



# Optimising Internal Audit value in the new world

**WEBINAR**  
**24 July 2020**

**Facilitated by:**

CPA Denish Osodo  
Director, Internal Audit  
Safaricom Plc

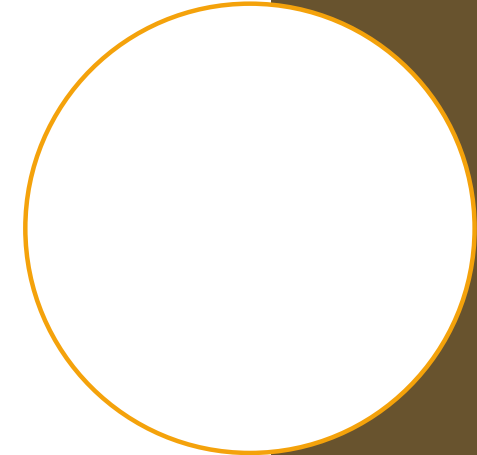
# Optimising Internal Audit in the new world

The world as we knew it has changed. The world is facing unprecedented fights on both a health and economic front. The COVID 19 impact on world economies and business will take years to reverse. The disruption caused by COVID 19 has brought forth changes such as closure of entire businesses, downsizing, rethinking the supply chain, employees working from home and changing business models etc. Prior to the COVID period, rapid technology changes was already bringing significant disruptions in the business world and Internal audit functions.

Throughout this period and after, the role of internal audit will be critical. Internal Audit cannot continue operating business as usual. In the midst of the disruption, the following questions arise:

- How can internal audit deliver value to organisations?
- How does Internal audit remain relevant as businesses struggle to stay afloat in the midst of a crisis?
- How does Internal audit conduct audits from remote environments and still deliver quality audits?
- How will IA assess the reliability of evidence provided whilst remote working?
- With the new normal what should IA consider once the crisis has abated?
- With the new normal, how should IA functions keep staff motivated and supported whilst working in remote environments?
- With stakeholders competing priorities, how can IA continue to provide assurance to organizations?

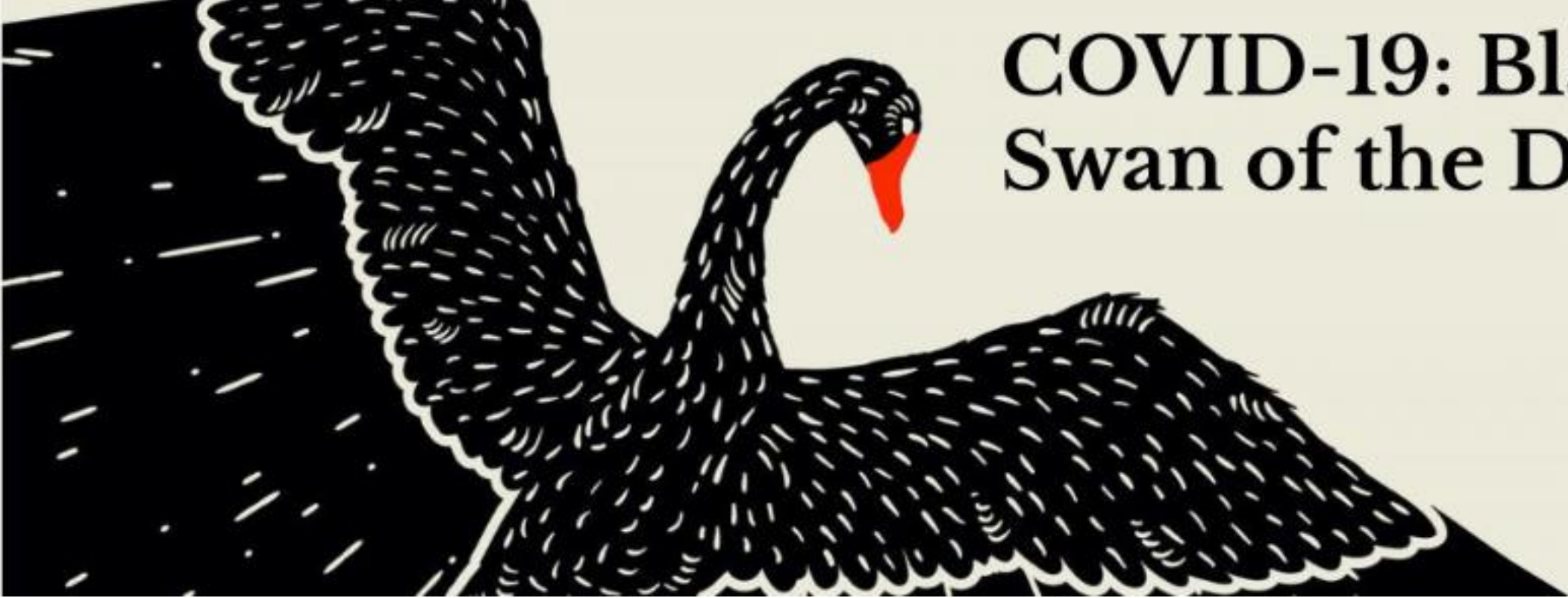
This new world will require a shift in mindset for the auditor, adoption of new ways of working, upskilling to fit into a digital world and effort to remain relevant in the organisation.





# Agenda

1. Risk management in light of a pandemic – Preparing and responding to a black swan event
2. Role of internal audit in business continuity planning
3. Impact of Covid-19 Disruptions on internal Audit
4. Responding to cybersecurity Risks in the Covid-19 pandemic
5. Bean counting or bean growing? The internal auditors Dilemma
6. Remote auditing procedures and audit evidence in times of remote working
7. Automating internal audit function



# COVID-19: Black Swan of the Decade

Risk management during a pandemic – Preparing and responding to a black swan event

---



# 2020 - The year that never was!

- In December 2019, a flue like outbreak caused by severe acute respiratory syndrome **coronavirus 2** (SARS-CoV-2) was first identified in Wuhan, China. The World Health Organization declared the outbreak a Public Health Emergency of International Concern on 30 January 2020 and a pandemic on 11 March.
- As late as February 2020, organisations and individuals in Kenya were operating 'Normally'.
- 12 March 2020 – Kenya confirms its first case of Covid 19.
- As of 15 July 2020, more than **13.2 million** cases of COVID-19 have been reported in more than 188 countries and territories, resulting in more than **577,000** deaths; more than 7.37 million people have recovered.



# Black Swan Events....

- **A black swan event is an extremely negative event or occurrence that is impossibly difficult to predict. Black swan events are events that are unexpected and unknowable.**
- **Has the following attributes;**
  1. **Have the potential to exhibit drastic, wide-reaching consequences;**
  2. **Have a nature of unpredictability**
  3. **Typically be accompanied by “hindsight bias,” meaning that once the event has passed, many individuals tend to rationalize that the event was actually predictable (due only to the fact that they are now aware of what the outcomes from the said event are).**

The black swan events is a metaphor that describes an event that comes as a surprise, has a major effect, and is often inappropriately rationalised after the fact with the benefit of hindsight. The term is based on an ancient saying that presumed black swans did not exist – a saying that became reinterpreted to teach a different lesson after the first European encounter with them. The term “black swan” was originally coined in 1697, when William de Vlamingh discovered a real black swan in Australia. In 2007 essayist Nassim Nicholas Taleb popularized the term when he theorized how humans try to make sense of unexpected events.

## Examples of black swan events in the World

### The black death

- The Black Death/plague was the deadliest pandemic recorded in human history. It resulted in the deaths of up to 25–200 million people in Eurasia, North Africa and Europe from 1347 to 1351. It was spread by fleas living on black rats that moved across continents on merchant ships. The plague may have reduced the world population from an est. 475 million to 350–375 million in the 14th century

### The Spanish flu

- The Spanish flu, also known as the 1918 flu pandemic, was an unusually deadly influenza pandemic caused by the H1N1 influenza A virus. Lasting from February 1918 to April 1920, it infected 500 million people—about a third of the world's population at the time—in four successive waves.

### 9/11 Attacks

- The attack on the Twin Towers of New York's World Trade Center prompted the closure of the NYSE and NASDAQ on the morning of September 11, 2001. Stocks plummeted during the first trading week after 9/11 – \$1.4 trillion in stock market value was lost within a week.

### The 2008 Global Financial Crisis

- The global financial crisis in 2008 caused Lehman Brothers to file for bankruptcy – the largest bankruptcy filing in US history. Over 25,000 Lehman employees went jobless and more than \$46 billion of Lehman's market value was wiped out. In total, over \$10 trillion was eventually wiped out in the global equity markets.

### Covid 19

- **The COVID-19 outbreak has characteristics that classify it as a black swan: the pandemic has had — and will continue to have — an extreme impact, both on people and on national economies.**

# Risk management during a pandemic – Preparing for a black swan event



Black Swan events continue to be unpredictable and unpreventable. Although its impossible to prepare for every scenario, but you can establish principles and protocols to be better prepared for the unexpected.

PREPARE

01

## Scenario planning and response

Construct a series of scenarios that could happen and potential responses. Create a crisis response team and reporting channels

02

## Threat assessment

This should cover human safety, physical damage, long term disruptions and overall business continuity plan.

03

## Prepare a Comprehensive Situation Response

Create and disseminate those plans, keep them up-to-date, and review or practice them regularly.

04

## Mitigation responses

Plan and execute redundant mitigation responses in case the primary response fails.

## Resources

Know your resources and how to use them during a catastrophe. Keep track of internal and external resources personnel, financial, and physical resources.

05

## Make use of advisers

Incorporate outside perspectives and experiences into the response strategy

06

## Moral Ground

Maintain the moral high ground by planning and executing responses based on what is right, rather than planning for only the company's best interest.

07

## Evaluate Response Strategies

Challenge your response strategy with an independent perspective to help identify weaknesses before the Black Swan does.

08

PREPARE

# Preparing for a Black Swan Event – Internal Audits' Role

## Preparedness Review

Review adequacy of contingency plans and helping the business identify failure points.

## Response Review

Carry out an assessment of the business response plans and whether it covers all key risk areas.

## Scenario planning and testing

Review of the business risk exposure against the pandemic and assist in developing plans, testing disaster recovery plans.

## Real time reporting

Real time monitoring of key metrics for processes that are currently under stress.



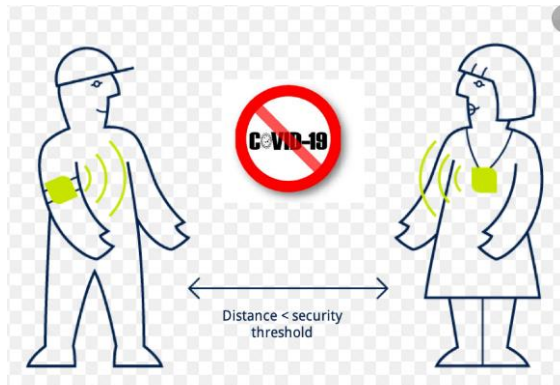
## Regular Audits

Periodically, audit the business BCP to review adequacy and ensure it reflects the current business environment.

## Challenging management forecasts

Review management forecasts of business impact i.e. of going concern, goodwill, revenues etc and whether financial impact is estimated correctly.





5-perspective/2020/03/us-job-losses-due-covid-19-highest-great-depression

News & Perspective Infectious Disease Topics Antimicrobial Stewardship Ongoing Programs

FEATURED NEWS TOPICS Novel Coronavirus Ebola MERS-CoV Chronic Wasting Disease

## US job losses due to COVID-19 highest since Great Depression

Filed Under: **COVID-19**  
Stephanie Southeray | News Reporter | CIDRAP News | May 08, 2020


Share Tweet LinkedIn Email Print & PDF

The US jobs report for April brings sobering, if not unexpected news: The country has lost 20.6 million jobs since mid-March, resulting in an unemployment rate of 14.7%, a level not seen since the Great Depression in the 1930s.

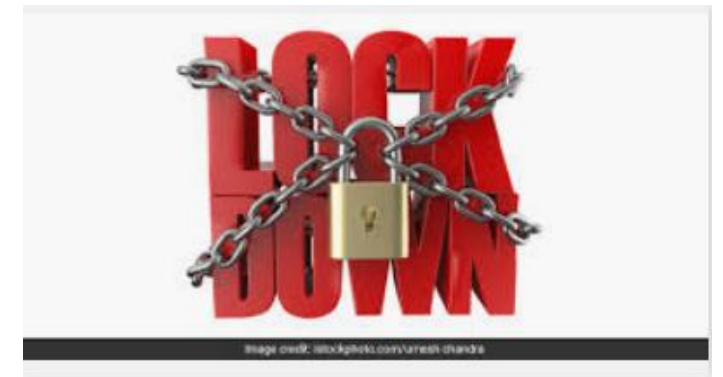
The number of jobs lost more than doubles the number seen in the 2007-2009 Great Recession, when 8.7 million Americans lost jobs.

Before the pandemic, the United States marked a 50-year unemployment low in February, with just 3.5% of Americans unemployed.

According to *USA Today*, of the 20.6 million jobs lost, 18 million are expected to be temporary when the pandemic recedes.



Natalie\_magie / iStock



# The event has occurred....

# Managing and responding to a black swan event

## Identify risks

1

- COVID-19 may have brought to light risks you had not yet considered.
- Catalogue risks in this season and update risk profile.
- Develop risk recognition criteria in order to know when and how to respond.

## Containment team

2

- Active a response team led by senior management that should concentrate on containing and minimizing the event. This team should include personnel from across the business functions and external advisers.

## Emergency Response Team

3

- Create a response team to assess the situation, risks and response goals in order to initiate the correct response plan.
- This team will be in charge of activating the enterprise's emergency response or resiliency plan

## Develop and evaluate Options

4

- Develop multiple response options and categorize them base on largest contribution toward response goals.
- Evaluate each option by its risk/reward and whether the organization has the capabilities to carry out the plan.

## Implement responses

5

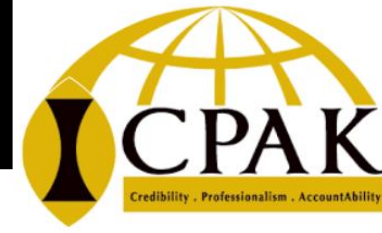
- Implement the response following the guidelines and procedures previously established during pre-event planning.

## Assessment

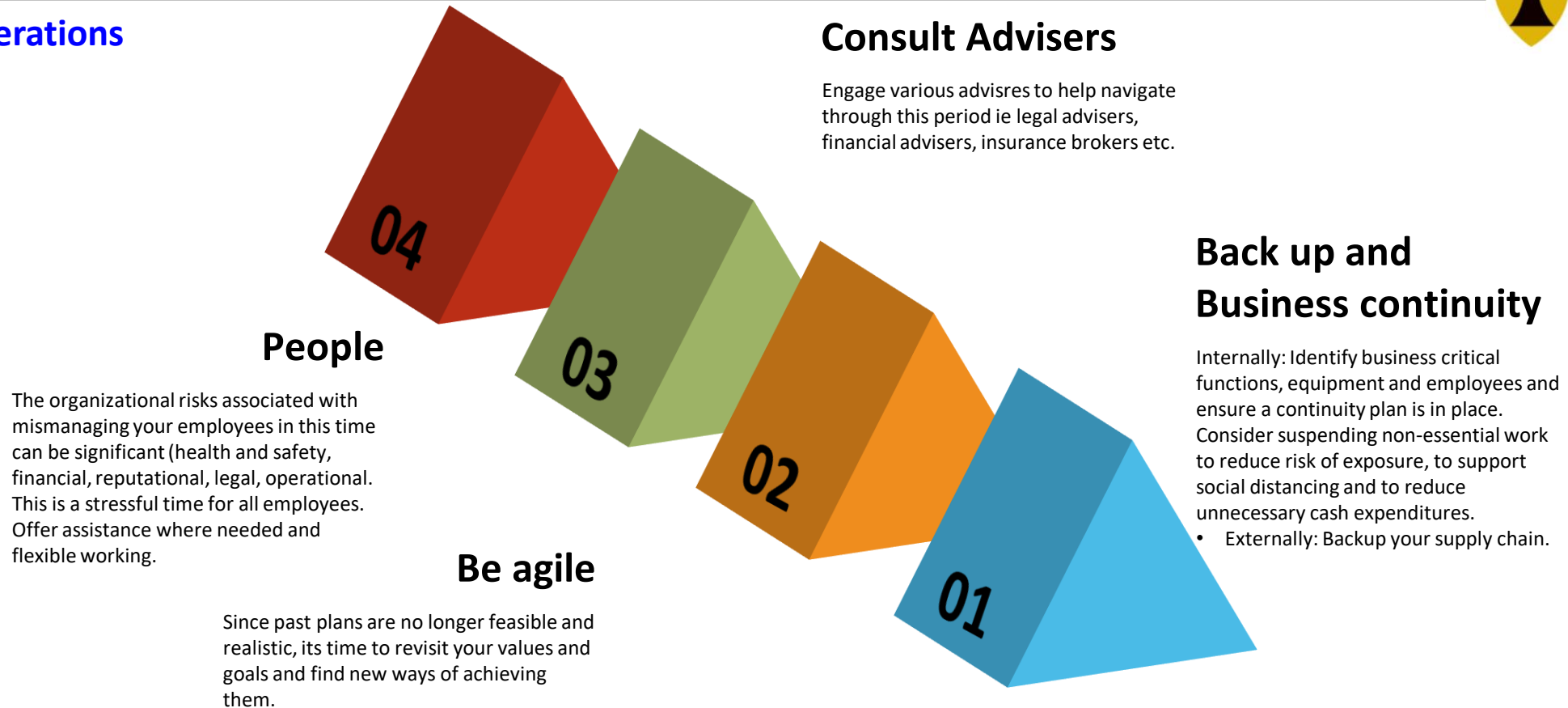
6

- Assess continually the effectiveness of the response by making corrections as need. After the event, management should discuss lessons learned and incorporate these lessons into training and future response planning.

# Managing and responding to a black swan event



## Other Considerations

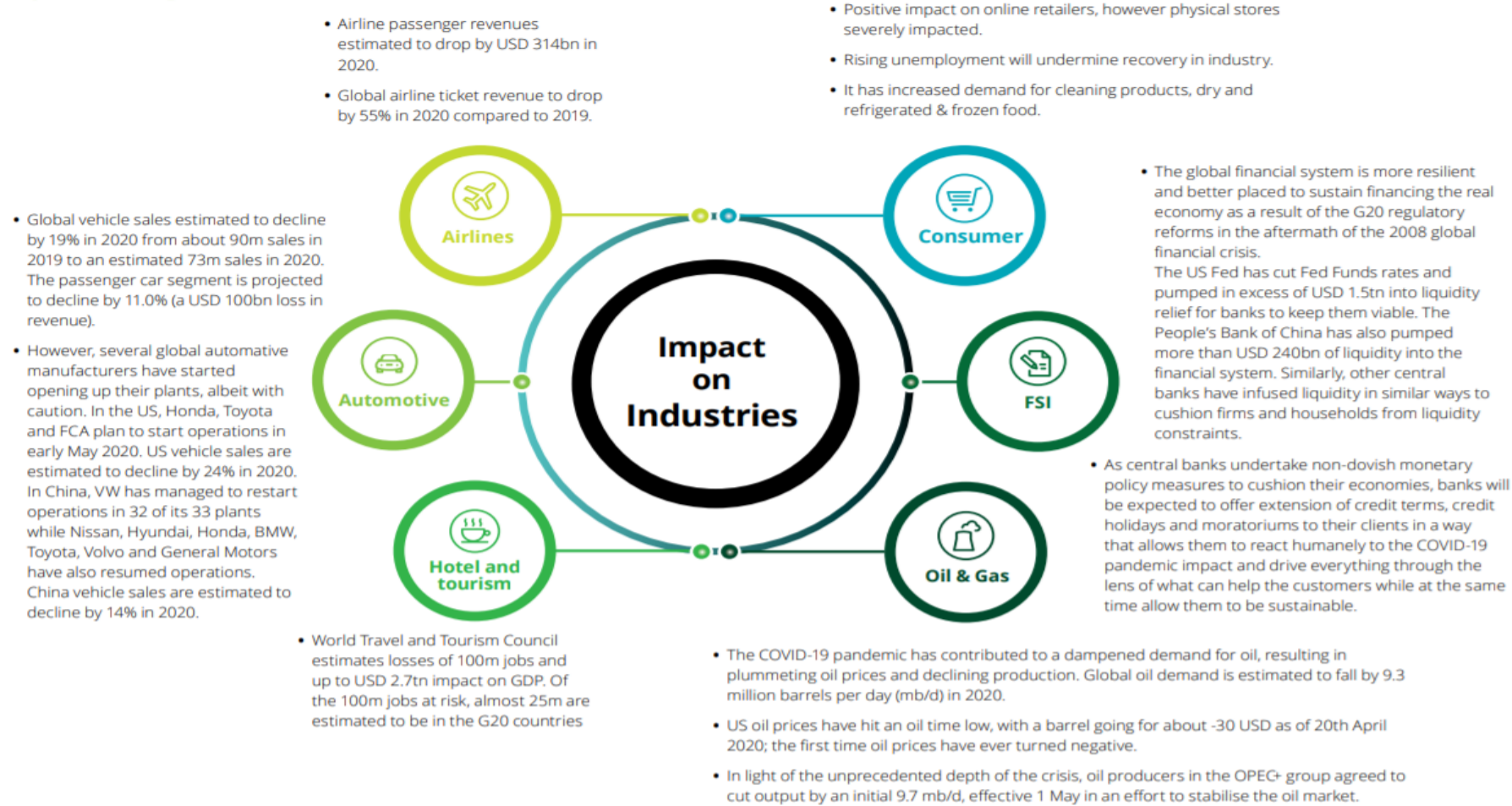


***Lastly, consider your reputation. The success stories of COVID-19 will be the people and organizations whose reputation was improved with their response to the pandemic. When the dust settles, we will remember those organisations that operated for the good of the society and the executive teams that took pay cuts to maintain their staff. For those organizations that take a short-sighted view of the pandemic, by price gouging or supply hoarding, the long-term negative reputational impact may far outweigh the short term benefits experienced.***

# COVID 19: Economic Impact of the COVID-19 Pandemic on Global Economies

## Economic Impact of the COVID-19 Pandemic on East African Economies

### Impact on global industries



Source: International Air Transport Association (IATA), World Travel & Tourism Council (WTTC), Financial Times, International Energy Agency (IEA)

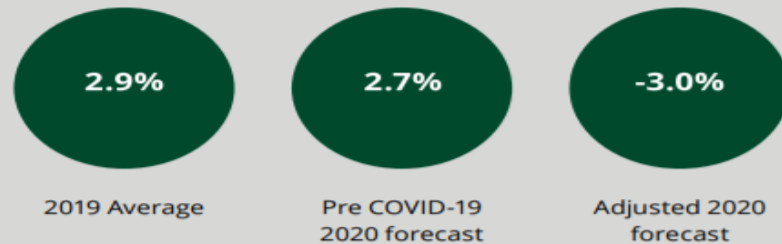


# COVID 19: Economic Impact of the COVID-19 Pandemic in Kenya

## Impact on Kenya's economy

### Global and Africa Economy

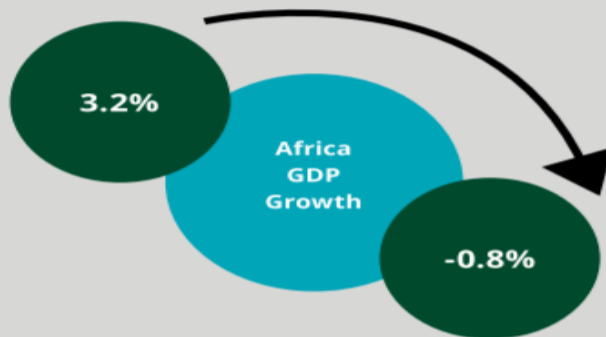
#### Global GDP Growth



Source: IMF, Fitch Solutions

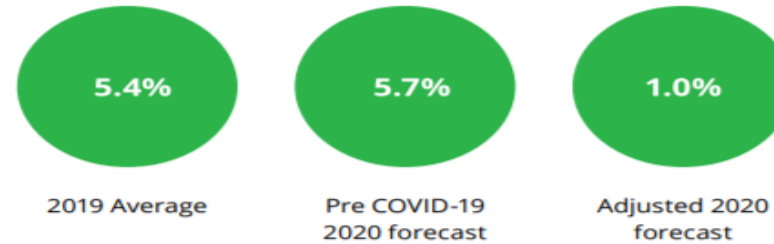
#### Africa GDP Growth

Africa's projected GDP growth of 3.2% for 2020 is now expected to recess to -0.8%.



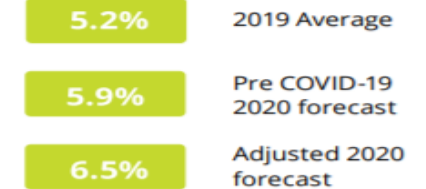
Source: IMF, African Union (AU)

### Kenya's GDP Growth



Source: IMF, Fitch Solutions

### Kenya's Inflation



Source: IMF, Fitch Solutions



- **USD 658m** drop in revenue collections in the remaining 3 months to the 2019/20 fiscal year end.



- **Lending rates, Savings and Deposit rates remain largely unaffected** and currently average 12.24%, 4.02% and 7.11% respectively.



- **3.1% (USD 545m)** estimated decline in total import value and a 36.6% decline in Chinese imports.



- A minimum of **25% (USD 1.5bn)** decline in export revenue expected.



- Tourism and travel contributes about **1.6m jobs (8.5% of total employment)**. Most of these jobs are at risk due to closure of hotels and shut-down of global aviation.



- **Kenya shilling** is under pressure due to reduced forex earnings mainly on account of reduced exports and **stood at KES 106.00: USD 1 as of 08 May 2020**, down from **KES 100.9: USD 1 as of 01 January 2020**.



- The flower sector is losing approximately **KES 250m** per day and is estimated to lose half of its value (**KES 60bn**) by end of 2020. Approximately **30,000 temporary workers laid off** and another **40,000 permanent staff sent on unpaid leave**.



- Downside risks remain evident on FX reserves that currently stand at **USD 7.7bn (4.7 months of import cover)** as at 30 April 2020.



- Current account deficit estimated to worsen to between **5% to 6%** of GDP in 2020.

# Responding to Covid-19 Disruptions on internal Audit

## Risk assessments and Audit plans

- New risks hence the need to revise risk assessments and activities in light of the new risks.
- Audit delays: Need to re-prioritize audits depending on significance, regulation and ability to execute them in a potentially disrupted environment.

## Workforce

- Redeployment of staff- When audits and assessments are delayed, other critical functions and processes may take precedence. Audit executives can redeploy audit staff to support these functions as they learn, build and expand new skill sets.
- Participate in crisis management committees
- Work closely with those with first- and second-line roles, as well with external audit, by asking “How can we help?”

## New and emerging risks

- Specific areas of risk are emerging from this new work environment. Internal audit needs to be keenly aware of these risks and work with the business to understand the effectiveness of the company's risk management practices.
- Such areas include: Fraud, data privacy, health and safety risks, liquidity and finance, cyber threats, business continuity and disaster recovery etc.



## Real time Reviews

- Assist the business in identification of new and emerging exposures brought forth by the Covid 19 reality.
- Performing real-time reviews in those areas (advisory or more real-time assurance), and providing innovative recommendations to resolve challenges.

## Remote work environments

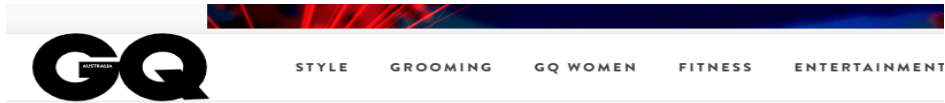
- Audits will be completed without physical access to offices hence the need for incorporating data analytics to execute internal audits without the need for a traditional site visit.
- Collecting evidence and reviewing documentation remotely via Microsoft Teams, WebEx or Zoom may solve the need to go on-site to perform an audit.
- Mandatory onsite tests can be pushed to later in the year.

# Repositioning for the future



***Do not waste a crisis: Its time to get ready for the future***

# Cybersecurity in the Headlines



HOME ► ENTERTAINMENT ► TECH

## WHY YOUR CYBERSECURITY IS AT RISK: GOOGLE DETECTS 18M COVID-19-RELATED MALWARE MESSAGES A DAY

GQ STAFF 14 JULY 2020

As Covid-19 cases increase across Victoria and NSW, the global pandemic has seen a significant spike in phishing attacks and scams.

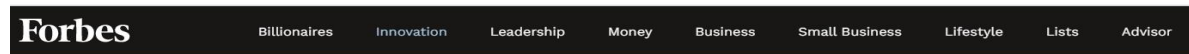
Here's what you need to know and look out for.



## FBI sees major spike in coronavirus-related cyber threats

BY MAGGIE MILLER - 06/24/20 04:59 PM EDT

41 COMMENTS



ADVERTISEMENT

**AUTOMATED CONTACT TRACING  
CAN SAVE LIVELIHOODS - AND LIVES.**

LEARN MORE >  
sas

EDITORS' PICK | 5,964 views | Mar 22, 2020, 05:44am EDT

### Healthcare Workers Targeted By Dangerous New Windows Ransomware Campaign Using Coronavirus As Bait



**Davey Winder** Senior Contributor @  
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



ADVERTISEMENT



5,514 views | Mar 26, 2020, 11:46am EDT

### Google Data Reveals 350% Surge In Phishing Websites During Coronavirus Pandemic



**Jesse Damiani** Contributor @  
Consumer Tech

I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.



# Cybersecurity Risks in the Covid-19 pandemic

The introduction of remote working due to COVID 19 pandemic has left most businesses exposed to an increased risk of cyber security attacks. This has been brought about by shift in management priorities into navigating the crisis brought about by the disrupted business making security efforts take a low priority. Hackers have also taken note of these and as a result, there has been increased cases on phishing and malware attacks.

## Examples of Risks



### PHISHING

Since mid-February, there has been an increased number of cybercriminals using COVID-19 themed spear-phishing attacks looking to bait targets to fake websites and collect Office 365 credentials.



### PERSONAL USE OF COMPANY DEVICES

Working from home with company devices has brought new temptations to use company equipment for personal use. This opens up the possibility and increases the risk for these devices to become infected with a virus or malware.



### REMOTE CONNECTION

Insecure remote connections to company systems and databases poses a major risk. Its Challenging to enforce, detect and respond to security issues in a remote working environment



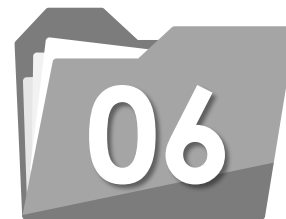
### FINANCIAL DISTRESS

The stress of uncertainty in a time of a pandemic can cause employees financial concern as well as concern over loss of employment. That concern has been known to be exploited by competitors to lure them into giving away corporate data.



### CONFIDENTIALITY

Brought about by working in households with multiple people, sharing of company computers and potential exposure of company information to third parties.



### FRAUD

Increased numbers of frauds perpetrated by fraudsters masquerading as company employees

# Responding to cybersecurity Risks in the Covid-19 pandemic

## What can Internal Audit do?

### Training

Ensure the business has carried out training on common security measures, like protecting devices, password complexity, phishing attack awareness and data protection.

### BCP Reviews

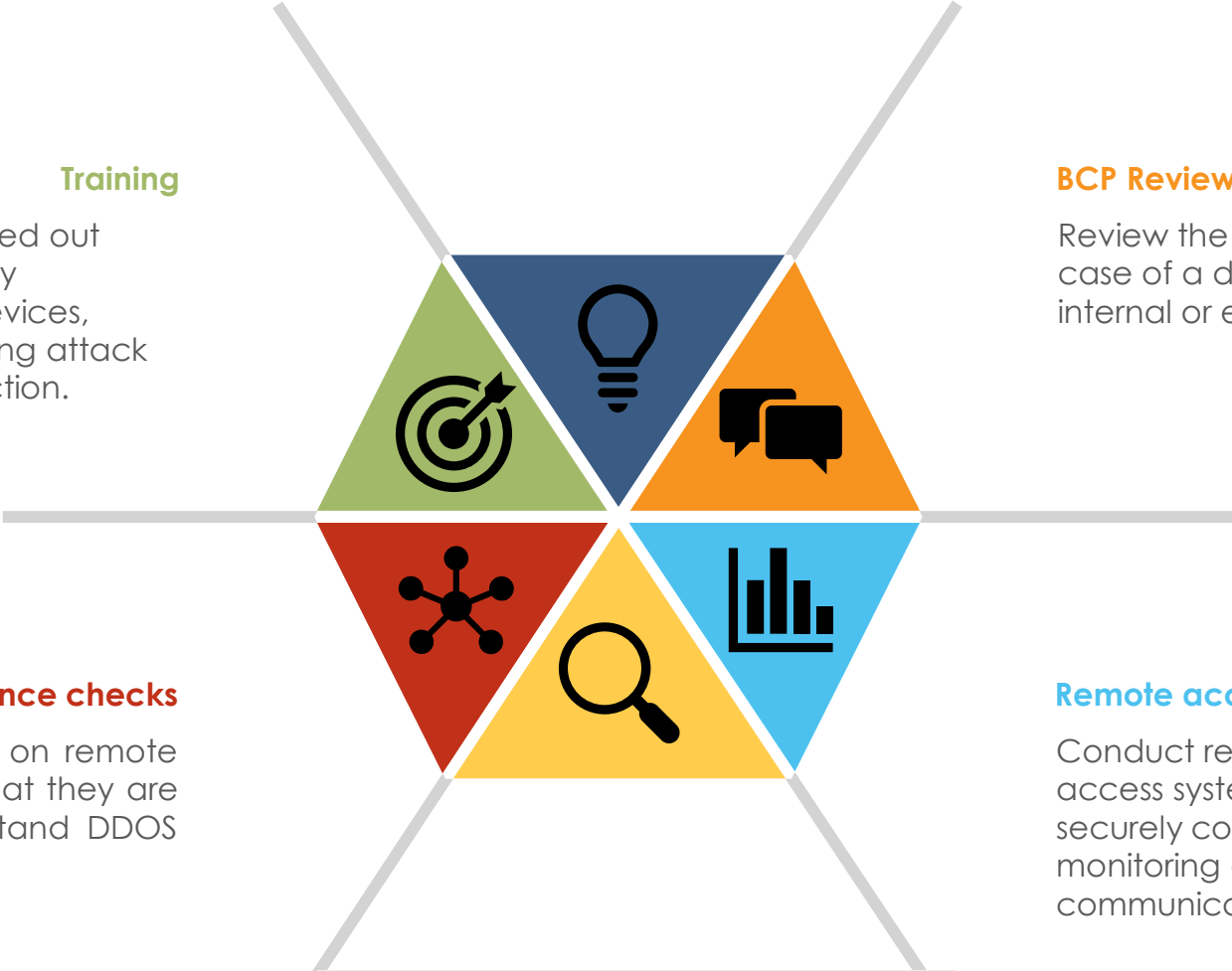
Review the business continuity plan in case of a data breach caused by internal or external remote workers.

### Resilience checks

Carry out penetration tests on remote access systems to ensure that they are sufficiently resilient to withstand DDOS attacks.

### Remote access Reviews

Conduct reviews to check that remote access systems are fully patched and securely configured. Continuous monitoring of these systems and timely communicate lapses.



Real time assurance of cyber security risks and prompt implementation of actions to close out areas of exposure.

# Bean counting or bean growing? The internal auditors Dilemma

*"We used to count the beans, but today's internal auditors are more apt to be examining how the beans are grown, how they are harvested, and how they are taken to market." Richard Chambers, President, IIA Global.*

## Bean Counters

- Internal auditors focus solely on financial records review
- Box Checkers: Focus on compliance checks



## Change Agents

- Modern day auditors who ask probing questions, seek to understand the 'why' in any review.
- Internal auditors scope of work has significantly grown and encompasses much more than assessing the adequacy of financial controls ie fraud risks, compliance issues, and operational issues.
- Auditors are now involved in root cause identification and insight generation to provide greater value and improvements to their organisations.



**Its time to change the narrative and correct the stereotype that Internal Auditors are bean counters**

# The internal auditors Dilemma.. Bean counting or bean growing?



*'Its time to put all efforts on bean growing'*

## Provide Value

- Participate in Crisis management committees
- Work with first and second line and offer assistance.
- Identify new and changed risks.

## Contribute and Help

- Play an advisory role in matters to do with risk management in the current situation.
- Participate in crisis management, fraud monitoring and help management prepare to transition out of the crisis.



## Demonstrate leadership

- By identifying changing risk exposures, as well as the need for corresponding changes to risk responses, internal audit can exhibit leadership that supports the organization's efforts to move forward.

## Embrace Technology

- Embracing technology is critical at this time. Advanced use of data analytics, robotic process automation, and artificial intelligence allows practitioners to continuously monitor for and more easily detect fraudulent activity and patterns of corruption, and it can be done remotely.

**How does internal Audit Remain independent and still assist management?**

Identifying risks and making contributions, all the while staying independent, can be done by refraining from decision-making and "owning" associated risks. If that becomes untenable, if "lines "are crossed, internal auditors can either assign subsequent assurance engagements of areas they worked on to a teammate or hire a third party.



# Remote auditing procedures and audit evidence in times of remote working



## Background and Challenges

**REMOTE AUDIT-** A remote audit, also known as virtual audit, is the method of conducting an audit remotely, using electronic methods such as video conferencing, email and telephone to obtain audit evidence, just like you would during an on-site audit. Remote auditing provides a springboard for tools such as file and screen sharing, video conferencing (Skype and Zoom are common platforms), and live data analysis. During this type of audit, auditors are able to adopt standard auditing techniques which they use during on-site audits, including being open minded, diplomatic, listening and being respectful to the auditee.

- According to a report by KPMG, many organizations have put their audit work on hold. Yet, given the adjusted risk landscape and changes in procedures, it is imperative that internal audit resumes their tasks as soon as possible. Given the travel restrictions and citizens being obliged to work from home, remote auditing is not an option anymore. It has become a necessity!

### Advantages of Remote Audits

- Restoration of a much-needed sense of normalcy.
- Reduced travel costs. For an audit program with multiple annual audits, remote audits can provide significant savings.
- Expanded coverage. Remote audits allow for more coverage when competing priorities of volume and time limitations occur.
- Expanded use of specialists. Specialists can connect remotely for selected interviews or parts of audit planning, and they need not be present for a full audit.
- Improved document reviews. Remote reviews of plans and documentation, at the auditor's own pace, contribute to a higher quality review and a deeper dive into the documentation.
- Improved use of available technology strengthens documentation and reporting.
- The audit burden to facility operations is mitigated. Time required to gather and digitize documentation, video, and images can be spread over several weeks, instead of concentrated into an audit period that takes personnel from their daily activities.
- Improved organization and confirmation of required documentation. Because facility personnel have to review and assemble the required documents, remote auditing provides an opportunity to organize and confirm that all documentation required for a regulatory inspection is readily available.

### Challenges of Remote Audits

- Delays in receiving information. Auditees may have competing priorities, responsibilities with family and children at home and other commitments. Internal audit should factor in additional time for delays.
- Some audit procedures may not be possible to be completed remotely i.e. stock counts
- First-hand observations cannot be replaced. There is nothing like seeing processes first-hand and observing body language,
- Technological constraints and connectivity issues could hamper completion of an audit.
- Remote auditing makes it hard to build rapport with auditees. Direct interaction with the auditee and the ability to read body language can be lost which can be crucial to exploring issues and audit trails further during an on-site audit.
- Some organisations may not support remote audits due to system access issues outside the confines of the office
- The lack of in-person interaction opens other opportunities for fraud. The opportunity to present doctored documents and to omit relevant information is increased.

# Remote auditing procedures and audit evidence in times of remote working



**Remote working:** The requirement to social distance as a way of preventing the CORONA virus spread, brought forth a new way of working. Remote working is a way of working outside of the traditional, centralized workplace, usually with the help of digital technology.

Although this is easy for companies with the IT infrastructures and work that can be done online, what happens to government institutions and banks?

## Remote working for Banks

- Barclays CEO Jes Staley, said that putting thousands of workers in a corporate office building may never happen again, during an earnings report call last month. "There will be a long-term adjustment in how we think about our location strategy ... the notion of putting 7,000 people in a building may be a thing of the past."

Banks have special considerations: safeguarding customers' financial information from both a nefarious employee and a potentially less secure environment that hackers could exploit.

### **What can banks do?**

- Use a virtual private network (VPN) that remote employees log into at home or in a coworking space. This VPN keeps data on a server back at the organization. When the employees log off, nothing remains on their computer.
- Make sure devices used by remote workers are accessible and controlled by the IT department. They should have up-to-date security patches and information security protocols in place.
- Create a remote-work policy that details specific dos and don'ts, and train employees on security measures.
- Emerging end-use technology can be installed on bank-issued devices that can visually monitor remote workers' activities.

### **Go Digital**

- Invest in the digital tools and solutions that will reduce the need for traditional branches.

## Remote working for Governments

- Identify and evaluate functions that can—and cannot—be performed remotely. Identifying options for functions that could be done over the internet may require some modifications to existing policies or systems, so flexibility is key if there are few risks in doing so.
- Provide appropriate infrastructure supports. Virtual private networks help employees maintain security while connecting into the agency or company network.
- Ensure logistical supports are in place. This includes training on telework and telework tools, agency policies, which should cover security/access protocols, use of personal digital equipment (computers, phones, tablets, etc.).
- Support engagement through communication. Remote employees can connect with each other and with on-site employees through collaboration tools supporting functions like chat, videoconferencing, screen-sharing, and collaborative document-editing.
- Track productivity appropriately to increase management buy-in, reduce fraud, and recognize telework benefits and shortcomings.

# Considerations For Auditing Remotely

## Technology

- Adopt technologies such as Microsoft teams , zoom, skype for work and consider recording such interactions to enhance audit evidence with privacy laws being followed.
- Secure web portals, ensure secure sharing of documents
- Lack of appropriate technology that would hamper remote audits

## Standards and procedures

Practitioners still are required to meet the auditing standards as they fulfill their duties.

- IPPF, IPSAS, IAS etc

## Communication

- Auditors should mirror their procedures for on-site audits as much as possible when they are auditing remotely. Team communication and status update is paramount.
- On camera discussions

## Security

- Beware of the potential for cyberattacks. There is an increased risk related to hackers trying to take advantage of the coronavirus situation to get access to systems by having phishing scams related to the coronavirus.



## Access

- Appropriate system access to facilitate audits is required for auditors.

## Culture

Challenge of transitioning from an onsite mode of working and ensuring that employees remain productive. It would require a change in mindset and performance metrics.

## Regulation

Requirement by the regulators to keep places of work open may hamper remote working.

## Business Model

Working in an organisation where all work has to be done onsite due to technical or system constraints would hamper remote audits.

## Approach to Remote Auditing

### 1. Plan

- ❖ Review the annual audit plan in light of the current circumstances and prioritize activities that add value to the business at this point. Update the risk assessment and determine areas of focus.

### 2. Prepare

- ❖ Check availability of auditees
- ❖ Use of tools: Determine the tools for interaction and document sharing
- ❖ Planning the audit-scope the audit on key risks bearing in mind that the effects of technical issues (e.g. connectivity, sound quality, etc.) could have a larger impact and may require more time to resolve.
- ❖ Clarify the new process to stake holders and the differences with face-to-face audits

### 3. Execution

- ❖ The execution phases of a remote audit is quite similar to that of a traditional audit. With the main differences being that video conferencing will replace the interviews and documentation needs to be transferred to you through a document sharing platform.
- ❖ Ensure accessibility and security of the platform as well as confidentiality of the information provided is maintained.
- ❖ Alignment with auditees: While working remotely, it is important to keep in close contact with the auditee to remain aligned.

### 4. Reporting

- ❖ For remote audits, reporting protocols might need to be revisited with regard to their frequency and the way in which audit teams report to the auditee as sufficient interaction is crucial.
- ❖ Validation of findings: Each observation needs to be discussed and validated with the auditees before finalizing the report. This is important because the use of video conferences may lead to misunderstandings between participants. Any feedback received should be incorporated in the report, and previously identified risks and opportunities should be updated accordingly.

### Audit Evidence during remote auditing

- a) Recorded video conference meetings
- b) Digital files uploaded through secure file sharing sites
- c) Walkthrough meetings held through platforms like zoom/ Microsoft teams that allow sharing of screens
- d) Security camera feeds
- e) Phone Interviews

### What to do if Remote Auditing is not feasible

- a) Reschedule audits to a future time
- b) Time to shift focus on '**Repositioning for the Post-Covid opportunities**'

**Remote audits are the future of auditing**



# REMOTE AUDITING IN PUBLIC SECTOR

**Due to lack of adequate technology and systems to facilitate remote auditing in public sector entities, the auditor should consider the following:**

**❑ Have an ear on the ground**

Even with inability of the auditor to continue with business as usual, the auditor should not sit back. It's a time to have their ear on the ground, understand what the organization is focused on, lend a hand with the crisis management and ensure that management is aware of the changed risk landscape.

**❑ Be a digital solutions advocate- Optimize IFMIS**

With public sector institutions using IFMIS which is an oracle based financial system, the auditor should review whether the system is being utilized at its maximum capability. Have all the processes that can be carried out on the platform being onboarded on to? Can the auditor champion the move to digital solutions? The government cannot be left behind with advancement in technology.

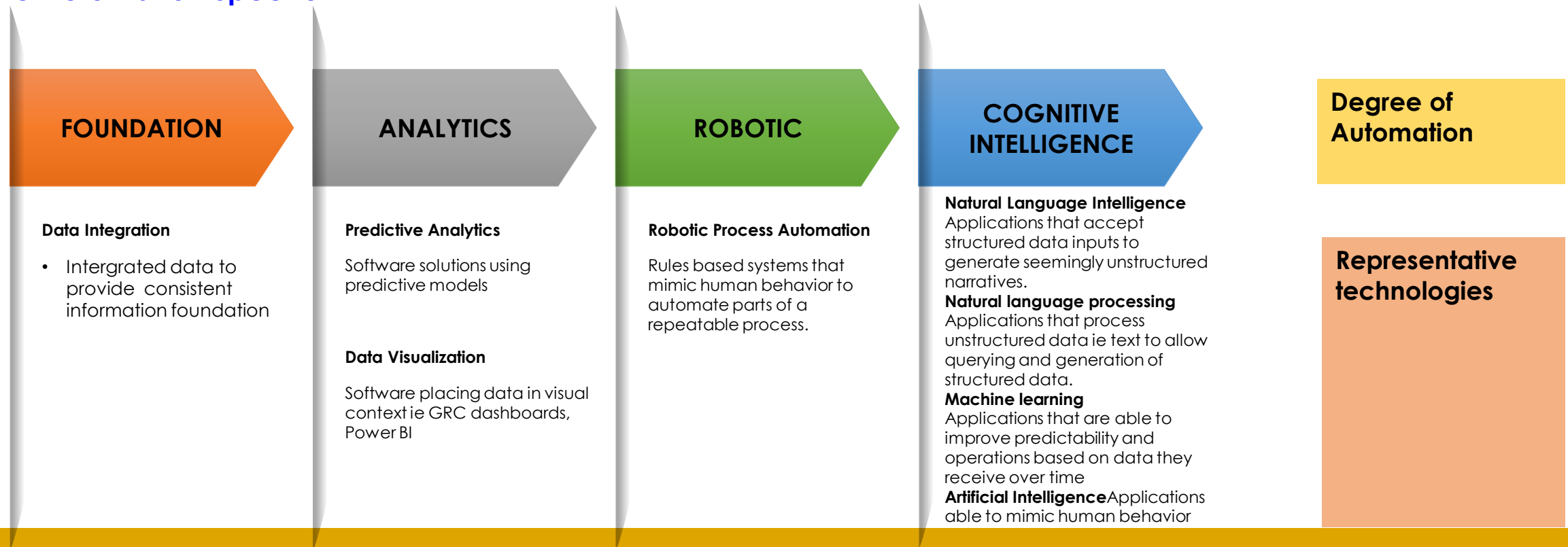
**❑ Regulation**

Plan to resume audit activities as soon as possible. The pandemic has shifted priorities in first line and this may leave room for fraud, errors and mistakes. The Public Finance Management Act Section 73 stipulates that every National Government entity must maintain internal auditing arrangements. The auditor should still deliver their mandate while adhering to social distancing guidelines which can take the form of shift work.

# Automating Internal Audit Function

- ❑ Audit automation refers to the use of information technology in the planning, controlling, execution and recording of audit work.
- ❑ Since many internal audit processes are manual and repetitive in nature requiring significant time to perform and remain consistent year-on-year, IA departments are beginning to realize that automation can make their work increasingly efficient and improve audit coverage.
- ❑ This, in turn, can free up time for more strategic, value-adding work (e.g., work that requires a depth of evaluation and judgment not available through RPA solutions).
- ❑ Further, organizations are rapidly adopting technologies such as cloud computing, robotic process automation (RPA), machine learning, blockchain, and cognitive computing to create tomorrow's business in today's market. Internal audit needs to transform its processes to keep pace with these changes, and IT audit processes are an excellent place to start this transformation.

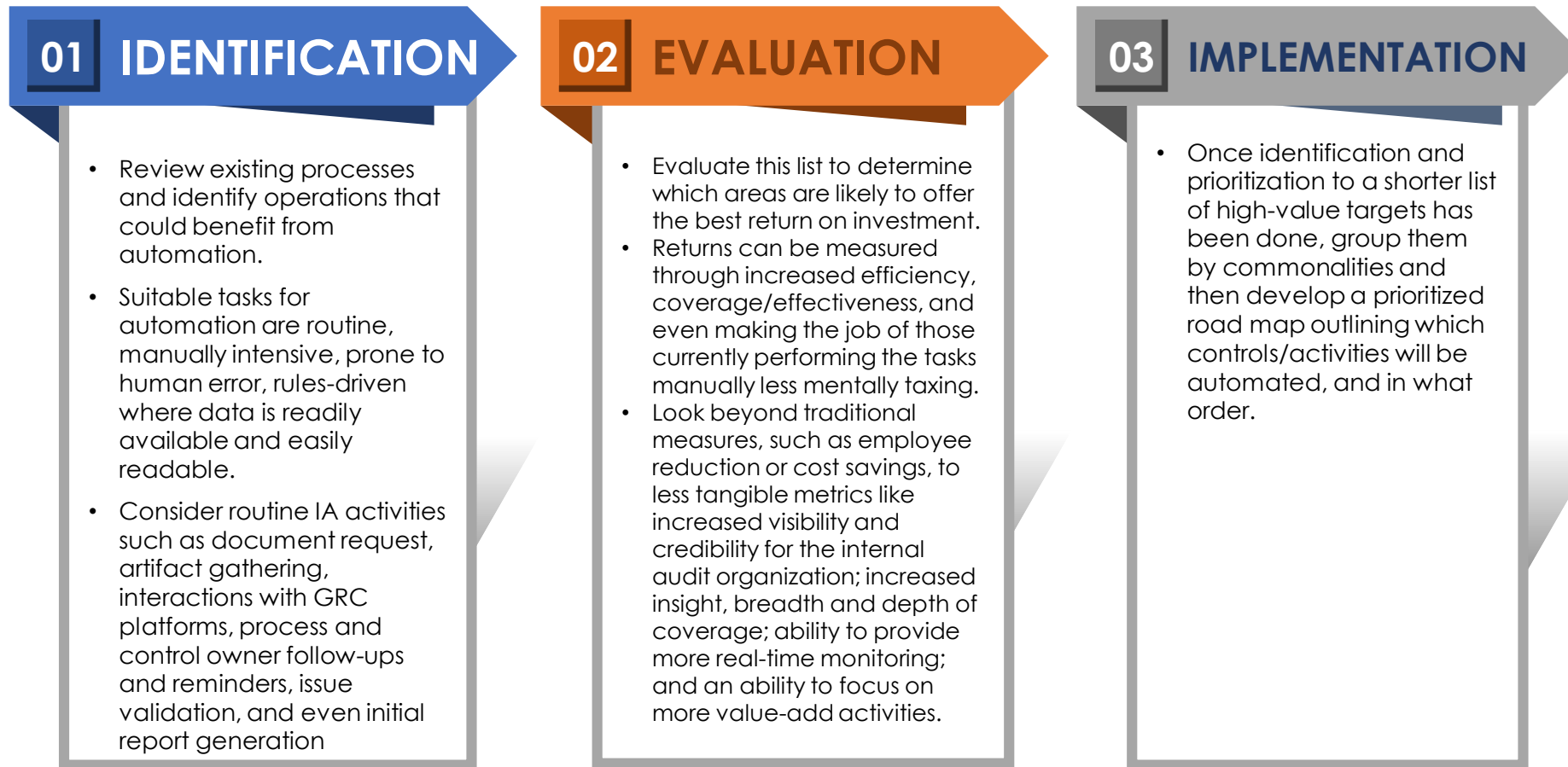
## The Automation Spectrum



# Automating Internal Audit Function – Where do we start?

- Experience indicates that auditors will likely attempt to first automate the processes that they already use, are comfortable with and are already accepted for auditing and reporting purposes rather than trying to start from scratch, especially when dealing with audits of ongoing operations.
- Areas best suited for automation include: rules based, repetitive tasks that are time consuming and areas that may be demanding and expensive to monitor independently.

## Process of Automation



# Automating Internal Audit Function – Areas of Automation and Benefits

## Activities that can be Automated

- ☐ Document request from management
- ☐ Evidence gathering and review of documents i.e. invoices, POs etc.
- ☐ Issue follow up and reminders-Identifying open items, sending emails to responsible parties, conducting follow-up when due dates are not met and documenting remediation status.
- ☐ Initial report generation
- ☐ Controls testing
- ☐ Tracking progress against the annual audit plan or tracking and monitoring key risk indicators (KRIs)
- ☐ Populating audit committee and management report templates or internal audit's balanced scorecard
- ☐ Completeness checks

## Benefits of Automation

- ☐ More time is freed up time for more strategic, value-adding work (e.g., work that requires a depth of evaluation and judgment.
- ☐ Automation can help internal audit increase productivity, expand its risk coverage and help address the ongoing compliance burden by doing more with less.
- ☐ Increased insights, breadth and depth of coverage
- ☐ Increased credibility of the internal audit function.
- ☐ Real time monitoring and thereby timely reporting and rectification of gaps.
- ☐ Increased efficiency and effectiveness of the IA activities.
- ☐ Cost savings in the long run

# Automating Internal Audit Function – How do Auditors remain relevant?



## A. JUDGEMENT

- With the advancement in technology and the ability to automate most routine tasks, how do auditors remain relevant? The answer is simple: **JUDGMENT**. Auditors can remain relevant with their judgment and their skills will increase when augmented by AI, robotics and machine learning. Auditors can use the available tools to automate processes and leverage technology to create additional value in their organisations. This value often comes in the form of advisory or consulting services, rather than compliance services.
- Auditing is judgmental in nature, and, although automation can support the judgment process, it cannot replace human judgment. Technology should reduce the barriers and repetitiveness of time-consuming sampling. Auditors can leverage technology to get greater coverage but you never can automate the human judgment component.

## B. INSIGHTS AND FORESIGHT

- As a result of increased audit automation, auditors can now spend more time reviewing analyses and interpreting results rather than performing tasks. This will result in greater number of insights and value adding foresight for the business.

## C. AUDIT OF AREAS THAT REQUIRE HUMAN REASONING AND WHERE MACHINES CANNOT REVIEW

- Culture is the risk that underlies all business risks. As boards and audit committees sharpen their focus on corporate culture, many are turning to internal audit to help them better understand and assess the organisation's culture. This risk cannot be reviewed and audited through automation tools and there is need for human review.





**What does the future look like for the Auditor?**

## How the future looks like

### Real time Auditing

Continuous and real time audit will be the norm.

### Strategic involvement

Internal audit will be part of board and C-suite discussions

### Multiskilled

Internal audit teams will have a mix of skills across audit, technology and data analytic skills.

### Priorities

Future focused and emerging risk reviews will be prioritized.



### Audit Coverage

The use of technology will enable a 100% coverage of audit populations.

### Reporting

Audit reports will be concise and have visualized reporting on impact

### Technology

Audit work will go beyond data analytics and automation.

### Audit plan

Flexible audit plans responsive to disruption and flexes to meet strategic demands.

# Participants Questions during the webinar

Thank you for sharing your questions during the webinar. We have grouped the ones not addressed during the webinar in broad categories and provided responsive comments in the table below. Some of the questions have already been addressed in detailed sections of this participant pack and some of the responsive comments here came from participants chats during the webinar.

## Questions

### 1. Remote working

- Comment on remote working; As an external internal auditor this has been quite challenging and in fact we have found ourselves taking more time to complete an audit compared to before.
- On remote work environments, which data analytics tools may you recommend ?
- How do we handle audits where we have to confirm items physically e.g cash?
- Do you have a remote audit guideline, policy and audit program which you can share with us?
- There is need for increased investment by management in supporting internal auditing in the new norm especially with remote auditing-**agreed but also depends on stage of readiness for by the audit team and competing investment needs in crisis time.**

### 2. Licensing regime

- Clarity on licensing requirements for External and Internal Audit

**3. In the context of what you have shared, what would you say is the difference between an internal audit engagement and Risk and Compliance audit**

## Comments (including those from participants)

### 1. Remote Auditing

- Be understanding and empathetic is critical more so understand the audit client situation because of the crisis.....be flexible... The early days also had effects of shock on both parties as the crisis unfolded.
- For remote auditing, let auditors clarify the remote auditing approach to the audit client. You need to schedule recurring short meetings to discuss audit status but also capture any worries and concerns. Validate audit findings since with video conferences, lot of misunderstandings arise. Consider recording video sessions but get consent of the audit client. Also redefine your risks and response steps to address any changes in business model.
- There are many analytics and robotic tools in the market and not to appear to advocate for a particular vendor, happy to discuss this offline as it depends on many factors.
- Reconsider how you need to get assurance on items that would previously have required physical inspection e.g review controls for stock dispatch and reconciliation or cash collection, banking and reconciliation and then get custodians to certify their stock/cash holding at a higher than normal frequency such as daily if necessary.

### • Licensing regime

- Currently all external audit firms and practitioners are licensed by ICPAK through issue of practicing license to the individual members and firm license to the firms. SO practitioners who provide only consulting, accounting or Internal Audit services are currently not licensed. ICPAK is in the advanced stages of launching multiple licenses that will cater for all categories of Accountancy as defined by the Accountants Act. Those with experience in, and wishing to practice, say Internal Audit or taxation, will get a category of license to allow them to offer that specific service.
- Risk and compliance are a 2<sup>nd</sup> line management function to identify, manage and report risk. Internal audit is primarily a 3<sup>rd</sup> line Assurance line than provides comfort to those charged with governance on how well the 1<sup>st</sup> (management controls) and 2<sup>nd</sup> line are functioning.

**Are you still valuable to your  
Organisation?**

*Thank You!*