IRMSA Conference 2024

The impact on the effectiveness of risk management software and the basics of risk management

02 October 2024

Presented by Jonathan Crisp

BARNOWL

Agenda

- The need for risk management and the standards
- The benefits of risk management
- The need for risk management software
- Why Excel doesn’t cut it
- Risk management basics
- Embedding risk management (non intrusively)
- Conclusion

The need for Risk Management

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

Risk Management Standards #1

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.

Risk Management Standards #2

4. LEGISLATIVE MANDATE

- **Public Finance Management Act 29 of 1999 as amended.**
  - **Section 38 (1)(a)(i):** The accounting officer of the department, trading entity or constitutional institution must ensure that the department, trading entity or constitutional institution has and maintains effective, efficient, and transparent system of financial and risk management and internal control.
- **Municipal Finance Management Act 56 of 2003.**
  - **Section 62 (1)(c)(i):** The Accounting Officer of a municipality is responsible for managing the financial administration of the municipality and must for this purpose take all responsible steps to ensure that the municipality has and maintains effective, efficient, and transparent systems of financial and risk management and internal control.
- **Treasury Regulations**
  - **Section 3.2.11:** The internal audit function must assist the accounting officer in maintaining efficient and effective controls by evaluating those controls to determine their effectiveness and efficiency, and by developing recommendations for enhancement or improvement. The controls subject to evaluation should encompass the following –
    a) The information systems environment;
    b) The reliability and integrity of financial and operational information;
    c) The effectiveness of operations;
    d) Safeguarding of assets; and
    e) Compliance with laws, regulations, and controls.

The governance structures should ensure that:

- There are regular and accurate reports on the risk profile of the organisation;
- There is regular assessment of the effectiveness and adequacy of the controls;
- There is periodic assessment of any new and emerging risk; and
- There is regular review of the risk tolerance and the breaches thereof.

The benefits of Risk Management

- 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 / accounting officer protection

The need for Risk Management software

An organisation cannot manage risk effectively without the use of specialised risk software. Risk management software:

- facilitates and embeds risk management in your organisation
- facilitates 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, risk & control self-assessments (RCSAs), KRIs etc.
- enables a common risk taxonomy which improves the quality and consistency of data captured and gives you one version of the truth (with audit trails)
- facilitates 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.
- provides up to date reporting and dashboards of your risk universe including consolidated and trend reporting at all levels of your organisation (at the click of a button)
- ensures Director / Accounting officer protection through a formalised system-driven approach

Why Excel doesn't cut it #1

- Multiple 'versions of the truth' with little or no version control with 100s of spreadsheets floating around the organisation
- Unstructured data (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)
- Data is not relational (e.g. Controls are lumped together and not linked to the relevant CFs, APs are lumped together and not linked to the relevant object making them too vague to be effective)
- The quality and completeness of data is compromised
- Information is not consolidated in a single repository
- Security / Permissions on data is non-existent in most cases
- Excel is silo based and ignores interdependencies of risk across business units and functional areas
- 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 with no ability to send out automated email notifications, reminders, escalations etc. based on system triggers
- Complex spreadsheets are 'lost' when the creator leaves the organisation and are re-invented again and again by a new person, wasting time, money and effort.

Why Excel doesn't cut it #2

- Importing risks from Excel into your system on a periodic basis means that you are not embedding and driving ownership of risk management in your organisation. (i.e. not using RCSAs, APs, KIs effectively)
- It means that risks and controls are not updated regularly enough and too much time is spent by the risk function gathering information rather than analysing and providing decision-making insight to the business.
- It means that your risk reporting is always out of date
- It means that risk management will never serve as an early warning system
- It's important to remember that the risk function is the facilitator of risk and not the owner of risk.

Getting the basics right #1 – structured data

One of the most significant reasons for the failure of any system or process is the principle of 'garbage in, garbage out.' This holds true whether you are dealing with a highly sophisticated IT system or the basic tools like Excel or Word.

Essentially, if you feed low-quality or irrelevant data into a system, it will produce outputs of similar quality, if not worse.

In essence, a system or process inundated with poor-quality data does little more than expedite the generation of undesirable results. Such a system or process, cluttered with useless information, provides no value..

Getting the basics right:

Step 1: Objective: Identify an Objective / Outcome. E.g. *1. We act with integrity*

Step 2: Risk: Identify the risks that will prevent you from achieving the objective or a risk that you would like to take to achieve the objective. e.g. *1.1 Cyber threat*

Step 3: Contributing Factor (CF) / Cause: Identify the contributing factors / causes that cause the risk. E.g. *1.1.1 Unauthorised access to data, 1.1.2. Phishing and social engineering, 1.1.3. Denial of service attack, 1.1.4 Malware infections*

Step 4a: Preventative Controls: Identify preventative controls to mitigate the contributing factors. One control can be used to mitigate more than one contributing factor so be sure to reference correctly. E.g. *1.1.1 Anti-virus software (linked to CF 1.1.1 and 1.1.4 above)*

Step 4b: Mitigating Controls: Identify the controls you have in place to manage the risk should it materialise. These controls are linked directly to the risk or can be linked to individual Impacts/ Consequences. E.g. *1.1.2 – Contain the data loss as soon as possible, 1.1.3 Consider whether data breach notification is required*

Step 5: Action plans Create action plan/s against the specific control/s and assign a responsible owner and due date. E.g. *Install the latest anti-virus software by dd/mm/yyyy assigned to responsible owner Joe Soap* linked to control: *1.1.1 Anti-virus software.* To ensure the effectiveness of action plans, it is crucial to link them to the appropriate object/s (Risk or CF or Control), making them specific and providing relevant context. Generic action plans, such as 'Manage cyber risk', linked to the risk 'Cyber threat' state the obvious and offer no tangible value.

Getting the basics right #2 – Objective>Risks>CFs

Example of a structured risk register

Ideally, it is best to put each data item in separate cells in Excel. In the example below, contributing factors are in separate cells:

Objective	Risk											Contributing Factor	
Objective Title	Risk Reference	Risk Title	Risk Category	Risk Subcategory	Risk Description	Risk II	Risk IL	Risk IR	Risk RI	Risk RL	Risk RR	Contributing Factor Reference	Contributing Factor Title
We act with integrity	010a	010a - Cyber threat	Cyber	Cyber	Cyber criminals exploiting technology to conduct cyber-attacks with the aim of defrauding and/or disrupting the business or committing espionage	12.00	3.00	36.00	12.00	2.25	27.00	010a.C01	010a.C01 - Unauthorised access to sensitive or personally identifiable information (Data Breach)
												010a.C02	010a.C02 - Deceptive communications designed to elicit users' sensitive information (including network credentials) (Phishing and Social Engineering)
												010a.C03	010a.C03 - Overwhelming an ICT network with traffic such that it cannot process, sometimes causing the network to fail. (Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks)
												010a.C04	010a.C04 - A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host (Malware Infections)
												010a.C05	010a.C05 - A tool used to encrypt or lock victims' data until a ransom is paid (Ransomware)
												010a.I01	010a.I01 - Loss of customers confidence/ loss of volumes
												010a.I02	010a.I02 - Regulatory Breach resulting in fines / penalties / loss in licenses
												010a.I03	010a.I03 - Subsequent reputational impact to the Company Group (from all)
												010a.I04	010a.I04 - Non-compliance with regulatory requirements (financial reporting requirements)

Getting the basics right #3 – CF>Controls

Controls are also captured in separate cells against each contributing factor. If you decide to put multiple controls in one cell, then referencing is critical so that the user / system knows which controls belong to which contributing factors. In some cases, the same control can be used to manage more than one contributing factor. Therefore referencing of contributing factors and controls is critical.

Contributing Factor		Control	
Contributing Factor Reference	**Contributing Factor Title**	**Control Reference**	**Control Title**
010a.C01	010a.C01 - Unauthorised access to sensitive or personally identifiable information (Data Breach)	010a.CPC05	010a.CPC05 - Network intrusion detection sensors
		010a.CPC06	010a.CPC06 - Application log records multiple failed login attempts from an unfamiliar remote system
		010a.CPC07	010a.CPC07 - Email administrator identifies a large number of bounced emails with suspicious content
		010a.CPC08	010a.CPC07 - Network administrator identifies an unusual network traffic flows
010a.C02	010a.C02 - Deceptive communications designed to elicit users' sensitive information (including network credentials) (Phishing and Social Engineering)	010a.CPC02	010a.CPC02 - Staff are trained to avoid redirection to a malicious URL that installs malware on their device
		010a.CPC03	010a.CPC03 - Staff are trained to avoid engaging with email/attachments designed to steal information or install malware on their device
		010a.CPC04	010a.CPC04 - Staff are trained not to engage with email messages or websites that have created to imitate the genuine user or site in an attempt to deceive victims
010a.C03	010a.C03 - Overwhelming an ICT network with traffic such that it cannot process, sometimes causing the network to fail. (Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks)	010a.CPC05	010a.CPC05 - Network intrusion detection sensors
010a.C04	010a.C04 - A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host (Malware Infections)	010a.CPC01	010a.CPC01 - Antivirus software detects that a device is infected with malware
010a.C05	010a.C05 - A tool used to encrypt or lock victims' data until a ransom is paid (Ransomware)	010a.CPC01	010a.CPC01 - Antivirus software detects that a device is infected with malware

Getting the basics right #4 –APs linked appropriately

You will notice below that action plans are captured in separate cells against the controls or at least referenced correctly so that the user / system knows which action plan is addressing which item (the risk, the contributing factor or the control). The more specific the action plan is, the more effective it will be and the more chance you have that something will be done about it.

Control				Action Plan					
Control Reference	Control Title	Control Adequacy	Control Effectiveness	Action Plan Title	Action Plan Status	Action Plan Percentage Complete	Action Plan Start Date	Action Plan Due Date	Action Plan Owners
010a.CPC05	010a.CPC05 - Network intrusion detection sensors	Adequate	Partially Effective						
010a.CPC06	010a.CPC06 - Application log records multiple failed login attempts from an unfamiliar remote system	Adequate	Effective						
010a.CPC07	010a.CPC07 - Email administrator identifies a large number of bounced emails with suspicious content	Adequate	Ineffective	Formal process to monitor bounced emails	Not Started	0.00	2023/11/07	2023/11/30	Manager, IA (Responsible)
010a.CPC08	010a.CPC07 - Network administrator identifies an unusual network traffic flows	Adequate	Partially Effective						
010a.CPC02	010a.CPC02 - Staff are trained to avoid redirection to a malicious URL that installs malware on their device	Adequate	Ineffective	Cyber security awareness training including social engineering	Half Way	50.00	2023/11/07	2023/11/30	Manager, Risk (Responsible)
010a.CPC03	010a.CPC03 - Staff are trained to avoid engaging with email/attachments designed to steal information or install malware on their device	Partially adequate	Partially Effective						
010a.CPC04	010a.CPC04 - Staff are trained not to engage with email messages or websites that have created to imitate the genuine user or site in an attempt to deceive victims	Partially adequate	Partially Effective						
010a.CPC05	010a.CPC05 - Network intrusion detection sensors	Adequate	Partially Effective						
010a.CPC01	010a.CPC01 - Antivirus software detects that a device is infected with malware	Adequate	Partially Effective	Install the latest anti-virus software	Not Started	0.00	2023/10/23	2023/10/31	Preparer, IA (Responsible)
010a.CPC01	010a.CPC01 - Antivirus software detects that a device is infected with malware	Adequate	Partially Effective	Install the latest anti-virus software	Not Started	0.00	2023/10/23	2023/10/31	Preparer, IA (Responsible)

https://barnowl.co.za/knowledge-base/tip-of-the-month/tip-of-the-month-getting-the-basics-right/

Download the BarnOwl Risk Register Template here

Embedding Risk Management (non intrusively)

Risk & Control Self-assessments (RCSAs)

Risks and controls are not updated regularly enough and too much time is spent by the risk function gathering information rather than analysing and providing decision-making insight to the business.

BarnOwl's simple web-based RCSAs make it much easier to embed and drive ownership and accountability for risk management down to the business owners (1st line of defence). In addition, BarnOwl enables action plans to be captured with due dates and owners driving ownership for remedial action. BarnOwl automatically sends out email notifications and email reminders to owners with a simple web link to complete their RCSAs and / or action plans online, including the attaching evidence.

Key Indicators (KIs)

Key Indicators provide a strategic early warning system, driving preventative and predictive capability, with real time insights, facilitating effective business decision making and business improvement. BarnOwl provides extensive key indicator functionality facilitating continuous risk monitoring.

Action Plans

The BarnOwl action plan portal (intranet) is freely available to all users in your organisation. All users should have an icon and / or link on their desktop to access the BarnOwl action plan portal at any time to view and update their action plans (where they are owners). Action plan owners do not need to wait for email notifications and reminders (with a link in the email or a consolidated list of their action plans) in order to access their action plans. You can find a video clip on how to use action plans here.

Reporting - transform your risk, compliance and audit data into visual information facilitating business decision making

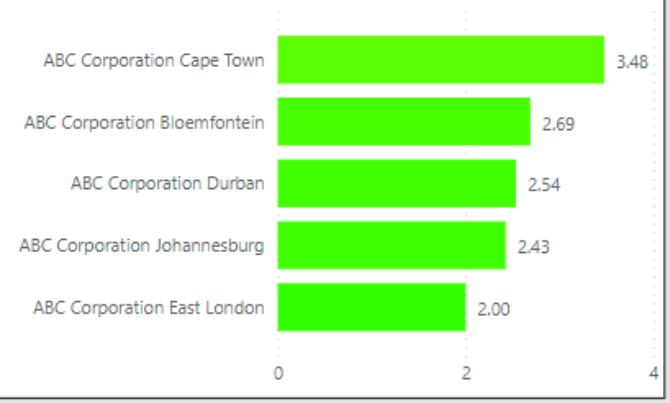
Getting value out of Risk Management - Reporting

Risk Dashboard

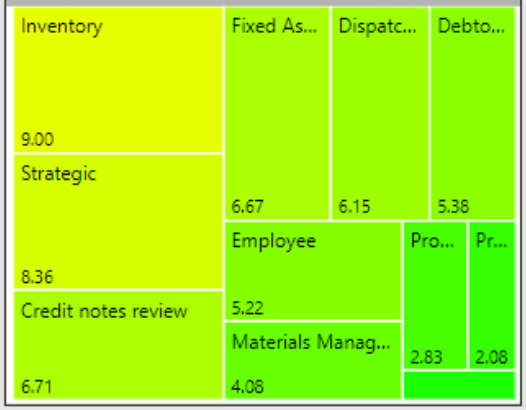
BARNOWL

Organisation Structure: Multiple selections | Risk Category: All | Risk S *** tegory: All

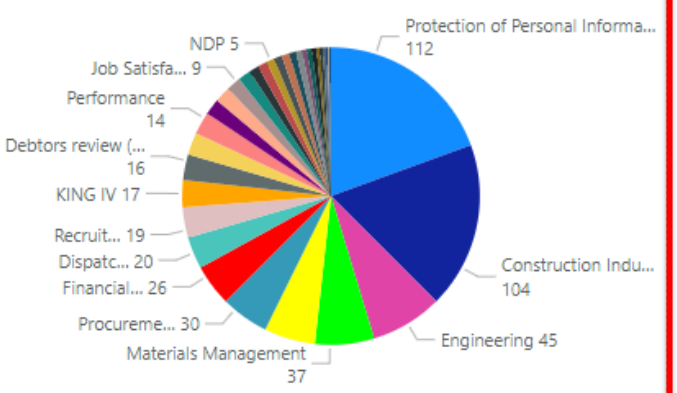
Average Residual Risk Rating per Unit



Average Residual Risk Rating by Risk Category



Count of Risks by Risk Subcategory



Risk Register

O-Rank	U-Rank	UnitPath	RiskTitle	RiskCategory	RiskSubcategory	II	IL	IR	RI	RL	RR
2	1	Root\ABC Corporation\Cape Town\Compliance	Noncompliance - 0015.Publication of codes of conduct	Regulatory Risk	Financial Advisory and Intermediary Services Act	5.00	5.00	25.00	5.00	4.00	20.00
3	1	Root\ABC Corporation\Johannesburg\Finance	Unacceptable level of bad debts due to poor credit control.	Debtors review (Credit Applications)	Debtors review (Credit Applications)	5.00	5.00	25.00	5.00	4.00	20.00
1	1	Root\ABC Corporation\Johannesburg\Jhb HR	Lack of core competencies	Employee	Competency & Training	5.00	5.00	25.00	5.00	4.00	20.00
7	1	Root\ABC Corporation\Bloemfontein\Finance	03. Accountability of goods not accepted by the customer.	Dispatch review	Dispatch review	4.00	5.00	20.00	4.00	4.00	16.00

IR vs RR Comparison | Risk Exposure Dashboard | Risk Spider Diagram | Top Risks View | Control Dashboard | Action Plan Dashboard | Risk Heatmap | Risk History

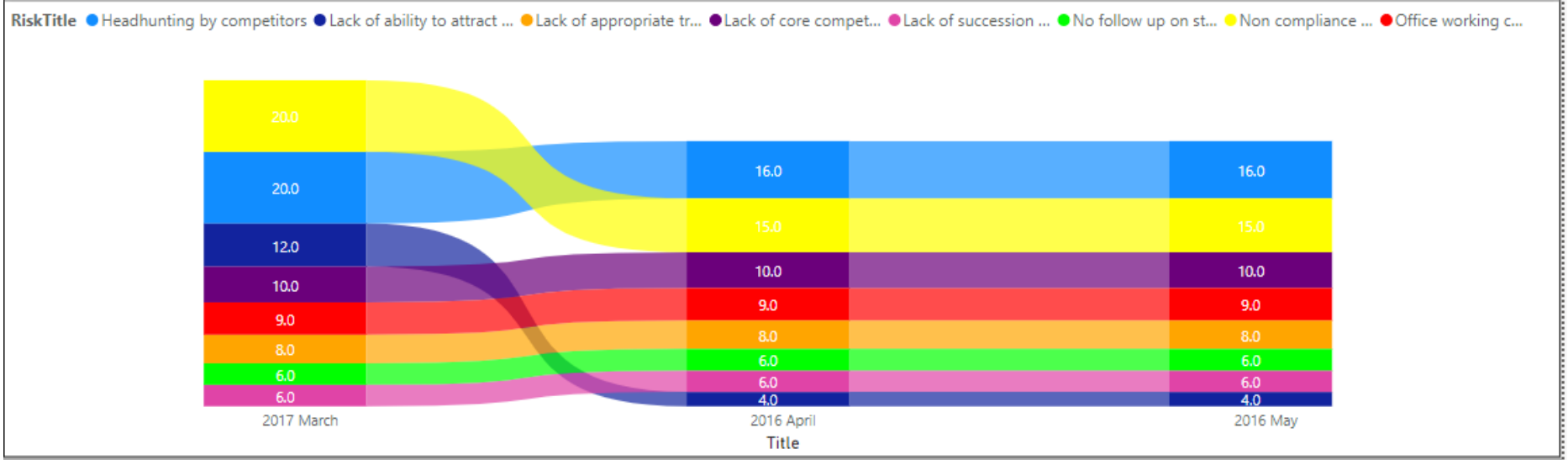
Getting value out of Risk Management - Trends

Risk History

BARNOWL

Organisation Structure	Risk Title	Risk Category	Risk Subcategory	Rating Type	Data Periods
ABC Corporation (lvl1) + Johannes...	All	All	All	Residual Rating	Multiple selections

Residual Rating per period

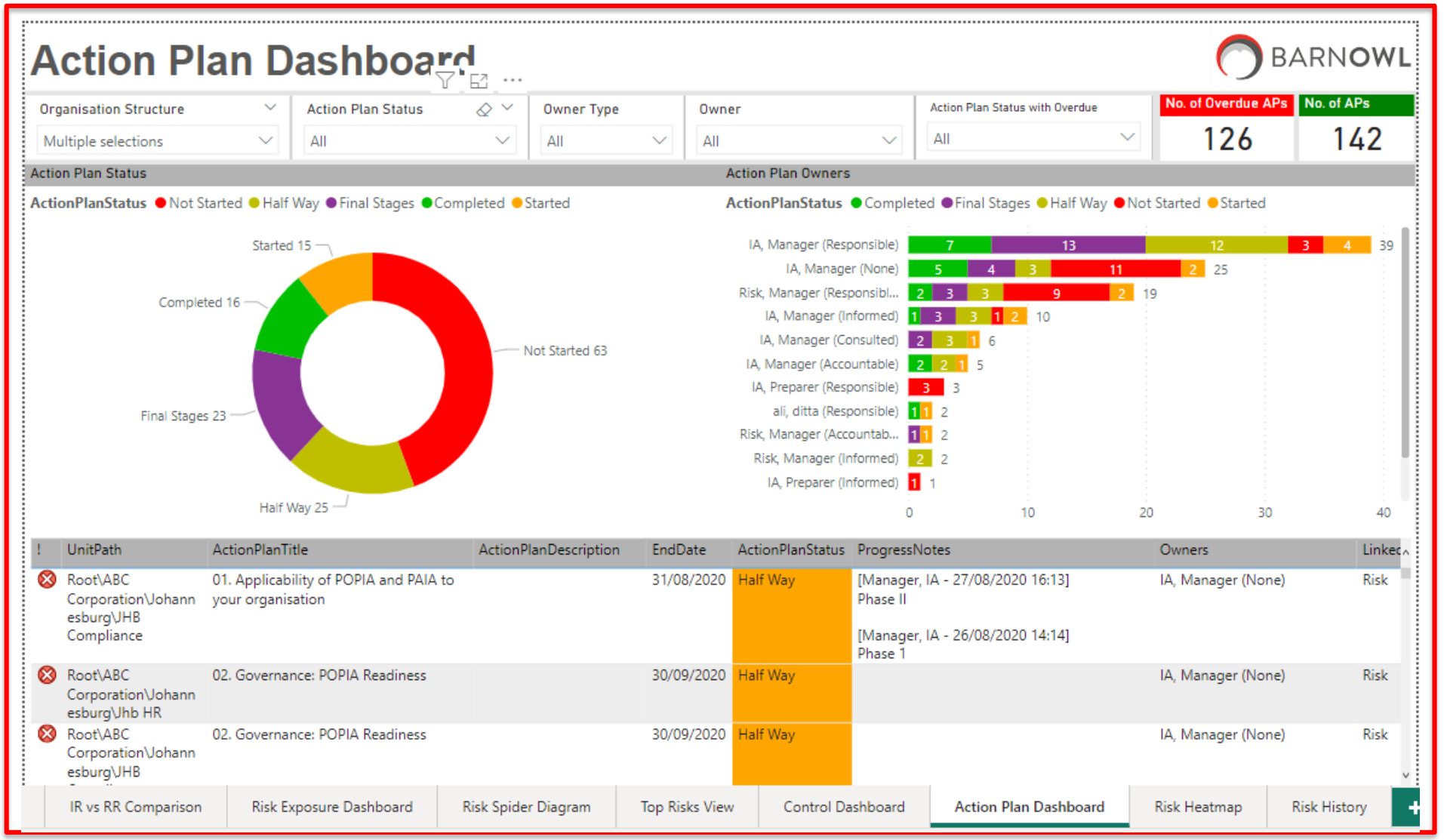


Risk Register

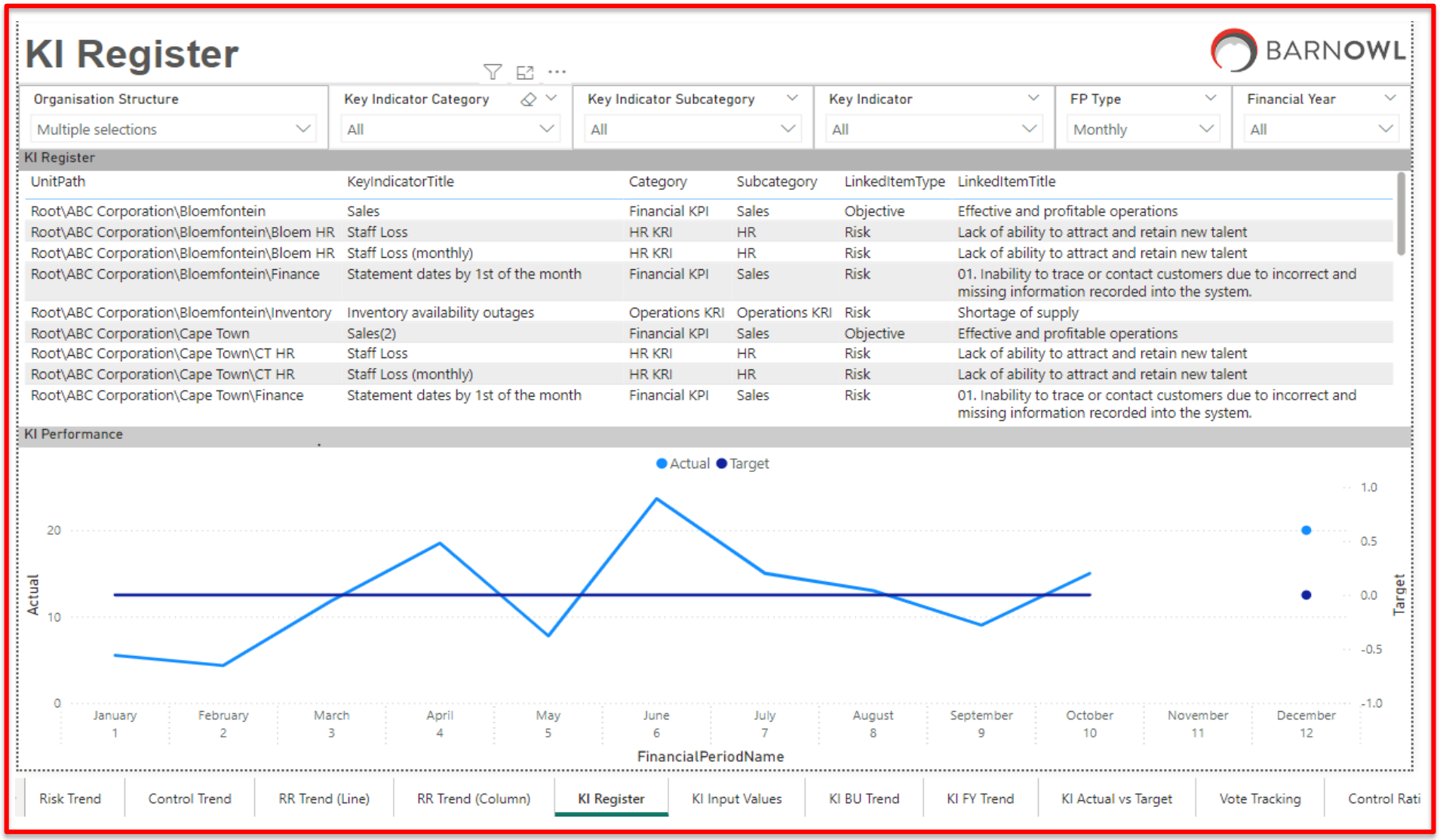
UnitPath	RiskTitle	RiskCategory	RiskSubcategory	II	IL	IR	RI	RL	RR
Root\ABC Corporation\Johannesburg\Jhb HR	Lack of core competencies	Employee	Competency & Training	5.00	5.00	25.00	5.00	4.00	20.00
Root\ABC Corporation\Johannesburg\Jhb HR	Unplanned sick leave	Employee	Policies & Compliance	4.00	5.00	20.00	4.00	4.00	16.00
Root\ABC Corporation\Johannesburg\Jhb HR	Lack of ability to attract and retain new talent	Employee	Recruitment & Retention	5.00	5.00	25.00	5.00	3.00	15.00
Root\ABC Corporation\Johannesburg\Jhb HR	No follow up on staff losses	Employee	Recruitment & Retention	5.00	3.00	15.00	4.00	3.00	12.00
Root\ABC Corporation\Johannesburg\Jhb HR	Non compliance with laws and regulations	Employee	Policies & Compliance	5.00	4.00	20.00	5.00	2.00	10.00
Total				4.20	4.10	17.30	4.05	2.70	11.00

IR vs RR Comparison | Risk Exposure Dashboard | Risk Spider Diagram | Top Risks View | Control Dashboard | Action Plan Dashboard | Risk Heatmap | Risk History

Getting value out of Risk Management – Action Plans



Getting value out of Risk Management – KIs



Conclusion

- Understand the business, which will enable you to solicit quality information. Garbage in, garbage out, no matter what tool / system you use
- Structure and stratify your risk data in line with best-practice risk management standards (e.g. COSO, ISO31000, National Treasury framework)
- Educate and get business to own their risks and keep them up to date in a system (e.g. non-intrusive RCSAs, Action Plans and KIs)
- This will alleviate last minute crisis reporting as your system is kept up to date by risk owners and reporting (at any level) can be done at the click of a button
- This will allow you to spend more time analysing and providing decision-making insight to the business and less time doing mundane administration such as collecting and consolidating Excel spreadsheets
- It’s impossible to run risk management effectively without a system

Thank You

info@barnowl.co.za

https://barnowl.co.za/barnowl-knowledge-base/

BARNOWL