ADAPTING TO THE NEW NORMAL

COMPLIANCE IN TIMES OF A PANDEMIC

A Pocket Guide for Businesses

Alliance for Integrity

Alliance for Integrity

The Alliance for Integrity is a business-driven, multi-stakeholder initiative seeking to strengthen corruption prevention measures in the economic system and global supply chains. As a global learning and implementation network, the initiative promotes collective action by all relevant actors from the private sector, the public sector and civil society.
www.allianceforintegrity.org

Disclaimer

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

TABLE OF CONTENTS

1. INTRODUCTION

The Covid-19 pandemic has had adverse effects on businesses across the globe and caused unprecedented disruption to supply chains and business systems. Approximately, 76.69 billion US dollars is projected to be the monetary GDP loss of businesses globally in best scenario cases[1]. Consequently, it has become necessary for businesses to adapt to the changes in the economic system and adjust to the 'new normal' of transacting business. Adjusting to the 'new normal' requires innovation and the adoption of technological tools for business engagements. This no doubt poses many risks, known and unknown to business operations and systems, and can be turbulent for organisations with static structures.

It has become even a more daunting task to maintain business integrity and compliance during these times. 90 % of respondents (almost 3,000 respondents from 33 countries) in a 2020 survey conducted by

1 Impact of the coronavirus pandemic on the global economy – Statistics & Facts

Ernst & Young believe that disruption, as a result of Covid-19, poses a risk to ethical business conduct.[2] There is therefore the need for increased awareness creation and capacity strengthening on compliance in critical areas where business integrity could be adversely impeded.

The Alliance for Integrity is positioned to provide practical solutions to businesses in strengthening their compliance capacities; trickling down to their supply chains. Having studied and examined the current global trends with its team of trainers and compliance experts, the Ghana Hub presents in this publication, discussions on selected topics on compliance and integrity in an era of crisis.

Central to this publication is the issue of "Data Protection and Application Security", where essential cybersecurity elements necessary to ensure efficient safeguard of data for businesses are extensively discussed. The issues of "Managing and Maintaining Skilled Labour in Times of Crisis", "Alignment of Programmes to Reflect Current Business Trends During a Pandemic", "New regulations and Impact on Businesses" as well as the "Role of compliance in Crisis Management", are also thoroughly explored.

We believe that this publication will serve as an effective tool for companies to identify, prepare and position themselves for current and future threats ensuing to a crisis. The publication is a collection of articles from experts in the Alliance for Integrity network in Ghana.

Gideon Mankralo
Network Manager, Ghana & Nigeria

2 Global businesses divided on implications of Covid-19 crisis for company ethics.

2. NEW REGULATIONS AND IMPACT ON BUSINESSES

By: **Dr. Alex Ansong, Head of Public Law Department, Ghana Institute of Management and Public Administration**

The outbreak of the Covid-19 pandemic has had a huge global impact on people all over the world. Globally, the social, cultural and especially health effects of the Covid-19 pandemic are unprecedented in the 21st Century. The impact of the pandemic has also had a devastating effect on businesses the world over with massive disruptions to hitherto trusted global supply chains. Compared to other regions of the world, Africa has relatively been spared the seismic health impacts of the pandemic even though infections are on the increase. Ghana's experience of the pandemic reflects the typical African situation of relatively lower infection rates. However, the economic effects of the pandemic in Ghana and generally in Africa are quite dire. The World Bank's Africa Pulse Report predicts that the economic impact of Covid-19 will likely result in the first recession in Sub-Saharan Africa in the past 25 years. Economic growth will diminish into the negatives. If these bleak economic predictions materialise fully, it will plunge millions into dire poverty. The World Trade

Organisation also estimates that global trade will plunge by between 13 % to 32 % in 2020. Recovery in the global economy is uncertain as the lifting of some state-imposed restrictions on economic activities will most likely hinge on discovery of a vaccine or medicine to tackle the spread of the pandemic. For developing countries like Ghana that were making positive strides in contribution to international business and trade pre-Covid-19, the slump in international trade flows will certainly have a chilling effect on, especially export oriented, domestic business.

Considering the seismic global impact of the Covid-19 pandemic, this article discusses the international and domestic legal responses to tackling the pandemic and how these have impacted businesses.

International Regimes and their Impact on Businesses

The most relevant international regime with a direct impact on business is the World Trade Organisation (WTO). The core objectives of the WTO are, among others, to eliminate discrimination in international trade and promote market access for goods and services through the reduction and elimination of tariff and non-tariff barriers to trade. These core objectives are operationalised under treaty provisions in Article 1 of the General Agreement on Tariff and Trade 1994 (GATT 1994) which forbids WTO members from discriminating against goods coming from other member states. Article 11 of the GATT 1994 also forbids WTO members from imposing bans or quantitative restrictions on import of goods into their countries or export of goods from their countries. These two provisions ensure that businesses in WTO member states can enjoy non-discrimination and market access when they export their products to the territories of other member states. Similar treaty provisions mandating non-discrimination and market access in the services sector are

enunciated in Articles 2 and 16 respectively of the General Agreement of Trade in Services (GATS).

WTO members can however legally deviate from the stated rules on non-discrimination and market access based on several exceptions provided for in Article 20 of the GATT 1994 and Article 14 of the GATS. Of significance for this discussion on new domestic rules and their impact on business is that Article 20(b) of the GATT 1994 and Article 14(b) of the GATS allow WTO members to legally deviate from their obligations if this is necessary to protect human, animal, or plant life or health. In essence, this is a public health exception to non-discrimination and market access, among other obligations. Domestic regulations leading to the closure of ports of entry into Ghana for road, sea and air transport services have, for example, been undertaken in consonance with Ghana's obligations under the WTO system and the exceptions available to it in Articles 20 and 14 of the GATT 1994 and GATS respectively. Other WTO members adopting similar border closures and restrictions on trade have, like Ghana, availed themselves of the public health exceptions in the GATT 1994 and the GATS. The domestic regulatory measures adopted by Ghana and other countries to combat the spread of the Covid-19 pandemic have however also come at a huge economic cost to businesses.

New Regulations in Ghana in Response to Covid-19

In Ghana, the Imposition of Restrictions Act, 2020 (Act 1012) establishes the legal framework for the measures that have been adopted to combat the spread of the Covid-19 pandemic. Section 2(1) of Act 1012 states that "The President may, acting in accordance with the advice of relevant person or body, by Executive Instrument, impose restrictions specified in paragraphs (c), (d), and (e) of clause (4) of article 21 of the Constitution."

Article 21 (1) of the Constitution generally deals with provisions on fundamental freedoms like the freedoms of speech, assembly, association, and movement. Article 21 (4) however provides exceptions to the exercise of the freedoms listed in Article 21 (1). Specifically, paragraphs (c), (d), and (e) of Article 21 (4) provide that:

Nothing in, or done under the authority of, a law shall be held to be inconsistent with, or in contravention of, this article to the extent that the law in question makes provision

(c) for the imposition of restrictions that are reasonably required in the interest of defence, public safety, public health or the running of essential services, on the movement or residence within Ghana of any person or persons generally, or any class of persons; or

(d) for the imposition of restrictions on the freedom of entry into Ghana, or of movement in Ghana of a person who is not a citizen of Ghana; or

(e) that is reasonably required for the purpose of safeguarding the people of Ghana against the teaching or propagation of a doctrine which exhibits or encourages disrespect for the nationhood of Ghana, the national symbols and emblems, or incites hatred against other members of the community.

The authority granted the President under Act 1012 to impose restrictions on the freedoms of Ghanaians thus emanates from the above stated exceptions provided in Article 21 (4) of the Constitution. For example, in pursuance of this legal mandate, the President by Executive Instrument (E.I. 64), on 23 March 2020 imposed a ban on public gatherings including conferences, workshops, funerals, festivals, political rallies, sporting events, private parties, night clubs and event centres, and religious activities in churches, mosques, shrines and at crusades, conventions, pilgrimages and

other religious gatherings. Subsequent measures adopted on 30 March 2020 imposed a partial lockdown in some parts of the country for three weeks. While currently, the partial lockdown has long been lifted and the ban on public gatherings has been eased, restrictions on social gatherings and travel to and from the country persist.

Impact on Businesses and Compliance

The regulatory measures adopted by the Government to combat the spread of the pandemic have evidently had an impact on businesses in the country. The leisure and its allied industries in Ghana are, perhaps, the hardest hit. Industry operators in hotels, tourism, entertainment, recreation and sports have virtually ceased their operations due, among others, to social distancing rules and the closure of land, sea and air ports of entry into the country. For other sectors of the economy like banking, retailing and transportation, compliance with current measures are not that drastic in terms of impact on conduct of business. Compliance with hand-washing, social distancing, and nose mask rules requires making available the needed logistics to ensure conformity with current Covid-19 measures.

Admittedly, it has not been all doom and gloom for domestic businesses. Restrictions on social gatherings have, for instance, necessitated resilience in the uptake of e-commerce in Ghana. Educational institutions that have been slow to incorporate online learning in their engagement with students have been forced to move their lessons to virtual classrooms. The shortage of imported nose masks on the Ghanaian market has created a big market for local dressmakers to repurpose their operations to meet the huge domestic demand. Thus, while generally, the effect of the measures to combat the Covid-19 pandemic has had a negative economic impact, the silver lining in this dark cloud is the rediscovery of the domestic

capacity to competently produce products that hitherto would have been imported into the country. It is hoped that this resilience will not wane in the post-Covid-19 era but would become a catalyst for a resurgence of the industries that have had to bear the brunt of the necessary measures the Government has had to put into place to combat the pandemic.

3. THE NEW NORMAL FOR COMPLIANCE: CHANGING TRENDS FOR COMPLIANCE OFFICERS

By: **Daniel Boateng, Senior Compliance Officer, Ecobank Ghana**[3, 4]

There is no doubt that Covid-19 has created unimagined changes to the landscape of the compliance function as we know it. Prior to the pandemic, businesses focused on aligning their compliance programme objectives with laws, and local rules and regulations – a complex goal that may have taken months or years of planning and oversight to achieve. Seemingly overnight, the pandemic has thrust us into a new environment.

Our new challenge is to use deliberate steps and phases to build a bridge from the pandemic of today to a new and better compliance function for tomorrow.

3 Compliance and Covid-19 – Moving to a new normal.

4 COVID-19: How to mitigate the next phase of compliance risks.

The Role of Compliance in Critical Crises Management

1. Risk Assessment

As companies improvise new methods to keep going during this period, there is the need to understand the new risks that come along with the substitutes. For example, work from home policies can reduce employees' exposure to Covid-19 but come with it attendant risks such as data security, to fraudulent transactions, new safety procedures for service industry and factory workers with additional liability: Who will be responsible if an employee ignores them?

Compliance teams need to quickly pivot and consider the risks and challenges created by these rapid and radical changes. That is to:

- Perform a frequent and dynamic (non-formalistic) risk assessment in order to quickly understand the new circumstances and address the risks in a holistic way.
- Manage the changing risks through expedited actions (for example seeking relief from regulators, updating policies and controls and escalating issues.

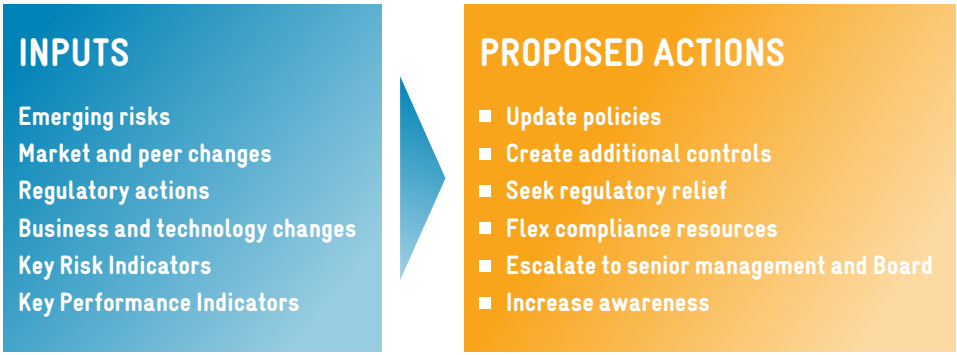
Steps for Managing Changing Risks:

- Perform frequent and dynamic risk assessment;
- Shift activities and focus to support a new normal;
- Refocus the medium-term compliance strategy;
- Manage compliance in a new remote working environment.

A new normal requires compliance to ensure that:

- Appropriate tools and access needed to perform key duties identified through the dynamic risk assessment are developed and maintain connectivity to each other and the business as co-location is not an option. (As working together or jointly is not possible because of social distancing).
- Productivity management is critical for key areas (transaction monitoring) where backlogs are high risk, and it is important to communicate with compliance teams to make sure they feel productive and that they are contributing, and also find ways to foster a sense of community and maintain employee morale.

Dynamic Risk Agenda (Example)



2. A Tailored Plan

The WHO has published industry-specific guidance for businesses[5] to determine whether they are allowed to open under governmental orders.

- Is re-opening consistent with applicable governmental orders?
- Can the business implement the recommended health and safety actions?
- Can the business conduct ongoing monitoring?

The following are recommended before allowing all employees back to site:

- Promote healthy hygiene practices such as hand washing and employees wearing a face mask;
- Intensify cleaning, disinfection, and ventilation in the workspace;
- Encourage social distancing and enhance spacing between employees via physical barriers, changing layout of workspaces, closing or limiting access to communal spaces, staggering shifts and breaks, and limiting large events;
- Consider modifying travel and commuting practices;
- Promote telework for employees in appropriate roles who do not live in the local area;
- Train all employees on health and safety protocols.

5 Country & Technical Guidance – Coronavirus disease (Covid-19)

3. Training

Companies are improvising new ways to do business and new ways to govern risk. HR teams are having to manage staff working from diverse locations and this creates challenges for training. Identifying training needs during this crisis is a key function which compliance can advise on. Training on new policies and delivering the required training materials for this purpose should be joint effort between HR and compliance for virtual presentation.

4. Above All, Leadership Matters

The quality and the ability of the compliance staff is key in the delivery of the compliance programme and the collaboration with management. Leadership skills are being tested by Covid-19 and compliance will have to assist HR, Legal, Security or Business operations and through this convince them to consult/engage closely with compliance.

The understanding of business operations by compliance officers is key in the realisation of this objective. Good interpersonal skills, communication/presentation skills and good grasp of legal or risk management are also vital in this new compliance function. Still, the fact remains that corporate ethics and compliance programmes are about getting large groups of people to behave in certain ways, so the enterprise can achieve certain business objectives, and that is something the compliance team should be equipped to manage.

Conclusion

A safe return to work will involve:

- Social distancing measures – Washing of Hands well, avoid contamination and cover your mouth and nose with tissue or sleeve when coughing or sneezing and discard used tissue immediately
- Anti-corruption strategies
- Reinforcing IT & Data Protection
- Operational Changes
- New ways of interaction with customers
- Information gathering and privacy
- Strategies to minimise AML and Fraud fueled by the following factors:
  - Online activities
  - Demand for and scarcity of certain goods
  - Payment methods
  - Economic downturn
  - Rising unemployment

4. DATA & APPLICATION SECURITY IN THE ERA OF A PANDEMIC: GOING BACK TO THE BASICS

By: **Frank Abdulai Iddrisu, Financial Crime Investigator, Fidelity Bank Ghana**

In 2017, The Economist published a story in which it metaphorically tagged data as **"The World's most precious and valuable resource and not oil which has over the years occupied the summit as the most valuable resource. I believe this phrase was in support of Clive Humby's indication that Data is the new oil of the 21st Century".** To some extent this adage looks exaggerated. However, if we look at the current global dependence on data and its impact on the global economy then I am tempted to follow the line of thought of those who believe that data is indeed the new oil of the 21st Century. Being that precious, information systems technocrats and technologists are compelled to keep this resource protected against unauthorised access, unauthorised modifications whilst ensuring continuous availability for persons, processes and technologies that are authorised to have access to such data in fulfillment of the Information Security's building blocks of Confidentiality, Integrity and Availability of data. In the context of Data and Application Security, most organisations have over the

years jumped into implementing controls in order to prevent their adversaries from being able to breach their systems and have access to their information assets especially the data that sits with them. To some extent, this approach has worked even though not to the desired expectation. Effective Data Privacy and Security regimes are built and aligned towards Governance, Risk and compliance frameworks. That is to say that organisations must ensure that their operations like the management of its data are aligned in a way to support the strategic goals of the entity. Also, of much relevance is the organisation's ability to identify its data risk exposures and possible opportunities by ensuring that a comprehensive IT Risk Management process exists and aligns with the overall Enterprise Risk Management Framework of the organisation. Notwithstanding the above, organisations must ensure that their activities meet the requirements of existing laws and regulations by ensuring that IT systems and the data that sits in those systems are used and secured properly.

In this piece, I will highlight on cybersecurity touchpoints or building blocks necessary for ensuring efficient safeguards for the protection of data, especially during a pandemic. To ensure privacy of data in the 21st Century, most data owners and entities jump into putting controls around data without recourse to the basics building blocks which is critical to safeguarding the "New Oil", Data. Two key fundamental processes necessary for ensuring a robust data security framework which has been neglected to the background leading to multiple data related breaches and compromise are amongst other things **Data Inventory and Data Classification.**

Data Inventory

For individual data users, businesses and governments to protect data the first touch point is the need to have a comprehensive **Data Inventory** of all of the entity's information assets. By implementing and having a robust inventory of data, data owners and organisations can understand where all its data is emanating from. In the 21st Century where data comes from multiple streams, Data Inventory ensure that the entry of data into an organisation is known. Inventory of data brings about a better understanding of the data in terms of organisation, accessibility and makes protection of such data easy. To have a proper inventory of our data regime, data owners must have data inventory checklist on its information assets on Operating Systems, Web Applications, Databases, Client Applications, Documents, Storage Media, Cloud Services, Unstructured Data(files) as well as integrated Third-Party Systems. By implementing an inventory of our data along the aforementioned information assets, data owners are able to tell where their data is residing either internally on Data centres, laptops, desktop computers, storage media, printers amongst others and or externally on through Cloud Services like Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), mobile devices, flash media etc.

As the need for data inventory becomes one of the integral building blocks of an effective data privacy and or information security measures, entities should now embrace the building of their Data Inventory as the first touchpoint to effectively design around securing that data. The best approach in building data inventory is centered along the following paradigms:

(a) Designing the scope of the data along the entity's requirements;

(b) Implementing the data inventory design and framework;

(c) Populating the data inventory; and

(d) Developing a process to maintain the data inventory.

Data Classification

Takeaways from data breaches of recent history has shown that individual data users, corporate organisations and governments has mostly used data without cognisance to an effective Data Classification regime. Such actions which leaves vulnerabilities and exploitable gaps are cut one of the major causes of data breaches of our time. Whenever data is classified, it improves efficiency in terms of its use and ability to protect the data owners "Crown Jewels" (its most critical Information Assets) across the enterprise. This in essence contributes immensely to the strengthening of the Risk Management framework and compliance systems in place. For instance, classifying data along lines like **RESTRICTED, CONFIDENTIAL, GENERAL BUSINESS RECORDS AND PUBLIC ACCESS DOCUMENTATION** minimises the risk of unauthorised access due to the defined access control measures at each level of the classification ladder. By classifying data, data owners get to know their data better before the issue of protecting such data then comes to the fore. When data categorisation using Data Inventory combined with Data Classification is carried out, entities are able to design effective data access policies rigorous enough to get good insights into their data which in turn results in a robust control framework for Data Privacy and Security.

There are three related topics which cannot be separated when it comes to Data: Privacy, Trust and Security. Preservation of data privacy and security rely mostly on trust. Whilst trust is built over time, data privacy and security dwells on the collection of data and its related subject's rights to the data along the following lines:

(a) Ensuring freedom from authorised access to private data;

(b) Preventing inappropriate use of data;

(c) Ensuring accuracy when collecting data about a person by technology;

(d) Ensuring the availability of data.

Protecting Our Data

Once inventory and classification are carried out, then the next thing that comes to mind in terms of importance is how to secure or protect that data. The ability to effectively protect data is based primarily on an understanding of the key states data can find itself. This brings about the building block of the entire information or data security i.e. confidentiality, integrity and availability known in tech parlance as the CIA TRIAD.

Confidentiality of Data

As the name suggests, confidentiality of data aims at preventing or at best minimising unauthorised access to data. With data confidentiality guaranteed, capturing network traffic, stealing user login credentials, social engineering users, eavesdropping on data or communication, sniffing on networks and attacks like escalating privileges are eliminated or reduced to insignificant margins.

To assure data confidentiality in an era like the global pandemic of the Covid-19, data owners, entities and governments must endeavour to implement countermeasures to counteract attempted confidentiality breaches some of which has been mentioned above. Notable amongst confidentiality countermeasures are Encryption of Data (data at rest, data in transit or data in use), ensuring network traffic padding, putting in place strict access control measures around the Principle of Least Privilege, strong authentication procedures, data classification and most importantly end user awareness training sessions.

Other equally important confidentiality concepts that entities must embrace as part of measures to protect their data against confidentiality breaches in these times are Criticality of the Data based on the Business Impact Analysis carried out, Data Isolation and Data Concealment amongst others.

Data Integrity

As data grows, stakeholders (internally or externally) who are not authorised to have access to such data attempt to alter or change the state of data without authorisation. The motivations of such individuals may vary but their goal is similar to gain unauthorised access to the data. To achieve their aim of altering data and compromising the integrity of that data, such individuals employ crude methods like the use of viruses, the throwing of logic bombs, intentional or errors in coding with intent to leave vulnerabilities as well as deliberate creation of application backdoors. As a result of the Covid-19 pandemic, there is a paradigm shift from brick and mortar office work attendance to the new normal of "working slim and thin". To counter the threat to Data Integrity during times like this where the data touchpoints and streams are numerous, data owners, corporate entities and governments need to ensure the implementation of rigorous

authentication procedures, deployment of Intrusion Detection Systems, Effective Data Encryption mechanisms, implementation of hash totals verifications, interface restrictions, input/output checks etc. To assure that integrity is not easily compromised, data owners can also look at other integrity concepts like authenticity, accountability, completeness and non-repudiation. Implementation of the above measures will eliminate and or minimise the successful attacks on data integrity along its three main perspectives namely:

(a) Preventing unauthorised subjects from making modifications to data;

(b) Preventing authorised subjects from making unauthorised modifications through omissions or mistakes;

(c) Maintaining the internal or external consistency of objects so that their data is correct and a true reflection of the real world.

Data Availability

The main objective of Data Availability is to ensure that data subjects are granted timely and uninterrupted access to data and information assets. For entities to ensure business continuity especially in a pandemic, it is important to put in place measures which counteract attacks on the availability of data and interruptions to other information assets. Measures such as designing intermediary delivery systems, the proper use of access control systems, effective monitoring and performance management. Also, of equal importance is the use of fault tolerance at various levels of access, storage, security etc. with the goal of eliminating Single Points of Failure to maintain availability of critical information systems is highly encouraged.

Understandably, it is better for data owners to understand their business well before implementing data privacy mechanisms through the tenets of cybersecurity/data security notably Confidentiality, Integrity and Availability. As individual data owners, entities and governments, it thus becomes very important to ensure a good balance and make the right choice on which of the three tenets of data security states should supersede the other in the fight against data breaches to ensure privacy because there is nothing like perfect security in place since increasing one item on the CIA TRIAD lowers the others.

To this end, as part of measures to ensure data privacy, entities should consider implementing the following data privacy mechanisms:

(a) **Defense-In-Depth (Layering):** Putting in place multiple defenses so that if one fails the others may succeed in preventing unauthorised access.

(b) **Abstraction:** This implies the grouping of similar data elements together.

(c) **Data Hiding:** This involves the placement of data in logical storage compartments that are not seen by data subjects except persons authorised to do so.

(d) **Encryption:** Hiding the meaning of data from unauthorised or unintended recipients.

The Use of Applications and its Related Data Privacy Concerns

Over the years, the protection of enterprise networks was solely based on deploying Firewalls and later Intrusion Detection Systems to filter inbound and outbound traffic to the enterprise. Such actions by IT Professional was aimed at protecting the applications that sit with the entities internally and externally from harm posed from staff or threats from the internet. With the addition of Demilitarised Zones (DMZs), IT environments and their implemented controls were very effective at ensuring that unauthorised persons did not gain access into IT systems from within and externally from the internet. Unfortunately, this pendulum has shifted and the attack surface of almost all entities has widened. The simple reason being that organisation's now carry out the publication of some of their sensitive applications to the internet. The main aim of pointing these applications to the internet are numerous but key amongst them is to enable the entities to provide high value business functions to their customer-base for example banking and E-commerce. Even though most organisations have perimeter defense mechanisms in place, the opening of their environments and applications to the internet makes their defenses obsolete, leaves them vulnerable and widens their attack surface. This assertion was confirmed by Gartner's report which stated that two thirds of all Web Applications are vulnerable and further corroborated by Veracode's 2017 state of Software Report which also indicated that 77 % of web applications have at least one security vulnerability.

To complement the effort of data owners and entities, I will be adding my thoughts and suggestions on Securing Web-based applications with the aim of complementing already existing perimeter security to enable us gain insight on some key controls needed over our enterprise data. Organisations nowadays allow their external stakeholders to have access to their internal applications using the web. This practice which increases

customer satisfaction on service delivery however opens the entities up for data breaches and malware-based attacks.

One other factor which contributes immensely to hacker's success with regards to data breaches and hacker activities is failure by organisations to adhere to basic security best practices. Failure to change default passwords of technology devices and applications, poor password ageing and complexity rules coupled with failure to update operating systems with current patches and hotfixes are just but a few best practices that are relegated to the background. A typical example of the impact of failing to patch information systems is the EthernalBlue of attack which the world got to know and identify as the WannaCry Ransomware. The impacts of such cybersecurity related breaches include but not limited to Financial Loss, interruption to business continuity, possible closure of business, unauthorised disclosure of business information and corporate secrets, reputational damage amongst others.

The Biggest Myth to Securing Web-based Applications

Unfortunately, most organisations conclude that because they have a network-based firewall in their IT infrastructure, it means their website and its applications are protected. These two are two different worlds apart. Unfortunately, perimeter firewalls which play a vital role in enterprise network security by filtering inbound and outbound traffic to their environments to prevent unauthorised access from hackers, disgruntled employees as well as mistakes from authorised employees has been found to be ineffective in securing web applications. The key risk indicator here is that because enterprises open to the world through the public internet it also means that Technology units allow all inbound traffic on port 80 (HTTP) and port 443 (HTTPS). The huge risk exposure that arises as a

result of allowing all traffic through these two main ports to the entire world is that traditional Network Firewalls cannot analyse traffic from the web applications which run on these ports. Inability to block traffic from script kiddies and hackers who may try to exploit web vulnerabilities through popular web-based attacks like Cross-Site Scripting and SQL Injection means there is the need to employ different strategies and tools to protect web-based applications to ensure their security. Let' look at Technology based approaches and or tools that will mitigate this huge risk exposure.

Web Application Firewalls (WAFs)

Mostly known in technology parlance as WAF, Web Application Firewalls are embedded with the ability to scrutinise and analyse web traffic both on the HTTP and HTTPS ports. One good thing about WAFs are their ability to identify hacker activities at the Application layer. Unfortunately, WAFs can detect only known web application vulnerabilities. This goes to explain why WAFs are only able to determine malicious activities based on preconfigured patterns. As a result, WAFs are unable to detect Zero-day Attacks. This is an indication that even though WAFs provide some level of comfort, they are not the ideal solution to securing web-based applications with security for entities.

To be able to secure web-based applications amid this Covid-19 pandemic, one key measure which will lessen this problem is the identification of vulnerabilities within these web applications before we think of securing them. To achieve this goal, technologists have deployed numerous strategies and tools notable amongst these include but not limited to

(a) Scanning web applications with a black box scanner;

(b) Doing a manual source code audit;

(c) Using an automated white box scanner to identify coding problems; or

(d) Carrying out standard Penetration Tests.

Web Vulnerability Scanner

Web application scanner also known as black box vulnerability scanner automatically scans websites, and the related applications therein where they can identify performance, security issues and vulnerabilities. The merit of using these tools stems from the fact that they automate almost all their detection processes. They are also very easy to use. The major advantage they have over white box scanners is that the latter demands advanced or technical know-how and access to the source code before scanning can be done. Having identified Web Vulnerability Scanners as a good resource, one biggest challenge is the ability to identify which one is good and fit for purpose. Making such choices is not easy because there are a lot of commercial and free versions available. The only good approach when making such choices is to test and identify which one is ideal for your environment. In order to make informed choices on which web vulnerability scanners are good for your business, let us look at some of the industry's best guidelines.

Using the Commercial or Free Version

The motivation to use a commercial or free version of a web application security scanner is borne out of numerous factors. However, because the use of non-commercial software applications has been known to give rise to security related problems, I will go ahead and suggest that we rele-

gate that option to the background and use commercial web application scanners which has numerous advantages like frequent updates, regular bug fixes, ease of use and consistent end user support. One key factor of very good web vulnerability scanners is their ability to crawl and scan the website and the applications that sit in it notwithstanding the underlying technologies there.

Unfortunately, most entities make the wrong decision in terms of their choice of a web vulnerability scanner based on results acquired through web ratings built over time.

The best approach in identifying the right web application security tool is to launch several security scans using different scanners against your web applications.

(a) **How will you identify your Web Application Attack Surfaces?** The ability of an automated black box scanner to detect all entry points and attack surfaces in a web application prior to an attack should inform your choice. The reason is simple. The ability of the crawler to detect vulnerability at the entry point is key. To determine which scanner can identify all your attack surface, a comparison should be done on the list of packages analysed, directories, and files and input parameters which each crawler identified. The scanner which identified the most is the ideal.

(b) **Identifying Web Application Vulnerabilities** – One other key performance measure entities must consider in their choice of a web security scanner is its ability to identify vulnerabilities. In some instances, the scanners give huge false positives ratio bigger than 60%. Such high false positive margins burdens professionals and make it difficult to identify which issue is a true one. Hence to make such choices, choose versions which give lower false positive rates with accurate predictions.

(c) **Automation is the Key** – Whilst the use of manual testing has become a thing of the past due to time and processing constraints automation has been identified to be the best approach due to its ability to process quicker and accuracy ratios. For instance, manual scans normally take days and sometimes weeks to complete a simple scan depending on the volume of data. Same data when subjected to automated analysis will have your job done in a matter of minutes to few hours with very high detection rate.

(d) **When should we use Web Vulnerability Scanners** – Ideally, the best approach in the usage of web application security scanners is to include them at every stage of the development and design of the web applications. Embedding them earlier makes the web applications more secure and reduces the cost to fix issues that may come up in future.

(e) **Identifying Logical Vulnerabilities** – As most Technology tools do, web application scanners exist to do the identification of technical vulnerabilities which could give rise to attacks like Cross-Site Scripting, SQL Injection, Remote Code Execution etc. To achieve optimum performance, automated web application security scanners should always be complemented with manual audits to aid in the identification of other vulnerabilities. This will ensure that we give business the assurance that web applications are working per their requirements.

(f) **Securing the Web Server** – A lot of technologies come to play in forming the basis of the web application farm. In a normal web application farm, there is the server which runs on open source (Apache) or Windows (IIS), web server operating system (Windows or Linux), Database (such as MySQL, MS SQL, Oracle) and network based services that allow updates to such websites (such as FTP or SFTP). Looking

at the above technology applications, it only reasons to secure each of them because the moment one of them is compromised or breached, then the attacker will gain access to the web application and retrieve data or temper with the integrity of data or even sometimes jeopardise availability. The best approach in solving such high-risk exposure is to use the security guidelines and best practices documentation that accompany such technologies. Alternatively, we could adopt some basic security guidelines which could be applied to any type of Server and Network based service.

1. Disabling of unnecessary functionalities

The more technologies, processes or functions that run on an information asset the wider its attack surface. This goes to confirm the technology paradigm that the fewer the functionalities or processes of a system the lesser the vulnerabilities and exploitable points. As data owners, it is advisable to disable and or switch off functions, services or processes that are not used by the web applications on your environment.

2. Limiting Secure Remote Access

As we make such security hardening efforts, it is necessary to ensure that any form of tunnelling through remote access is encrypted. Another point worth considering is to limit remote access to only few identified IPs.

3. Minimising Privileged Account Use

As we strive to achieve reasonable security, there is also the need to strike a good balance between security and the reality. Whilst the use of standard user credentials presents administrators with limited privileges, the use of administrative accounts too has got a huge disadvantage. To solve this anomaly, it is advisable to use standard user accounts to perform most tasks but to grant and use just-in-time administrative

privileges to perform tasks that require administrative rights. By such implementation strategies, we will be limiting the level of harm that could be done if one of the administrator accounts is taken over by hackers.

4. Access Rights

Based on the Principle of Least Privilege, it is advisable to analyse the available applications, the services running and all applications on your environment and grant privileges that are necessary for tasks to be performed and nothing beyond that. Such actions ensure greater level of confidentiality, integrity and availability of your restricted resources.

5. Segregate Development, Testing and Live Environments

To prevent unintentional error, omissions and/or malicious manipulations it is better to segregate the live environment from the development and test environments. For instance, developers in their efforts to make their code readable leave comments on blocks of code which explains their activities. Such comments easily leave traces to their work. This easily helps hackers to understand the logic behind the work which enables them to easily breach such environments.

6. Segregate Data

As enumerated during our discussion on the need to classify data, it is paramount that non-related information is not kept together. One of the best practices in industry is to ensure that the operating system and web files, i.e. the directory which is published on the web server should be on a separate drive from the operating system and log files. This will ensure that we are not exposing operating system files to hackers in case we are exploited over the web.

7. Regular Installation of Patches

As has always been trumpeted, installation of security patches and hotfixes is one very important security governance best practice mostly ignored by entities. By using the latest versions of an application and applying the vendor security patches and hotfixes, we ensure that the hacker community will find it difficult to exploit common and known vulnerabilities of the application in use.

8. Monitor and Audit the Server Logs

Log analysis enables administrators to know whatever is occurring on their environments. Even though difficult to perform, IT teams should cultivate the habit of analysing their server logs. By studying server logs, administrators can trace user behaviour and identify unusual behaviour when some occurs. Such trend analysis by the administrators minimises the risk exposure and makes it easier to contain breaches early in the event of an attack.

9. Use of Security Tools

As mentioned earlier on the importance of layering in protecting information assets same applies to web-based application security. Thus, apart from a web application security scanner, entities should also use the traditional network scanners and other related tools to scan the web server to ensure that all services which are running on the server are secure.

10. Never Go To Sleep

Going to sleep simply means that you are not ready to safeguard your web application services knowing very well that data lives 24/7. The best way out is consistently finding valuable information on the internet from several web application security blogs and websites. To be forewarned they say is to be forearmed. Being aware simply means we will be better prepared in the event of a breach.

Supply Chain amid a Pandemic

It is an established fact that operating in the global market offers numerous advantages. Notable amongst these advantages are resource optimisation, lower production and labour costs as well as ease of scaling operations. With the arrival of the Covid-19 pandemic with its attendant subset of lockdowns across nations with most airlines grounded and supply chains hugely impacted, there is the need to re-examine the status quo and take a paradigm shift as the global supply chain has been hit harder than anyone ever anticipated.

The pandemic having forced governments and businesses into the reality that sourcing supplies from other countries, which until now was the best practice, makes supply chains vulnerable. Why?

Typically, multinational companies set plants and offices across the globe with the aim of reducing human capital costs. However, by March 2020 multinational companies as well as their domestic stakeholders they serve had suffered lockdown restrictions, business closures and other economic hardships due to the global public health crisis caused by the Covid-19 pandemic. The impact globally can never be overemphasised. It is worth to mention however that the businesses that carry out importations are the ones most hit. This has created a bitter reality. This is how come the Chinese Effect needs to be looked at and possible solutions to prevent such global supply chain crisis from recurring.

The Chinese Effect

Statistics available to industry confirms that China is the biggest giant in the global supply chain economy due to the following reason:

(a) Seven out of 10 of the world's largest ports are in China;

(b) China produces 16 % of the world's output;

(c) China is America's third largest export market.

The basic reason why the Chinese are making such global strides is their highly skilled labour force and developed infrastructure. According to the Economist, "Half of the world's electronics manufacturing capacity is based in China". This directly gives China a big influence on the global economy and supply chain.

Mitigating Risks for Long Term Success

To safeguard supply chain problems as evidenced during this Covid-19 pandemic, businesses must make a paradigm shift and consider some alternatives to their supply chain regimes as noted below:

(a) **Shorten supply chains:** The best way to shorten supply chain crisis is near sourcing. This helps organisations to deliver suppliers quickly, automate processes and customise business units. This enables the organisations to become more resilient. Bearing in mind that businesses are struggling to meet their supply demands, the production of goods close to such businesses would have helped such entities to react faster when the need arises.

(b) **Building Redundancies:** The normal way of going about the supply chain business was not to stock inventory unnecessarily. Companies rather

opted for just-in-time production lines. Unfortunately, the Covid-19 pandemic has shown that just-in-time businesses cannot survive consistent demand increases. This is where the need now arises for companies to think of employing redundancies in their supply chain so that if one supplier fails, they will get reserves to replenish their supply and keep on running operations. This offers flexibility and multiple pathways to delivery.

(c) **Maintaining relationship with more suppliers:** Companies with single or fewer suppliers have few choices to make whenever the need arises. In times of difficulties or shortages companies with multiple suppliers gets the competitive edge.

Data Security Best Practices for mitigating Supply Chain Risk

1. Integrate Data Security into Supplier Governance

The saying that a "Chain is only as strong as its weakest link" comes to play when dealing with third parties. No matter how much security and data privacy controls an entity has in its environment if their supplier is vulnerable then you are equally exposed and vulnerable. To solve this menace, organisations must ensure accountability and respect for standards by its suppliers. To this end, entities must ensure that their suppliers have a good data security management programme to ensure that data they access, and process are done securely.

2. Define and classify suppliers and Data

The classification of critical suppliers should be matched with the relevant data made available to them. Understanding how, when and where an organisation's data sits with their suppliers will go a long way to determine if the third-party supplier has an effective regime to secure the data in

their possession. Failure to ensure strict adherence from your supplier may make you equally liable in the event of a breach.

3. Appointing a Data Protection Officer

The appointment of a Data Protection Officer (DPO) which is a trademark of the European Union's General Data Protection Regulation is an excellent approach at data governance. The existence of a DPO will ensure that strategies are put in place alongside data protection implementation management. In terms of getting the right person, the choice of candidate should be based on someone who understands data flows through suppliers, clients and business relationships.

4. Auditing Suppliers

Audit exist to give reasonable assurance to business owners and business stakeholders about the robustness of an organisation's control environment. It thus becomes very necessary for organisations overtime to carry out data privacy and security audits of their suppliers to assure themselves that the suppliers have effective controls measures and a security programme to mitigate the risk of a data breach. Failure to audit one's suppliers leaves the entity vulnerable if their suppliers are exposed.

5. ALIGNMENT OF PROGRAMMES TO REFLECT CURRENT BUSINESS TRENDS

By: **Patrick Kwadzie, Managing Director, Kenycorb**

Months passed, early in the year, the business stage has been drastic with changing trends, each month indicating a show of diversity. The pandemic has posed challenges to businesses globally. Many are already suffering financially to overcome all these burdens. Businesses are becoming more agile in customer satisfaction, embracing change, software applications, team spirit, motivation and trust, technical excellence, simplicity of work roles, self-renewing etc.

Technology is rapidly changing business platforms. In today's business, technological advancement is the main component as far as creativity and innovation in the marketplace is concerned. Companies that are not in the position to adopt new methods of technology have challenges being on the market. The stagnation of companies' research and innovation can make it belly-up. Innovation is a tool used to rout the competition. Different fields have different arch-rivals and so far, for a business to stay afloat

innovative new ideas are necessary. Can you embrace creativity and innovation in your company? Moreover, the answer to the above question gives you an idea of the plans that different businesses should have.

Creativity and innovation are part of business solutions which are the driving forces of the future of businesses. This requires strategy, planning and consultation that add to the best details and oriented result. In today's business world, creativity is part of the innovation process, doses of ideas and concepts should be encouraged by businesses. Generation of new ideas is the way forward post pandemic for businesses. Outcome of diversity is a larger perspective that will help in dealing with incoming challenges that the business will face. Productivity of business grows largely when new ideas are brought to bear. Workers are to be supported regularly to come up with new insight into various situations. The energy to motivate them places the business in a better position in the market. Analysis have shown periodically that despite innovation being the key driver of bottom-line of businesses, few businesses can make it happen. The phone and car markets, among others have seen dramatic innovations.

Notwithstanding the above, there will be debt after the pandemic and businesses need to be resilient in tapping into the opportunities they present, adopting changes, generating labour required for the continent, entering new markets for the world, upscaling and collaborating with industry players. Africa has a large landscape; this must be cultivated by irrigation ending up with agro processing and value addition. Support for small and medium enterprises (SMEs) is key, they must be properly equipped, network among themselves and be able to link to international markets to build support and excellence.

The big issues are, the health system has been exposed largely and government support is needed in curbing these drawbacks, inadequate human resource for health, protective equipment availability is still a problem, lack of adherence to pandemic protocol, poor level of individual responsibility in wearing of face mask, wavering capacity of health authorities to respond swiftly to pandemic issues.

6. MANAGING AND MAINTAINING SKILLED LABOUR IN CRISES PERIOD: THE CASE OF COVID-19

By: **Frank Owusu-Ansah, Former Manager for Central West Africa Area HSSE & Business Continuity, Maersk**[6, 7, 8, 9]

According to ILO Director General (Guy Ryder) "ILO standards provide a tried and tested foundation for policy responses that focus on businesses and their recovery from crises that is equitable and sustainable". This statement implies that all companies are required to have structured systems and processes in place to manage business against incidents and crises with their related impact on businesses and their workers (Labour). In economics, the term labour refers to manual labour and mental health also. Labour refers to "any physical or mental work which is undertaken for getting income and not for attaining pleasure".[10]

6 5 Experts on How to Manage Employees Through Difficult Times

7 Beyond hiring: How companies are reskilling to address talent gaps

8 Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently

9 To emerge stronger from the COVID_19 crisis, companies should start reskilling their workforces now. Protecting Business Data During a Natural Disaster: A Hurricane Irma Story

10 Labour: Meaning, Kinds and Importance | Economics

According to Kimberly Amadeo (Feb 2020), "Labour is the amount of physical, mental, and social effort used to produce goods and services in an economy. Labour supplies the expertise, manpower, and service needed to turn raw materials into finished products and services. This definition believes in four types of Labour such as Professional, Semi-skilled, Unskilled and Skilled Labour. Judging from ILO standards, companies and businesses are being encouraged to apply ISO 22301 (2019) requirements, plans and management systems to their businesses to help them deal with crises and handle disasters of all types.

For a company to manage and maintain skilled labour (is any worker who has special skill, training, knowledge, and ability in their work), through effective engagement with key staff, following key factors should be considered.

Business continuity Management (BCM) Framework

BCM or Business Continuity Planning (BCP) is the process of creating systems of prevention and recovery to deal with potential threats to a company. In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.

This BCM and BCP provide step-by-step processes which include developing a policy and strategies which define the annual programme scope, key parties; identifying key workers at all levels charged with responsibilities to handle companies' tasks and process implementation. The implementation should cover: Business impact assessment or analysis (comprises data the company holds, how it is collected, how it is accessed, which of those data or activities is considered most critical and what amount of downtime is acceptable and beyond which limit the company begins to record impact and losses of revenue because of actual business disruptive incident such as Covid-19).

The next is the Risk Assessment to identify potential effects of incidents and crises to propose required hierarchical controls. To ensure BCP control processes become effective, then companies are to test those processes before crises and ensure they remain dynamic to overcome actual pandemic effects like Covid-19. This crisis has forced companies and their workers to change the way they work almost overnight. The classical practical example of a strategy for companies to deal with crises as Covid-19 is the activation of BCPs to include specific strategies such as: **Work from home (WFH); Workload Distribution (WLD); and Relocation (RL).**

These days the common strategy adopted by Companies, States and Individuals across the world in managing Covid-19 risks is "Work from Home" – where the potential risk of company employees getting infected at work places is eliminated by sending workers home and providing them with internet connectivity to work and continue to serve their customers. It has taken companies with tested BCM/BCP processes to withstand the effects of Covid-19 better than those without it. Also, engagement with employees or workers during the Covid-19 period have been effective for those companies with BCP than those without it. Through BCM/BCP control processes, workers are effectively communicated to as tasks and strategies to manage effects of Covid-19 are shared.

Covid-19 had let to a series of publications by professionals, scholars, well known institutions and global world bodies such as WHO, ILO and McKinsey seeking to investigate, measure and analyse the impacts and effects of Covid-19 on workers and how companies be they small or big, medium or sole proprietorship are managing workers to sustain their business. Despite initial fears that the pressure would be too great for companies and states, realism has thought us to discover that this new way of working could be a blueprint for the long term.

According to Julia Fournier (Feb 2019), companies during Covid-19 are struggling to find skilled workers that will take their companies and organisations to the next level to support further growth. Also, the shortage of skilled workers has become a common concern for businesses across the globe. We therefore discuss the following key five pointers or best practices as measures helping companies to manage and sustain skilled labour or to handle shortages of skilled labour issues:

Firstly, **companies need to invest in training:** There is the need for companies to value available skilled labour as critical resources by providing training for existing workers. As companies invest in re-skilling of existing staff, they will be able to tailor workers skills set to fill the current or future gaps. Businesses are advised to also focus on hiring workers that will fit into the company's culture of doing business.

Secondly, **companies and business owners are required to prioritise skilled labour retention:** There is the need to motivate existing staff through various modes of recognition and reward schemes. Business owners should acknowledge a job well done by their hard-working workers that had sustained the company before Covid-19.

In recent McKinsey global survey, "85% of employees report being over-worked and under-appreciated." Effective managers keep their employees engaged by recognising their hard work. There are many fun ways to acknowledge workers success. Yum Brands, which owns Pizza Hut, KFC and Taco Bell, hands out recognition in the form of swag: rubber chickens, wind-up teeth, tiny racecars, and more, each little prize symbolising something unique that an employee has accomplished. Small businesses on a budget stick to the "employee of the week" tradition. Employers appreciation could be as simple as thanking someone at the end of the day. Just make sure you are providing positive feedback and encouragement to build

your team's confidence. Prioritising skilled labour in the company will also require introduction flexible working hours, increased leave pay, and days as done by top giants such as Facebook, Amazon and Apple.

Thirdly, **companies are to set employees up for success:** To lead effectively, employers must remove any roadblocks that would prevent an efficient team from doing their job successfully. Ask your team regularly what they need in order to do their jobs better or more efficiently. For instance, it might be helpful to open your restaurant an hour earlier to give the kitchen team more time to prep food. Or, maybe you add some time between salon appointments, so clients do not complain about having to wait for a chair. "Removing roadblocks tells your employees that you care about making their work experience the best it can be," writes the experts at Square.

Again, **communicate frequently:** today's performing workers value open, transparent leadership. Employers should share clearer business strategy and annual plans for guiding your organisation through the crises to help decrease anxiety and give your team a sense of direction. When employers assign a task, leaders should tell their team members why assigning it to them and how it will help achieve overall business results. If an employee asks for something you cannot say yes to, such as more paid leave or additional resources, leaders should explain reasons for saying no. There is really no such thing as overcommunication. "You may not know your strategy, but you can certainly talk about your values, priorities, and observations," **Jeanne DeWitt, the CRO of UberConference, told Harvard Business Review.**

Other measures include prioritising professional development of skilled labour: One of the benefits of working at a small business is that your team works more closely than at a big enterprise. "Junior-level" employees work side by side with managers and even you, the business owner. This

gives the owner the opportunity to invest time in mentoring his workers, no matter whether they are starting their first job out of college or learning the ropes as a first-time manager. Learn what it is that motivates each member of your team and take the time to invest in their specific goals. For instance, if you own a cafe, send your barista to a workshop on latte art or to learn the latest techniques. For managers who want to advance, consider paying for a certification course in project management. An investment in your workers is, inevitably, an investment in scaling and perfecting your business. It shows that business owner cares about the team, not just about the bottom line.

Tap into the Contingency Workforce: Business owners are required to adapt to the new trends and make use of skilled labour outside their companies by tapping into the increasing number of freelancers, contractors and consultants to save money and cost of expensive hiring processes associated with full time employees to be able to access highly skilled experts to fill gaps in operations at incredibly short notices.

Last but not the least, **employers must improve digitalisation and invest in IT infrastructures:** Covid-19 pandemic has proven that today and future business operations and continuity depends on digital evolution. This is because face-face service delivery is losing its value as online services are becoming the order of the day. For instance, customers are purchasing online, doctors are assessing patients via phone and internet, companies are recruiting via video links etc.

In conclusion, we are undoubtedly living in extraordinary times, never has freedom of physical movement of humanity been so constrained, whilst connectivity to the wider world remain so high. At these moments, uncertainty lingers like an unwelcome visitor as every family, society, organisations, and state wonder how the pandemic's consequences will affect

its future. People's response to the health crises facing all members of society has been at times diametrically opposite: some scholars terming this period as 'the age of wisdom'. Employers are highly required to engage labour both vertically & horizontally to ensure workers remain connected whiles working from home or virtually to keep them motivated, refreshed and be recognised for their inputs and as well be supported mentally at this critical moment. Employers should continue to find new ways of keeping workers skills relevant for their businesses future that include remote working, telecommunicating, permanent strategy to keep certain percentage of workforce at home now and post Covid-19. Again, companies must realise the challenge facing learning curves with new ways of doing business because of Covid-19. Employers must figure out how to lead teams virtually as they build social capital to maintain cohesion without benefits of informal coffee, lunch, or corridor chats and manage new skill sets.

Further Readings

Ethical Dilemmas in Times of Crisis.
Alliance for Integrity, 2020.

Accountability and the prevention of corruption in the allocation and distribution of emergency economic rescue packages in the context and aftermath of the Covid-19 pandemic.
United Nations Office on Drugs and Crime (UNODC), 2020.

No eXcuses! – Countering the 10 most common excuses for corrupt behaviour.
Alliance for Integrity, 2016.

Imprint

Published by:

Alliance for Integrity
c/o Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH
Blue Building II
10 Agbaamo Street
Airport Residential Area
P. O. Box KA 9698
Accra, Ghana

Layout:
Eva Hofmann, Katrin Straßburger
W4 Büro für Gestaltung, Frankfurt, Germany

As at:
November 2020

ISBN 978-3-948779-56-6