SNG Grant Thornton

Global

Quality

Collaborative

Business Risk Services Newsletter

Q4 2022 | Summer Edition 1

"The best way to predict the future is to create it." Abraham Lincoln

As we are nearing the end of 2022, wrapping up activities and concluding engagements, I typically reflect on what I have learnt this year and start planning for the upcoming year.

In this edition

On a personal note, I have learnt a few valuable lessons this year, a few of which are:

1. It is all about Values: The universe and business are connected, and people make it work, or not. Every person is on a different journey and stage in their lives. Our values are the glue that enables us to work together constructively. Despite the rapid changes around us, our values have certainly not changed, and we should be proud of that.
2. Teamwork: These rapid changes imply that daily, we encounter new technologies, new regulations and new ways of work. Alone we might not be able to succeed, however together as a diverse network we are resilient and stronger. Companies are able to face any changes head-on through collaborative actions.
3. Taking Initiative: We only moving forward if we take initiative and strive towards achieving our plans and goals, through being agile and responsive to the changes we face.

Looking ahead to 2023. Some of our initial plans include themes such as:

- Collaborating using innovative means and bringing the best of the best together for success;
- Deepening the use of data both internally and externally; and
- Flexibility, be more responsive to changes in the environment.

Thank you for your continued engagement and support.

Have a blessed festive season.

Ria

Evolving the internal audit function

and the perspectives on the top risks and internal audit focus areas.

Gerdileen Taylor and Fana Manana

Gerdileen Taylor

Fana Manana

We will be approaching the time of year soon where many internal audit departments and functions will initiate their internal audit planning process for the upcoming year.

In the past, internal audit functions undertook an annual risk assessment that fosters an initial current one year internal audit plan and a three year rolling internal audit plan. The trend in this regard has changed significantly, where risk assessments are conducted quarterly or at least twice a year instead of annually.

Internal Audit evolved over the past couple of years in such a way that internal audit teams start early with the identification of emerging risks for the year ahead.

The European Confederation of Institutes of Internal Auditors' (ECIIA) Risk in Focus report is the product of collaboration between 12 IIA bodies in Europe and is based on surveys of 738 CAEs from across the world.

In addition to the survey results for the Auditors' ECIIA Risk in Focus report, interviews were conducted with 35 CAEs, 12 audit committee chairs, and 3 CEOs from companies around the world. This research conveys an insightful summary of how COVID-19 has impacted the profession, but also paints a vivid portrait of where the profession finds itself as the world slowly emerges from this extraordinary global experience.

According to the research, the internal audit function is evolving and the perspectives on where internal audit and risk will be focusing on will be rolled out over the next 3 years.

As the report aptly conveys: "*Organisations and their internal audit functions face a dizzying pace of change and unprecedented uncertainty. The pandemic has destabilized operations and labor, disrupted supply, and demand, and undermined previously sound business models to an extent few would have thought possible. Many countries are witnessing a resignation crisis, staff shortages and high vacancy rates demonstrating how profoundly the pandemic has exacerbated the talent management risks that existed long before 2020.*"

Looking ahead, the report projects that "*change and uncertainty will define 2022 and the years that follow. Internal audit must understand this change in the outside world, articulate how well it believes the organisation is adapting to these pressures and identify how effectively associated risks are being accounted for and managed.*"

When looking ahead at 2022, the survey's respondents provided the top 5 risks in 2022 are projected to be:

1. Cybersecurity and data security
2. Changes in laws and regulations
3. Digital disruption and new technology
4. Human capital, diversity, and capital management
5. Business continuity, crisis management and disasters response

The survey found that the Top 5 areas of focus in internal audit's 2023 plans are likely to be:

1. Cybersecurity and data security
2. Organisational governance and corporate reporting
3. Changes in laws and regulations
4. Business continuity, crisis management and disasters response
5. Financial, liquidity and insolvency risks

As the report notes, gaps between an organisation's risks and internal audit's coverage should be approached with a degree of caution. For example, "Digital disruption and new technology" were seen as the 3rd highest risk facing organisations, but the risk came in 9th in internal audit coverage. The gap between technology-related risks and internal audit coverage reflects internal audit expertise in technology-related areas – it being simply easier to audit the areas we know. Such gaps in coverage heighten the risk of a "where were the internal auditors?" moment.

Projections of risks and audit coverage for the future in the research report reveals the projections of where internal audit's focus is likely to be the next three years and beyond in 2025:

1. Cybersecurity and data security
2. Digital disruption and new technology
3. Changes in laws and regulations
4. Organisational governance and corporate reporting
5. Business continuity, crisis management and disasters response

What about climate change and environmental sustainability? Although there is an intermediate and long-term criticality view of climate change-related risks, it's often not seen by internal audit functions as a "burning platform" worthy of immediate audit-related coverage as per the research conducted.

The Risk in Focus report does project that technology-related risks and climate-related risks will increasingly be making their way into audit plans in the years ahead. While projections for technology-related risks made the most obvious leap by surging into the Top 5 for 2025, "climate change and environmental sustainability" coverage wasn't far behind. But as the report notes: "Audit leaders must push for the resources to build highly competent and highly relevant functions that can tackle these shifting assurance needs with confidence. This should be addressed urgently. Waiting until 2025 may be too late."

Climate change has been steadily rising the agenda of audit committee meetings, board meetings and risk committee meetings. Internal audit teams have prioritising spending significant time and effort preparing for the 'existential risk' of climate change. So, we encourage organisations to act now to avoid disruption in the future.

The ECIIA recommends that organisations consider climate change a 'forever risk', and act to defend against this now by:

- Ensuring climate change and sustainability is central to the organisation's values, mission, and strategic goals,
- Establishing sustainability goals,
- Investing in projects that will future proof products and services,
- Planning for any climate-related physical and political risks which may jeopardise an organisation's future,
- Reducing organisational greenhouse emissions and moving away from harmful or unsustainable manufacturing processes or materials.

Other related and relevant issues for the current and future internal auditor to consider:

- IT security: response and recovery
- Rising sustainability regulations
- Supply chain strains
- Workforce fatigue and cultural erosion
- Health and safety amid the continued COVID-19 threat

Please contact **Gerdileen.Taylor@sng.gt.com** or **Fana.Manana@sng.gt.com** for any assistance on internal audit, risk management, governance and also to learn more about the emerging trends and steps for internal audit to consider.

Audit Planning

The agile way

Omar Hassan

Omar Hassan

Its that time of the year again, where Internal Audit departments are scrambling to close off the current years audit plan and at the same time the audit plan and coverage for the year ahead is being crafted.

As most Internal Auditors would know, its the busiest and most hectic time of the year, which includes tasks such as risk assessments, updating of the audit universe, identifying key risk themes, and debates with management on high-risk areas and which audits to include. All of this done in a matter of a few weeks, eventually leading to a detailed locked down and extensive 12-month audit plan. Sounds efficient? Maybe, but certainly can't be that effective in the current VUCA world we live in.

Ironically, the organisations risk posture keeps changing as the business responds to market conditions, applies agility to operations, explores innovative ideas and is challenged by internal or external factors! New risks are emerging, business strategies are evolving and organisations are experimenting with Technology! Surely, all of these risks and changes can't be factored into a few weeks of audit planning at the end of the previous year!

The need for Internal Audit to be Nimble, Lean and Agile is critical to support organisational objectives and the management of the organisations risk exposure! Remember the plan will guide execution and value will follow!

Should Internal Audit consider planning differently in order to prevent a less chaotic period?

Will this new approach allow more retrospection and force new behavior?

Should we demand more participation from our business partners in order to allow Internal Audit to add more value, and bring more insight required be them?

The Adoption of an Agile and Value Stream Audit Planning approach challenges the Internal Auditor to be constantly engaged and immersed in the organisation to identify the risk areas of most value to the organisation. It is not a measure of the number of audits planned and executed but rather a view of value derived over the coverage of key risk themes. Imagine a world where Internal Audit is seen as an independent Partner to business, being constantly aligned to changing business risk exposures and delivering real value to their stakeholders. Below are some key elements for Internal Audit to consider in adopting a more Agile Audit Planning Approach:

- **Establishing Risk Theme Coverage**

Instead of focusing on the number of audits to be delivered over the year, the focus should be on the identification and coverage of key risk themes and the value thereof. Internal Audit functions should identify what are the key risks they would need/want to cover, group them and build the assurance coverage around these themes. This requires a shift in mindset of establishing autonomous teams to determine the assurance coverage within the Risk Themes, which includes prioritization of which assurance objectives to execute on.

- **Use of Backlogs with Continuous re-prioritisation**

Audit backlogs are a collection of key audit scoped items linked to the risk themes that are identified to be reviewed. These are high level (Epics) that the audit team would prioritise on a regular basis. The Internal Audit team would prioritise these items on a quarterly basis. The backlog is dynamic and continuously updated with new items and priorities are reviewed every quarter. Prioritisation of the backlog is based on the retrospective of backlog items delivered and value derived, organisational changes, risk assessments, team capacity and business needs. This allows Internal Audit to easily adjust its assurance coverage plan to align to the needs of the oganisation.

- **Defining Objective and Key Results (OKRs)**

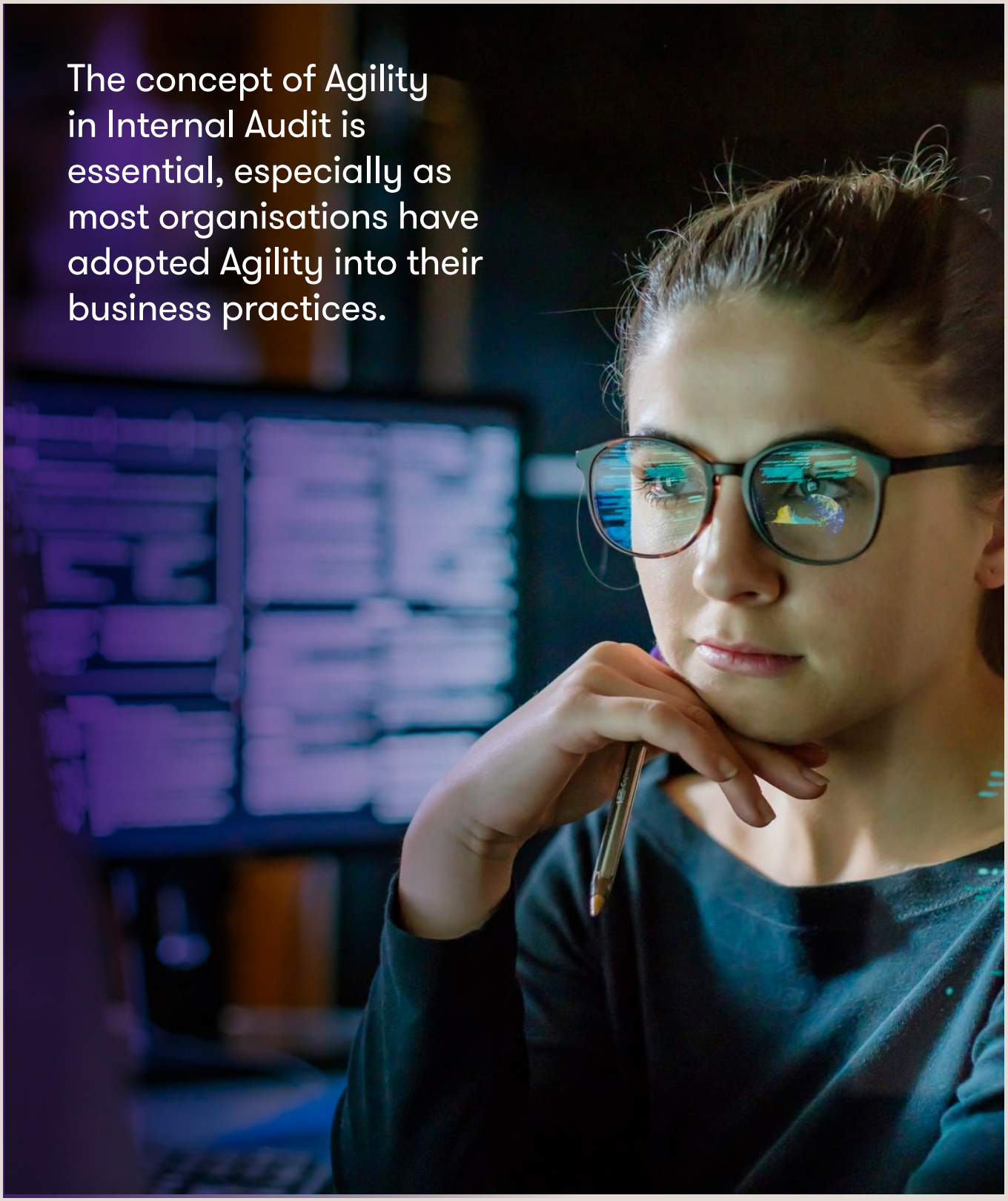
Agile focuses on customer centricity and is based on priositisation, responding to client needs and working in short feedback cycles in delivering value early. OKR's allow agile teams to align around measurable goals in assessing value and benefits derived. Internal Audit should set OKR's at a Macro (Epic) audit plan level as well as individual team level that is aligned to their risk themes and value streams. This enables focus on common objectives and results that can be a measure of value for the Internal Audit department.

- **Adopting a Value Stream approach**

The value stream concept in Lean-agile relates to how value flows within an organisation. It is the deconstruction of vertical teams and crossing functional boundaries to establish teams to work together in delivering value. Internal Audit should explore structuring itself into value streams from an organising, planning and execution perspective. This would require Internal Audit identifying which are the areas that they would add the most value to the organisation.

The identification of value streams does not happen in isolation, it takes into account the organisational strategic drivers, key risk themes as well as other internal and external challenges. The value streams will provide a consistent view of the areas that will broadly be covered from an assurance and risk perspective. Internal Audit should establish cross functional teams within the value stream who would prioritise the execution of the Internal Audit backlog linked to that value stream. For example, a review should include cross functional skills such as Data Analytics, Cyber Specialists, IT Auditor, process and control auditors.

The concept of Agility in Internal Audit is essential, especially as most organisations have adopted Agility into their business practices. We have only touched on a few concepts above, please reach out to our team to engage on how we can explore the future of Internal Audit planning together and deliver value faster!



1 + 1 = 2 or 3?

Combined assurance

Ria Pretorius

Ria Pretorius
Head of BRS

Combined assurance is all about assurance providers (internal and external) working more closely together to ensure:

- Appropriate levels of assurance in the right areas;
- Assurance is obtained from the right resources; and
- Assurance is obtained in the most cost-effective way possible.

The appropriate level of assurance depends on the risk appetite of the organisation. There should be alignment of control validation/assurance approaches and efforts across the organisation, driving efficiency and the right levels of comfort. Risk management is the foundation of the combined assurance process and organisations should establish risk-based criteria for dealing with control failures on a consistent and strategically aligned basis to ensure organisational objectives and goals are achieved. Identifying opportunity risks provides us with an option to be proactive in terms of the risks we may face.

The King III report introduced combined assurance in 2009.

- The recommendation was made following a general understanding that more can be done to improve assurance coverage and quality through better coordination of assurance providers.
- King IV report in 2016 expands on this concept by indicating that a combined assurance model incorporates and optimises all assurance services and functions so that, taken as a whole, these enable an effective control environment, support the integrity of information used for decision-making by management, the governing body and its committees; and support the integrity of the organisation external reports.

Benefits of combined assurance Some organisations have seen benefits such as:

- Assurance efforts that are directed to the risks that matter most.
- Commitment to enhance controls is demonstrated.
- Dashboards that provide an integrated, insightful view.
- Reduction in assurance costs through elimination of duplication and better resource allocation.
- A reduction in the repetition of reports by different committees, resulting in improved and more efficient reporting.
- A comprehensive and prioritised approach in tracking of remedial actions on identified opportunities/weaknesses.
- Clarity on risk and audit.

How should organisations go about achieving this?

1. **Collate Information:**
Obtain requisite information in order to understand risk areas, where they impact the business, how they are mitigated and who provides assurance thereon.

2. **Map Key Risks:**
Link key risks areas to processes, organisational & governance structures and assurance providers to obtain a holistic view of the current assurance landscape.

3. **Analyse:**
Determine areas of sub-optimal assurance.

4. **Implement:**
Develop an implementation strategy to implement activities to obtain consistent, effective, optimal and economic assurance.

5. **Reporting of Assurance Results:**
Ensure that an effective integrated reporting mechanism exists which aggregates the results from all assurance providers per significant risk area and provide this information to the appropriate governance structures.

6. **Maintain and Monitor:**
Regularly review, monitor and update the Combined Assurance model in order to ensure that it remains current and up to date.

How can organisations get more value from combined assurance?

Organisations can get more from combined assurance by involving different assurance providers in the planning stages and by regularly updating their risk assessments. Collaboration of the different lines of defense in respect of specific focus areas result in deeper understanding of the real issues and providing valuable assurance as well as practical recommendations in a cost effective manner.

Organisations that adopted a process and methodical method of engaging achieve greater success and value.

The process should include updating baseline information regularly as well as progress on reviews and results.

The right technology enables the recording of information and keeping track of audit results makes a significant difference to maturing combined assurance. Not only is the record keeping easier and efficient, it is also a common platform for all the role players to collaborate on and to prepare reports from. Up to date information also make it easy to change the focus of resources should the environment change radically.

In conclusion, many organisations focus on combined assurance only weeks before an audit committee to perform some level of joint reporting in stead of true collaboration and combining the information intelligently from different role players. True value from combined assurance can be obtained with advance planning, obtaining commitments on actions and authentic collaboration.

A Reflection of Business Continuity and Disaster Recovery

Sithabile Zungu

Sithabile Zungu

Year after year we conduct IT general controls reviews for various organisations, some in the public sector or private sector and some large, medium, and small. In most cases this would cover a review of controls pertaining to disaster recovery planning.

A general observation from these reviews is that more than 90% of the time these organisations do not have effective controls on disaster recovery planning. We have noted:

- Lack of disaster recovery plan;
- Disaster recovery plans not derived from business continuity plans;
- Disaster recovery plan that are old and not reviewed periodically; and
- Disaster recovery plans that are in draft and not finalised and signed off.

For most of the organisations disaster recovery planning is hampered by non-established business continuity planning processes. We are all aware that IT plays a pivotal role in enabling business, however, it is business that aligns its processes to meet the strategic goals of an organisation and therefore IT aligns itself with what business has proposed to achieve. Similarly IT needs to align itself with the business continuity needs of an organisation, without business taking the leading role in establishing continuity processes, it becomes difficult for IT to effectively enable business to recover priority and mission critical operations. It is business that has a full understanding of how soon recovery should occur before experiencing business disruptions and subsequently hampering strategic objectives. We have noted the following draw backs in establishing business continuity process:

- No ownership of business continuity planning processes within an organisation;
- The misconception that IT is responsible for business continuity planning; and
- Management not being aware of the required business continuity planning processes.

It is true that most organisations, more especially in the private sector were able to switch effectively to working from home during the pandemic but for some organisations the switch was abrupt due to lack of business continuity preparedness. There was a rush in procuring tools and systems to enable remote working without ensuring that such tools had the necessary safeguards to ensure data integrity, security and availability etc. In some instances, organisations totally failed to continue providing their products and services during the pandemic thus resulting in a total shut down of the organisations or significant downsizing and high job losses.

In August 2022 BUSINESSTECH published an article showing a surge in liquidations and some of the factors sighted as contributing to the surge were struggles to recover from the Covid pandemic, civil unrest and flooding in KwaZulu-Natal.

Table 1 – Total liquidations according to industry (number)

Industry	January – August 2022			August 2021			July 2022			August 2022		
	C	V	Total	C	V	Total	C	V	Total	C	V	Total
1.Agriculture, hunting, forestry and fishing	4	8	**12**	0	1	**1**	0	0	**0**	1	3	**4**
2.Mining and quarrying	1	2	**3**	0	1	**1**	0	1	**1**	0	0	**0**
3.Manufacturing	13	32	**45**	0	5	**5**	0	3	**3**	4	8	**12**
4.Electricity, gas and water	1	2	**3**	0	1	**1**	0	0	**0**	0	0	**0**
5.Construction	13	67	**80**	1	4	**5**	2	4	**6**	2	12	**14**
6.Trade, catering and accommodation	30	245	**275**	1	34	**35**	4	25	**29**	3	44	**47**
7.Transport, storage, communication	1	18	**19**	0	4	**4**	1	2	**3**	0	3	**3**
8.Financing, insurance, real estate, business services	46	395	**441**	4	48	**52**	3	72	**75**	5	78	**83**
9.Community, social, personal services	9	75	**84**	0	21	**21**	1	13	**14**	1	20	**21**
10.Unclassified	50	325	**375**	4	36	**40**	6	28	**34**	4	51	**55**
Total number of liquidations	**168**	**1 169**	**1 337**	**10**	**155**	**165**	**17**	**148**	**165**	**20**	**219**	**239**

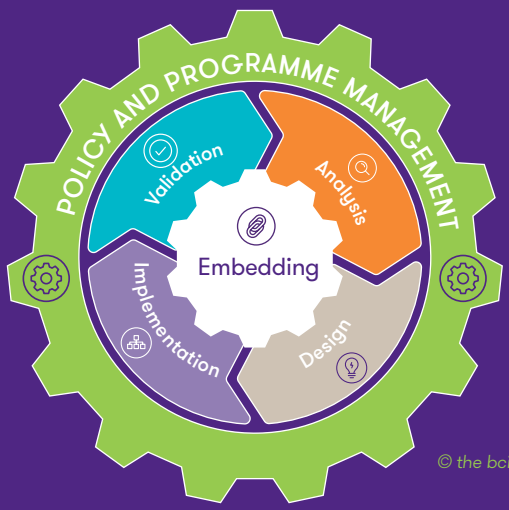
The devastating effect of Covid-19 not only on Southern Africa, but globally has provided for a huge opportunity in learning from those organisations that survived during the pandemic, as well as those that suffered challenges. This is where organisational surveys provided for an opportunity to analyse aspects such as remote or working from home, and what worked well, and what areas needed addressing.

Some of the surveys we conducted gave a huge insight into the day-to-day challenges staff members experienced whist working remotely from home, the most common issues were:

- Network (mobile data) challenges which included restriction to a single provider and data allowances;
- Loadshedding (with no work arounds for staff to continue working during loadshedding);
- Expectation to work outside of standard office hours;
- No established processes to support staff in a remote working set (Manager / Supervisor);
- Difficulty in accessing specific applications via mobile data;
- Aging laptops or no equipment available due to staff being allocated with desktops and therefore only able to work from office;
- Inability to access server;
- High reliance on paper-based documentation and use of non-editable PDF's necessitating printing and scanning;
- No call forwarding options from office landline resulting in personal cellphones having to be used;
- Lack of guidance over online meetings;
- Not having an office chair and desk at home; and
- Concerns of general health and wellness / wellbeing.

These challenges are not unique to Southern Africa, and provided an opportunity to help many organisations take a deep dive into their operational needs. This also brought about ensuring that a workable Business Continuity Solution was provided for, to help address the many gaps, threats, and risks. These also included reviewing the design of a Hybrid remote working policy, improving the existing ICT policy covering off-site working, and allowing staff to choose an internet provider, be it mobile data or fibre to the home (FTTH). In addition, as Technology is the key enabler for working from home and remote access to server, internet security has become even more important then ever. Therefore, it is vital that where an organisation is handling highly confidential information the correct ICT access protocols need to be in place, more especially when working remotely.

Are you ready should another pandemic or similar disruption strike? Business Continuity is the key discipline that sits at the heart of building and improving the resilience of organisations. By identifying what is critical to the organisation, the relevant dependencies, resources required, considering any threats or risks, and then put the Business Continuity Plan to the test, will go a long way in ensuring readiness and building resilience. Effective business continuity planning is undertaken using best practice framework such as the BCI Good Practice Guidelines (2018) life cycle as illustrated in the diagram below. The BCM lifecycle provides for six (6) key phases, thus ensuring the correct methodology is utilized. We have also highlighted the deliverables for each phase:



© the bci Good Practice Guidelines (2018)

To help build resilience, organisations need to embrace the hybrid approach allowing the workforce to work from anywhere including home, office and alternative premises that offer Wi-Fi (coffee shops, restaurants, or malls). Organisations therefore need to carefully consider emerging technology that enable remote working during the development of IT strategies, digital strategies and other initiatives related to digital transformation. Likewise other business processes like human resource management need to evolve to accommodate the hybrid way of work.

Crisis in Ethical leadership

It is time to sink or swim

Ronel Van Wyk

Ronel van Wyk

South Africa is experiencing a failure in ethical leadership. This failure and the impact that it has is at a catastrophically high level. The financial implications and the subsequent impact on our society are enormous.

The failure in ethics has a ripple effect and these actions are a real threat to our economy. It is our view that the continuous involvement of individuals from private and public sector in fraud, corruption, the failure in ethics and the seemingly incompetence of leadership to address the unethical and criminal behavior, could even be a direct threat to our democracy.

Some leaders have lost their moral bearing and have succumbed to temptations. It could be argued that one of the causes of the problem is the inculcation of a culture in which finding unethical options is seen as the easiest route to conduct business. Bad decisions are rationalised and there is a sense of untouchability, supported by a view that there are no consequences for these behaviors.

South Africa cannot afford any further ethical failures in terms of leadership. The failure in ethics amount to billions of rands. The cost of state capture is reported to be more than R250 billion. The Steinhoff scandal, in one day, wiped R200 billion from the Johannesburg Stock Exchange. The implications of the collapse of Steinhoff to its investors and other stakeholders are immense.

The following questions need to be desperately answered:

- How do we address the failure in ethical leadership?
- How do we build ethical leaders?
- How do we enforce an ethical culture in the workplace?
- How do we protect those who blow the whistle on unethical conduct?

The answers to these questions are complex and the solutions do not include "quick-fixes".

One of the solutions to the failure in ethical leadership could be to guide our young leaders to believe that the outwards conspicuous demonstration of wealth does not necessarily reflect their worth. Leaders from all ages and backgrounds need to understand the principles of corporate citizenship and they must recognise that they form part of a broader society. This affords them with rights, responsibilities, and obligations. What leaders do and how they do it is vital to ensure sustainability. How and what leaders do matters more than what they say. We need to guide our young leaders to understand and accept that it is rather the intrinsic values of integrity, trustworthiness, honesty, and selflessness that define them.

The way we guide our young leaders is by adopting these qualities in our own leadership roles, providing them with role models. Young leaders take on the characteristics of their leaders. It is essential that leaders' ethical behaviors are visible, consistent, have credibility and are seen to be authentic.

These credible and authentic actions will lead to a culture in which leaders are trusted and will inculcate an ethical culture that will become part of the DNA of an organisation. It is suggested that organisations should not only focus their efforts by simply looking at the profit it makes, but rather its shared value and how this benefits the society. Businesses should acknowledge that ethical standards must be fully integrated into their strategies to ensure long-term survival and sustainability.

We acknowledge the brave work that whistleblowers have done in identifying and speaking up against fraud, corruption, and unethical behavior.
We owe them a debt of gratitude.

We support a culture in which people are comfortable to speak openly about unethical behavior and we provide a protective environment to them. Big business needs to come to the party and provide employment to these brave men and women that had the inner courage to do the right thing. We encourage organisations to protect and to employ a whistleblower and acknowledge the contribution these people are making in our country. We salute the whistleblowers that had the courage to speak out against criminal and unethical practices in companies and government institutions despite huge pressure to look the other way. It is this inner and moral courage that whistleblowers displayed that South Africa desperately needs.

Individualistic ethical leadership without being able to influence the values and ethics of an organisation is not sufficient in the complex world leaders operate within. To fortify their reputation as ethical leaders they must be known for their principled decision-making, authentic behavior, and judgment of ethical dilemmas. We have a duty to pave the way for leaders who are driven by values of truth, integrity, and respect for others and to encourage and support those who have already embarked on this journey.

SNG
Grant Thornton

sng-grantthornton.co.za