IIA Malaysia e-techline
October 2021 Issue 3/21

*CURRENT ISSUE*

## FUTURE READY: UPSKILLING TODAY FOR THE PROFESSION OF TOMORROW (BY CHARLIE T. WRIGHT)

The world is on the threshold of extraordinary technological change. Technological change is happening at a much faster pace than in the past. The pandemic, which underscored how important digital transformation is to the survival of most organizations, only accelerated this process.

The internal audit function's assurance over governance, risk, and control processes, its objectivity, and— most importantly — its insight and foresight are needed now more than ever.

While assurance services remain essential to internal audit's mission, mature internal audit functions go beyond traditional assurance by becoming "change agents," wading into less familiar and complex topics and risks, embracing technology, and being willing to experiment with new procedures and techniques in their own work.

"Internal auditors help the trains run on time. Change agents identify the need for and add new routes."

### Evolving Technology Landscape

Advances in IoT and AI have helped to mature the field of automation. Because scientists now have the capability to access and store more data related to IoT, robotics can be deployed to automate activities and processes. By applying AI, robots can be trained to perform certain tasks and ultimately learn and make improvements to their own software.

Easily automated tasks like information and data processing, data retrieval, administrative tasks, and some types of traditional manual labor will be reallocated to algorithms and machines, which will be putting in as many hours as humans.

### Workforce of the Future

The workforce of the future will look different, and changes are already underway.

For the workforce at large, competencies that are seen as the most valuable are also changing. While critical thinking and analysis, as well as problem solving, have been identified as highly prized "skill groups" on previous WEF surveys, an emerging skill group of importance is "self-management," which includes active learning, resilience, stress tolerance, and flexibility.

The top five overall skills for 2025 are Analytical thinking and innovation; Active learning and learning strategies; Complex problem solving; Critical thinking and analysis; Creativity, originality, and initiative.

This not only speaks to the need for employees to be lifelong learners, it also indicates that employers recognize the need for a workforce that can be adaptive and pivot in times of disruption and change.

Because internal audit—more than any other function—has the ability to spend dedicated, quality time understanding the many processes in an organization, auditors are in an excellent position to explain governance, risk management, and controls to management or governance groups, like the board audit committee or risk committee.

Further, internal audit can provide unique insight and perspective to management and the audit committee during business transformation. Practitioners have the opportunity to add value by consulting during the development of innovative processes and providing assurance of new processes.

**Becoming Future Ready: An Imperative for Internal Audit Workforce of the Future**

As the multiple technologies converge and mature over the next few years, internal auditors must ask themselves how disruptive innovation may change their organizations, the expectations of stakeholders, and the profession itself. If the work of internal audit is indeed to enhance and protect, then the function must be prepared to adapt to new risks and the new demands that come with them.

For instance, robotic process automation (RPA) is an area where many internal audit teams are gaining experience. RPA tools can be programmed to conduct tedious, multi-step processes, greatly increasing the amount of data that gets analyzed and freeing auditors to do work involving higher-level thinking.

AI and machine learning will also be very helpful as organizations learn to use technology for fraud analysis. Auditors can train these tools to look for patterns or anomalies in large amounts of data. They can also be used to provide insight into many other areas of the organization, such as for reputational analysis or to improve customer service.

Innovation presents both risks and rewards. According to IIA President and CEO Anthony J. Pugliese, there is an imperative for greater competencies and experience in technology. Internal auditors who cultivate the right skill sets, show creativity, and apply critical and analytical thinking, especially around disruptive technology, will be valuable partners and resources to help drive organizational initiatives and achieve objectives.

"There is tremendous potential for internal auditors to elevate themselves through innovation and collaboration, particularly in the areas of cybersecurity and technology," said Pugliese.

**What Internal Auditors should do?**

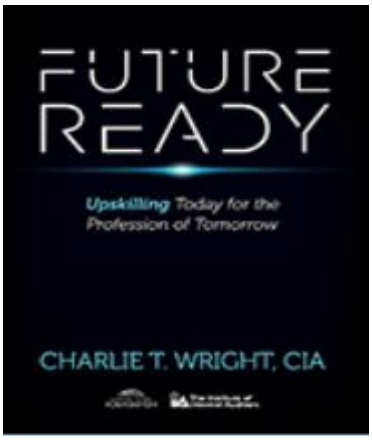
Internal auditors must be proactive in following trends and developments, perceiving how new technologies may apply to his or her industry and the risks and opportunities they present.

Internal auditors must prepare themselves and their internal audit function to meet these technological changes by developing new competencies and embracing new methods for getting the job done.

Internal auditors must not only communicate to the organization the risks and opportunities on the horizon, they must also make plain to the organization the value of the internal audit function on this journey.

By being future ready, internal auditors can help establish internal audit as an innovative profession and an indispensable part of the organization.

This would also enable internal auditors to perform its responsibilities with proficiency and due professional care through continuing professional development, in conforming with Standard 1200 and 1300 of the IPPF 2017 Edition.




**Reference:**

https://global.theiia.org/iiarf/Pages/Latest-Research-and-Products.aspx

*GOVERNANCE*

## SC URGES AUDITORS TO HEIGHTEN DILIGENCE, PROFESSIONALISM (BY NST BUSINESS)

On 29 July 2021, the Securities Commission's (SC) audit oversight board (AOB) urged auditors to be more vigilant and diligent in the execution of their duties during the current period of economic uncertainties due to the Covid-19 pandemic.

In its Annual Inspection Report 2020, the AOB noted that it is the responsibility of the directors and audit committee to assess their company's ability to continue as a going concern when preparing financial statements.

This responsibility extends to ensuring disclosure on significant judgements arrived at in order to reach those conclusions.

“Quality financial reporting that adheres to internationally recognised standards promote trust and confidence in the reliability of audited financial statements in Malaysia," said SC Chairman Datuk Syed Zaid Albar.

"Regular inspection programme helps to identify gaps and remediate any weaknesses within audit firms, and ensure the firms continue to strengthen their internal capacity and put in place adequate resources to promote high audit quality in Malaysia," said AOB executive director Alex Ooi.

SC further mentioned the qualifying audit firms are required to disclose information pertaining to their legal and governance structures measures to uphold audit quality and manage risks, as well as the measurements of audit quality indicators.

The audit committees of Public Interest Entities (PIEs) should take into consideration the information presented in the Annual Transparency Reports when deciding on the appointment and re-appointment of its auditors.

Directors and Audit Committees are also reminded of the need for vigilance in managing the expanding range of issues and risks, particularly those relating to complexities in financial reporting caused by Covid-19.

Lastly, the AOB also urges audit firms to invest adequate levels of training and resources to ensure that high-quality audits are carried out at all times, SC noted.

**What Internal Auditors should do?**

Standard 2110 Governance of the IPPF specifically identifies the internal audit activity’s responsibility for assessing and making appropriate recommendations to improve the organisation’s governance process.

Auditors are required to verify and challenge the appropriateness of the going concern assumptions, as well as the adequacy of the related disclosures.

It is even more important now for auditors to exercise appropriate professional scepticism in conducting their audits.


**Reference:**
https://www.nst.com.my/business/2021/07/712946/sc-urges-auditors-heighten-diligence-professionalism

*INTERNAL AUDIT*

## GETTING TO THE BOTTOM OF IT: WHY ROOT CAUSE ANALYSIS IS VITAL (BY HAL GARYN)

Root cause analysis is a way for internal auditors to get at the underlying reasons for why a particular condition exists.

Too often, an internal audit might identify areas of concern, such as control weaknesses, error conditions, process failings, risks not being adequately managed, and more. The audit might also propose recommendations for corrective actions. But what if the underlying reasons that cause the condition to exist go much deeper? Without root cause analysis, the reason for the condition could be misreported and the recommendations offered would not actually address the real issues.

- **Getting to the Source**

  Reporting on the cause that gives rise to a reportable condition is what internal auditors must do.

  Certainly, nearly every internal auditor is familiar with the common construct for writing good audit findings for their audit reports, known as the 5-C's: Condition, Criteria, Cause, Consequence, and Corrective Action. Cause is one of the key elements.

  The Chartered Institute of Internal Auditors has a great definition for root cause analysis. It reads, "Root cause analysis is a process for understanding what happened and solving a problem through looking back and drilling down to find out why it happened in the first place. Then, looking to rectify the issues so that it does not happen again, or reduce the likelihood that it will happen again."

- **Keep It Simple**

  There are a few formalized methodologies to root cause analysis, including fishbone diagrams, fault tree analysis, and other methods.

  Simplicity is often the best when complex issues are involved, and therefore the easiest thing to do to get at root cause is to employ the "five whys." Sometimes, we must keep digging at the "why" of something until we reach some point of discomfort.

- **Can It Be Easy to Get It Wrong?**

  Basically, doing root cause analysis is like working your way through a decision tree. As you answer each "why" question there are a number of possible paths or answers. It is through analysis of data and evidence, and most importantly wisdom and experience, that will guide you down the path to the likely potential root answer.

**What Internal Auditors should do?**

As The Institute of Internal Auditors articulates regarding using due professional care when doing root cause analysis in its Practice Guide 2320 – Analysis and Evaluation, "Root cause analyses enable internal auditors to add insights that improve the effectiveness and efficiency of the organization's governance, risk management, and control processes. However, these analyses also sometimes require extensive resources, such as time and subject matter expertise. Thus, when conducting a root cause analysis, internal auditors must exercise due professional care by considering effort in relation to the potential benefits."

**Reference:**

https://internalaudit360.com/getting-to-the-bottom-of-it-why-root-cause-analysis-is-vital/

*INFORMATION TECHNOLOGY*

## REINING IN CYBER RISK (AN UNDERSTANDING OF TECHNOLOGY, THIRD PARTIES, AND THE HUMAN FACTOR OF SECURITY IS VITAL TO PROTECTING THE ORGANISATION)

Year on year, cybersecurity has featured prominently on organisations' risk registers. Cyber risks are constantly evolving, while the level of harm they are capable of has grown to such an extent that they can pose an existential threat to businesses.

### Securing the Supply Change

Internal auditors should check how much of an IT application or programme is based on open-source software. The best way to gain assurance, is to attain a full inventory of software assets. This is to identify if there are any unpatched open-source vulnerabilities, and also identify if there are missing updates or patches to keep the organisation's IT infrastructure and data safe. Shawn Chaput says, there are several key risks that should be on internal audit's radar, particularly around the use of cloud services and other third-party IT service providers.

1) **Identity and Access Management**

   The organisations' increasing reliance on identity and access management programmes has become the most important risk since cloud computing came to prominence. As everyone moved to the cloud or started working from home, organisations had to adapt to this new 'zero trust' architecture where identity is the new perimeter. Even with authenticating individuals and hardware, phishing and spear-phishing appears to be highly effective in exploiting this decentralisation of cybersecurity and granting nefarious actors unauthorised access to company funds or administrative access to cloud infrastructure.

2) **Supplier Management**

   Chaput says the risk of a service provider having a breach — and what the organisation should do if that happens — should also be on every internal auditor's cybersecurity risk agenda. To mitigate the risk, the organisations need to consider how they should respond to the incident, how they should communicate the news internally and externally, and whether they need to switch providers immediately.

3) **Data Classification**

   Internal auditors should question the levels of security their organisations give to certain kinds of data they store in the cloud. Many of clients who use cloud service providers say 'we protect all of our data as though it is the highest sensitivity' instead of classifying and labelling the data to allow it to have different levels of security controls.

4) **Talent Deficiencies**

   Ultimately, the fact that the cloud encompasses so many different technologies and services lends itself to another difficult risk for organisations to manage — finding and retaining IT staff familiar with constantly evolving technology. It used to be that to hire an individual based on their experience with a specific enterprise resource planning package, like SAP, or with some deep technical knowledge in a vendor platform like Cisco routing and switching.

### Get to Know the Technology Team

Internal auditors need to understand how these functions work, and they need to form a deep and trusting relationship with them to provide the appropriate level of assurance to the company that cybersecurity risks are being properly identified, prioritised, and mitigated. The internal audit has a strong role to play in establishing a solid response to cybersecurity risks.

Working alongside other assurance functions such as enterprise risk management (ERM) and, in his organisation, the cyber counsel. The organisations should establish and regularly review and update a cybersecurity risk framework, as well as examine the governance around the organisation's IT architecture and cybersecurity risks.

Likewise, if the profession is to help mitigate cybersecurity risks, it needs to know how the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) identify and mitigate these challenges and the approach they take to cyber risk management.

It is important for internal audit to understand the company's ERM programme, as well as understand where cybersecurity appears in the organisation's risk heat map. If internal audit is to understand technological risks, it has to understand technology.

**Faults on the Front Line**

Not all cybersecurity risks are technologically complicated. Indeed, the most often cited cybersecurity threat is from people, usually employees who is ignoring protocols or using the technology incorrectly.

Other experts agree that effective cybersecurity requires a strong "human touch." George Finney, Chief Security Officer says forming strong relationships more widely is vital if internal audit is going to play a key role in improving cybersecurity risk management and resilience.

However, if end users perceive policies as impacting their ability to get their job done, it's highly likely that they will attempt to work around the controls — not in a way to try and steal data or with any bad intention, but in fact to help the company, which puts security teams at a disadvantage." To address this problem, Guntrip says organisations should look to implement solutions that are "invisible" to end users.

**Partnering With Business Units**

It is also important for internal audit to develop relationships with department heads. If other department heads invite internal audit in to help with project reviews and to test risk controls, it sends a signal throughout the rest of the organisation that the audit function is one to call in a crisis — and that is a huge win. In fact, Finney says one of the cornerstones to any successful cybersecurity risk management policy is to get enterprisewide buy-in.

If you approach audits from a positive perspective — rather than from the 'internal policeman' approach — you get fuller engagement. Since cybersecurity is such a key risk to every organisation, it should be used as an opportunity by internal audit to push for executive support for initiatives that you know need to happen. In addition, when the internal audit assesses cybersecurity policies and controls in different areas of the organisation, it presents an opportunity to build relationships with clients.

**An Ongoing Threat**

Recent high-profile hacks and other IT security disasters should remind internal audit to widen its focus away from just the technology to other equally dangerous aspects of cybersecurity risk, such as policy noncompliance among employees or lack of third-party cyber-resiliency.

Internal audit can help bind together different parts of the enterprise to form a unified front against cyber threats and help keep the organisation protected from would-be attackers.

**What Internal Auditors should do?**

Standard 2120 Risk Management of the IPPF 2017 Edition specifically identifies the internal audit activity's responsibility for evaluate the effectiveness and contribute to the improvement of risk management processes.

Internal auditor must understand what those charged with cybersecurity are doing to manage risks, what measures business unit leaders are taking, how well employees are complying with established procedures, and where vulnerabilities may lie in the extended enterprise.


**Reference:**
https://iaonline.theiia.org/2021/Pages/Reining-in-Cyber-Risk.aspx

If you missed out the previous issues of e-techline, you may visit our website at https://iiam.com.my/technical-qa-services/e-techline/.

***GLOBAL PERSPECTIVES AND INSIGHTS***

**REMOTE AUDITING: CHALLENGES, RISKS, FRAUD, TECHNOLOGY, AND STAFF MORALE**

**Reference:**
https://global.theiia.org/knowledge/Public%20Documents/GPI-2021-Remote-Auditing-English.pdf

***GLOBAL KNOWLEDGE BRIEF***

**AUDITING RISK CULTURE: A PRACTICAL GUIDE**

**Reference:**
https://global.theiia.org/knowledge/Public%20Documents/GKB-Auditing-Risk-Culture-IIA-Australia.pdf

***IIA PRACTICE GUIDE***

**GLOBAL TECHNOLOGY AUDIT GUIDE: AUDITING IDENTITY AND ACCESS MANAGEMENT**

**Reference:**
Pages - GTAG: Auditing Identity and Access Management (theiia.org)

***BOARD MEMBER RESOURCE EXCHANGE***

**INTERNAL AUDIT'S ROLE IN ESG REPORTING: INDEPENDENT ASSURANCE IS CRITICAL TO EFFECTIVE SUSTAINABILITY REPORTING**

**Reference:**
https://global.theiia.org/about/about-internal-auditing/Public%20Documents/White-Paper-Internal-Audits-Role-in-ESG-Reporting.pdf