Association of Chief Audit Executives of Banks in Nigeria

Design+printbyProwess08039221516

ACAEBIN
Plot 1398B, Tiamiyu Savage Street, Victoria Island, Lagos.
Office Line: +234-1-3424805
E-mail: info@acaebin.org
website: www.acaebin.org

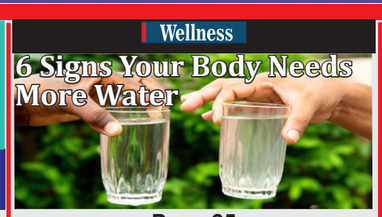
Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q3, 2020

Elevating Internal Audit Role In The Face Of Emerging Risks And Opportunities

Auditing Knowledge Management

Page 36



Page 25

Post-pandemic Planning

Page 41

ACAEBIN EXCO MEMBERS

Yinka Tiamiyu
(Chairman)

Uduak Nelson Udoh
(1st Vice Chairman)

Felix Igbinosa
(2nd Vice Chairman)

Gboyega Sadiq
(Treasurer)

Aina Amah
(Auditor)

Prince Akamadu
(Chairman Research & Publication)

Adekunle Onitiri
(Chairman Payment & Systems)

Dele Dopemu
(Ex-officio I)

Samuel Ekanem
(Ex-officio II)

CONTENT

Editorial

Our lead article that focuses on the theme of this quarter's general meeting avers that it is difficult to predict any patterns to the economic outlook in 2020 as the microeconomic assumptions seemed to have changed negatively while the unstable microeconomic environment had impacted negatively on the economy, social activities and general survival across the globe with particular reference to the Nigeria nation and banks.

The author continues that Internal Audit role is changing in approach and scope as activities and events begin to alter the business dynamics across the globe with immense risks and uncertainties assuming unprecedented folds. The immediate consequence is that Internal Audit role has become elevated in view of the changes to economic and business tides with multiple risks and opportunities becoming heightened.

Given the impact of the COVID 19 on the world in general and banks in particular, we have another article that lists five assurances that Board audit committee members are looking forward to receive from chief audit executives. Please ensure to read the article.

Our article on the Economics of Pandemics and the Role of Internal Audit Function argues that there are three major ways COVID-19 is pushing fundamental economic shift. One is the shift in perception of what can influence economics, secondly is the need to embrace technological solutions and finally is the importance of strong institutions. The authors posit that the banking sector should set the pace and define what post COVID-19 holds for the country and the people of Nigeria. Furthermore, it is their opinion that the internal audit function has both an obligation and an opportunity to help their companies manage the most critical risks that COVID-19 has either created or magnified while helping their organizations to weigh risks and opportunities, as these ensure that informed decisions are reached by their organizations.

We have included a well written article on types, pricing and auditing of bonds. The author concludes that the 'auditor has a significant role to play for corporate as well as for major individual bond investors, in validating substance, existence, completeness, accuracy, and valuations of bonds portfolios, which role should be performed meticulously and with high sense of professionalism'.

Often times, we get carried away by fashionable and trending terminologies and relegate, to our later discomfort, basic but important matters. Hence, we have added an article on corporate fraud. The writer, in simple flowing prose highlights types, causes and methods to detect and prevent fraud.

Given the times we are in where ransomware attack is now a major event that has long-lasting effects we have culled an article from ISACA titled Responding to and Protecting Against Ransomware. It is a useful article

Do you desire a healthy liver? How do you know if you need to drink more water? We have got answers for you in our health and wellness section.

As we progress into the last quarter of year 2020, let us continue to exercise care and abide by all relevant medical protocols. We surely shall overcome.

Prince Akamadu
Chairman, Research and Publication.

Elevating Internal Audit Role In The Face Of Emerging Risks And Opportunities With Emphasis On

- *Internal Audit Role (Assurance, Advisory Consulting)*
- *Emerging Risks (COVID-19, Cybersecurity)*
- *Opportunities (Digitization, Etc)*

1.0 Background

The Internal Audit function occupies an enviable position in Nigerian Banks, from the provision of assurance on the systems of internal controls, governance and management risk, maintaining mutually beneficial relationships with various stakeholder groups.

The entire world has continued to battle with the current plague – COVID-19; a virus that has subjected everyone to *'a new world order and norm'*.

2.0 Internal Audit Role (assurance, Advisory Consulting)

While it has become increasingly perilous to predict any patterns to the economic outlook in 2020; the microeconomic assumptions seemed to have changed negatively. The unstable patterns of microeconomic assumptions had impacted negatively on the economy, social activities and general survival across the globe with particular reference to the Nigeria nation. These microeconomic assumptions include amongst others the following:

Unemployment, Inflation, Monetary policy, Manufacturing output, Official exchange rate, Bank autonomous credit expansion, Oil prices, Development finance credit expansion, National geopolitics.

The Internal Audit role continues to change in approach and scope as activities and events begin to change the business dynamics across the globe with immense risks and uncertainties assuming unprecedented folds. The Internal Audit role has become elevated in view of the changes to economic and business tides with multiple risks and opportunities becoming heightened.

2.1 What Is The Assurance And Advisory Roles Of The Internal Auditor At Such A Time?

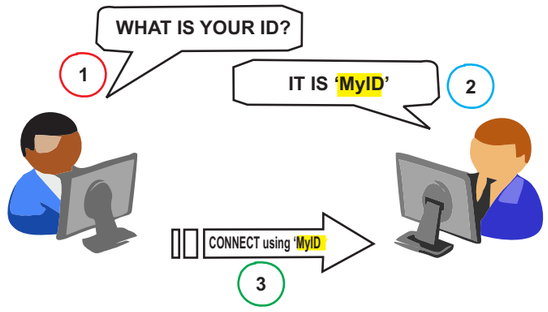
The Institute of Internal Audit (IIA) defined 'internal auditing' as ''an independent, objective assurance and consulting activities designed to add value and improve organisations' operations'' This definition did not envisage critical events that could occur and take the Internal Auditors' roles beyond the provision of assurance and advisory roles.

In the face of the unpredicted outlook of the dynamics of doing businesses across the world; the roles of the Internal Auditors seemed elevated in scope; thus, my re-coined perspectives below:

An Internal Auditor (IA) is a trained professional individual saddled with the responsibilities of providing independent and objective evaluations of company financial and operational business activities. They are employed to ensure that companies follow proper procedures and execute functions that would minimise income leakage, that policies are duly followed, assets and human resource are safeguarded; defined processes are closely monitored as established by Management in order to reduce the impact of system vulnerabilities.

Internal audit operates within a demanding regulatory and legislative regime that can limit innovation for today's risk techniques and approaches. The Internal Auditors of today (2020 and beyond) need to be able to resolve to learning and adapting expertise and unique skillsets in developing other detective solutions that will better meet stakeholders' needs in view of their elevated roles.

3.0 Emergent Risks (COVID-19, Cybersecurity)



IT and business innovation provide endless possibilities for internal auditors to better serve their clients and improve audit quality. Even though technology can automate audit procedures, people are crucial to interpret data, provide ethical judgement and strategic advice – Thus, only an internal auditor that nurtures the belief that **'learning is a journey'** would continue to be relevant in view of the emergent risks (COVID-19, CYBERSECURITY).

3.1 What Are The Emerging Risks And How Do The Risks Elevated The Roles Of Internal Auditors?

The COVID-19 pandemics has continued to shape transaction patterns in Nigeria and all over the world. Business decisions have been taken differently by those charged with governance of entities as a result of the impact of **'social distance rules'** established by different countries; the **'work from home orders'** etc; the current dispensation thus makes it impossible to conclude transactions using physical contacts from beginning to the end.

Transactions are majorly driven by electronic or online channels, thus creating more vulnerabilities for individual and entities who get attacked by electronic fraudsters and hackers. The emergent risks have therefore increased in leaps and bounds as highlighted below:

- **Shift in attack targets** - attacks have shifted to cloud-based systems and internet of things – (IoTs);
- **Shift in attack magnitude –** Number of attacks have increased due to increase in online channels
- **Shift in identification and authorisation** – increase in attempts to steal credentials
- **Shift in monitoring** – Increase in the use of artificial intelligence for monitoring people and organisations.
- **Shift in regulatory oversight –** Regulators will tighten regulatory requirements and ensure safeguards arounds Data Privacy (DP).

The emergent business protocol designated as '*the new normal'* has become households' lyrics across the globe as the COVID-19 pandemic has created an abrupt need for companies' entire workforce to be re-located out of their corporate facilities and into virtual environment to aid remote working arrangement.

The roles of the Internal Auditors became tweaked to mirror current business dynamics and realities; thus, **'auditing remote workstations techniques' (ARWT)** also became prominent amongst Chief Audit Executives (CAEs) within banks in Nigeria and across the world.

The elevated roles of the Internal Auditors manifested as their security focus has shifted from companies' perimeters to devices outside their networks in order to provide assurances on enterprise resources as well as safeguard customers transactions on online platforms when faced by any of the underlisted vulnerabilities

- Phishing
- Insecure wireless-fidelity (WIFI)
- Data leakage and privacy
- Attacks on remote infrastructure

- Unauthorised insecure devices
- Misconfigured cloud infrastructure

4.0 Opportunities (digitilisation Etc)

There are opportunities and challenges to the current world order which organisations have described as the biggest event that have slowed economic indices and halt so many businesses; however, it also came with some opportunities. Let's dwell on challenges, opportunities and actions to take by Internal Auditors in combating these challenges:

Cost of no service/business shutdown

Organizations most times shut down their systems to contain the effect of attack during this period and as a result, earnings were lost.

- **Direct monetary loss** - This is the loss that occur as a result of cyber-attack or cost of increasing the defensive mechanism (fire walls) as a result of persistent cyber threats (successful and unsuccessful attempts).
- **Cost of investigation -** This is the cost of paying experts like (Internal Auditors) to investigate a cyber incident.
- **Non-monetary impact** - Such as reputation/brand value loss and probable loss of customer loyalty.
- **Increased operational overhead costs** - These costs include amongst others: (1) regulatory costs (2) legal costs, (3) repairs and rebuilding costs (4) marketing and public relations costs.

Combating Challenges By The Internal Auditors

- Perform security assessment on remote working infrastructure.
- Implement and monitor minimum security baseline for remote devices. Examples: multiple factor authenticator; robust encryption and antivirus.
- Review and communicate remote BYOD agreement. BYOD stands for ''bring your own device'' staff members working remotely could decide to use their own computer machines; a corporate agreement should be prepared by the Legal Department in concurrence with the Information Technology Group. Staff members working remotely with their personal devices would be required to execute such agreement; excerpt of the agreement should automatically become part of the remote working policy (RWP).
- Review and ensure that business continuity plans and business resilience strategies are periodically updated.
- Check to ensure that platforms are in place for staff to institute and communicate measures for staff to report cyber security incidents.
- Review SLAs with cloud providers as it relates to business continuity and backups.
- Develop strategy for cloud and perform security assessment on cloud infrastructure.
- Institute staff awareness jingles timeframe to aid security awareness for all staff and assess evidences of internal combinations against set time-frame – ensure that contents of internal communications are reviewed and that it conveys current security trends and threats.
- Review configuration of third-party services – (e.g. Microsoft teams, zooms, drobox etc) to aid data privacy.
- Review data leakage and loss prevention solution periodically.

Opportunities Arising From Digitalization of Business Processes

The current wave of COVID-19 pandemics has also brought a hype in businesses digitization processes. This has created opportunities for entities to see the ***new normal*** from the other side of the coin. These opportunities include amongst others the following:

(1) Reduction in the costs of erecting bricks and mortals

Online transactions are consummated anywhere without customers visiting offices or branches of companies. Companies do not need to spend scarce resources on erecting structures for the sake of either housing their staff members or customers. Millions of naira are being saved with the advent of this era, with businesses being closed successfully at remote locations like never before.

(2) Comfort and convenience of conducting businesses online real time

Transactions are consummated at the comfort of ones' room remotely without attributable costs of getting such businesses done without hazzles as well as total elimination of high turnaround times as these businesses are done online real time. All transactions are therefore designated as '*spot in nature'.*

(3) Greater reduction in the conveyance of cash instruments

Digitization has brought lots of conveniences to business landscapes across the globe; currencies are no longer being conveyed in abundance as physical contacts with persons have been greatly reduced by the *'social distance rules'* initiated by the governments of different jurisdictions.

(4) Electronic payments solutions as aids to foreign exchange rates computations.

Payments for goods and services could be done remotely without recourse to ascertaining or computing the exchange rates, rates are automatically computed and charged to customers' accounts as a result of digitization. Electronic master cards etc have indeed paved way for this; businesses are concluded remotely with the aid of this means of payment.

(5) Remote trainings possibilities and elimination of cost overheads

Trainings across all parts of the world are now being done seamlessly without physical presence. This is made possible by digitization. Companies overheads on trainings have been grossly reduced; as foreign trainings would involve huge costs such as airfares, staff benefits-in-kinds like per diem and other factors such as feeding and hotel accommodations. Prior to the advert of COVID-19 pandemics, companies do not believe that value added trainings could be implemented successfully via virtual platforms such as zooms, Microsoft teams etc.

(6) Remote working capabilities across the Globe

The use of virtual private network (VPN) was not this echoed, current events had shown that workplace is no longer designated to one location; majority of the organisations have their staff members working remotely from homes, and this has proven to be very effective with most entities clamouring that this might just be the way forward whether the pandemics goes or stays. The use of VPN, intelligent CCTV cameras, wireless networks for guests' access have paved ways for remote working capabilities.

(7) Broaden the e-commerce horizons effectively

Digitalization has quite broadened the horizons for electronic commerce, meetings such as annual general meetings, extra ordinary general meetings of customers, board committee meetings with such meetings appearing as if they were physically held. Passengers are onboarded into flights electronically while internet of things have continued to pave way for broader sophistication of the e-commerce horizons; the use of artificial intelligence to aid business decisions and carry out some domestic tasks have continued to be improved upon.

(8) Increase use of internet of things (Iots)

The current dispensation has created a greater learning curve for persons who perhaps have taken for granted the importance of technology. Board of entities have committed funds towards creating awareness and building tech-skills amongst her staff members. Lots of companies/individuals have deployed electronically operated devices to resolving daily challenges at work places and homes respectively with less human intervention.

5.0 Conclusion

The Internal Auditors would have to do lots of reading and researches on how best to mitigate threats; Data privacy protection is pivotal to the Internal Auditors of today than before – relaxation of data protection practices while using online collaboration tools and techniques (Example video calls, online meetings, online drives) to share personal data could lead to exposure, any online meeting without a password is a target for hackers. Risks associated with remote audit executions should be the basis for all internal audit engagements in the current dispensation.

To this end, attacks on remote infrastructure had led companies to create new infrastructure for remote working, deployment of VPN-servers, moving internal applications to the demilitarized zone (DMZ) by expanding their internet facing perimeters.

It is therefore a wake-up call to the **Internal Auditors, CAEs, Board Audit Committees of entities** to note that the roles of Internal Auditors have been elevated with the emergent of these risks and opportunities embedded in COVID-19 pandemics.

Julius Oreye A.
Lead Internal Auditor
Heritage Bank Plc, Lagos, Nigeria

CORPORATE FRAUD:
TYPES, CAUSES, DETECTION AND PREVENTION

What Is Corporate Fraud?

Corporate fraud occurs when illegal activities are done by a person or a company in a manner that is dishonest or unethical. Some examples of cases of corporate fraud are complex, highly secretive, and when found out involve evasions of financial responsibilities or economic scandals.

In some situations, fraudulent activities begin small and are never intended to be ongoing. As a result, it is difficult to detect fraud early enough. Most times, fraud goes on uncovered for long periods of time before:

- the scheme is detected by a whistleblower,
- inabilities of the scheme to keep up with the demands of its expansion or
- the lack of planning on the perpetrators' part.

Types of Corporate Fraud

1. Corporate Service Fraud

a) **False Accounting Fraud:** This involves the alteration of the way in which business accounts are presented in order not to show the true value or financial activities of the business. This type of fraud mostly includes the overstating of assets and/or understating of liabilities.

b) **Procurement Fraud:** Procurement which is the process of acquisition from third parties and which entails the acquisition of goods, services and construction projects. Procurement fraud mostly involves collusion to perpetrate a fraud covering tendering irregularities, the rigging of bids or claims for payment – mostly regarding goods that were not delivered or are inferior to what was stated in the order.

c) **Payment Fraud:** This has to do with falsely creating or diverting payments. Examples include the creation of fake records and bank accounts which enable the fraudulent payments to be made. Other examples include intercepting and altering payee details, making fraudulent payments to oneself or generating false payments

2. Institutional Investment Fraud

a) Pension Fund and Hedge Fund Frauds: This relates to fund managers targeting institutions and corporations to make financial investments that promise very high returns, but which often becomes "too good to be true". For these types of frauds, investors are misled by fund managers by making false disclosures, or through failure to provide full information about the investment opportunity.

b) Pyramid or Ponzi Schemes Fraud: This involves a non-sustainable business model in which the investments of earlier investors are used to pay later investors, giving the appearance that the investments of the initial participants dramatically increase in value in a short amount of time.

3. Business Trading Fraud

a) Long and Short Firm Fraud: This occurs when a legitimate business is started with the intention of defrauding its customers or suppliers. This fraud is a long-firm fraud if the business has developed a good reputation and credit history or a short-term fraud when the apparent business has only been in operation for a few months.

Causes of Corporate Fraud

1. Lack of clear moral direction from senior management: Leadership as it is known comes from the top. If the senior management indulge themselves in behavior that are 'semi corrupt' in addition to a demanding target; there will be more temptation to manipulate results, such as year-end sales figures, to reach that target.

4. Greed: Good old-fashioned human nature intervenes when an individual, or group of individuals see an opportunity to make quick money. For example, this can be seen in those cases where people 'adjust' their expense claims upwards.

Methods for Detecting Corporate Fraud

1. Fraud Detection by Tip Lines: Tip line is by far the most common method of initial fraud detection and it is one of the most effective ways to detect fraud in organizations. It is desirable that these tips go directly to an organization's Internal Auditor, Inspector General, Legal department, or

others in the organization will follow.

2. Non independent internal audit department: If an organization's internal audit department is not independent, that is, where it does not report directly to independent audit committee. When there are signals that a fraud is occurring, they will more likely be ignored.

3. Excessively generous performance bonus payments: when bonus is very generous in even to outside Legal Counsel so they can be independently investigated. Also, for tip lines to be very effective, organizations should promote them and incorporate them into employee training.

2. Fraud detection by external auditors: Auditors of financial statement are to conduct their audits in such a manner to obtain reasonable assurance that financial statements are free from material misstatement, either caused by fraud or error. As a result, in some cases, especially those with large

losses, an organization's external auditors may detect fraud.

3. **Fraud detection by internal auditors:** Majorly, internal auditor is concerned with all fraud rather than just the fraud that affects the financial statements. Consequently, an internal auditor will likely uncover some frauds as a routine part of internal auditing work. Further, an internal auditor plays a key role in developing a system of fraud indicators, so that activities that are suspicious are flagged and investigated. Finally, internal auditors may be concerned with violations of the organization's policies and procedures even when they do not involve fraud.

4. **Fraud detection by accident:** This is also known as passive fraud detection and it refers to cases in which the organization discovers the fraud by accident, confession, or unsolicited notification by another party.

Fraudsters most of the time do not cover their tracks adequately. Consequently, efficient organizations will train their employees to spot and report irregularities.

Prevention of Corporate Fraud

1. Know Your Employees and Partners

a) ***Employee Behaviours:*** An employee who for one reason or another has not missed a day of work might be considered a dedicated employee, but they might also have something to hide. When an employee never goes on vacation, never calls in sick, never goes for lunch and always works overtime. Such employee may worry that someone will detect their fraud while away from the office. It is important to monitor vacation balances, mandate days off and even rotating employees to other jobs in the department can assist in preventing (or exposing) corporate fraud.

b) ***Know Your Vendors and Partners:*** As much as you need to know your employees, you also need to know your vendors and partners. Conduct regular audits of new vendors and have some form of defense before getting into any relationship requiring trust. This can be as simple as having a person's or company's physical address or trustworthy references.

c) ***Formalize Hiring:*** A formal hiring routine is a must-have for large corporations to prevent fraud. A formal process which consist of background checks and scrutiny of past jobs will reduce the opportunities of bringing a former fraudster into the company. Truly getting to know prospective employees can prevent corporate fraud and other potential issues down the line.

2. Create and Use A Reporting System

a) ***Look into Every Report:*** It is important to follow up on and check into every report that are received from whistleblowing hotline. If you have implemented various reporting procedures but fail to follow up when whistleblowers report their suspicions, it will all be for nothing. When whistleblowers do their part by reporting fraud, you should do yours by following up.

b) Raise Awareness: As it is known that whistleblower tips are responsible for discovering 40 per cent of occupational fraud. Raising awareness about a fraud reporting hotline will improve the likelihood that employees will use it. For dishonest employees who are considering committing fraud, ongoing reminders about reporting suspicions activities will act as a deterrent.

3. Implement Internal Controls

a) ***Segregate Duties:*** The general best practice is to ensure no one person has control over all parts of a financial transaction. Segregating accounting duties is a great method of internal control.

b) ***Limit Access:*** Transparency is important but giving employees unlimited access to financial information and physical assets is asking for trouble. Access to financial account data, inventory, assets and checks should only be given to appropriate people in the organization.

By Bolaji Ajayi
(ProvidusBank Ltd)

The Economics of Pandemics and the Role of Internal Audit Function:

How COVID-19 Calls for Fundamental Economic Shift

The most notable thing about the prevailing economic situations in countries around the world is that, the source of the economic woes is not directly an economic problem, but a medical crisis. This is a clear indication that, the various aspects of human society can exert tremendous influence over the economy, to the point of driving strong economic powers into landmark economic crisis. Before now, direct link between economics and politics have been established.

The synergy between politics and economics has been variously acknowledged and in fact, it is self-evident that economics and politics share an unbreakable bond. Much so to the extent that, elections in politically unstable countries or countries with likelihood of post-election violence and uncertainties, usually have impact on markets. Investors are often kin about how an election turns out, because it is universally acknowledged that politics shapes economics through policies, actions, and political affairs, persuasions or leaning of the leader or party in power. Yet, nothing has shaped the economics of Western powerful countries and Third World countries alike in recent memory, like COVID-19, which is a world-wide medical emergency unconnected to economics.

In perspective, there are three major ways COVID-19 is pushing fundamental economic shift. One is the shift in perception of what can influence economics, secondly is the need to embrace technological solutions and finally is the importance of strong institutions.

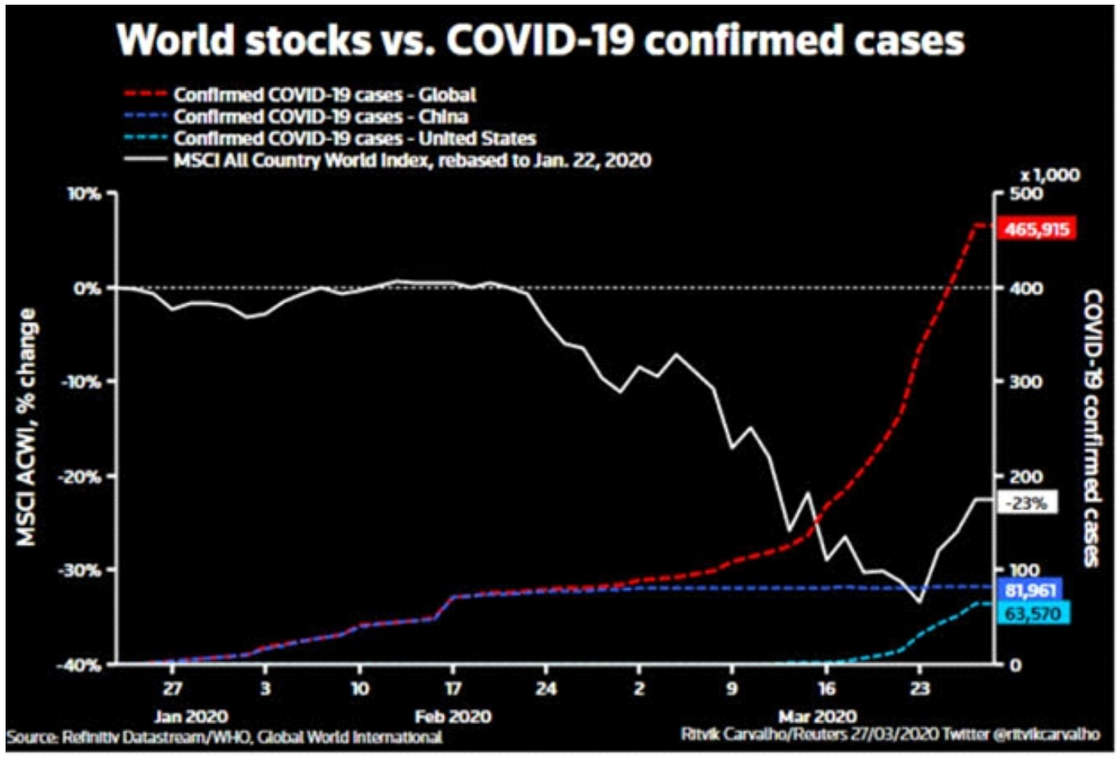
Each economic downturn has been distinctive and usually caused by economic problem. The 2007/2008 economic meltdown is the most recent in memory. And it was caused by financial crisis. It was so serious that Western economies felt the severity of the shock, where the United States under President Obama voted billions of dollars to America's big auto companies, to help the companies withstand the hard times so as to cushion the impact on the economy. COVID-19 is entirely different. It is a medical crisis that spilled over into economic problem due to initial response, trial and error that characterized governments' policy directives in an attempt to bring the deadly virus under control. Lockdowns has now proved to be far more expensive and out rightly impoverishing, especially for countries like Nigeria. Yet, there was and still is little humanity can do to curb the spread of the killer virus, without taking such extreme cautions.

Governments all over the world subscribe to one form of lockdown or another, thus, to a larger part, crippling the economy. Airlines were grounded as flights were banned; some international flights are still banned, costing billions in revenue to airlines and governments alike. Production was halted. Extraction was nearly halted, because those previously extracted were not sold, like the Nigeria's crude oil. Markets were shutdown. These sent unprecedented shock

waves to economies, forcing developed economies to retrieve to their savings. But for countries like Nigeria, it created fear and uncertainty.

The lesson is that moving forward, medical emergencies in form of pandemics and epidemics especially ones that are highly contagion, must be treated as both medical emergency and economic crisis put together. This therefore calls for solid investments in medical science in Nigeria. Medical science should be prioritized, with robust research and investments, as one of the safety nets for future medical crisis. Nigerian banks should fund and invest in medical research, as well as ensure efficient management of these medical investments, just in the same pattern like the banking sector.

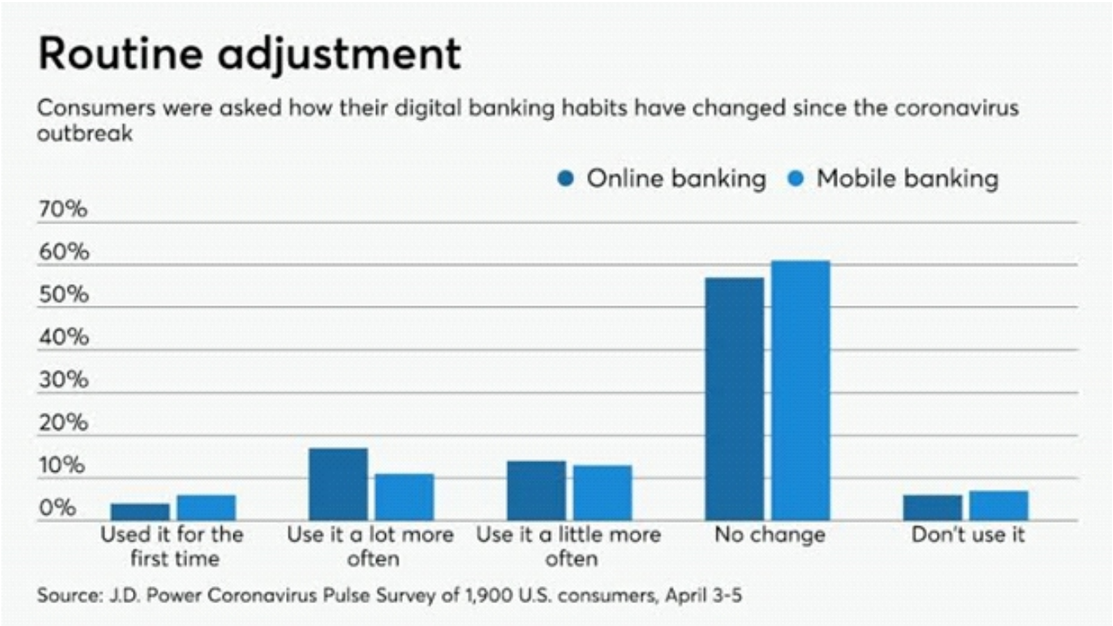
The pandemic also has a direct impact on the value of investments. World stock prices have crashed due to uncertainties; traders have panic-sold out of fears and investors' confidence is at an all-time low. The graph below shows the relationship between increase in confirmed covid-19 cases and its impact on world stocks.



Legend: MSCI = Morgan Stanley Capital International
ACWI = All Country World Index

The pandemic has shown that, there is no serious alternative to the use of technological solutions in times of emergencies like this. Bank services like internet banking and mobile banking helped in no small measure, to ease the burden of the lockdown on people across the world. Going forward, the world is gradually moving into an era of minimal human contacts and optimized virtual interactions. What this means for the banking sector is an imminent transition and in truth, the inevitable drastic cut down on staff strength in the banking sector. Automated systems have altogether become unavoidable. The below graph is the result of a survey that shows increased use of bank mobile applications and internet banking platform by U.S consumers.

Equally, the concept of working from home should now be more seriously considered by the Nigerian banking sector. Banks should now look for other ways to cut running costs, and we propose in two ways; embracing or creating secured technological solutions to the day to day banking needs of customers, so that customers may no



longer have a need to go to banks in person, and also adopting the concept of working from home, for most of her workers. With these, Nigerian banks will serve customers better, and will be ready for future emergencies with economic implications, as well as better manage running costs.

Importance of strong institutions cannot be fully explained in just one piece. As a matter of fact, the major difference between how developed Western countries reacted to COVID-19, is their strong institutions as against countries like Nigeria, where institutions barely exist. The impact of this is that in place of institutions, we have people, individuals who we use to replace the institutions. With that comes natural uncertainty and implicit limitations. On the part of government, the identities of governments' institutions must be deliberately preserved, and allowed to run without interference. For the banking sector, every department must develop its own identity and run as a system, that it can stand and run its full cause, with or without any form of human interference.

The banking sector as the most organized economic sector in Nigeria, should be able to set the pace and define what post COVID-19 holds for the country and the people of Nigeria.

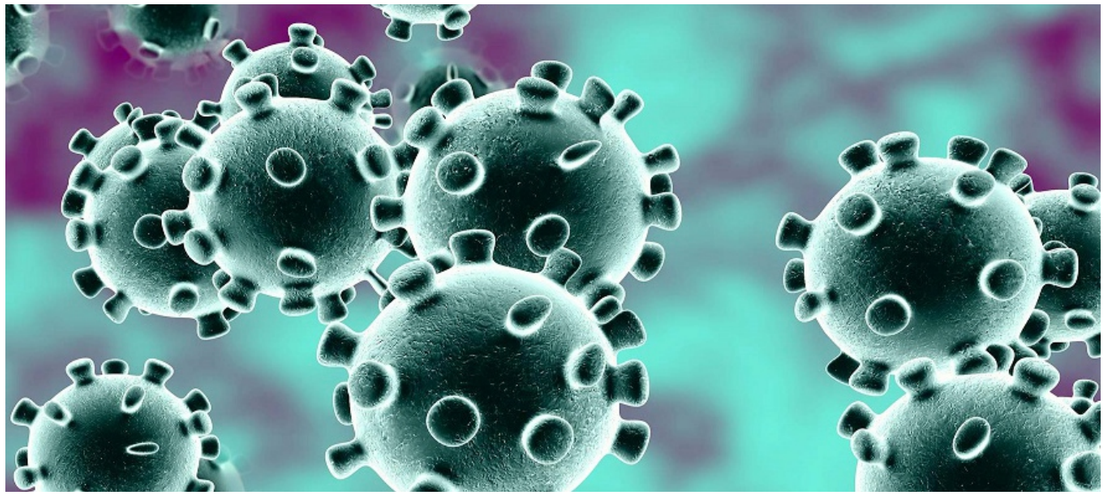
In these challenging times, **internal audit function** has both an obligation and an opportunity to help their companies manage the most critical risks COVID-19 has either created or magnified. The internal audit function can help their organizations to weigh risks and opportunities, as these ensure that informed decisions are reached by their organizations.

The guidelines below concerning risks, can help internal audit maximize its contribution to the COVID-19 response:

- Redirect your risk expertise to COVID-19 priorities.
  - ✶ Help stress-test operational risks and potential vulnerabilities in the light of COVID-19; then offer insights to help mitigate these risks.
  - ✶ Help confirm that the response team is rolling out and executing its actions appropriately, effectively, and swiftly.
- Evaluate the emerging risks of newer operating models and business practices and redirect your attention to the most time-sensitive risks.
- Understand COVID-19's impact on your industry and business. Assess existing and emerging COVID-19 related risks in key areas, such as these:
  - ✶ Crisis management and response should look at increased cybersecurity threats, greater network connectivity needs, and increased VPN or mobile device usage, as more employees work remotely.

- ✶ Workforce disruption may go beyond health risks, to possible impacts on productivity, collaboration and adherence to company policies, as employees who now work from home may face new stress.

- ✶ Operations and supply chains may face disruption, possible declines in quality or availability, and new third-party risks.



- ✶ Finance and liquidity challenges may arise from revenue shortfalls, debt servicing requirements and rising customer credit risk. This may require changing SOX processes and controls.

- ✶ Tax and trade is dealing with immigration issues, the implications of shifting business or suppliers to different jurisdictions, and the potential need to change the organizational structure.

- ✶ Strategy and brand may be affected by your response to the COVID-19 crisis, which may require changes in long-term plans, while defining your brand for years to come.

- **Internal Audit executives** should proactively communicate risk issues to management and audit committee:

  - ✶ Articulate the potential impact of COVID-19 on your business, risk assessment, and audit response.

  - ✶ Share emerging risks that you identify, to help the company manage or intentionally accept the risks. Also, share how you are altering your focus and approach to help address these risks.

  - ✶ Communicate how you are changing your audit plans. Be transparent about the limitations you face, but also use this opportunity to ask yourself if you could do more to adapt your plans, find innovative ways to execute or help in new areas.

  - ✶ Identify and explain the value of your proposed new projects or activities. Common examples of value include providing real-time feedback to management, mitigating potential for misconduct, and enabling regulatory compliance.

- The times are difficult, but internal audit's potential contribution in enormous: helping to provide trusted risk perspective during these months, when critical risks are both rising and changing quickly.

- In developing your response to this crisis, knowing the fluid environment requires you to continually reset priorities, keep your eye on medium and long term future. At some point, a new business-as-usual environment will emerge. If internal audit provides guidance now, while also preparing for that future, it will emerge as a stronger team, providing even greater value to the department and the business.

Victor Okpara and Victoria Morah (Access Bank)

Responding to and Protecting Against Ransomware

There have been many recent successful ransomware attacks, and there is frustration that in today's cybersociety, information security safeguards and best practices are not being followed by local governments, financial services, law enforcement, academia, government agencies, healthcare organizations and businesses and commercial enterprises. The cyberattack threat vector has become a lot more serious than a simple denial-of-service attack to the network infrastructure (i.e., online business) or to a website that offers services, a means of acquiring goods or information. A ransomware attack is now a major event that has long-lasting effects and can jeopardize government services, the existence of commercial enterprises and, as we have seen recently, even our schools.

This attack vector has become a loud bell that rings over and over as a reminder that information security must be implemented effectively, otherwise an organization can lose money (because of gaps in business and services) or potentially the entire business. The people in charge of protecting against cyberattacks can also lose their jobs.

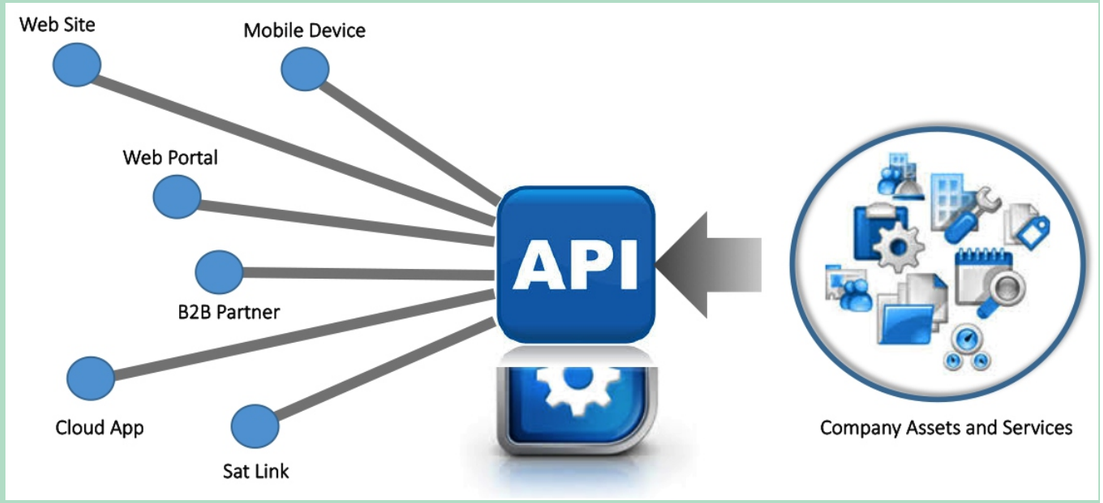
Cyber insurance is an option, but it cannot always be used if attacks occur over and over again. Paying the ransom can be a waste of money if lessons are not learned and new safeguards are not put in place. Attackers may come back because of a previous success. Although detection, response and recovery are important, they should only be used when prevention fails.

School systems appear to be a fruitful target for ransomware. In 2019 there were over 1,000 recorded attacks on US schools alone, and we have seen renewed attacks in the new school year. Part of the reason has been that the schools were paying the ransom, thereby painting a target on themselves as a source of income. To add wood to the fire, some obtained cyber insurance and made themselves a definite source of revenue for the attackers. One way of going forward is for the schools to meet and compare notes (via lessons learned), and exchange ideas and best practices. Endpoints (i.e., laptops, desktops, etc.) should be protected by using a common baseline that can be quickly reinstalled. Enterprise system software could be common (but isolated) in school districts to provide a network of recovery avenues. Data should be backed up locally and in a cloud data storage service, the cost of which could be shared by participating schools. These are just some ideas, and I encourage other industries to make an effort to join together and establish a more secure digital environment.

There are five areas to focus on when working to make an organization more secure: prevention techniques as they relate to network architecture, configuration safeguards and computer operations; protection best practices; advance detection techniques, tools and resources that can be used to alert the response team; response options; and recovery.

Organizations need to be aware of the various aspects of ransomware, know how to fortify their enterprises and know how to plan for and respond to cyber-attacks.

Culled from: isaca.org



Choosing the Ideal API with Security in Mind

Application programming interfaces, or APIs for short, provide very secure and standardized ways for applications to work together and deliver greater information and functionality for end users. But with so many different APIs available, choosing the right one can be a challenge of epic proportions. Do you know where to begin?

The Importance of Security

The API marketplace continues to grow by the day. But not all APIs are created equal. For any specific challenge, task, or solution, you'll find an array of competing APIs. And while they may appear similar on the surface, they almost certainly feature significant differences "under the hood." And out of all the different elements to consider, security is arguably the most important of all.

A weak API can provide a massive point of entry for hackers into your business. Because of the way in which businesses use APIs to connect different services and transfer data between multiple points, a broken or exposed API can lead to a serious data breach.

Different API technology uses different API security methodologies. The two most common are:

- REST API Security. This security format uses HTTP and supports Transport Layer Security (TLS) encryption. TLS helps to maintain a private internet connection and continually verifies that all data sent between two systems is encrypted and unmodified.
- SOAP API Security. With a SOAP API, there are built-in protocols known as Web Services Security (WS Security). Under these protocols, there's a defined set of rules that are guided by principles of confidentiality and authentication. They use a combination of XML signatures, XML encryption and SAML tokens to authenticate and authorize users.

As you evaluate different APIs for your next project, take security into account. This is by far the most important element to consider. Everything else stems from a strong and comprehensive security foundation.

In addition to API security, you'll also want to consider the following six factors:

1. Documentation

One of the first steps is to check the documentation of all APIs that you're considering. The documentation should be clear, transparent and easy to understand. If the language is too technical or complex, this could mean any number of things – none of which are positive. For example, it may indicate that the API developers don't fully understand it themselves. Or it could mean they're hiding something (like a lack of functionality) by using what they deem to be impressive language.

Clear documentation should tell you precisely how to implement the API right away. Clarity bodes well for successful integration when the time comes.

2. Data Formats

After analyzing the documentation, take some time to consider the data formats. While XML has traditionally been the dominant format, other options like JavaScript-based JSON are becoming extremely popular.

It's also important to consider the source of the data (particularly with APIs that deliver real-time information). Take a stock API as an example. Inaccuracies in the data can lead to thousands of dollars in lost earnings for the users of an investment website or application. A failure on your part to vet the source of data could come back to bite you.

3. Totality of Features

You'll discover that there's no such thing as a perfect API. However, you should do your best to find APIs that offer as many of the features you need to be successful. (This requires you to know what you're looking for, so that you can make a qualified selection.)

4. Interface

From a very practical perspective, consider the API interface. You can learn more about this in the documentation. Study the method and parameter names to get an idea of naming conventions and other related elements.

You'll find that many modern APIs try to get cute and require custom headers and HTTP verbs. This might be fine with you, but it's something to consider. (Again, the more you know ahead of time, the more informed your decision will be.)

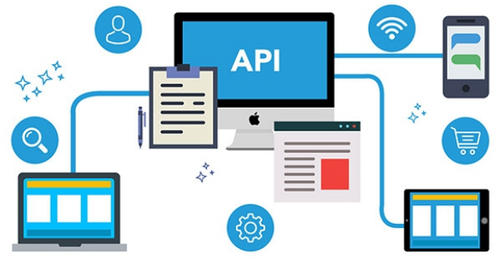
5. Limits and Interaction

API providers set limits to avoid abuses by customers. However, these limits can potentially be flexible depending on the type of customer. Consider the rules regarding limits and interaction so that you understand how they may impact your functionality and scalability moving forward.

6. Community and Support

Even the best API integration will prove troublesome at times. It's never going to be rainbows and butterflies 100 percent of the time. The question is, when issues arise, is there a community and/or support team ready to help you overcome your unique challenges?

Whether it's timeouts, broken requests, or issues with API limits, support forums, chat features, and smooth customer service will prove extremely helpful.



Choosing the Right API

It's important to recognize that there might not be a "right" answer, in terms of which API is ideal for your next project. There could be multiple options. The goal is to filter out the ones that aren't a good fit so that you can narrow your search to the ones that are practical selections. From there, you can compare and contrast – making sure to compare apples to apples – and move forward with the one that you believe best aligns with and supports your project.

Even if you've done a thorough job of researching and vetting APIs, it's always necessary to conduct API testing to ensure compatibility, eliminate errors and promote optimum functionality. You're almost certain to encounter issues. The critical step is how you handle these issues so that you can keep the project moving forward.

Culled from: isaca.org

The Practical Aspect: Working From Home Reassessing Risk and Opportunities

The technology for remote communication through distributed networks existed in rudimentary form during the 1990s, but sophisticated applications for distance learning, video teleconferencing, online chat and telemedicine developed modest acceptance in the early 21st century. Expanded bandwidth and network development partially explain this trajectory, but several other factors—particularly, human factors—must align well for the adoption of new technology.

Habits and routines sometimes require an exogenous nudge to initiate change. The coronavirus pandemic prompted changes in behavior that have contributed to the ubiquity of telecommuting and remote conferencing. Survival depended on keeping distance and limiting face-to-face interaction. For many workers, technology became a lifeline to salvage the disrupted routines of business and society following lockdowns intended to slow the spread of the virus. Comparing today's pandemic to the influenza pandemic of 1918, one could surmise that the ability to resume essential activities—even with an acceptable sacrifice of effectiveness—provides a distinct advantage that allowed toleration of public health policies without even greater disruption of the economy.

For a change to occur, it seems one needs to be "in a pinch." Even when the technology is rough around the edges and the end user seems unprepared or unwilling, pressing needs produce efforts to accommodate new technology. Online teaching is better than no teaching; committee meetings on Zoom or Teams are better than no meetings (although we all prefer fewer, more impactful meetings). Everyone had to invest new energy to adapt to new technology, and this investment appears to be paying off. Not everyone has developed the required proficiency for online work and some even hate it, but the technology has allowed us to accomplish more today than in the past.

But our journey into the future continues, leaving us with questions. How much of this virtual world will remain part of our lives after the pandemic has passed? Will the technological shift leave lasting changes in the habits and practices of business and society? For auditors, navigating through this future requires an examination of the changing risk environment and our ability to identify and mitigate these risk areas. We should examine these questions further.

How Did We Fare?

Balancing healthcare benefits from lockdowns with the negative impact on the economy has been a challenge around the globe. While Denmark locked down the economy, Sweden did not. The outcomes are quite different in each country and it is too soon to say which approach proved superior. South Korea avoided the lockdown, but it tested people extensively and followed the test results by isolating infected individuals and contact tracing others who were likely at risk. Such measures may be effective, but they may not be compatible with privacy expectations (and laws) in other countries.

Variations in these approaches permit the study and assessment of outcomes, with possible benefits to future efforts to address pandemic conditions. Preliminary information suggests that targeted measures aligned to the risk of each community could have fared better than a blanket shutdown . Problems of overreach from regional edicts tend to disparately impact some communities with lower demographic risk. The US federal system mitigates those risk areas to some extent, but variations within the US states remain: Rural Virginia, for example, differs from areas within the state bordering the District of Columbia (DC).

Workplaces experienced differential impacts based on "essential" and "nonessential" designations by governments. For those with compatible work requirements, remote officing increased dramatically compared to pre-COVID times. These workers faced new challenges, including technology issues, increased (and perhaps different types of) distractions, reduced team cohesion and difficulties with communication. But offsetting benefits were also realized from avoiding the time and costs of commuting, not to mention eating meals at home and reduced wardrobe costs.

mid-semester transition to remote learning. The amount of effort was overwhelming for teachers and students; even parents had to go through the frustrations of taking on new ways of doing things. Despite all these efforts, preliminary research on school-age students suggests only 70 percent of normal school year reading skills learning and approximately half of math learning was achieved. This presents a potentially lasting detrimental impact on the educational system, which will have to adapt to lower achievement in future years.

> "GETTING BACK TO NORMAL MAY ENTAIL A NEW NORMAL"

From Crunch Time to Calm

Getting back to normal may entail a new normal. The benefits of remote officing may attract some workers who prefer to continue this arrangement. We Company, a space renting firm, may find lesser demand for its services from organizations whose workers choose to remain at home. But other remote workers may find temporary office space attractive to provide options for in-person meetings or to get away from the distractions of the home environment. The net effect of these preferences is difficult to gauge, as tremendous variations exist across the world.

Other workers did not have the option of performing remotely but instead had to adapt to the restricted environment. Retail grocers focused on maintaining customer loyalty while assisting employees with staying healthy. Curbside pickup, home delivery of online orders and special shopping hours for seniors were among the steps taken by stores to adjust to the new conditions. Restaurants and bars offered takeout menus, adapting to online orders and pick-up or delivery options. The privately held office supply distributor W.B. Mason, recognizing that people away from the office still need supplies wherever they work, began delivering products such as coffee, paper towels and bathroom cleaners directly to consumers at their homes.

Most schools and universities were not prepared for a

Workers residing in low-cost housing environments are presented with economical alternatives to acquire and develop home-office space, while high-rent locales present greater pressure from multipurpose use of smaller living spaces. Employers will also be looking at their own space needs—if more of their workers prefer remote officing, dedicated offices may be inefficient. Meeting spaces and temporary workspaces may become the new normal in commercial real estate configurations. Demands for convenient access by workers may also change the location of these spaces, shifting them away from current headquarters and closer to where most employees are living.

The ability to work remotely may create a new demographic division within the workforce. Rather than white-collar and blue-collar labor, we may see a division based on those who work in the IT space

(haves) and those who need to be physically present at work to add value (have nots). Workers in manufacturing, construction and other production work will continue to commute to their workspaces, along with many intermediaries dealing with moving material goods. However, the breakdown of labor needs within this space may shift. Personal customer contacts may become more limited if organizations shift to remote delivery instead of in-person contact, affecting the demand for fulfillment staff and telephonic or Internet contact instead of cashiers. As technology-leveraged skill sets become more demanding, it is possible that more jobs might be lost for those who are already in the have-nots category, while the haves gain even greater importance.

Although it may be too early to judge, the expectation is that the share of remote work in the total workspace will increase over time. Facebook Chief Executive Officer (CEO) Mark Zuckerberg asserts that in the long run, the company will permanently reconfigure its operations so that about half of its employees work from home (WFH). Twitter has announced that most of its employees will be allowed to keep working from home even after the pandemic passes. Unfortunately, job losses resulting from the pandemic have fallen disproportionately on those workers who cannot perform their work from home. Empty offices do not need cleaning crews; those lunching at home do not generate work for restaurant workers; and even Uber drivers may see fewer customers as people choose to stay close to their home bases.

Lasting Changes That Stick

While more organizations and workers are embracing the benefits of remote work during the pandemic, there are indications that the long-term value of WFH may not hold in all cases. A report on LinkedIn indicates that some experts believe extended remote work threatens a "decay in culture" as out-of-office workers face increased isolation, distractions and blurred lines between work and home life. The report also asserts that short-term success of WFH amid the pandemic has largely been rooted in established relationships, which are harder to build and maintain online. People lose touch when they are not personally present with some degree of frequency, and existing relationships may end, for example, due to retirement. It has been said that innovation and creativity can be built only with good rapport, which stems from personal contact, not a remote connection. While these are not proven assertions, the possibilities of human factors derailing a technological solution deserve consideration.

> **"AS TECHNOLOGY-LEVERAGED SKILL SETS BECOME MORE DEMANDING, IT IS POSSIBLE THAT MORE JOBS MIGHT BE LOST"**

Economic benefits from working at home can be expected to continue beyond the pandemic, when lockdowns have been lifted. Savings measured by avoided costs for commuting, reduced office space, and reduced friction in remote conferencing with others will tend to incentivize business leaders and their employees to keep the gains they managed to achieve while fighting the virus. If work role expectations stabilize, some employees may even consider moving to a more remote residential area, reducing congestion and improving quality of life. At a macro level, environmental protection and energy savings could show visible improvements.

But the shifts will have proven detrimental to some workers and in some environments. For example, educators involved in kindergarten, elementary, or middle school, where face-to-face interaction is extremely important for the development of young people, are likely to find the WFH option to be unsustainable. The in-school vs. out-of-school options do not appear to present comparable achievement of the end goal of a student's personal development. Health counselors may also find that remote sessions fail to deliver the same progress with their patients. When you cannot achieve your goals, preferences for comfort and convenience are insufficient to sustain remote work practices.

Changing Risk Landscape and the Auditor

Fellow *ISACA® Journal* columnist Steven J. Ross aptly puts it, "(C)hanging the definition of work necessitates a corresponding redefinition of security over the information with which we work."

> **"BECAUSE THOSE WHO WFH ARE MOSTLY KNOWLEDGE WORKERS, ISSUES OF DATA PROTECTION, SYSTEMS SECURITY, INCIDENT MANAGEMENT AND PRIVACY REQUIRE CAREFUL RECONSIDERATION."**

The growing acceptance of WFH qualifies as the redefinition of work, bringing along new challenges of information security. Because those who WFH are mostly knowledge workers, issues of data protection, systems security, incident management and privacy require careful reconsideration. Risk mitigation in the context of WFH requires a thorough and careful exercise in risk assessment; without it, the organization and its stakeholders could be vulnerable to new or heightened risk.

The single most important source of new or elevated risk is that remote work extends the boundaries of the formal information system of the entity. An elevated level of remote engagement calls attention to a comparatively porous system having more windows and gates than the wall protecting the traditional business edifice. Diverse communication carriers, varied end-user hardware and generous authentication protocols all lead to greater risk from increasing the porousness of the system.

Disaffected, disengaged or depressed employees also present organizational risk. Are those working remotely maintaining positive mental attitudes about their work and their employer? Organizations may need to invest additional resources to help affected

employees with their needs. Current tax and economic conditions present challenges for employee self-help when it comes to technology investment, which employees must make with after-tax dollars. Enhanced employer investments to equip employees to function effectively and efficiently in a WFH environment, including access to technical support, may be required. Providing regular opportunities for feedback and finding new ways to measure the effectiveness of remote work may be needed to avoid productivity losses and potential risk scenarios from careless or thoughtless behavior. Efforts to provide regular opportunities for interaction and avenues for accessing assistance may be more important than ever.

Remote work arrangements can present new tax consequences for both enterprises and employees, presenting compliance and fiscal demands that had previously not been considered. Activities by employees in remote locations may also trigger new regulatory responsibilities, affecting not only those employees, but the entire business enterprise. Where will firms get the resources to devote to these new compliance efforts? Perhaps some resources will come from travel budgets, which have been widely slashed after the pandemic.

Organizations with staff working remotely should consider their policies governing that work. Such policies provide anchors to identify and develop measures to mitigate related risk. An ISACA® blog post lists specific areas organizations should address:

- Switch to cloud-based storage.
- Require regular password changes.
- Limit access.
- Provide for remote support systems.
- Keep software and programs up to date.

Other factors to consider might include responsibilities for ownership, access, maintenance, and acquisition of hardware and software tools needed to function effectively in a remote role. For such a significant development in the life of an organization's information systems, a disciplined approach to meeting these requirements, such as resources (including training), applications or procedures, and documentation, will be necessary to produce consistent and coherent standards that permit management to measure and assess employee and organizational progress.

The COBIT® framework naturally suits in this case, although other frameworks may also be effective in achieving the goal of systematically incorporating control risk factors of WFH. The application of COBIT to remote work was well illustrated in a recent article. The article emphasizes these areas of the COBIT framework:

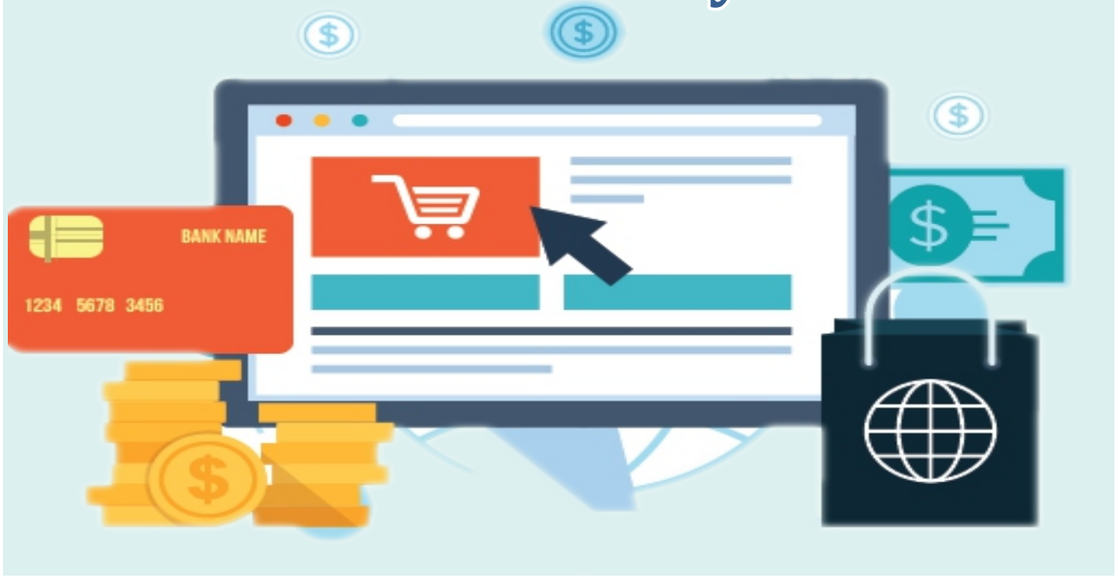
- Manage critical assets.
- Manage network and connectivity security.
- Manage endpoint security.
- Manage business resilience.

Whether one likes it or hates it, the new normal that incorporates WFH in a significant way is here. It is important for every organization to develop an impact analysis for WFH and consider putting in place a plan to suitably address its impact.

> **"IT IS IMPORTANT FOR EVERY ORGANIZATION TO DEVELOP AN IMPACT ANALYSIS FOR WFH AND CONSIDER PUTTING IN PLACE A PLAN TO SUITABLY ADDRESS ITS IMPACT."**

Culled from: isaca.org

Where Did All the Payments Go?



Nearly two decades after the Enron scandal, another big company is embroiled in a scandal over irregular accounting.

More than $2 billion in missing funds led to the resignation and arrest of Wirecard's CEO recently. The scandal broke when the company's external auditors couldn't find the money in trust accounts and refused to sign off on the digital payment company's financial statements. The missing amount equates to one-fourth of Wirecard's assets and set off a global search for the funds.

German authorities suspect that former CEO Markus Braun used fake transactions to inflate Wirecard's revenues and balance sheet. The company says the missing money may never have existed and has withdrawn preliminary results for 2019 and the first quarter of 2020. At the time of Braun's resignation, he said the company had been the victim of a massive fraud. Wirecard has since fired its chief operating officer.

Lessons Learned

This story about Wirecard's financial scandal may bring make memories for internal auditors. The infamous 2001 case of Enron and its CEO, found guilty of accounting fraud, became a major driver of the U.S. Sarbanes-Oxley Act of 2002 financial regulatory reform.

Germany's finance minister summed up the essence of the Wirecard scandal, saying, "Critical questions arise over the supervision of the company, especially with regards to accounting and balance sheet control. Auditors and supervisory bodies do not seem to have been effective here." So what can internal auditors learn from this case?

The Association of Certified Fraud Examiners defines *accounting fraud* as "deception or misrepresentation that an individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual or to the entity or some other party." Financial statement fraud can take multiple forms, including:

- Overstating revenues through outright falsifications, manipulations such as recording future expected sales, or irregular accounting practices. An example is when a company understates revenues in one accounting period and maintains them as a reserve for future periods with worse performances to reduce the appearance of volatility.
- Inflating an asset's net worth by knowingly failing to apply an appropriate depreciation schedule.
- Hiding obligations and liabilities from a company's balance sheet.
- Incorrectly disclosing related-party transactions and structured finance deals.

Several actions are key to reducing the threat of financial statement fraud.

Strengthen and rigorously implement internal controls over balance sheet account reconciliation. Efforts to sustain a timely and accurate account reconciliation process should include:

- A strong management focus.
- Sufficient understanding of the process.
- Written policies and procedures.
- Adequate employee training.

Identifying and addressing any weaknesses in this process can help auditors and companies detect and correct errors before they file their reports. Organizations need to reconcile all high- and medium-risk accounts that could contain a significant or material misstatement and make all necessary adjustments to the general ledger timely. Because account reconciliations are so important, organizations also should adopt a continuous improvement process aimed at reconciling all accounts before the post-closing adjustment review process.

Pay close attention to the work of external auditors. That scrutiny should include the audit committee asking questions of the external auditor and regularly reviewing the renewal process for selecting the auditor. The company also should be listening to its investors' concerns and complaints.

The focus in the Wirecard case has turned to its external auditors, who reportedly failed to report the company's unorthodox financial arrangements in the past. Wirecard's missing $2 billion allegedly involved an unconventional measure in which the company used third-party partners to process payments in countries where it wasn't licensed. Those businesses deposited revenue in trust accounts rather than pay it straight to the company. Wirecard explained that the money was kept that way to manage risk, saying it could be saved to provide refunds or chargebacks if needed.

External auditors need to be vigilant in self-regulating the quality of their work. The external auditors allegedly did not confirm that Singapore's Banking Corp. held large amounts of cash on Wirecard's behalf. Instead, they relied on documents and screenshots provided by a third-party trustee and Wirecard, itself.

Culled from: iia.org

5 Healthy Habits That Can Help Reduce The Risk Of Having Liver Disease

Every day we hear smoking and drinking can affect the liver. While this is true, there are other habits that can be emulated or avoided to have a healthy liver. Below are some:

Coffee

There is extensive research on the benefits of coffee and liver disease. According to Rockford Yapp, MD, a member of the board of directors for the American Liver Foundation:

Several studies have shown that coffee helps to slow or prevent liver cancer. It also has been shown in several studies to help prevent fibrosis, which is a scar tissue that can be so damaging to the liver. Some research also shows that patients with hepatitis C, a common liver infection, who drink one to four cups of coffee per day slow down the virus.

The specific reason coffee helps is unclear, and Dr. Yapp notes that some people should avoid coffee because of other health conditions such as high blood pressure.

Mediterranean diet

A Mediterranean diet is filled with lots of healthy fats like avocados, lower carbs, and healthy proteins, especially fish. Although fats such as olive oil, walnuts, and avocados help the liver perform well, maintaining an overall healthy weight by ingesting an appropriate number of calories will benefit your liver more. A healthy and balanced diet is good for your liver because it processes most of the foods we eat.

Limit alcohol intake

When it comes to liver disease, the most obvious and detrimental risk factor is alcohol intake. Dr. Lucero advises drinking in moderation, meaning no more than the daily recommended amounts of one drink per day for women or two drinks per day for men. Women and people with a family history of alcohol-related problems are at a higher risk for liver disease, so it is essential to honestly discuss your current and past alcohol intake with your doctor.

Antioxidant-rich foods

Antioxidants from different foods likely benefit the liver by replacing the natural antioxidants the liver uses to detoxify the foods, chemicals, and other substances that people are exposed to. Broccoli, spinach, carrots and potatoes, artichokes, cabbage, asparagus, avocados, beetroot, radish, lettuce, sweet potatoes, squash, pumpkin, collard greens, and kale are rich in antioxidants.

Avoid supplements

Liver toxicity from supplements and alternative medicines is common. Often, the safety and effectiveness of supplements are not evaluated before they're marketed. So it is advisable to talk to your doctor before you use anything before it causes trouble for your liver.

The medical information provided in this article is provided as an information resource only. This information does not create any patient-physician relationship and should not be used as a substitute for professional diagnosis and treatment.

Culled from: guardian.ng

The human body needs water daily as it loses water every day even when the body hasn't done anything stressful. The amount of water lost by the body varies depending on your activity levels and climatic conditions.

One good fact however is that the body is tuned to tell you whether you need to replenish your water reservoir. The easiest way to judge if your body needs water is how thirsty you are.

Water is needed for good health and there is no replacement for water. Most studies show that about two in three people are dehydrated and need to drink more water. It is necessary to understand the subtle signals that your body sends, indicating you need to drink more water.

Hunger even though you've recently eaten

When the body is dehydrated, it tends to think it needs food. Eating food at this period only creates more work for the body, whereas drinking water purifies body organs and supplies it with the fuel it needs to go through the other processes a body goes through.

Joint aches

The human cartilage and spinal discs are made up of about 80% water. This is an absolute necessity to keep the bones from grinding against each other with every step taken. By keeping your body hydrated, you ensure that your joints can absorb the shock of sudden movements, such as running, jumping, or falling awkwardly.

Dull, dry skin and/or definite wrinkles

As the body's largest organ, the skin needs to stay hydrated. Dry skin is one of the earliest signs of full-on dehydration, which can lead to much larger problems. A lack of water means a lack of sweat, which leads to a body's inability to wash away excess dirt and oil accumulated throughout the day. To avoid breakouts, drinking more water is advised.

The colour of your urine is an important marker. Dark urine indicates a need to drink more water

In addition to thirst, it is also important to look at the colour of your urine. You should be drinking enough water to turn your urine a light-colored yellow. Dark-colored urine is a sign that your kidneys are retaining fluids in order to maintain your bodily functions, which includes detoxification. As a result, your urine will seem highly concentrated and dark in color.

Infrequent urination; and/or constipation

You may also urinate less frequently, for the same reason stated above. Since the thirst mechanism tends to become less efficient with age, older adults need to pay more careful attention to the color of their urine to ensure adequate water intake. The incidence of urination can also be used to judge your water intake. A healthy person urinates on average about seven or eight times a day. If your urine is limited or if you haven't urinated in several hours, that too is an indication that you're not drinking enough fluids.

Exhaustion and/or mood swings

When the body is dehydrated it "borrows" water from your blood. A lack of properly hydrated blood leads to a lack of oxygen being brought throughout the body. A lack of oxygen leads to exhaustion, sleepiness and mood swings.

Conclusion

There's no doubt that you need water for good health. A simple effort of substituting all the sweetened, bottled beverages you indulge in with regular pure water can go a long way towards improving your health. It works wonders to help you manage your weight too. The amount of water your body needs, however, is something you need to fine-tune based on your circumstances. It is necessary to understand the body requirements and the obvious signals that it's high time to replenish your fluids.

Culled from: guardian.ng

Pandemic-Driven Remote Working and Risk Management Strategies

One of the most visible results of the 2020 COVID-19 pandemic has been the mainstream transition from traditional office-based work to remote work-at-home arrangements. Government officials worldwide mandated that nonessential employees stay home. Enterprise leaders followed the government mandates by directing employees to isolate at home to keep the virus from spreading throughout employee populations. A primary lesson from that experience is that employees and the critical functions they perform can be protected and maintained by initiating secure remote teleworking operations. Unfortunately, as **figure 1** depicts, remote working introduces new IT-related threats that require unique threat mitigation countermeasures.

Figure 1—Remote Work Threats and Countermeasures

Threat	Countermeasures
Theft of teleworking endpoints and devices	Work-from-home policy, endpoint encryption, identity and access management (IAM) and, preferably, multifactor authentication (MFA), endpoint management technology (e.g., mobile device management [MDM], mobile application management [MAM])
Unauthorized monitoring, collection or modification of traffic passing over teleworking networks	Work-from-home policy, hardened virtual private network (VPN) infrastructure, enhanced logging of VPN infrastructure, IAM and preferably MFA, encryption, backup and restore
Telecommuting-specific increases in endpoint malware infection	Work-from-home policy, antimalware services, endpoint and remote access system vulnerability management, network access control (NAC), application security, security information and event management (SIEM)
Pandemic-specific phishing attacks	Employee training, email antiphishing services, SIEM
Pandemic-specific malicious website infections	Employee training, web content filtering, SIEM
Remote teleworker outages and service request management	Enhanced technical support, hardened high-availability remote access systems and VPNs
Theft or destruction of enterprise intellectual property by temporarily furloughed or laid-off employees	IAM and preferably MFA, MDM, MAM, SIEM, cloud access security broker (CASB)

These countermeasures can be organized under five categories:

1. Employee security
2. Endpoint security
3. Network security
4. Security monitoring
5. Security reporting

Each of these categories contains security areas that, if ignored, could result in serious risk both during the transition and longer term operational approach to predominantly working remotely. Enterprise leaders should evaluate each one for applicability to their unique environments.

Employee Security

Employee security is one of the five categories that require unique countermeasures. Employees are often the weakest link in enterprise security because they have countless opportunities to make decisions that could lead to a security breach. Employee security focal points include teleworking policy, training, antiphishing, and identity and access management (IAM):

- **Teleworking policy** A solid work-from-home policy that accounts for pandemic-related threats is an essential starting point for maintaining safe and continuous business and IT operations. The work-from-home policy should specify what

enterprise leaders expect from employees who are working remotely. It should emphasize cybersecurity considerations, such as safe remote computing, acceptable use and sanctioned applications. Acceptable use is a general concept that may have been in effect before the pandemic, so enterprises should create an exception to policy and procedure to enable users with special-case scenarios to perform functions that would otherwise be restricted as unacceptable. The policy should provide information such as who to contact in the case of lost or stolen devices, phishing, or the observation of suspicious computing events. The teleworking policy should also intersect with enterprise training and provide a list of mandatory training courses aimed at mitigating the threats specific to telecommuting. Critical to a safe remote work environment is the virtual private network (VPN) that provides connectivity from home offices to enterprise systems. Remote workers should have access to all the how-to information they need to connect remotely over the VPN.

- **Employee training**: Training managers should consider creating specialized training content to empower employees with the knowledge to manage the unique threats they will face while teleworking. Training should include policies governing work-from-home computing rules and tutorials that prepare end users for potential threats, such as laptop thieves or pandemic-specific phishing emails.

- **Email antiphishing services:** Enterprise leaders should prepare for new pandemic-specific phishing tactics. For example, hackers may send malicious emails to employees under the guise of pandemic-related subjects to make them seem more relevant and to trigger an emotional impulse to click on the malicious link or file attachment. The enterprise should implement or fine-tune antiphishing platforms to account for messages with pandemic signatures coming from external sources.

- **IAM:** IAM teams need to both grant new access and remove existing access based on unique pandemic-specific considerations. Onboarding and offboarding employees remotely will require IAM actions to create, temporarily disable and delete employee IAM credentials and underlying authorizations. Multifactor authentication (MFA) is also imperative, particularly for anyone connecting from remote locations to perform elevated administrator and high-risk functions. Certain industries and job functions that involve sensitive data should ensure that all systems that store, process and transmit sensitive data are hardened through enhanced IAM security measures such as centralized log correlation, monitoring and retention of user login attempts and access. MFA is wise for users performing job functions involving high-risk sensitive data.

"BY DIRECTING THE ENCRYPTION OF ENDPOINT HARD DRIVES AND SENSITIVE FILES, ENTERPRISE LEADERS CAN BE ASSURED TH AT LAPTOP AND MOBILE DEVICE THIEVES WILL NOT BE ABLE TO ACCESS DATA."

Endpoint Security

The endpoint security category is the second of five categories that require unique countermeasures. Weaknesses in endpoint and device security can provide an abundance of opportunities for threat actors to gain unauthorized access and damage the integrity and availability of data. Endpoint and device security focus areas include endpoint encryption, endpoint management services, antivirus services, endpoint vulnerability and patch management, backup and restore, web content filtering, application

security, and cloud access security broker (CASB):

- **Endpoint encryption:** With so many employees working remotely, many more laptops will be used outside the office in remote locations without physical security protection. By directing the encryption of endpoint hard drives and sensitive files, enterprise leaders can be assured that laptop and mobile device thieves will not be able to access data.

- **Endpoint management services:** Managing laptops and devices remotely over the Internet is more important when the majority of employees are teleworking. For example, existing patching platforms may double as mobile device management (MDM) platforms. Windows System Center Configuration Manager (SCCM) and Apple Jamf have remote wiping and locking capabilities that IT and security leaders can use to maintain the confidentiality of data, intellectual property and trade secrets. These platforms can also be used to partition and ultimately wipe, if necessary, enterprise data without impacting personal data on personal mobile devices if the enterprise has a bring-your-own-device (BYOD) program.

- **Antivirus services:** Next-generation antivirus services inhibit the execution of malicious logic on endpoints, servers and devices. These types of preventive security tools do not rely on static malware signatures alone, but block the execution of malicious logic based on artificial intelligence (AI) and machine learning to protect against zero-day exploits. Next-generation antivirus services provide better protection than legacy signature-based services.

- Endpoint vulnerability and patch management—More remote teleworking translates into more scanning and patching and greater exposure to threats. Remote workers connecting to insecure home and public networks, particularly those bypassing centralized enterprise IT security services, are much more vulnerable than typical in-office workers. Patching endpoint vulnerabilities is part of basic computing hygiene that becomes more important during teleworking.

- **Backup and restore:** The ability to restore data from backup is essential to any operating environment exposed to threats that can alter the integrity and availability of enterprise data. If user data are backed up, enterprise leaders can mitigate threats such as ransomware viruses and stolen laptops and other devices by ensuring that lost data can be recovered and restored.

- **Web content filtering:** Hackers may create malicious pandemic-related websites containing malware that could compromise remote user endpoints and, ultimately, allow hackers to enter the enterprise network or steal data from the end user. Content filtering services can be tuned to filter out malicious pandemic content.

- **Application security:** Employees may use their enterprise endpoints to access consumer cloud applications (e.g., messaging, video) that can expose the enterprise to significant risk. Enterprise IT leaders should identify and patch these third-party applications or remove them from employee endpoints.

- Cloud access security broker (CASB)—CASB services can provide enterprise leaders with insight into what types of applications employees are using and what types of data they are uploading and downloading. The CASB also allows the enterprise to control risky cloud activities.

"MORE REMOTE TELEWORKING TRANSLATES INTO MORE SCANNING AND PATCHING AND GREATER EXPOSURE TO THREATS"

Network Security

Network security is the third out of the five overall categories that require unique countermeasures. A network is the "highway in" and should be both resilient and robust while also serving as a "checkpoint" into restricted areas with restricted data. Network security countermeasures include high-availability remote access infrastructure, network access control (NAC) and enhanced technical support:

- **Hardened high-availability remote access infrastructure:** With a shift to remote teleworking, VPN system security and resilience become more important. Without hardened, strong encryption, attackers can exploit weaknesses in remote connectivity systems to either gain unauthorized system access or collect and/or modify data in transit. Network staff can harden VPN systems by requiring MFA to augment the simple stand-alone username and password, making it much more difficult to exploit and gain access. Scanning for VPN infrastructure vulnerabilities and then patching and configuring them to a hardened and secure state are critical when work is performed remotely over VPNs. The VPN system should be resilient and implemented in a redundant, high-availability architecture to ensure that there are no single points of failure. The network team must also provision the VPN to support large increases in remote user traffic, making centralized Internet capacity and circuit redundancy more critical as well.

- **Network access control (NAC)**—NAC services perform a gatekeeper function by not allowing users and their laptops or devices to connect to enterprise services without passing system checks. NAC systems also provide an actionable compliance status for each endpoint based on a set of enterprise security policy requirements. Managers can designate which segments and resources VPN-connected users can access in accordance with the principle of least privilege based on compliance status and employee identity. Security leaders can effectively cordon off endpoints that might be susceptible to threats based on the NAC system-generated risk profile for each endpoint prior to connecting to the network.

- **Enhanced technical support**: Technical support processes, which would typically include physically bringing laptops and other devices to work for repair and inspection, need to be updated to conform to constrained pandemic operations when only remote access is feasible. Technical support teams will require secure remote desktop applications. IT leaders should evaluate all remote management applications and ensure that staffers harden them to the fullest.

Security Monitoring

Security monitoring is the fourth out of five overall categories that require unique countermeasures. Every node on the network produces event logs that

security professionals can leverage when piecing together clues during an investigation. Security practitioners can deploy security information and event management (SIEM) platforms to centrally correlate and store event logs for future analysis during investigations. A shift to remote teleworking involves specific systems that produce unique logs that need to be a new focus.

SIEM includes central correlation and monitoring of events from security platforms that indicate potential compromise from pandemic-related threats. The monitoring team should ensure that specific events from the following types of sources are being monitored for malicious activity:

- Security system availability
- Endpoint malware infections
- VPN
- Identity and access authentication requests and failures
- MDM
- Email antiphishing services

"ENTERPRISE SECURITY LEADERS SHOULD CONSIDER CREATING SPECIALIZED REPORTING CAPABILITIES THAT PROVIDE THE STATUS OF SECURITY SERVICES AIMED AT MITIGATING PANDEMIC-RELATED THREATS."

Security Reporting

Security reporting is the fifth and final category that requires unique countermeasures for a shift to remote teleworking. Enterprise security leaders should consider creating specialized reporting capabilities that provide the status of security services aimed at mitigating pandemic-related threats. The following are examples of specialized reporting:

- Number, type, purpose and criticality of remote user endpoints not reachable by endpoint management systems such as patching, antivirus, MDM and encryption
- Access logging and monitoring of privileged administrative access to high-risk systems and functions
- Employee and system compliance reports with current vulnerabilities, prioritized by the most critical vulnerabilities
- VPN-specific indicators and metrics, such as availability, employee logins and data specifics
- Remote user backup status
- CASB reports on risky remote user cloud data transfers and risky public cloud application use
- Remote worker policy exceptions
- Remote worker acceptable Internet usage

Conclusion

When pandemics such as the COVID-19 outbreak lead to a widespread, rapid shift to remote working in home offices, the enterprise threat landscape changes, and enterprise IT security leaders must deploy specific enhanced threat mitigation countermeasures. By implementing enhanced IT security countermeasures in employee security, endpoint security, network security, monitoring and reporting, enterprises can ensure that business systems will continue to operate in an unimpeded, secure manner.

Culled from: isaca.org

How to Build a Strategic and Effective GRC Operating Model

Many organizations are facing a set of challenges with regard to governance, risk and compliance (GRC)-related processes, technologies and overall programs embedded within their IT and business enterprise architecture. Problems arise because organizations manage multiple decentralized GRC programs, deploy and misconfigure GRC technologies, and misalign GRC policies and procedures with business strategy. To overcome these issues and increase the maturity of the GRC program, management should go through a regular assessment of the GRC program to define the as-is state and tweak it to align with the to-be state (target operating model).

An effective and mature GRC program is one that has proper business requirements as well as the right blend of automation and technology support. If you want to increase the maturity of your GRC program, then the following 4 steps will allow you to build a road map and a business case to create and implement the right GRC operating model, eliminating any pain points the organization might be experiencing today:

1. **Define compliance, business and IT future-state requirements.**
   - Identify future-state requirements by assessing the functional and technical design principles across the legal, compliance, business and IT scope dimensions.
   - Rank the gathered target-state requirements to facilitate their prioritization and to determine the desired (i.e., nice to have) vs. the required (i.e., must have) GRC program operating model key requirements.
2. **Perform the automation and technology fit, costing model and value return assessments.**
   - Identify the GRC technology solutions that will meet your key requirements based on your current and proposed GRC technologies and functionalities.
   - Develop a costing and value return model that accounts for the impact on technology, data, people and processes for the solutions identified.
3. **Develop and socialize the business case and road map.**
   - Create a dynamic business case that can be used as an operational tool to document program operating model and success factors.
   - Identify a path (i.e., a road map) for building out the target operating model, including project scope, timeline and technology deployment plan.
4. **Test and verify the GRC target operating model.**
   - Verify the functionality and performance of the GRC target operating model by working with business and IT organizations.
   - Define and execute the go-live procedures through working with the GRC program stakeholders and deploying the new technologies, data model and processes.

Effective GRC and risk management programs are critical to business operations, allowing stakeholders to appropriately understand and respond to overwhelming regulations and business policies.

Assurance leaders need to assess the maturity of the organization's GRC program regularly and create a program that aligns with the business strategy. In my experience, creating a point-in-time maturity assessment across the 4 steps outlined here is a great way to evaluate the effectiveness of a GRC program.

Culled from: isaca.org

FUNDAMENTALS OF BONDS INVESTMENTS, ITS BENEFITS, AND THE ROLES OF THE AUDITOR,

What makes a bond a bond?

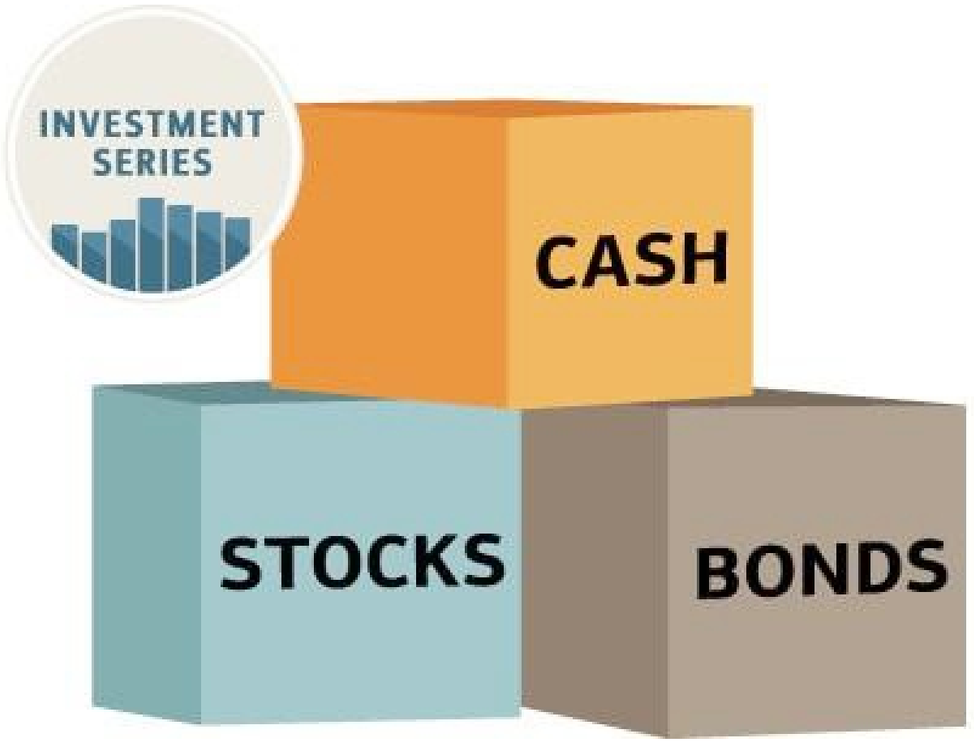
A bond is a loan or advance that the purchaser or holder, provides to the issuer. Federal Government, State Governments, Local Governments, and Corporate bodies issue bonds, when they need to raise capital. An investor who buys a government bond is lending the government money. If an investor buys a corporate bond, the investor is lending the company money. Like a loan, a bond pays interest periodically and repays the principal at a stated time, known as maturity.

If for example, a company wants to build a new factory for N100million and decides to issue a bond to help pay for the factory, the company might decide to sell 100,000 bonds to investors for N1,000 each. In this case, the "face value" of each bond is N1,000. The company – now referred to as the bond issuer – determines an annual interest rate, known as the coupon, and a time frame, within which it will repay the principal, i.e. the N100million. To set the coupon, the issuer considers the prevailing interest rate environment to ensure that the coupon is competitive with those on comparable bonds and attractive to investors. The issuer may decide to sell five-year bonds with an annual coupon of 7%. At the end of five years, the bond reaches maturity and the company repays the N1,000 face value to each bondholder. How long it takes for a bond to reach maturity can play an important role in the amount of risk as well as the potential return an investor can expect. A N100million bond repaid in five years is typically regarded as less risky than the same bond repaid over ten or twenty years because many more factors can negatively impact the issuer's ability to pay bondholders over a 10/20-year period relative to a 5-year period. The additional risk incurred by a longer-maturity bond has a direct relation to the interest rate, or coupon, the issuer must pay on the bond. In other words, an issuer will pay a higher coupon for a long-term bond. An investor therefore will potentially earn higher returns on longer-term bonds, but in exchange for that return, the investor faces additional risk.

The bonds which pay coupons twice a year are known as semi-annual coupon bonds. There are also bonds that make coupon payments annually, known as annual coupon bonds. Bonds which make no coupon payments are called zero coupon bonds, or deep discount bonds.

Also, every bond carries some risk that the issuer will "default", or fail to fully repay the loan. Independent credit rating services assess the default risk, or credit risk, of bond issuers and publish credit ratings that not only help investors evaluate risk, but also help determine the interest rates on individual bonds. An issuer with a high credit rating will pay a lower interest rate compared to one with a low credit rating. Again, investors who purchase bonds with low credit ratings can potentially earn higher returns, but they must bear the associated risk of default by the bond issuer.

In Nigeria, bonds are safe investments and as such, are appealing to nervous investors. Bonds can generate a steady stream of income for these set of individuals, even when the stock market becomes volatile.



Types of Bonds in Nigeria

Several bonds are issued each year, but there are only a few types of bonds because ultimately, majority of bonds issued fall into the categories of bonds listed below.

1. Treasury Bonds
This bond is issued by the Federal Government of Nigeria (FGN). Treasury bonds are the safest bonds you can invest in. This however depends on the government of the country issuing it.

The bonds issued by the government of United Kingdom for instance, cannot be ranked the same way with the bonds issued by FGN, because UK is economically and politically more stable than Nigeria.

As expected, Treasury bonds have the lowest yields compared to other types of bonds because they are almost safe and, the safer an asset, the lower the yields.

2. Municipal Bonds
Municipal bonds are bonds issued by States and Local governments to fund capital expenditures such as building of hospital, construction of bridges, roads, etc.

As exemplified in Treasury bonds above, states also differ in terms of economy, political stability, size and security, and all these inform the risk investors are willing to take on the states.

The wealthier and more secured a State or Local government is, the more an investor is willing to buy its bond. Hence the bond of Lagos State for instance, will be of a higher value to an investor than that of Zamfara State.

3. Corporate Bonds
When companies need to raise capital to expand or improve their businesses, they issue corporate bonds.

Compared to Treasury bonds and Municipal bonds, Corporate bonds have more credit risk, because the probability of default in corporate bonds is higher

Corporate bonds can be divided into investment grade and speculative grade.

Investment grade bonds are rated higher by rating agencies and they are relatively safe, while speculative grades are rated lower. The risk of default in corporate bonds is even higher with speculative grade bonds, when compared to investment grade bonds

4. Asset-Backed Securities (ABS)
Asset-backed securities are bonds that are backed by financial assets.

They are bonds in which assets are brought together and resold to investors as bonds.

Car loans and mortgage loans for instance, can be bundled together and resold to investors, such that the investors provide the funds needed to fund the immediate purchase of the cars and homes.

How is the price of a bond determined in the open market?

Bonds can be bought and sold in the "secondary market" after they are issued. While some are traded publicly through exchanges, most bonds trade over the counter (OTC) between large broker-dealers acting on their own, or on behalf of their clients.

The value of a bond in the secondary market is determined by its price and yield. Obviously, a bond must have a price at which it can be bought and sold (see "Understanding bond market prices" below for more), and a bond's yield is the actual annual return an investor can expect if the bond is held to maturity. Yield is therefore based on the purchase price of the bond as well as the coupon.

A bond's price always moves in the opposite direction of its yield. The key to understanding this critical feature of the bond market is to recognize that a bond's price reflects the value of the income that it provides through its regular coupon interest payments. When prevailing interest rates fall – notably, rates on government bonds – older bonds of all types become more valuable because they were sold in a higher interest rate environment and therefore have higher coupons. Investors holding older bonds can charge a "premium" to sell them in the secondary market. On the other hand, if interest rates rise, older bonds may become less valuable because their coupons are relatively low, and older bonds therefore trade at a "discount".

Understanding Bond Market Prices

When bond prices are quoted in the market, it is as a percentage of the bond's face value. To understand bond prices, simply add a zero to the price quoted in the market. For example, if a bond is quoted at 99 in the market, the price is N990 for every N1,000 of face value and the bond is said to be trading at a discount. If the bond is trading at 101, it costs N1,010.00 for every N1,000 of face value and the bond is said to be trading at a premium. If the bond is trading at 100, it costs exactly N1,000 for every N1,000 of face value and the bond is said to be trading at par. Another common term is "par value," which is simply another way of saying face value. Most bonds are issued slightly below par and can then trade in the secondary market above or below par, depending on interest rate, credit or other factors.

To break it down, when interest rates are rising, new bonds will pay investors higher interest rates than old ones, so old bonds tend to drop in price. When interest rates are falling however, mean that older bonds are paying higher interest rates than new bonds, and therefore, older bonds tend to sell at premiums in the market.

On a short-term basis, falling interest rates can boost the value of bonds in a portfolio and rising rates may hurt their value. However, over the long term, rising interest rates can actually increase a bond portfolio's return as the money from maturing bonds is reinvested in bonds with higher yields. Conversely, in a falling interest rate environment, money from maturing bonds may need to be reinvested in new bonds that pay lower rates, potentially lowering longer-term returns.

Auditing Bonds in an Organization
As an auditor, saddled with the responsibility of reviewing the security investments, such as Bonds, in an organization, you must make sure that the figures shown as investment assets in the organization's books are not materially misstated and that all income and changes in an investment's value are properly recorded.

Firstly, there is need to confirm the existence of the organization's investments as stated in the records. Banks are generally required to engage the services of custodians, hence, the first audit step is to request a confirmation from the custodian. This may come in the form of custodian's statement. The confirmation should address what types of securities the organization owns. Receiving confirmation from the organization's investment custodian is typically adequate to verify the existence of the investment.

- Upon receipt of the statement, review the position on the CSCS statement against the organisation's in-house records.

- Match Bonds by their maturity dates on both documents, and ensure that the in-house balance on every line of investment is same with the balance in custodian's statement.

Another very important test is to confirm that daily valuation of the organization's positions is carried out, on a mark-to-market basis, and that rates are interpolated where needed.

To do this:
- Firstly, confirm that only approved sources of market information, majorly Financial Markets Dealers Quotation (FMDQ) are accessed to obtain information on real time basis.
- Do a comparison of prices quoted by FMDQ for all existing security investments and the prices recorded in the organization's books, to ascertain that there are no material discrepancies.

- Carry out an independent mark-to-market calculation of the organization's portfolio, to ascertain that the correct valuations are recorded for securities in the organization's books.

- Confirm that all Bond purchases and sales are not carried out off market rate, i.e. significantly different from the mark-to-market (MtM) price quoted by FMDQ for the said instruments.

Lastly, it is also pertinent to confirm that all investment-related interests and dividend incomes, have hit the income statement as revenue. If, however, there is any investment income reflecting in the income statement that cannot be matched to an investment, that situation indicates that there is a completeness issue, i.e. all investments are not reflecting on the balance sheet.

In conclusion, bonds, and other types of fixed-income securities, play a significant role in an investor's (corporate and individual) portfolio, in return for coupon payments.

Possessing bonds in Nigeria can help you diversify your portfolio, because the bond market hardly rises or falls alongside the stock market.

Also, bonds are known to be safer and less volatile than stocks.

Lastly, the auditor has a significant role to play for corporate as well as for major individual bond investors, in validating substance, existence, completeness, accuracy, and valuations of bonds portfolios, which role should be performed meticulously and with high sense of professionalism following the procedures outlined in the previous section.

Ibukun Ayoola Akintunde,
Risk Audit Unit, Access Bank Plc

Auditing Knowledge Management

Knowledge assets' increased value and contribution to business objectives obliges internal auditors to focus on how they are safeguarded.

Technological advances are transforming the nature and importance of the organization's knowledge assets — intellectual property, software, data, technological expertise, organizational know-how, and other intellectual resources. The value of the global knowledge management market was around $2 billion in 2016 and is expected to exceed $1.2 trillion by 2025, according to Zion Market Research. At this worth, organizations should want to know if their knowledge assets are safeguarded.

Knowledge assets are vulnerable to loss and can be compromised by internal and external sources. In a 2018 study from the Ponemon Institute and Kilpatrick Townsend & Stockton, 82% of respondents acknowledged that their companies very likely failed to detect a breach involving knowledge assets, up from 74% in 2016.

Often, audit of knowledge assets is limited to assessing risks, controls, and value derived from the technologies used in their processing (knowledge flow) and the digital records maintained that focus on effective document management. This is only a part of knowledge management auditing in the true sense. It does not get to the core issues of the effectiveness of their protection, how they promote business objectives, and the new opportunities they exploit.

What has been missing is a structured approach to

assess the interplay between strategic and operational risks and controls in enterprisewide knowledge assets management. Unfortunately, there are no comprehensive professional guidelines to assess the adequacy of risks confronting knowledge assets, particularly living knowledge assets held by individuals. Internal auditors must adapt to the evolving risk landscape in knowledge management by reorienting their methodologies and practices to recognize the role of knowledge assets in achieving business objectives.

percentage of core knowledge held by people nearing retirement, and high market demand for key personnel. It is likely in such cases that these assets will be lost.

Assess Strategic Risks

Explicit and Tacit Knowledge Comparison

With disruptive technologies at the forefront, knowledge management tends to be a high-risk activity for most organizations. Risks to knowledge assets are any loss that may decrease the potential to effectively pursue an organization's business objectives. Key risk indicators in a typical knowledge-based organization include uncertainties about critical knowledge needs, potential business opportunities lost in their absence, and their impact on business objectives. Other indicators may be process related, such as multiple repositories of information in IT-based systems such as an intranet, collaboration platform, or emails that are not integrated. These indicators can lead to wasted resources and inefficiencies and weaknesses in access restrictions to intellectual property.

Attrition is a common risk involving significant replacement costs that can destabilize even the most successful and steady organizations. It is estimated that the average cost of turnover is 1.5 times the annual salary of the job. Internal auditors also should be vigilant about risks specific to tacit knowledge assets management, which include a high tacit-to-explicit knowledge ratio, high staff turnover, a high

There are two types of knowledge defined in business. The first, explicit knowledge, is easy to codify, store, and share. It includes textbooks, journals, white papers, patents, literature, audio-visual media, software, and database access. The second, tacit knowledge, comes from personal experience and is not easily replicable or transferrable, such as know-how, methodologies, training algorithms, and professional skepticism.

Within tacit knowledge, there are two dimensions: technical and cognitive. The highly subjective and personal insights, intuitions, and inspirations derived from an individual's experience fall under the first category. The second category consists of beliefs, perceptions, values, and emotions ingrained in individuals over years.

Some argue that tacit knowledge accounts for about 80% to 90% of the knowledge held in a typical organization. Knowledge assets are created at the intersection of, and interaction between, explicit and tacit knowledge.

Strategy-related risks in knowledge management

typically include the absence of, or a weak, knowledge management strategy; lack of involvement from senior management in knowledge management activities; and lack of alignment between key processes and knowledge assets in place.

If knowledge is a key driver for the business or is one of the main products of the business entity audited, such as a consulting firm or an educational institute, internal auditors should ask:

- What is the critical knowledge at risk and who determines it?
- What are the core activities?
- How does information flow through those activities?
- Is there a knowledge management strategy?

Next, internal auditors should remap the business' critical processes to identify what information is

needed to run them. If these needs are not being met, they should determine who needs the missing knowledge. Practitioners should review the enterprisewide risk register to assess whether knowledge management-related risks are recognized, paying attention to the risks of loss of knowledge when core capabilities are outsourced. The instances of high staff turnover and poor knowledge retention among outsourced providers could hamper service quality, involving potential legal risks.

A robust knowledge management strategy should focus on capturing knowledge assets that are critical to success and that underpin performance to create growth and a competitive advantage. Are there sound human resources policies and succession planning strategies for mentor and peer support before, during, and after key staff with the best situational awareness leave the organization? Are there processes to capture results of lessons-learned exercises, particularly with lawyers, consultants, and accountants' knowledge and experience that is incorporated into organizational knowledge and change processes? The knowledge lost in such cases could be costly to replace and may require intensive corrective training or retraining.

In public sector audits, practitioners should pay attention to the procedures followed for valuation of investments in knowledge assets used to support the provision of public services such as water, transportation, and healthcare. There may not be well-defined standards and methodologies for estimating the social, economic, and financial value derived from the assets as they don't have market-determined equity value.

Assess Operational Risks

Employees spend almost one-fourth of their time searching for information, according to a survey from The Economist Intelligence Unit. Unclear data definitions, ineffective data governance, and poor search engine performance lead to barriers requiring analysts and developers to resolve them. The root cause of most operational risks in managing knowledge assets is lack of alignment between the strategy and the processes built around it.

To start, internal auditors should review the accuracy and reliability of the knowledge assets inventory and the core processes they support, and the responsibilities of the people who manage them. The review results will help identify weaknesses in data governance — such as data silos where data is divided across various databases and divisions accentuating memory loss and poor internal coordination of information. The starting point for the review is identifying and using performance criteria for key activities approved by management. While doing so, internal auditors must be able to determine how the key activities are aligned with key stages of knowledge management in the organization, such as needs identification; acquisition; storage, retrieval, and dissemination; archiving; and performance management. If they do not align, that is a strong indicator that these assets are not generating a tangible return.

Intellectual property in the form of formulae, practices, processes, designs, instruments, patterns, commercial methods, or compilations of information can be subject to loss or compromised by internal or external sources. Internal auditors should assess that the owners of the intellectual property assets have

appropriate controls to prevent cyberattacks that could lead to infringements and inappropriate access.

Internal Audit's Strategy

Auditing knowledge assets requires specific strategies and skills. Each organization's knowledge needs are unique. As internal audit leaders prepare their audit plans beyond 2020, they should have a multipronged strategy to audit their clients' knowledge assets from a value-for-money perspective:

- Retain the best internal audit talent through valuing and investing in the tacit knowledge asset held in the internal audit function.
- Develop and maintain a risk-based audit universe of clients' business operations with significant investments in knowledge assets. This should provide a basis for identifying areas of audit engagement related to knowledge management.
- Identify and map the knowledge held in the audit department to capture and use the tacit knowledge held, particularly related to complex audit engagements. This information could be used to develop an appropriate knowledge management strategy and system to facilitate collaboration within the audit team.
- Empower audit teams to recognize the strategic importance of knowledge assets to the business. This will allow them to provide assurance on legal, commercial, technical, social, and financial aspects of the knowledge assets and the relevant risk indicators. For example, develop a bank of risk indicators — quantitative and qualitative — for assessing the processes used in tacit knowledge assets management.
- Review the adequacy of audit programs used for knowledge management audits. Strengthen them by focusing on strategic and operational aspects of the processes in place to highlight risks of inefficient use of knowledge assets.
- Focus on the value-for-money aspect of the engagement. Do not get distracted by the technologies and processes used to manage knowledge assets, particularly in engagements involving significant investments in them.

Closing the Gap

The five most valuable companies in the world report just £172 billion ($223.2 billion) of tangible assets on their balance sheets, though their total worth is £3.5 trillion ($454.2 billion). Almost all of their value is in the form of intangible assets, including intellectual property, data, and other knowledge assets, according to a 2018 budget report from Her Majesty's Treasury in the U.K. Despite their critical role in business performance, knowledge assets are not traditionally audited with a focus on how organizations safeguard them to retain their competitive position and how they contribute to business performance. As key partners in the assurance process, internal auditors can take a strategic approach to bridge this gap and maximize its influence.

Culled from: iia.org

The IIA Updates Three Lines Model

New release considers risk and governance in a complex world.

In today's fast-paced, technology-driven world, risk-based decision-making is as much about seizing opportunities as it is about defensive moves. A long-overdue update to the popular Three Lines of Defense risk management model embraces this new reality.

"Risk management goes beyond mere defense," says IIA President and CEO Richard Chambers. "Organizations need effective structures and processes to enable the achievement of objectives and support strong governance and risk management. The updated Three Lines Model addresses the complexities of our modern world."

The IIA spearheaded a task force of audit practitioners, risk and compliance executives, stakeholders, and others to identify the relationships between the central and common components of organizations and consider the continued relevancy of the Three Lines concept. "The update reinforces that organizations must determine appropriate, pragmatic structures for themselves, taking into account their objectives and circumstances against a backdrop of an ever-evolving risk landscape," says task force leader and IIA Global Chair Jenitha John.

The Three Lines Model is based on six principles: governance, governing body roles, management and first and second line roles, third line roles, third line independence, and creating and protecting value. It presents the accountability of the governing body for oversight, of management to achieve organizational objectives, and of an independent internal audit function for assurance and advice.

The model notes that although the governing body, management, and internal audit all have distinct responsibilities, "the basis for successful coherence is regular and effective coordination, collaboration, and communication."

"For implementation by organizations on both a reactive and proactive basis, these updates help modernize and strengthen application of the model to ensure its sustained usefulness and value," Chambers says. **A. Millage**

Culled from: iia.org

Post-pandemic Planning

The audit plan that existed before the pandemic is based on an old risk paradigm. In a post-pandemic world, chief audit executives (CAEs) must think differently about their organizations' risks and how to redeploy audit resources. Here are some questions CAEs should ask in rethinking their audit plans.

What does the organization's new normal look like?

Even businesses that were least impacted by COVID-19 will have systemic changes in their risk environment (see "Questions for CAEs" at the end of this article). There may be major fallout to institutions and systems that organizations rely on, and regulators, financial institutions, and supply chains may experience disruptions well past the point when stay-at-home orders are relaxed. Some may no longer exist.

Is my risk assessment process agile enough?

This question will be critical as CAEs begin prioritizing how to redeploy resources to address elevated risk in legacy risk areas as well as in new, uncharted territory. Risk assessments need to be agile because risk dynamics may change frequently in the near term. CAEs should evaluate and streamline legacy risk assessment processes.

Does my team still possess the skills to execute the risk assessment and audit plan?

In the post-pandemic world, risk profiles probably will change — in some organizations, dramatically. CAEs need to evaluate the talent in their teams and internal audit's ability to identify risks and execute engagements that focus on new types of risk. They need to address questions such as:

- ☐ How has internal audit's staffing changed?
- ☐ Are staffing levels different, and have there been any changes in talent?
- ☐ Are there new talent needs as a result of changes to the organization's risk profile?

Does my team still have an objective mindset? Unprecedented times call for unprecedented measures, and during the COVID-19 emergency, many internal auditors have been called to duty in ways they never imagined. If auditors were engaged in nonaudit activities within the business or performing activities that normally would be incompatible with professional standards, CAEs should evaluate staff objectivity.

Culled from: iia.org

A New World of Risk

The world is different now, with different risks. Internal audit functions must recalibrate how they view the inherent risks their organizations face as the recovery period begins.

Although pivoting from the old world to a new one is not a new phenomenon, the magnitude of COVID-19 impacts is more global and more severe than anything most auditors have experienced. Internal audit's ability to respond is vital not only to how its business recovers, but also how audit realigns with its stakeholders' needs.

Questions for CAEs

To assess their situation during the COVID-19 crisis, CAEs should ask:

- What does organizational staffing look like now? Have there been reductions or reorganizations?
- Have key stakeholders changed? What new audit clients should I anticipate?
- Have workforce reductions or reorganizations impacted how internal controls are executed? Are there new segregation of duties concerns or controls that no longer have control owners?
- What processes have been temporarily or permanently changed?What systems were temporarily modified or permanently changed? Were appropriate IT general controls followed for these changes, and, if not, what are the implications?
- What controls were modified to accommodate unique business situations or risks?
- Have there been any key personnel changes such as loss of unique subject-matter expertise or loss of key leaders in strategic areas?
- Has the organization's strategic focus changed in the near or long term?
- How have cost structures changed?
- Have there been fundamental changes in the organization's debt and capital structures? Are there new or different debt covenants?
- What new legal or compliance challenges is the organization facing (lawsuit exposures, changes to compliance infrastructure)?
- Have new business opportunities emerged and have corresponding risks been identified?·Have the fundamentals of business-unit operations or strategies changed?
- How have business continuity dynamics changed (key infrastructure changes, key customer changes)?
- How have enterprise risk management dynamics changed (key risks, key risk indicators, response plans, and risk appetite)?
- How have U.S. Sarbanes-Oxley Act of 2002 dynamics changed, including changes with external auditors, regulatory dynamics, and control owners?

Culled from: iia.org

5 Things Internal Audit Must Tell the Audit Committee Now!

As we continue to navigate the treacherous risk landscape that includes an ongoing global pandemic, much is being said and written about whether internal auditors are stepping up for their organizations. I am certain we are contributing value during this time, but I also know it may not always be evident that's because many internal auditors are not comfortable extolling their contributions in audit committee meetings.

No relationship for a chief audit executive (CAE) has been transformed more in the 21st century than that with the audit committee. According to The IIA's Audit Executive Center, 90 percent of North American internal audit departments in publicly traded companies report functionally to the audit committee (and 80 percent overall). And in many companies, the audit committee holds a discussion session with the CAE at every meeting. Yet often these executive sessions are nothing more than a brief exchange of pleasantries with audit committee members tossing "hardball" questions like, "Do you have enough resources?"

The audit committee's success is tied to the effectiveness of the internal audit department. Accordingly, audit committee members must have complete confidence in the internal audit function and the CAE. That can be achieved only with a strong, continuous, and open dialogue between the CAE and audit committee.

Of course, dialogue is a two-way street: It's as much the responsibility of the CAE as the committee members themselves. But both parties must be willing to drive that dialogue in a way that provides evidence that internal audit is focused on the right risks — particularly in the COVID-19 environment.

If neither the audit committee nor the CAE is interested in consequential or provocative conversations, frankly, none will take place. But with so much at stake, I challenge CAEs to take the lead in discussing how internal audit is responding in the pandemic.

Here are five things the CAE should be able to tell the audit committee now and ensure that audit committee members are hearing.

1. Internal audit has altered its coverage dramatically to address the risks presented by the COVID-19 health and financial crisis. Recent surveys by The IIA and others confirm that sweeping changes were made to internal audit plans in the first half of 2020. Almost 50 percent cancelled some of the engagements on their annual plan, in most cases replacing them with new engagements to address pandemic-related risks. While it is likely CAEs are briefing their audit committees about changes to the plan, this presents a unique opportunity to explore the rationale behind such changes including whether they were requested by management or initiated by internal audit.

2. Internal audit is employing a continuous methodology to assess risks, and identifying those that present the most significant threats to the organization before they arrive. I have been expounding on the need to audit at the speed of risk for years. Risk velocity has never been greater than it is now. The IIA and International Federation of Accountants (IFAC) recently jointly issued Six Recommendations for Audit Committees Operating in the "New Normal." The first of those

recommendations is: "Staying informed: Audit committees must have a clear-eyed view and understanding of risk areas, and internal audit should support this by providing timely risk assessments. In a post-COVID world, those assessments will be more frequent and possibly continuous."

The audit committee will gain real comfort by knowing that internal audit is looking at and beyond the horizon in identifying risks for audit coverage. For more on this topic, check out my 2018 blog: Internal Audit and Emerging Risks: From Hilltops to Desktops.

3. Internal audit has adapted to a remote workplace environment, and no key risks are falling through the cracks because they can't be audited in person. In the face of the pandemic, a great many professionals have been working remotely. Internal auditors are no different. Adapting to this environment requires a resilient and transformative mindset. A recent whitepaper from AuditBoard, Building Operational Resiliency, offers five critical steps for internal audit to respond to crisis-related challenges:

- Reevaluate enabling technology.
- Reassess business priorities.
- Address the unknowns.
- Plan for efficiency.
- Learn from peers.

4. Internal audit continues to emphasize audit quality despite the obstacles. While it may be obvious, internal audit must not relax its commitment to quality or conformance with The IIA's International Professional Practices Framework (IPPF). Most internal audit departments have time-tested comprehensive methodologies for undertaking internal audits. In conformance with IIA Standard 1300, CAEs must "maintain a quality assurance and improvement program that covers all aspects of the internal audit activity."

When evidence can't be physically examined because of a remote work environment (as 25% of respondents to a recent survey by the accounting firm Frazier & Deeter reported), internal audit's policies and procedures must be updated to ensure that a basis for internal audit's conclusions can be established. In communicating with the audit committee, the CAE should embrace the opportunity to emphasize the department's commitment to quality and the steps being taken in the current environment to ensure the accuracy and timeliness of the information it provides.

5. The impacts from the pandemic will linger well into 2021. Internal audit is already assessing the risks and planning audit coverage. Finally, internal audit should already be focused on key risks for 2021. An ongoing dialogue with the audit committee will not only ensure its members are well-informed, but that their perspectives are

Audit Committees and its role in auditing process: Xerox experience

being considered. This year has been full of disruptive and unexpected events. While 2021 is still months away, it is likely that key risks will linger or become more severe. These risks are likely to include:

- COVID health and safety (employees and customers).
- Business continuity.
- Global macroeconomic instability.
- Severe pressure on the bottom line.
- Supply chain disruption.
- Cyber fraud.

There is obviously a lot to unpack from this blog. CAEs have a lot on their plates in 2020, and keeping the audit committee fully and currently informed should always be top of mind. Of course, I captioned my list as "five things the CAE should be able to tell the audit committee now." The list clearly implies that these are things we are doing. If not, you have more work to do than briefing the audit committee

Richard F. Chambers

Access Bank Plc
Yinka Tiamiyu
Plot 999C Damole Street,
Victoria Island, Lagos
tiamiyuy@accessbankplc.com
08023220367, 2364062

Bank of Agriculture Limited
Daniel Olatomide
1 Yakubu Gowon Way
Kaduna.
d.olatomidei@boanig.com
08067007183

Bank of Industry Limited
Yemi Ogunfeyimi
23, Marina
Lagos.
yogunfeyimi@boi.ng
08033059361

Central Bank of Nigeria (CBN)
Lydia I. Alfa
Plot 33, Abubakar Tafawa Balewa
Way Central Business District,
Cadastral Zone, Abuja,
Federal Capital Territory, Nigeria
lialfa@cbn.gov.ng
08033177216

Citibank Nigeria Ltd
Bolaji Ajao
27 Kofo Abayomi St
Victoria Island, Lagos
bolaji.ajao@citi.com
Tel: (234)1 2798400, 4638400 Ext. 8446
DL: (234)1 2798446, 4638446.
Mobile - 07057878877

Coronation Merchant Bank Ltd
Dele Dopemu
10, Amodu Ojikutu Street
Victoria Island,
Lagos.
ddopemu@coronnationmb.com
01-4614892, 07034109732.

Development Bank of Nigeria
Joshua Ohioma
The clans place
Plot 1386A Tigris Crescent,
Maitama, Abuja.
johioma@devbankng.com
08129145586

Ecobank Nigeria Ltd
Felix Igbinosa
21 Diya Street, Gbagada
Lagos
FIGBINOSA@ecobank.com
07068754692 ; 08023633203
D/L: 01 2260449

FBNQuest Merchant Bank Limited
Abdul-Azeez Bello
18, Keffi Street, Ikoyi
Lagos
azeez.bello@fbnmerchantbank.com
2702287, 08022923341

Federal Mortgage Bank of Nigeria
Wakeel Imam Galadanci
Plot 266, Cadastral AO, Central
Business District
P.M.B 2273, Abuja
wakeelimam@yahoo.com
08023040123, 01-4602102

Fidelity Bank Plc
Ugochi Osinigwe
Fidelity Bank Plc.
2, Adeyemo Alakija Street, V/I, Lagos.
ugochi.osinigwe@fidelitybank.ng
08023030298, 08092147012.

First Bank of Nigeria Ltd
Uduak Nelson Udoh
9/11, McCarthy Street, Lagos
Uduak.udoh@firstbannigeria.com
01-9054583, 08022902268

First City Monument Bank Ltd
Amarachukwu Okogbue
10/12 McCarthy St,
Lagos.
amarachukwu.okogbue@fcmb.com
08033062602

FSDH Merchant Bank Limited
Dare Akinnoye
Niger House (6/7 foors)
1/5 Odunlami St, Lagos
dakinnoye@fsdhgroup.com
08022017090

Guaranty Trust Bank Plc
Segun Fadahunsi
178, Awolowo Road, Ikoyi, Lagos
segun.fadahunsi@gtbank.com
08023285640

Heritage Bank Ltd
Prince Akamadu
130, Ahmadu Bello Way,
Victoria Island, Lago
Prince.akamadu@hbng.com
08037649757

The Infrastructure Bank Plc
Sadiku Ogbhe Kanabe
Plot 977, Central Business District
(Adjacent National Mosque)
P.M.B 272, Gark
F.C.T, Abuja
Nigeria.
skanabe@tibplc.com
08033039481, 08056900079

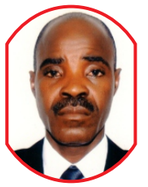
JAIZ BANK PLC
Abdullahi Usman
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja,
Nigeria.
ABDULLAHI.USMAN@jaizbankplc.com
09-4605138, 08032089010,
08086103555

Keystone Bank Limited
Clifford Odiase
707 Adeola Hopewell Street,
Victoria Island, Lagos
CliffordOdiase@keystonebankng.com
09087500658, 07035385884

NEXIM BANK
Mr Ichide Friday
NEXIM House
Plot 975 Cadastral Zone AO,
Central Business District,
P.M.B. 276, Garki,
Abuja, Nigeria.
ichidejnr@gmail.com
07085122928.

Nigeria Mortgage Refinane Company
Samuel Ekanem
No 18 Mississippi Street,
Off Alvan Ikoku Way
Maitama,
Abuja, Nigeria
sekanem@nmrc.com.ng
08023394068

Nova Merchant Bank
Ifeatu Onwuasoanya
23, Kofo Abayomi Street
Victoria Island, Lagos.
Ifeatu.onwuasoanya@novambl.com
08024114481



Polaris Bank
Olurotimi Omotayo
3 Akin Adesola St
Victoria Island, Lagos
romotayo@polarisbanklimited.com
08023096373

Providus Bank Ltd
Aina Amah
Plot 724, Adetokunbo Ademola Street
Victoria Island,
Lagos.
aamah@providusbank.com
08029087442

Rand Merchant Bank
Femi Fatobi
3RD Floor, Wings East Tower,
17A, Ozumba Mbadiwe Street
Victoria Island, Lagos
Femi.fatobi@rmb.com.ng
01-4637960, 08028514983

Stanbic IBTC Plc
Abiodun Gbadamosi
Plot 1712, Idejo Street
Victoria Island, Lagos
Abiodun.Gbadamosi@stanbicibtc.com
07057215563.

Standard Chartered Bank Nig. Ltd.
Emeka Owoh
142, Ahmadu Bello Way
Victoria Island, Lagos
emeka.owoh@sc.com
08037027452

Sterling Bank Plc
Cyril Osheku
1st Floor,
Sterling Bank Plc Head Office
(Annex), Ilupeju
239/241, Ikorodu Road, Lagos.
Cyril.osheku@Sterlingbankng.com
08023046639, 08056656866

SunTrust Bank Nig. Ltd.
Adedokun Aremu
1, Oladele Olashore Street,
Off Sanusi Fafunwa Street,
Victoria Island, Lagos
adedokun.aremu@suntrustng.com
09038989319, 08020663423

TajBank Nigeria Limited
Aminu Habu Alkassim
Plot 72, Ahmadu Bello Way,
Central Business District,
Abuja.
aminu.alkassim@tajbank.com
08032868266

Union Bank of Nigeria Plc
Kabir Garba
36 Marina,
Lagos.
unionbank,com
08033028899

United Bank for Africa Plc
Gboyega Sadiq
UBA House
57 Marina, Lagos
gboyega.sadiq@ubagroup.com
08025011046

Unity Bank Plc
Olusegun M. Famoriyo
Plot 290A, Akin Olugbadi Street,
Off Adeola Odeku Road,
Victoria Island, Lagos
ofamoriyo@unitybankng.com
08023145535

Wema Bank Plc.
Adekunle Onitiri
Wema Towers
54 Marina, Lagos
adekunle.onitiri@wemabank.com
+234 1 4622364, 08022245818

Zenith Bank Plc.
Mogbitse Atsagbede
Plot 84 Ajose Adeogun St
Victoria Island, Lagos
mogbitse.atsagbede@zenithbank.com
08023270998