

## GOVERNANCE

### THE AIRBUS BRIBERY CASE STUDY: SIX CORPORATE LIABILITY LESSONS FOR MALAYSIAN COMPANIES

There are six cautionary lessons for Malaysian companies, especially where we are on the brink of seeing the introduction of corporate liability on 1 June 2020.

#### 1. Persons Associated with Airbus

In summary, persons associated with Airbus, including Airbus employees and other intermediaries, offered very substantial sums of money by way of bribes to third parties in order to secure the purchase of Airbus aircrafts.

Under Malaysia's section 17A, the person associated with a commercial organisation will be as wide as the UK position. The categories of persons such as an employee, or an agent or intermediary carrying out services for a Malaysian company, would be such a person associated. The corrupt activities of the person associated would then expose the commercial organisation to the offence under section 17A.

#### 2. Airbus Compliance Procedures: Failure to have Adequate Procedures

The High Court Judge noted the following:

First, Airbus did have bribery prevention policies and procedures in place. There were written policies that governed payment and contractual relationships with third parties, and Business Ethics Policy and Rules, and with detailed due diligence process to be undertaken. However, those policies and procedures were easily bypassed or breached. There existed a corporate culture which permitted bribery by Airbus business partners and/or employees to be committed throughout the world. Second, the Judge took note of the wrongdoing of several very senior, senior and other employees of Airbus. This included employees with compliance responsibilities.

Some of the conduct included the creation of false invoices, false payment, and other compliance material, and the deliberate circumvention of both Airbus' internal compliance procedures and external compliance procedures. Third, the weakness of senior corporate oversight, and the seriousness of the offending overall, must be considered in the context of the increased awareness internationally of the pernicious nature of corrupt business practices. Also, considered as the obvious vulnerabilities of businesses operating in and selling in international markets, as Airbus does.

#### 3. Extraterritorial Effect

In Malaysia's corporate liability, there is also an extraterritorial effect especially for Malaysian incorporated companies. The corporate liability will extend to these Malaysian companies, whether carrying on business in Malaysia or elsewhere. Liability would also extend to foreign companies carrying on a business or part of a business in Malaysia.

#### 4. Cooperation by Airbus for Delayed Prosecution Agreement

Malaysia does not have the option of a commercial organisation entering into a deferred prosecution agreement (DPA). A DPA provides a mechanism for an organisation to avoid prosecution for certain economic offences through an agreement with the prosecuting authority.

#### 5. Transformation of Airbus' Procedures

Airbus also took significant steps to demonstrate that it had fully transformed itself from past bad practices. These are noteworthy items to demonstrate the level of compliance and steps taken to stamp out future misconduct.

First, the Judge noted that Airbus now had a change in the management team, with a largely different Board of Directors. Second, Airbus conducted disciplinary investigations against existing and former employees. Since 2015, Airbus parted with 63 of its top and senior management employees.

Third, Airbus had commissioned an Independent Compliance Review Panel for a completely independent review of Airbus' ethics and compliance procedures. Fourth, Airbus Ethics and Compliance teams had been restructured to ensure functional independence from the business. There was a merger of legal and compliance functions and the change of the reporting line to the newly appointed General Counsel. Fifth, the creation of a sub-committee of the Board, entitled the Ethics & Compliance Committee, to provide independent oversight of Airbus' Ethics & Compliance programme. Sixth, Airbus appointed a new Ethics & Compliance officer with changed reporting lines directly to the General Counsel and the Ethics & Compliance Committee. Seventh, the Judge also noted other examples of steps taken by Airbus including:

- Created numerous new compliance roles and extensively recruited highly experienced senior compliance professionals.
- Revised its Anti-Bribery and Corruption (ABC) policies and procedures in response to recommendations by external stakeholders.
- Launched a company-wide, systemic and comprehensive ABC Risk Assessment.
- Redesigned the 'onboarding', due diligence and ongoing monitoring for all third parties with a business relationship with the Airbus group.

### 6. Malaysia's Personal Liability of Directors and Management

In Malaysia, the corporate liability provision is graver. Where an offence is committed by the commercial organisation, it is then already deemed that the senior officer (i.e. director, controller, officer, concerned in the management of the company's affairs) has also committed the offence. The burden then reverses on the senior officer to have to show that the offence was committed without his consent or connivance and that he exercised due diligence to prevent the commission of the offence.

If it occurred to a Malaysian company, the facts of the Airbus case would have exposed the directors and senior management to a grave risk of personal liability under Malaysia's corporate liability provision.

### What CAE should do?

To ensure that the organisation they are attached to are ready for the enforcement of Corporate Liability on 1 June 2020.



### Reference:

<https://themalaysianlawyer.com/2020/02/05/airbus-bribery-cautionary-corporate-liability-malaysian-companies/>

### A VOICE IN THE BOARDROOM

The IIA's recent research, OnRisk 2020: A Guide to Understanding, Aligning, and Optimising Risk, has questioned whether reporting to the audit committee potentially constricts the value internal audit can add to some organisations. As businesses face a growing range of external threats, so internal audit's remit has expanded. Financial risk, once the mainstay of audit departments, today typically occupies only 20% of their time. Practitioners expend the rest of their effort on a diverse range of issues including cyber risk, disaster recovery, culture risk, climate change, and social responsibility, to name only a few.

This broadening of internal audit's remit raises the question of the extent to which a CAE should report to other board committees, and in what circumstances he or she should report to the full board. And, for those wishing to explore that route, how can they get the audience and credibility to play this enhanced role?

### Expanding Audit Influence

To serve this more diverse constituency, internal audit needs to adopt the right approach and clear communication to the board the scope and focus of its work.

As a CAE you have to emphasize the fact that you're pragmatic in your approach, you're proactive, you're collaborative, you're agile, you focus on integrated risk-based auditing, you are educational, and that you can school your governing body and your management teams on controls, risk management, governance, and organisation from the best process perspective. You don't only focus on communicating audit observations, but you talk about business optimisation and efficiencies by leveraging strengths across teams. That can help open the door to the various board subcommittees and, on critical strategic issues, to the board itself.

### Establish Credibility

Living up to that ideal is not easy. Many CAEs lack credibility because they tend to emphasize box-ticking rather than focus on what matters to the audit committee, let alone the board. CAEs must be able to bring matters to the board that is important to its members and demonstrate that the annual audit plan is risk-based and fits closely with the threats relating to corporate strategy. Informal meetings also can be a great place to build credibility. The audit team is invariably closer to the business than members of the audit committee, so it is best placed to detect trends across the organisation or in isolated parts of the enterprise.

### Demonstrate Value

But if internal audit wants to be credible with the board, or a board subcommittee, it has to be able to perform at the highest level. Executive management tends to have conservative views of what internal audit can deliver, and that view follows through to the board because many executive officers also sit on audit committees in other organisations.

CAEs need to be able to innovate and do things in ways that are above and beyond expectations to challenge those views. If you want to be perceived as valuable to the organisation, you have to *be* valuable to the organisation.

### Understand Emerging Technology

Emerging technologies are a risk and an opportunity for internal auditors. They are a risk because if you are unaware that robotic process automation is being used in your business, you are in the unfortunate position of missing an important risk to your organisation. If you are adding assurance to the board in such a critical area, on the other hand, you will gain credibility and may even have the opportunity to grow your team and scope of responsibility.

One of the challenges for internal auditors is to choose the technologies most relevant to their particular industries because trying to learn about several new technologies at once can be overwhelming.

### Reshaping the Audit Committee

While some may point the finger at the internal audit for being too focused on detail, or for not exploring emerging threat areas, audit committees may also need to reform. In the U.K., for example, the financial services industry regulators require regulated firms to have an audit committee and a separate risk committee. The requirement has helped raise the profile of risk within those businesses. Plus, recent guidance produced by the Risk Coalition, an industry body that aims to establish consensus on risk management practice, recommends that the risk committee invite the CAE to its meetings "as necessary or appropriate."

Reformulating the audit committee as a risk and audit committee could help internal audit develop a more strategic, risk-based role. The change has helped the organisation take a more holistic approach to manage its risks, and it has enabled the reformed committee to take deep dives into selected threats at its regular meetings.

On the other hand, with issues of strategic importance, CAE presentations to the full board can be worthwhile. What has been missing in the evolution of corporate governance is that internal audit has not had access to the full board. Perhaps the CAE does not have to sit through a full board meeting, but when the chair and company secretary are working on the board agenda, they should be considering whether there are issues on which the CAE could usefully come and give their perspective.

### Extending Internal Audit's Reach

More CAEs are finding a voice beyond the audit committee. As risk board subcommittees have emerged, auditors have been invited to contribute their expertise. Others have found a voice at other board subcommittees and, less frequently, in full board meetings. For those who have built up the credibility and clout, the opportunities to add value to their organisations have never been greater.

### What CAE should do?

CAE must consider to build up the credibility and clout, the opportunities to add value to their organisations.

### Reference:

<https://iaonline.theiia.org/2020/Pages/A-Voice-in-the-Boardroom.aspx>

## PUBLIC SECTOR

### PRACTICE GUIDE, INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK – UNIQUE ASPECTS OF INTERNAL AUDITING IN THE PUBLIC SECTOR

The internal audit activity bases its work on the chief audit executive's risk-based internal audit plan and the International Professional Practices Framework (IPPF). In the public sector, internal auditors also must give attention to the requirements put forth in the public policy and legislation related to the area, process, or program under review.

These inputs, along with other public sector standards, guidance, and regulatory specifications relevant to the organisation, comprise the public sector context.

The internal audit activity is expected to produce an internal audit report as an output, which must be communicated to senior management and the board (i.e., the body responsible for governance). Public sector organisations may also be required by law, regulation, or policy to produce a written report of the results of audit engagements.

The chief audit executive (CAE) is responsible for communicating to parties that can ensure that the final report is given due consideration (Standard 2440.A1) and for establishing a process to monitor the disposition of results (Standard 2500). Because certain types of information may be made public automatically or by request, internal auditors in the public sector must be especially careful to communicate prudently.

The unique aspects of internal auditing in the public sector, which internal auditors must take into account when performing their work, stem from the public sector context. Figure 1 depicts the interrelationship between all these elements.

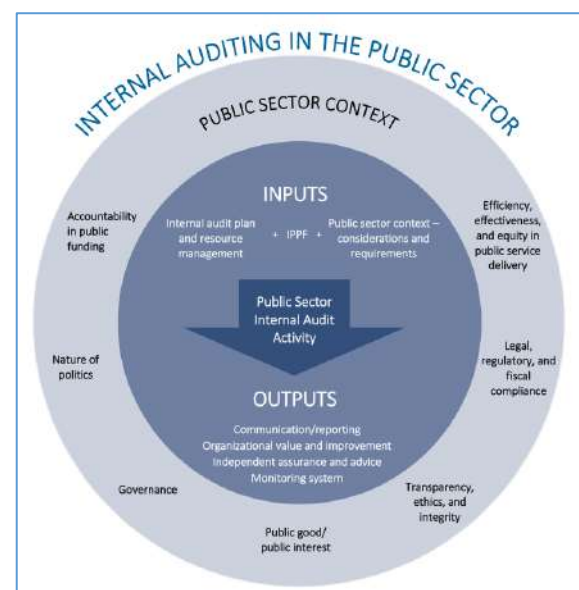


Figure 1

Internal auditors in the public sector must consider the public sector's mandate to serve the public good and to uphold the principles of good governance: (1) accountability for funds collected from the public and (2) efficiency, effectiveness, and equity in the delivery of public goods and services.

Good governance typically includes setting strategy, providing oversight, and instilling ethics in organisations. Independent auditing, including internal and external audit services, supports good governance in the public sector.

Auditors assure that public organisations are performing effectively and efficiently and by legal and ethical obligations to their public constituencies.

However, in democratic political systems, the nature of politics itself may put pressure on, or conflict with, the good governance principles of accountability, equity, integrity, and transparency. Sources of political pressure include, for example, election cycles, media attention, public interest and opinion, lobbying, politicians' personal interests, and more. These sources of political pressure and others may be present in autocratic political systems as well. Thus, internal auditors working in the public sector must delicately balance and properly handle the conflict between political pressure and the ethical principles of good governance.

Internal auditors must be alert to shifts and duly consider the unique characteristics and risk landscape of the public sector context because they may affect the continuity of the internal audit activity's work. For example, changes in political leadership and the related administration and bureaucracy may drastically affect the timing and resources related to the internal audit plan and may influence management's implementation of internal audit recommendations. In governance structures where the organisation's leadership is elected by citizens and where elections may change the organisation's strategic direction, internal auditors carry immense responsibility that must be balanced with resilient flexibility.

The internal audit activity must take all these factors into account when performing its work in the public sector.

The importance of ethics is not unique to the public sector. What is unique, at least in democratic political systems, is the way that four ethical principles help create a system of checks and balances to support the public sector's primary purpose of serving the public interest. This section explores these principles: integrity, accountability, transparency, and equity.

The public expects high ethical standards within the public sector to ensure that the funding they provide (via taxation and fees) is spent wisely. Therefore, public officials must be able to evidence that they are doing the right thing in the right way. Transparency enables this evidence.

Ethical principles are so integral to serving the public interest that laws and regulations are often in place to help deter and detect unethical behavior by public sector officials, employees, and those with whom they contract. Governments and public sector organisations may implement additional policies, procedures, and codes of behavior to monitor, measure, and enforce ethical principles. Maintaining an ethical tone at the top, sufficient internal control, and effective oversight are necessary to demonstrate the organisation's commitment to ethical principles.

It is equally important that internal auditors also apply the highest ethical standards in performing their work. Internal auditors certified by The IIA and candidates for certification are required to adhere to The IIA's Code of Ethics, which identifies integrity, objectivity, confidentiality, and competency as its primary ethical principles. This Code applies to individual internal auditors at any level and the internal audit activity as a whole.

In a nutshell, internal auditors in the public sector must consider the public sector's mandate to serve the public good; to properly manage the political pressures to uphold the ethical principles of good governance.

### What CAE should do?

CAE must consider the public sector's mandate to serve the public good; to properly manage the political pressures to uphold the ethical principles of good governance.

#### Reference:

[PG-Unique-Aspects-of-Internal-Auditing-in-the-Public-Sector.pdf](#)

### RISK MANAGEMENT

#### ONRISK 2020: A GUIDE TO UNDERSTANDING, ALIGNING AND OPTIMISING RISK

OnRisk 2020 brings together the perspectives of the board, executive management, and chief audit executives (CAEs) on the risks that are top of mind for 2020 and beyond. Based on quantitative and qualitative surveys, the report lays out how each respondent group views key risks. Respondents shared their perspectives on their knowledge of the risks and their views of their organisations' capability to address the risks. But the most innovative and powerful benefit OnRisk 2020 offers is a studied analysis of how those views differ and what that means to an organisation's risk management.

The 11 risks below were carefully selected from a vast assortment that is likely to affect organisations in 2020 and was vetted through in-depth interviews with board members, executive management, and CAEs.

**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.

**DATA PROTECTION:** Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organisations protect sensitive data in their care.

**REGULATORY CHANGE:** A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organisations face in a dynamic and sometimes volatile regulatory environment.

**BUSINESS CONTINUITY/CRISIS RESPONSE:** Organisations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organisations' abilities to prepare, react, respond, and recover.

**DATA AND NEW TECHNOLOGY:** Organisations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organisations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

**THIRD-PARTY:** Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organisations' abilities to select and monitor third-party contracts.

**TALENT MANAGEMENT:** Historically low unemployment, a growing gig economy, and the continuing impact of digitalisation are redefining how work gets done. This risk examines challenges organisations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

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

**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 are receiving complete, timely, transparent, accurate, and relevant information.

**DATA ETHICS:** Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organisational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

**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.

### What CAE should do?

CAE should review the analysis and recommendations related to each of the 11 key risks that follow and are encouraged to conduct a similar review of the knowledge and capability perspectives among their own organisation's board, executive management, and internal audit activity.

### Reference:

<https://na.theiia.org/periodicals/OnRisk/Pages/default.aspx>



## INTERNAL AUDIT

### AGILE INTERNAL AUDIT – LEADING PRACTICES ON THE JOURNEY TO BECOMING AGILE

A general idea about Agile Internal Auditing is to use sprints, which Planning, Fieldwork, Review, and Reporting are done simultaneously in a cycle of one to two weeks. The sprints are repeated until the audit is finished. At the end of every sprint, the findings will be discussed with the auditee.

The concept of Agile emphasizes fast-paced, repeatable, full transparency and collaboration between stakeholders and audit teams.

### Benefits for Adopting Agile Auditing

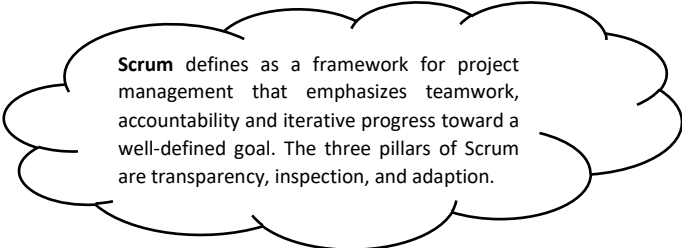
1. The improved collaboration, visibility, and transparency allow potential misunderstandings with auditees to be resolved quickly with minimal draft responses.
2. The final report turnaround time is much faster compared to the traditional auditing approach.
3. The improved ability to dynamically manage audit priorities.
4. More frequent and transparent interaction with stakeholders and more empowered, engaged and happy associates.

### Challenges in Adoption

1. It requires a change in mindset. For example, in the traditional auditing methodology, reports would be delivered to the client at the end of the audit. This does not apply with Agile because findings are delivered regularly, allowing the auditee to work on the findings and remove deficiencies as quickly as possible.
2. The agile methodology involves not working on items that do not add value. For example, if the team thinks a remaining area may need additional work, it can be put into the backlog of other audit priorities for reconsideration in the future.

### Impact on Organisational Structure

Agile requires reconfiguring the roles and responsibilities within an audit function. By adopting a "Scrum", employees at different levels, from associate up to the vice president, each can contribute differently to the audit based on the skills and knowledge they bring to the team, rather than what they see themselves permitted to do or not do based on their reporting relationships. The auditors are allowed to exchange of ideas, including disagreements, and without worrying about possible the impact on their performance ratings.



**Scrum** defines as a framework for project management that emphasizes teamwork, accountability and iterative progress toward a well-defined goal. The three pillars of Scrum are transparency, inspection, and adaptation.

It took adjustment for middle managers and CAE as well. For example, middle managers, who may not have been involved in the strategic decision may now lead up to the decision and slower to adopt it.

It also requires to apply Servant Leader/ Scrum Master concept under Agile best practices, which a leader to manage a team by not telling them what to do, but by removing impediments that get in their way by coaching them. For the leader, they require continuous learning and being comfortable with failure.

Audit Committee will also receive information more quickly and timely, and they are more often involved in the process and a better understanding of how the audit findings are developed.

### How to ensure the successful adoption of Agile?

- 1) The need for adequate support and better communications from stakeholders and audit committees.
- 2) It requires a coach who is an expert in implementing Agile auditing and able to demonstrate how the Agile process works.
- 3) Piloting and trial-and-error are ongoing and part of the process.

- 4) Continuously applied what you have learned about Agile auditing and these will be the fundamental working blocks that the engagement is built on.

### What are Common Concerns?

- 1) Does it require more meetings to be held?
  - It is more about different sequencing. For example, the reviews are held at the end of each sprint, so at the end of an audit, auditees are already aware of the observations. As a result, there is less negotiation compared with the old format, where alignment meetings often took place after the final review under Traditional audit.
- 2) Does it require more commitments are required by the Stakeholders?
  - Yes, but the trade-off will be enabling full transparency throughout the process.
- 3) Will audit miss any important information?
  - As it involves collaboration with stakeholders, any missing information or observations from earlier sprints could be updated with additional information, resulting in extra value in the audit function.
- 4) Will it enhance the effectiveness of the internal audit by adopting Agile?
  - The clear objectives established using Agile enables audit teams to work more efficiently, spending less time in the field and not over-auditing.

### What Internal Auditors should do?

To consider to embark the Agile auditing within the audit function as this is not only a way to retain the profession's relevance, but also enable auditors to highlight its value in a rapidly changing corporate environment.

### Reference:

<https://global.theiia.org/member-resources/Global%20Documents/GKB-Agile-Internal-Audit.pdf>



### INFORMATION TECHNOLOGY

#### RETHINKING PREPAREDNESS: PANDEMICS AND CYBERSECURITY

The coronavirus epidemic is bringing into sharp focus an issue that is often overlooked by organisations — business continuity and disaster preparedness.

Uncertainty about the scope and duration of the current epidemic is already making an impact, from organizations re-evaluating employee travel plans to jittery investors selling off stocks. With the potential to affect supply chains, worker productivity, and third-party relationships, the risk of an expanding outbreak should be on the minds of business executives and internal audit leaders alike. At a minimum, internal audit leader should be prepared to review and recommend necessary updates to pandemic, disaster preparedness, and business continuity plans.

Cybercriminals are taking advantage of the growing concern over the deadly virus. Malware-laced emails masquerading as guidance about the virus turned up in three Japanese prefectures, according to TechRadar Pro, a UK-based consumer technology news and reviews website. Hackers disguised the malware in email attachments purporting to contain information to protect against spreading the virus. Instead, they were laden with a virus of another kind, according to TechRadar Pro.

Cybercriminals taking advantage of crises is something that likely will become more prevalent. Organisations must build up their protocols and practices to defend against social engineering such as phishing, pretexting and baiting

#### General questions to assess your organization's disaster preparedness

The following are some general questions your internal audit department should ask to determine if your organization is properly addressing disaster preparedness and business continuity planning:

- ✚ When was the last time your organisation's resiliency plans were reviewed by key stakeholders? When was the last time your organisation's plans were tested and by whom?
- ✚ How do your current plans address natural disasters, pandemics, or other potential disruptors that could impact your facility? Your employees? Your cloud providers? Your suppliers? Your customers?
- ✚ When was the last time your organisation reviewed its contracts with business resiliency partners?
- ✚ How are vendors, emergency responders, regulators, insurance agencies, and other critical stakeholders notified of point of contact changes?
- ✚ How capable is your organisation to perform manual versions of business-critical automated activities? Are the needed forms and procedure manuals available? Are you appropriately staffed to do so?
- ✚ How often does your organisation verify the criticality of various business processes to make sure the order of recovery is appropriate? How does IT ensure the critical infrastructure components are enabled to allow for the business recovery requirements?
- ✚ What training have your employees and business associates received on what to do in the event of a natural disaster or a pandemic?
- ✚ Is your data center and/or your cloud provider capable of running "lights out," meaning no workers present for an extended period?
- ✚ What business-critical processes or activities would not be transferrable to an alternate location? Which have regulatory implications based on timing or duration of event?

#### General questions to assess your social engineering vulnerabilities

The following are some general questions your internal audit department should ask to determine your organisation's vulnerability to social engineering schemes:

- ✚ What are your organisation's practices, policies, and training involving the threat of social engineering?

- ✚ Is the threat of social engineering completely understood and communicated to all levels of employees at your organisation?
- ✚ Which systems and processes are particularly vulnerable to social engineering? Which key business processes have potential to be affected?
- ✚ What testing does your IT department do relating to areas of specific vulnerability to social engineering?
- ✚ Do you have plans to audit your organisation's areas of specific vulnerability to social engineering?

### What Internal Auditors should do?

The internal auditors should be prepared to review and recommend necessary updates to pandemic, disaster preparedness, and business continuity plans.



### Reference:

<https://global.theiia.org/news/Pages/IIA-Bulletin-Disaster-Preparedness.aspx>

### HOW TO TAKE YOUR DATA ANALYTICS PROGRAM TO THE NEXT LEVEL

According to the recent *PwC State of Internal Audit report*, 82% of internal audit functions surveyed say they have increased their investment in data mining and data analytics to facilitate monitoring of key trends and to support continuous auditing.

Besides many functions are finding their analytics programmes stalled and in need of a jump start.” Indeed, many internal audit departments find it difficult to take their data analytics programmes to the next level.

They want to implant advanced analytics into everything. They want analytics to inform risk assessments, audit planning, and to be used in just about every audit. They also want to move into predictive analytics, which relies on data mining, predictive modeling, and machine learning, to analyse current and historical facts to make predictions about unknown events.

Nowadays, internal audit functions are finding it hard to hire the audit staff with data analysis backgrounds and capabilities. Most CAEs will tell you that finding audit candidates with data analytics skills is never easy.

Furthermore, most internal audit departments are tight with the schedule to devote to coming up to speed on new technologies although it would save time in the long term. Technology is moving so fast that some CAEs decide they can't keep up with it all and just throw up their hands.

The companies where the internal audit is behind on data analytics, the problems often lie higher up in the organisation based on Michael Smith from KPMG. He added that the internal auditors have not been empowered to go and create their innovation.

### Seven Ways to Improve Data Analytics Maturity

#### 1. Demonstrate the potential.

Provide the demonstrations of analytics capabilities that can win over skeptics and build support in the organisation.

### 2. Name a data analytics champion.

Having champions could help organisations to bridge the gap between the analytics function and operational auditors. It also encourages the use of analytics, including basic usage by the whole team. This dedicated leader can be invaluable in finding ways that analytics can improve audits or find more efficient ways of conducting analytics.

### 3. Get board and management support for data sharing.

CAEs should explore opportunities to expand internal audit's access to quality data. That may include appealing to senior executives and even the board to push the importance of providing access to data throughout the organisation.

### 4. Don't get caught up on data analytics tools.

Making a decision too early can harm a data analytics initiative. Placing too much focus on learning the tools can intimidate internal auditors and keep them from advancing.

Most data analytics initiatives say, start with something as simple as Microsoft Excel and move on when it becomes limiting to what auditors want to accomplish. There's no reason to increase the complexity with advanced tools before your team has a good understanding of the data and what it can tell you.

### 5. Think creatively about data sources.

Data analytics practitioners must identify new data sources that can enhance internal audit's view of risk across the organisation. This can ensure that the organisation will be able to supplement data analytics procedures with a supply of quality data. Getting benchmark data can provide a good baseline and comparison for analysing the internal data.

### 6. Get stakeholder input.

CAEs should seek ways to increase the level of input stakeholders provide when building and using data analytics models and continuous auditing tools. Process owners have the best understanding of the data and can be vital in helping to determine what data should be monitored.

### 7. Measure and report results.

CAEs can implement steps to measure the success of their data analytics efforts and report success and value to management and other top stakeholders. Internal audit groups that successfully demonstrate tangible value are the ones that make a stronger business case for increased budgets and resources dedicated to data analytics. In the process, this can also boost the internal audit function's reputation.

#### What CAE should do?

CAE should explore and pursue data analytics without any fear will soon be expanding their capabilities and unlocking the powerful potential of what it can do.



#### Reference:

<https://internalaudit360.com/how-to-take-your-data-analytics-program-to-the-next-level/>

*Disclaimer: The findings and any views or opinions presented in this publication are solely those of the authors and does not reflect the views or opinions of the Institute of Internal Auditors Malaysia (IIA Malaysia).*