productive haggling over wording, a common problem in direct report internal audit, is reduced significantly
- IA actively participates in the process of optimizing risk treatment design by providing quality assurance reviews and feedback
- IA plays a role ensuring that the board is actively participating in the organization’s strategic planning process and meeting escalating risk oversight expectations

BARNOWL

Objective Centric Five Lines of Assurance

- In organizations with dedicated risk staff their role is to create and maintain the Risk Appetite/risk management framework. IA's role is to report on the process and reliability of the consolidated report from management on residual risk status
- Elevates ERM from what many see as a compliance activity done annually to a key part of strategy development, value creation and better managing potentially value eroding objectives.
- ERM work better supports the new expectation that boards are responsible for ensuring that effective risk management processes are in place and management is operating the organization within the board's risk appetite and tolerance
- ERM support staff receive clear instructions from senior management and the board on the level of risk assessment rigor and independent assurance they want on all objectives in the OBJECTIVES REGISTER

Tim Leech: Risk Oversight Solutions: http://riskoversightsolutions.com/ro-resources

BARNOWL

TopRisksFromFindings.pdf - Adobe Reader

FIGURE 2.6 – TOP RISKS BASED ON FINDINGS (BI)

File Edit View Window Help

My Files 1 / 1 80% Tools Sign Co

BARNOWL

All cells, rows and columns in this report filter all other cells, rows and columns. Click to SELECT, click again to DESELECT.

TOP 10 RISKS

RiskTitle	Year of EndDate 2011	2012	2013
Inadequate adherence to controls in place to prevent losses	27	3,483	2,412
Misappropriation of bulk deposit funds due to the Inability to identify the customer making the bulk deposit..	45	3,798	1,701
Inaccurate recording of working hours.	54	2,799	1,962
Stockholding Inaccurate		3,177	1,278
Excessive shrinkage due to inadequate stock monitoring		2,889	1,476
Lack of timely, complete and accurate banking of daily takings.			3,834
Injuries / death due to inadequate monitoring, maintenance and or operation of machinery.	9	1,737	1,602
Causes for not achieving targets not identified thereby not addressing the actual problem.	72	3,204	
Unauthorised price overides taking place	18	2,223	945
Out of stock situations arising due to poor supplier performance	54	2,169	738

TOP BUSINESS UNITS @ LEVEL 3

Unit Level 1	Unit Level 2	Unit Level 3	
ABC Retail Group Ltd	Operations	Ops Area 1	60,984
		Ops Area 2	45,945
		Ops Area 3	27,990
		Ops Area 4	54,225
		Roofbuild	504
	Support Office	Advertising (Ops / Dept Level)	81
		Creditors (New Program)	459
		Creditors (Old Program)	63
		Finance	171
		Legal	54
		Payroll	162
		Procurement (Ops / Dept level)	297
		SO - Debtors	18
		SO - Fixed Assets	27

FIGURE 2.7 – RISK AND ROOT CAUSE ANALYSIS (BI)

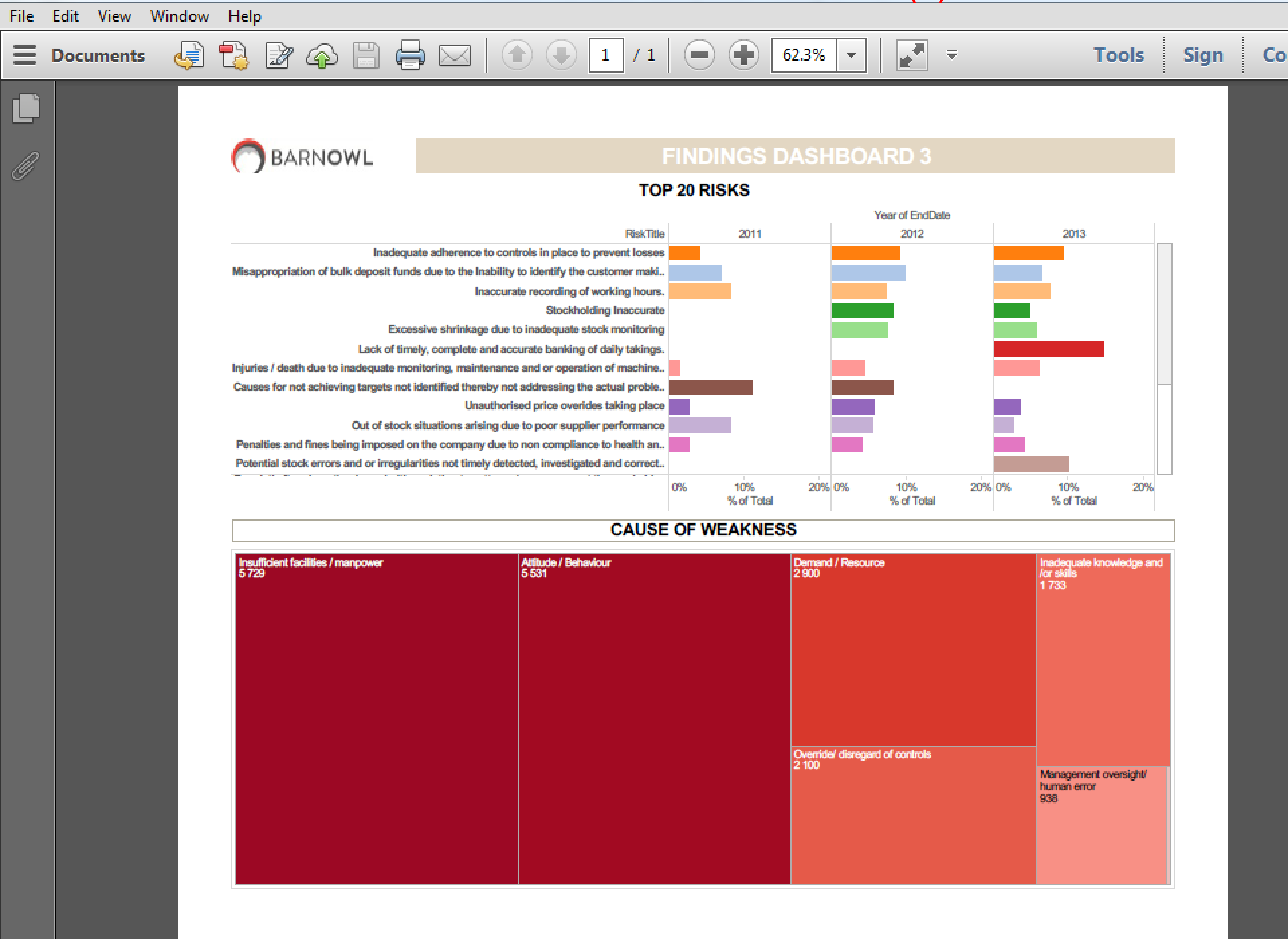
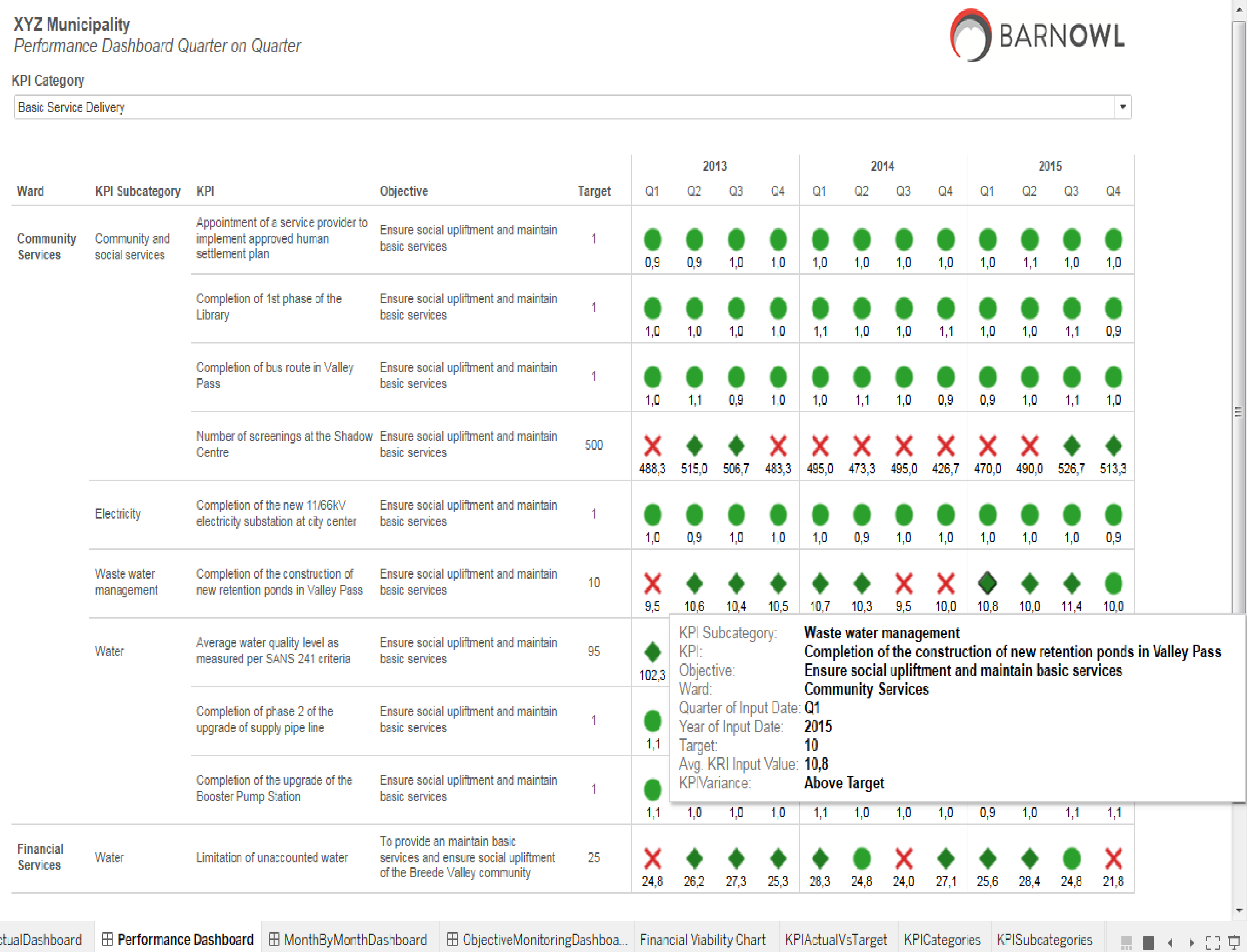


FIGURE 1.4.4 – KPIs



Ward	KPI Subcategory	KPI	Objective	Target	2013 Q1	2013 Q2	2013 Q3	2013 Q4	2014 Q1	2014 Q2	2014 Q3	2014 Q4	2015 Q1	2015 Q2	2015 Q3	2015 Q4
Community Services	Community and social services	Appointment of a service provider to implement approved human settlement plan	Ensure social upliftment and maintain basic services	1	0,9	0,9	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,1	1,0	1,0
		Completion of 1st phase of the Library	Ensure social upliftment and maintain basic services	1	1,0	1,0	1,0	1,0	1,1	1,0	1,0	1,1	1,0	1,0	1,1	0,9
		Completion of bus route in Valley Pass	Ensure social upliftment and maintain basic services	1	1,0	1,1	0,9	1,0	1,0	1,1	1,0	0,9	0,9	1,0	1,1	1,0
		Number of screenings at the Shadow Centre	Ensure social upliftment and maintain basic services	500	488,3	515,0	506,7	483,3	495,0	473,3	495,0	426,7	470,0	490,0	526,7	513,3
	Electricity	Completion of the new 11/66kV electricity substation at city center	Ensure social upliftment and maintain basic services	1	1,0	0,9	1,0	1,0	1,0	0,9	1,0	1,0	1,0	1,0	1,0	0,9
	Waste water management	Completion of the construction of new retention ponds in Valley Pass	Ensure social upliftment and maintain basic services	10	9,5	10,6	10,4	10,5	10,7	10,3	9,5	10,0	10,8	10,0	11,4	10,0
	Water	Average water quality level as measured per SANS 241 criteria	Ensure social upliftment and maintain basic services	95	102,3											
		Completion of phase 2 of the upgrade of supply pipe line	Ensure social upliftment and maintain basic services	1	1,1											
		Completion of the upgrade of the Booster Pump Station	Ensure social upliftment and maintain basic services	1	1,1	1,0	1,0	1,0	1,1	1,0	1,0	1,0	0,9	1,0	1,1	1,1
Financial Services	Water	Limitation of unaccounted water	To provide an maintain basic services and ensure social upliftment of the Breede Valley community	25	24,8	26,2	27,3	25,3	28,3	24,8	24,0	27,1	25,6	28,4	24,8	21,8

In summary…

- In order for the auditor to add value to and improve the company’s operations, it is important for the auditor to understand the business objectives of the organisation and the risks that threaten or need to be taken (opportunity) to achieve these objectives. Knowing where the biggest risks lie, makes it easier for the internal auditor to focus their audit effort on the areas where the most value can be added.

  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

BARNOWL

Thank You

Jonathan Crisp –Director

www.barnowl.co.za

jonathan@barnowl.co.za

+27 83 260 1653 (mobile)

+27 11 540 9100   (office)

BARNOWL