IIA Malaysia e-techline
December 2020 Issue 6/20

CURRENT ISSUE

MOST WORRISOME RISKS FOR COMPANIES IN THE POST-COVID WORLD AND WHAT COMPANIES CAN DO TO REMAIN RESILIENT

The COVID-19 pandemic has sent ripples through global economies, affecting lives and livelihoods. In a recent "COVID-19 Risks Outlook report" released by the World Economic Forum (WEF), the results revealed that a prolonged recession of the global economy is still the 'most worrisome' fallout for risk professionals.

On top of that, they were also concerned about other far-reaching societal, technological, geopolitical and environmental implications brought about by the pandemic. Let take a deeper dive into the top three categories of risks being – **economic**, **technology** and **geopolitical** as well as and examine steps companies can take to mitigate them.

1) **Protracted Disruptions of Global Supply Chains** (Economic)

A recent report published by DHL and the Business Continuity Institute (BCI) summarises a few steps companies should consider taking:

- ✓ Conduct deeper due diligence of suppliers beyond tier 1, such as determining their location, assessing their financial and operational health, and obtaining their business continuity plans. Good practice suggests that such due diligence should be done in the pre-contract phase so organisations can be aware of any potential risks before engaging suppliers (e.g. an over-reliance on a particular geography).
- ✓ Invest in specialised supply chain tools and leveraging on AI and supply chain mapping software that can dramatically improve visibility across the end-to-end supply chain.
- ✓ Diversify its supplier base, particularly to seek for local sources if possible.

2) **Cyberattacks and Data Fraud** (Technological)

The widespread and accelerated adoption of technology to enable the shift to work-from-home (WFH) during the pandemic has greatly increased the risks of businesses to cyberattacks and exposure of sensitive information, amongst others. Here are some initial areas that companies can address:

- ✓ Conduct a thorough review of new vectors for cyberattacks that can result from WFH arrangements and whether the company's existing tools and policies are in place to protect against them.
- ✓ Safeguarding measures include implementing VPN and multi-factor authentication, revisiting safe remote working protocols and training employees on guarding against malware or phishing threats.
- ✓ The companies should assess whether the scale of current security measures is sufficient to cover the increased activity on the digital platforms they operate (e.g. increased activity on customer service chat application or an online booking system).
- ✓ Test any security plans or measures implemented for managing technology and cybersecurity risks for efficacy and to close any vulnerabilities. Simulate cyber threats to assess the adequacy and effectiveness of their risk response as well as staff preparedness.
- ✓ Step up monitoring on areas with increased activity or exposure, such as customer-facing networks, collaboration tools, etc. to ensure early detection of potential data-loss incidents and malware threats before they are full-blown.

3) **Tighter Restriction on the Cross-Border Movement of People and Goods** (Geopolitical)

In our globalised world today, international trade and investments have always relied on the cross-border mobility of individuals. As countries worldwide impose sweeping travel restrictions, the only cross-border travel that remains today is the movement of "essential" workers and specially-created travel corridors with quarantine-free mobility between certain countries.

While the most direct casualties are industries such as tourism, aviation and education, almost all sectors have been affected by the loss of access to the global talent pool.

In these unusual circumstances where WFH is likely to become the norm, companies can consider investing in the following in the long recovery ahead:

- ✓ Take a deliberate effort to establish and maintain a positive culture among a remote workforce. For example, to recreate the 'watercooler effect' in physical office spaces by setting up a company online chat tool where employees can discuss topics of any interest.
- ✓ Invest in protecting the mental health of your employees. The pandemic will continue to take a toll on mental health due to social isolation, financial worries, and the strain of adapting to remote work and home schooling. This could well affect work productivity and morale. It would thus be worthwhile investing in initiatives such as establishing free counselling hotlines, training employees to provide peer counselling, or paying for subscriptions to wellness apps.

What Internal Auditors should do?

Internal auditors to collaborate with the risk management department to identify and anticipate the emerging risks and respond to change, which will ultimately be able to build a more resilient operating model for the business. Internal auditors also need to embrace the greater innovation and technological adoption during and after the COVID-19 pandemic era.

Reference:

https://bursasustain.bursamalaysia.com/droplet-details/corporate-governance/most-worrisome-risks-for-companies-in-the-post-covid-world-and-what-companies-can-do-to-remain-resilient

INTERNAL AUDIT

4 TIPS FOR CONDUCTING VIRTUAL INTERNAL AUDITS

As COVID-19 rages on, companies continue to go digital. With remote work and travel restriction limiting mobility in many parts of the world, audit leaders are in turn finding immense value in the benefits of going digital in terms of speed, broader stakeholder involvement and robust reporting.

Here are the 4 tips on how to conduct successful audits in a remote work environment.

1) Continually Reassess Priorities

Continually review and adjust your annual audit plan according to business conditions, management requests and industry/ market dynamics. Align your team and key stakeholders on the critical and urgent risks right now and focus your attention on auditing the areas and procedures that will protect the business the most.

2) **Invest In Tools That Foster Connectedness And Collaboration**

Videoconferencing with screen sharing, recorded meetings and whiteboard capabilities can remove distance barriers and enable auditors to review procedures or documents together, in real time.

These tools also help auditors pick up on helpful visual cues typically observed on-site during live interviews. And speaking "face-to-face" helps auditors build rapport and trust with audit clients.

3) **Ensure Your Team and Audit Clients Are Set Up for Success**

A successful remote audit requires quite a bit of preparation work and expectation setting. We can start off by providing guidance on how to effectively work remotely. Make sure all audit clients and stakeholders are aligned on the virtual audit process, including turnaround timelines, what is expected of them and what they need to share before and after the meetings. Let the audit clients know in advance what your priorities are as part of the audit, the specific documentation they will need to provide and what will be covered during the meeting to allow them ample time to prepare.

4) **Say Goodbye to Manual Processes and Spreadsheets**

A cloud-based automated system creates a repository of all audit-related information and easily shares it with all involved parties, so no one has to chase down needed information.

Audit and assurance professionals can be confident based they are basing decisions off the most up-to-date data and can assign colleagues tasks and reminders, so nothing falls through the cracks.

With advanced analytics and instant visual depictions of data, these tools also eliminate tedious manual reporting, accelerate the audit cycle and free up time for teams to focus on improving audit strategies.

What Internal Auditors should do?

During the current or post COVID-19 pandemic, the internal auditors to start adapting the new norm of remote auditing by learning on how to leverage technology tools in conducting an audit.

Reference:

https://www.corporatecomplianceinsights.com/virtual-internal-audits-pandemic/

HOW TO AUDIT FOR CONFLICTS OF INTEREST

The conflicts of interest can be difficult to identify, manage and audit. Furthermore, there are various types of actual, potential, and perceived conflicts of interest. Some conflicts may involve an outside job or serve in another organisation. Others may result from having personal and other types of relations with different stakeholders, which could influence decision-making. Thus, internal auditors should consider several aspects when designing their approach to conflict-of-interest audits.

1) **Clear Guidance:** Organisations need to define what constitutes a conflict of interest and communicate that such conflicts are not allowed. Organisations can do this by adopting an ethics policy, defining organisational values, establishing behavioral principles, or simply notifying employees. Providing guidance on conflicts of interest and how

... 3

to adequately communicate expectations to employees can be a good starting place for internal auditors to build their audit approach.

2) **Organisational Setup:** Businesses can organise duties related to managing conflicts of interest in different ways, as they can take various forms. For examples, the human resources (HR) department will take the lead. However, additional departments, such as ethics, compliance, or legal functions, are commonly involved in managing conflicts of interest. By doing so, it requires the organisation to clearly define roles and responsibilities, maintain adequate segregation of duties, exchange relevant data and information and collaborate across functions.

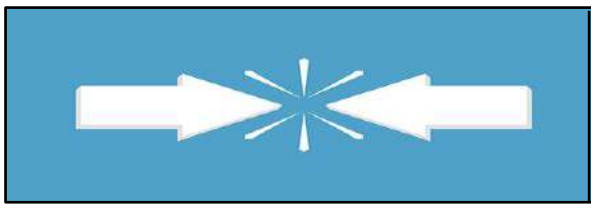
3) **Preventive Controls:** Internal auditors to identify which controls exist around conflicts of interest, which including (1) Processes for obtaining information from potential new employees and business partners. (2) "Know your business partner" procedures. (3) Conflict-of-interest clauses in employment agreements. (4) Noncompete clauses. (5) Conflict of interest management. (6) Prescribed response measures. (7) Gift register and policy. (8) Conflict-of-interest reporting. (9) Outside employment approval. (10) Documentation. (11) Training. (12) Past lessons.

4) **Risk Acceptance:** Organisations should consider establishing a risk acceptance process to determine whether some conflicts of interest are acceptable. The organisation needs to assess if the risk is acceptable from a risk appetite point of view. For those with highly sensitive and confidential risk acceptance topics could be dealt with by an organisational body such as a designated committee which consists of HR, ethics, compliance, legal, risk management, and internal audit etc.

5) **Post-transaction Controls:** Controls such as (1) Tools and records for obtaining information on how the reported conflict of interest was address. (2) Documented background checks on employees. (3) Documentation of design changes from previous control. (4) Effectiveness assessment of new, additional, changed and compensating controls to mitigate conflict-of-interest risks. (5) Documented follow-up of any compensating measures taken for cases of risk acceptance. The above controls could provide auditors insights on how a conflict of interest was identified as well as recognition and management process steps taken, outcomes achieved and follow-up results.

What Internal Auditors should do?

To provide awareness and guidance on the conflicts of interest and how to adequately communicate expectations to employees as well as organisation.



Reference:

https://iaonline.theiia.org/2020/Pages/How-to-Audit-for-Conflicts-of-Interest.aspx

LATEST DEVELOPMENT OF IIA GLOBAL

GOVERNANCE

TONE AT THE TOP – COVID-19 LESSONS LEARNED AND THRIVING IN THE NEW NORMAL

The global turmoil created by COVID-19 continues to impose itself in myriad ways on business operations, workplace culture, and in the larger societal context. As we surpass the half-year mark of restricted interaction, work-from-home scenarios, and heightened crisis management, the possible long-term impacts of the pandemic are becoming clearer.

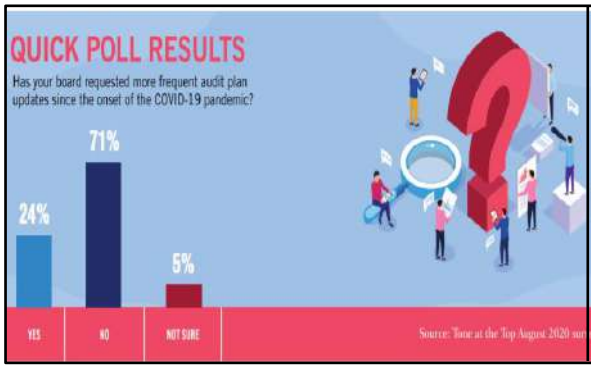
The pandemic has clearly accelerated the digital revolution. A recently published study from the IBM Institute for Business Value found nearly six in 10 C-suite executives report their organisations have sped up digital transformations, with perceived barriers such as technology immaturity and employee opposition falling away. This affirms similar reports from risk leaders interviewed for The IIA's OnRisk 2021 report, which is published in early November. One C-suite executive related, "It's amazing how [disruptive innovation] is driven by this virus. We're advancing the technology scale a few years in just a few months."

Beyond short-term tactics and technology shifts, organisations are beginning to explore how disruptions created by pandemic responses, such as remote workforces, greater emphasis on e-commerce, and changing consumer habits, will permanently change operations and strategies.

As the haze of the initial crisis response clears and organisations begin to assess the landscape of the new normal, repercussions from COVID-19 generally will fall into four categories:

1. Those we know about that are happening now, such as heightened cybersecurity risks created by vulnerable home-worksites.
2. Those we can reasonably anticipate, such as changing workplace cultures and talent management strategies.
3. Those we do not know about that are happening now.
4. Those we cannot reasonably anticipate.

COVID-19's impact on society generally raises a risk area that arguably will create the most significant long-term impact on business and economies — how the pandemic will influence the social contract. The concept of social contracts — an implicit agreement among the members of a society to cooperate for social benefits — invariably will be questioned and tested as the pandemic amplifies the divide between the haves and the have-nots.



What Internal Auditors should do?

Internal auditors should be flexible and dynamic in seizing the opportunity to understand and shore up weak area, leverage strengths and improving the use of technology.

Reference:

https://dl.theiia.org/AECPublic/Tone-at-the-Top-October-2020.pdf

RISK MANAGEMENT

ONRISK 2021 REPORT

The 11 risks were selected from a wide assortment that are likely to affect organisations in 2021 and vetted through in-depth interviews with board members, management, and CAEs. Some of the risks are unchanged from the inaugural OnRisk report, some descriptions have been updated, and other risks are new to the list. These risks should be relevant universally, regardless of an organisation's size, industry, complexity, or type. However, this list does not cover all the significant risks in every organisation; risks excluded from this analysis may have particular relevance — even significant relevance — to organisations, depending on their specific circumstances.

1. **CYBERSECURITY**: The growing sophistication and variety of cyberattacks continue to wreak havoc on organisations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organisations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

2. **THIRD PARTY**: For an organisation to be successful, it has to maintain healthy and fruitful relationships with its external business partnerships and vendors. This risk examines organisations' abilities to select and monitor third-party relationships.

3. **BOARD INFORMATION**: As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision-making. This risk examines whether boards feel confident that they are receiving complete, timely, transparent, accurate, and relevant information.

4. **SUSTAINABILITY**: The growth of environmental, social, and governance (ESG) awareness increasingly influences organisational decision-making. This risk examines organisations' abilities to establish strategies to address long-term sustainability issues.

5. **DISRUPTIVE INNOVATION**: We are in an era of innovative business models, fueled by disruptive technologies. This risk examines whether organisations are prepared to adapt to and/or capitalise on disruption.

6. **ECONOMIC AND POLITICAL VOLATILITY**: National elections, multinational trade agreements, new or extended protectionary tariffs, and uncertainty around the timing of routine macroeconomic cycles all create volatility in the markets in which organisations operate. This risk examines the challenges and uncertainties organisations face in a dynamic and potentially volatile economic and political environment.

7. **ORGANISATIONAL GOVERNANCE**: Governance encompasses all aspects of how an organisation is directed and managed: the system of rules, practices, processes, and controls by which it operates. This risk examines whether organisations' governance assists or hinders the achievement of objectives.

8. **DATA GOVERNANCE**: Organisations' reliance on data is expanding exponentially, complicated by advances in technology and changes in regulations. This risk examines organisations' overall strategic management of data: its collection, use, storage, security and disposition.

9. **TALENT MANAGEMENT**: A growing gig economy, dynamic labour conditions, and the continuing impact of digitalisation are redefining how work gets done. This risk examines challenges organisations face in identifying, acquiring, upskilling and retaining the right talent to achieve their objectives.

... 6

10. **CULTURE**: "The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organisations understand, monitor, and manage the tone, incentives, and actions that drive the desired behavior.

11. **BUSINESS CONTINUITY AND CRISIS MANAGEMENT**: Organisations face significant existential challenges, from cyber breaches and pandemics to reputational scandals and succession planning. This risk examines organisations' abilities to prepare, react, respond, and recover.

What Internal Auditors should do?

Internal auditors should be aligning of these players' views on risk knowledge, capability, and relevance toward achieving strong risk management in support of effective governance.

Reference:

https://dl.theiia.org/Documents/OnRisk-2021-Report.pdf

INTERNAL AUDIT

INTRODUCING THE IIA'S COMPETENCY FRAMEWORK

The IIA's Internal Audit Competency Framework© provides a clear and concise professional development plan for internal auditors at every level of their career. The framework defines four knowledge areas focused on various Standards, situationally specific functions, and key proficiencies, with three distinct competency levels that progress from general awareness to applied knowledge, and finally, expert practitioner.

The comprehensive and concurrent strategy defines and delivers the knowledge and skills necessary to navigate a successful career in internal auditing focused on best practices and practical applications.

The framework also serves as an effective onboarding tool or a multi-year training plan that helps chief audit executives and leaders continuously identify and fill skill gaps within the audit function.

What Internal Auditors should do?

Internal auditors should leverage this framework for their competency development growth and navigate a successful career in internal auditing.

Reference:

https://global.theiia.org/standards-guidance/Pages/Internal-Audit-Competency-Framework.aspx

GLOBAL KNOWLEDGE BRIEF

IT SECURITY IN A WORK-FROM-HOME ENVIRONMENT

IT departments within organisations face a constant challenge in dealing with an ever-evolving threat landscape involving the technology used by its employees. The COVID-19 pandemic forced enormous changes in the modern workplace that made this challenge substantially more complex.

Due to Pandemic COVID-19, workers were suddenly displaced from their offices to their homes as organisations struggled to stay in operation. These employees, some of whom were not tech savvy, suddenly found they needed to become their own IT support desk, setting up their home office. At the same time, they were increasing their organisations' exposure to potential risk in the process.

Biggest Threat Involves Devices

The sudden onset of the COVID-19 pandemic caused unprecedented upheaval in workplaces globally as organisations shuttered offices and sent employees to their homes to work.

The biggest threat involves devices, such as laptops and printers, now being used by workers on their home networks. Although they continue to work with corporate assets, many workers are now reliant on their home network controls. To complicate matters further, employee home networks often are shared with other members of the family.

If the company has a bring-your-own-device policy, the employee may be accessing company assets on a home computer, but the policy may not address home networks linked to the company's network through a VPN.

Home modems, routers and printers often still using their default passwords also are vulnerable. Many employees on their own download software without their IT departments' knowledge or consent – "shadow IT" such as Zoom or other web conferencing platforms, or apps needed to do their jobs. This exposes their companies to potential security issues.

The advantage of large companies is they can afford to give employees critical security awareness training. These companies also can assign a computer to an employee for home or office use. However, for the smaller companies find it challenging to educate employees about security awareness and/or keep an effective device inventory. If a company struggles to maintain the resources to track device capability in such detail, the potential for risk significantly increases.

Legacy companies which either are in the process of digital transformation or have just gone through it are also particularly vulnerable to security issues. These companies often make quick assumptions about the technology and assumptions about cloud security, in the rush to make the transformation. A company's cloud system may be secure, but that does not mean the applications the company is using and the software behind them are secure.

Dealing with all these new responsibilities can be frustrating for employees, who must address concerns and resolve problems for which they may not be trained or may not have time to solve in an already crowded workday. In addition, IT assistance is often not readily available.

Building A Plan - Companies Need to Think Holistically

Across the entire organisation, to build an effective culture of security. Visualise it as Four Rings of Security which consists of Database, Application, Network/ infrastructure, and User. The database is at the center, surrounded by the application used to interface with the data, which is in turn surrounded by the network/

... 8

infrastructure that connects the application to the database.

Meanwhile, organisations need to ensure controls are in place across all four rings, especially in this new environment. Importantly, in building an effective security culture, the tone starts at the top and needs to flow through the organisation.

Security Starts with Employees

Employees need to understand they have a vital role in their company's security environment because they have become front line defenders. This extends to family members as well because they have become users of the corporate network in the new environment.

Some common tips for users and family members that will make home computers and home networks more secure include:

- Run computers at the user level, which restricts access to the operating system, rather than at the administrator level.
- Do not share passwords or write them down.
- Use complex passwords or passphrases (Length offers more security than complexity).
- Use a password manager.
- Use multi-factor authentication (MFA) for both personal use and when using company devices.
- Lock the computer whenever you step away from it.
- Watch out for social engineering scams — someone claiming to be a higher-up in the organisation, someone asking the employee to circumvent established processes.
- Secure home wireless networks.

All steps emphasise the importance of educating employees and raising awareness about the importance of IT security as well as providing comprehensive help-desk support for employees.

What Employers should do – External, Internal Threats Need to Be Addressed

Security is a continuing responsibility, not something suddenly taken on because employees are working from home. This is especially important because threats are constantly evolving. A point to keep in mind, while the external threats make the news, a strong security program also addresses internal threats.

Many companies build security into existing company initiatives because security has a significant impact on company culture. If company policies and procedures are updated annually, the same should be true of security policies. The company should be the driver of change, not the employee.

What Internal Auditors should do?

Internal Auditor, especially IT Audit, they should take actions to educate employees and raising awareness about the importance of IT Security, as well as providing comprehensive help-desk support for employees.

Reference:

https://global.theiia.org/member-resources/Global%20Documents/GKB-Security-in-a-Work-From-Home.pdf

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/.