IA in the Age of Cyber, Big Data and Smart Devices

By Eric Lim and Teng Hui Yun

Disruptive changes in this digitalisation age are transforming business models, redefining and changing basis of competition in the new economy and these have brought about emerging risks and to some extent, opportunities. The following are some of the developments organisations encounter today:

a. Unprecedented large volume of data
b. Internet of Things enable connectivity to change the business models, delivery channels and business processes from end-to-end
c. Cybersecurity attacks getting sophisticated and cyber risk is amongst the top risk threats
d. New technologies such as machine learning, blockchain, etc. are now emerging rapidly

Technology risks are growing and becoming increasingly more complex. As such, the board is putting technology risks as amongst the highest of their concerns. Internal auditors are also expected to provide assurance that the organisations are managing the technology risks.

The CBOK report released by The Institute of Internal Auditors Research Foundation (IIARF) on "Navigating Technology's Top 10 Risks[1]" gives practical advice to the internal auditors in two categories. Firstly, the key questions for internal audit could ask about the risks and secondly, the key activities that are proposed for internal audit to perform for each risk. The top 10 risks identified in the CBOK survey are cybersecurity, information security, IT systems development projects, IT governance, Outsourced IT services, Social Media Use, Mobile computing, IT skills among internal auditors, emerging technologies and board and audit committee technology awareness.

Another valuable and useful guidance is the Global Technology Audit Guide (GTAG). There are 17 guides forming part of the Supplemental Guidance of the IPPF. The GTAG are written with the intention to address timely issues relating to information technology management, control, or security. In these two years, the following GTAG were released.

[1] Philip E. Flora, Sajay Rai, *Navigating Technology's Top 10 Risks* (The Institute of Internal Auditors Research Foundation, 2015)

- Assessing Cybersecurity Risk: Roles of the Three Lines of Defense[2]
    - The guide discusses the internal audit activity's role in cybersecurity, including:
        - The role of the chief audit executive (CAE) related to assurance, governance, risk, and cyber threats.
        - Assessing inherent risks and threats.
        - The first, second, and third lines of defense roles and responsibilities related to risk management, controls, and governance.
        - Where gaps in assurance may occur.
        - The reporting responsibilities of the internal audit activity.

- Auditing Smart Devices: An Internal Auditor's Guide to Understand and Auditing Smart Devices[3]
    - With smart devices like mobile phones, the mobility poses a different kind of risks to organisations. The guide helps internal auditors better understand the technology, risks, and controls associated with smart devices. This is useful as internal auditors need to understand the organisation's smart device strategy and also to provide assurance by identifying and assessing risks to the organisation arising from the use of smart devices; determining the adequacy of the governance, risk and controls; and to review the design and effectiveness of controls. The guide even provides an engagement work program, including risk assessment to evaluate risk management and controls related to smart devices.

- Understanding and Auditing Big Data[4]
    - This guide can assist internal auditors in understanding the big data concepts and how to align internal audit activities in support of the organisation's big data initiatives. It provides a framework of key risks, challenges and controls to be considered when planning an audit of big data.
        - It states that internal audit as part of their risk assessment and audit planning should consider the role of big data in their organisations.
        - Internal audit should also be included in advisory projects for the big data implementation programs, from the pre- or post- implementation reviews.
        - Internal audit should also verify that the objectives of the big data program is aligned with the oranisation's business strategy.

[2] GTAG – *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense* (The Institute of Internal Auditors, 2016)
[3] GTAG – *Auditing Smart Devices: An Internal Auditor's Guide to Understand and Auditing Smart Devices* (The Institute of Internal Auditors, 2016)
[4] GTAG – *Understanding and Auditing Big Data* (The Institute of Internal Auditors, 2017)

- Internal audit should provide assurance of the quality, security and privacy of the data used for analysis and the analytic outputs.

With the availability of useful guides being periodically released by The IIA, the IIARF also have useful reports that internal auditors can take actions as recommended. The IIARF published a research report on "Cybersecurity – What the Board of Directors needs to ask[5]". It included questions that the board should ask with regard to the topic of cybersecurity. This publication is useful for internal audit as the CAE should ensure board members are well-informed on cyber threats and the impact that cyberattacks have on the organisations. The set of questions will be the guidance on the areas that CAE should ensure that the board has adequate knowledge and information.

In the age with rapid changes in technology, the guidance and research papers by The IIA do provide useful tips for internal audit in their role to provide assurance to the board.

Eric Lim is the Immediate Past President of The Institute of Internal Auditors Singapore and Teng Hui Yun is the Assistant Director, Technical and Training, IIA Singapore

[5] Sajay Rai, *Cybersecurity – What the Board of Directors needs to ask* (The Institute of Internal Auditors Research Foundation (IIARF) 2014)