IIA Malaysia e-techline
April 2022 Issue 2/22

CURRENT ISSUE

GUIDANCE ON GOOD PRACTICE AND CHECKLIST FOR ADEQUATE PROCEDURES (BY TRANSPARENCY INTERNATIONAL MALAYSIA)

Transparency International Malaysia first published the Guidance on Good Practice and Checklist For Adequate Procedures in February 2022.

Section 17A of the MACC Act 2009 makes a commercial organisation strictly liable for failing to prevent the giving or even promising of gratification for the organisation's advantage. If a person associated with the organisation is found to have corruptly given, agreed to give, offered, or promised a gratification for the organisation's benefit, the provision presumes corporate liability on the part of the organisation and its directors. The only defence for the organisation and its board is to show that there were adequate procedures to prohibit, prevent, and detect such conduct.

Thus, Transparency International Malaysia has developed a checklist to guide commercial organisations in implementing a holistic anti-bribery and corruption programme (ABC Programme) covering the actions of employees and associates within the organisation's stakeholder network.

This checklist was adapted for the Malaysian context from the 2010 UK Bribery Act Adequate Procedures Guidance published by Transparency International UK (TI-UK). Every commercial organisation has its operating model that generates a unique risk profile for bribery and corruption. Thus, the depth of due diligence procedures, the level of communication, documentation, review, and disclosure that are considered adequate may vary depending on factors such as the size of the organisation, the nature of the risk, the level of risk exposure, and the complexity of its business relationships.

The checklist should not be considered a "ticking the box" exercise. Instead, it serves as a benchmark list of best practices for organisations implementing an ABC Programme for the first time or reviewing an existing programme. A commercial organisation committed to promoting integrity must implement a holistic ABC Programme that responds to the level of corruption risk inherent in its operations and stakeholder relationships.

Guidance for adapting the checklist procedure for SMEs

- **Tone From the Top**

  SMEs can use a single Anti-corruption and anti-Bribery Policy (ABC Policy) document to capture all its policies on acceptable and unacceptable Gifts, Hospitality and Entertainment, Charitable and Political Contributions, and Sponsorships.

  For SMEs which are too small to have dedicated compliance officers, a director, member of senior management, or a compliance task force or committee comprising suitable senior and trusted person could be empowered to oversee the risk assessment process, implement adequate procedures, oversee the review and monitoring, and provide in-house briefings on the ABC Programme.

- **Risk Assessment**

  Risk assessment should still cover all areas of the SME's operations and all stakeholders. An independent risk assessment exercise is encouraged.

  SMEs that are too small to engage consultants for independent assessment can consider assigning a manager or committee to be trained in basic risk assessment.

Self-assessment should minimise the risk of exposure to bribery and corruption according to the roles and functions of employees, agents, intermediaries, business partners, and other associates. Assessment should not be based on subjective perceptions or personal relationships.

- **Undertake Control Measures**

Due diligence procedures could involve minimally a background or reference check, a request to see the other party's ABC Policy, and an internet search for publicly reported incidents or court cases involving corruption.

Due diligence should be documented. A simple documentation process could include a signed checklist to acknowledge the above mentioned, checks, and a folder to save web searches and notes of reference checks before committing with the other party.

- **Systematic Review, Monitoring & Enforcement**

A manager or committee could undertake ongoing review and monitoring with the oversight of the board's independent directors or its equivalent.

SMEs are encouraged to include an assessment of adequate procedures within the scope of work of external auditors to obtain independent review and recommendations on the ABC Programme.

- **Training & Communication**

SMEs could source suitable external training programmes for employees or have a senior manager provide simple in-house briefings on the ABC Programme for training & communication.

SMEs that are vendors to MNCs or large local companies should actively participate in the latter's compliance programmes, if any, and ensure attendance of any relevant training or briefing.

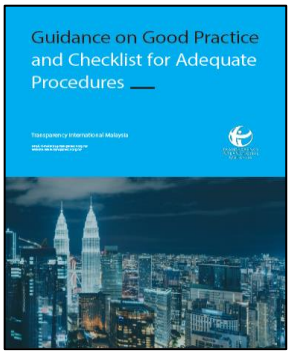
The checklist is divided into the five TRUST Principles. Some of the principles are further divided into multiple categories to provide structure to the assessment:

TRUST Principle	Category
TOP-LEVEL COMMITMENT	-
RISK ASSESSMENT	-
UNDERTAKE CONTROL MEASURES	· Human Resources · Facilitation Payments · Gifts, Hospitality & Expenses · Political Contributions · Charitable Contributions · Whistleblowing Channels & Advice Lines · Internal Controls · Accurate Books & Records · Subsidiaries · Significant Investments · Contractors and suppliers · Agents and other intermediaries · Joint ventures and consortia
SYSTEMATIC REVIEW, MONITORING AND ENFORCEMENT	-
TRAINING & COMMUNICATION	· Training · Communication

What should Internal Auditors do?

Today, the Directors, Senior Management, and those in charge of Integrity and Compliance are further extended with the need for an eye for detail and knowledge/expertise in the assessment and management of key bribery/corruption risks that their organisation may face.

Internal auditors are tasked to review their organisations' preparedness to comply with the requirements and assess the adequacy and operating effectiveness of the organisations' adequate procedures deployed in mitigating corruption risks.



Reference:
https://www.transparency.org.my/pages/news-and-events/publications/guidance-on-good-practice-and-checklist-for-adequate-procedures

INTERNAL AUDIT FOUNDATION

COSO RELEASES NEW GUIDANCE: ENABLING ORGANIZATIONAL AGILITY IN AN AGE OF SPEED AND DISRUPTION (BY COSO)

As radical change transforms the world we live in, organisations should regularly align their enterprise risk management (ERM) process with the current business environment and their strategic goals, according to new guidance issued from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The guidance "Enabling Organizational Agility in an Age of Speed and Disruption" highlights how organisations can succeed by being more anticipatory, agile, and adaptable.

- **Speed, Disruption, and Risk Are Causing Change**

  There are a variety of approaches to the speed of change and uncertainty, including moving faster, working differently, and becoming more agile in many areas. To make changes, companies can leverage COSO ERM's Governance & Culture component and principles relating to rethinking how they approach strategy and oversight (Principle 1), traditional organisational structures (Principle 2), traditional mindset and culture (Principle 3), and how they operate while aligning with their core values.

  Pivoting, adapting, and accelerating all are about managing strategic and business risk, but they also can create risk. Objectives are more likely to be achieved when the context is understood (consistent with Principle 6) and the potential new risks are identified (refer to Principle 10).

  ERM leaders will be more likely to stay in sync with the business when they regularly rethink and improve their ERM approach, as outlined in Principle 17. Understanding the changing strategic context (Principle 6) is critical.

  When adopting agile approaches, board risk oversight (Principle 1) must also be considered. The board can make a large difference by igniting the right conversations. In some countries, boards are legally mandated to assess emerging and principal risks, with principal risks being defined as risks that threaten the business model (note, this is strongly related to and supports Principle 15).

  When speed and agility are higher, the ERM function needs to help leaders rethink strategic risks and objectives (Principles 8 and 9).

- **Business Unit and Team Adoption of Agile ERM Applications**

  The ERM function has to balance (a) not slowing down (for all of the reasons agile was implemented) and (b) helping them to see and manage the risk portfolio (refer to Principle 14).

  Agile companies should have ERM embedded throughout the organisation's culture (Principle 3).

- **Agile Changes The ERM Approach**

  From a risk perspective, this mindset can turn into one that encourages taking risks and seeking opportunities. Companies that take an agile approach of speed and empowerment in innovations can improve risk-taking and ideation by encouraging this risk and opportunity mindset. When companies define the desired culture (Principle 3) as one that accepts and allows for failure, they build a culture that encourages new ideas and risk-taking.

  Agile practices will also impact talent — both current and new talent. Organisations wanting to develop talent and involve them in agile practices will need to train them in agile behaviours and skills (consistent with Principle 5).

... 3

The ERM function cannot remain rigid in its approaches in this environment. The ERM function might need to revisit policies and approaches for escalation and reporting (refer to Principle 19).

Assessing substantial change is a concept and principle (Principle 15 in COSO ERM) that appears especially important when adopted and implemented agile approaches. The principle emphasises the importance of organisations assessing substantial change that impacts the objectives.

The following summarises concepts that ERM leaders can use to succeed in an agile environment.

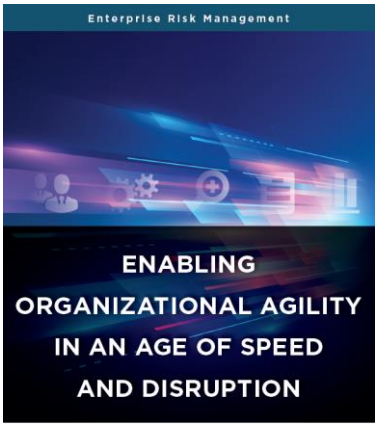
1. The speed of change, risks, and disruption drive organisations to rethink their vision and strategy.
2. Being agile is an extension of strategy and could also be the best strategic choice in certain environments; not being agile could be a strategic mistake.
3. Organisational leaders should regularly assess the environment in which they operate and the ability of the strategic approach to succeed in that environment.
4. Greatness includes taking risks but never blindly.
5. New normals and new business models must factor in the speed of change, risks, and disruption.
6. Agile helps manage some risks but can also lead to other risks.
7. New tools and methods are available for assessing noise, the environment, the strategy, the business model, and linking noise to the business model.
8. Superior ERM approaches can be a huge factor in helping the organisation succeed by focusing on the right strategies and risks.
9. Gathering and understanding the noise in the market and how it impacts the business and operating model and building an early warning system is becoming critical.
10. Organisations should regularly assess ERM and revisit the purpose, mission, and alignment of ERM with the current environment, strategic approach, and business units.

What should Internal Auditors do?

IPPF *Standard* 2100 – Nature of Work mentioned that the internal audit credibility and value are enhanced when auditors are proactive, and their evaluations offer new insights and consider future impact.

IPPF *Standard* 2120 – Risk Management mentioned that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

The internal audit department needs to be updated to keep up with these changes in the organisation and business units and play a crucial role in helping organisations improve the risk management processes.



Reference:

https://www.theiia.org/en/content/communications/press-releases/2022/march/coso-releases-new-guidance-enabling-organizational-agility-in-an-age-of-speed-and-disruption/?utm_source=linkedin&utm_medium=social&utm_postdate=03%2F15%2F22&utm_campaign=20212686-GLOB_AdvocacyPublicResponses_COSO-AgileERM_031522

INTERNAL AUDIT FOUNDATION

PRIVACY AND DATA PROTECTION PART 2: INTERNAL AUDITORS' VIEWS ON RISKS, RESPONSIBILITIES, AND OPPORTUNITIES (BY R. MICHAEL VARNEY, ADAM PAJAKOWSKI, AND AMANDA M. MARDEROSIAN)

This report explores how internal audits can become involved earlier in the data security and privacy processes, providing both guidance and support to the initial risk assessment and remediation activities. Of course, these functions need to be performed without jeopardising the essential objectivity and independence that are hallmarks of the internal audit profession.

- **Data Privacy Roles and Responsibilities**

  The survey appears internal auditors often might become more involved earlier in the overall data privacy risk management process. For example, an internal audit can provide insights that could be particularly helpful in enabling process owners to identify and quantify risks so they can more effectively prioritise and allocate resources. Internal audits also can offer valuable feedback and guidance on data privacy policies and governance issues. Such early involvement could help internal auditors build or strengthen their internal relationships with other departments and business functions within their organisations.

  Helping to refocus senior management's understanding of this shift is another way internal auditors can add value to their organisations. Even if an organisation is not subject to the General Data Protection Regulation, which could require the appointment of a Data Protection Officer, it could nevertheless benefit from assigning data privacy responsibilities to a compliance-oriented executive, such as a Chief Risk Officer or Chief Privacy Officer.

- **Data Privacy as a Material Risk**

  Some of the specific concerns raised by CAEs and directors who identified data privacy as a material risk is of particular interest. Their open text responses were analysed and grouped into general categories, and the five most commonly cited concern areas were:

  1. Regulatory requirements.
  2. Risk to reputation.
  3. The sensitivity or importance of the data held by their organisations (such as personal financial or healthcare information).
  4. Decentralisation of data systems and a lack of consistent procedures.
  5. The generally increasing likelihood of data breaches.

- **Internal Auditors' Views of Program Effectiveness**

  This result of the survey again suggests that internal auditors can provide value to their organisations by engaging earlier in the data privacy process, becoming more proactively involved in policy updates, and assessing the quality of data privacy policies as part of their compliance function.

- **Internal Auditors' Most Critical Concerns**

  Top concerns varied widely, but the largest number of those responding cited data inventory and classification. Other leading concerns included the accidental release of personally identifiable information, weak policies and processes in general, and employees who were either not informed or poorly informed about data privacy issues.

  Respondents who listed weak data privacy policies and processes as a top concern also expressed concerns about employees not being well-informed about privacy and data protection issues in general.

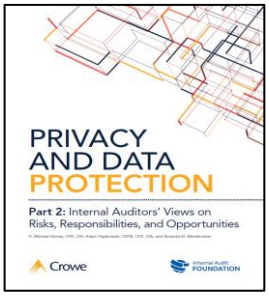
- **How Internal Auditors Can Add Value**

  Internal auditors can take broader, more proactive steps to improve the overall effectiveness of privacy policies and practices. Internal audits also can help the process owner identify which factors have the greatest impact on data privacy risk. By helping the process owner identify these priorities, an internal audit can help contribute to a more effective allocation of resources while at the same time improving the overall effectiveness of the data privacy effort.

What should Internal Auditors do?

IPPF *Standard* 1210 - Proficiency specifically identifies internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Internal auditors may expect increasing demand to review their organisations' compliance efforts and provide assurance of both their adequacy and effectiveness. In that environment, this review of the profession's current state as it relates to privacy and data protection concerns can provide a useful baseline for measuring and guiding internal audit's growing involvement in this critical area of risk.



Reference:
https://www.theiia.org/en/content/research/foundation/2022/privacy-and-data-protection-part-2-internal-auditors-views-on-risks-responsibilities-and-opportunities/

INTERNAL AUDITOR - BLOGS

BUILDING A BETTER AUDITOR: FOUR SKILLS INTERNAL AUDITORS SHOULD DEVELOP NOW (BY IIA VICE PRESIDENT JIM PELLETIER)

Leveraging data from two key studies — the 2022 North American Pulse of Internal Audit and the Internal Audit Foundation's (IAF's) Internal Audit Competency Study — four areas stand out as both critical gaps and significant opportunities for internal audit teams and internal auditors who want to become indispensable to the profession.

- **Data Analytics**

  In the Pulse report, among CAEs who say they plan to budget additional money for technology, 68% indicate they will spend it on data analytics software. This is a huge opportunity for auditors who are competent in data literacy, data governance, and the use of data analytics technology. Many internal audit functions have failed to apply data analytics successfully because they thought the technology alone was the solution. For data analytics to be successful, departments must have individuals with the data analytics knowledge and critical thinking skills to get to the right data and know what to do with it.

- **Fraud**

  Among the top fraud-deterrent measures being implemented, committee members put internal audit increasing its focus on fraud at the top. Internal auditors must rise to the challenge by developing a strong foundation of fraud knowledge to recognise and properly audit fraud. Importantly, that knowledge must be strong enough to combine with skills in data analytics (think fraud analytics) to expand understanding of fraud risks within the organisation and help detect potentially fraudulent activity.

- **Cybersecurity**

  Among CAEs, 85% ranked cybersecurity as a 'high' or 'very high' risk in the Pulse report. However, competency in this knowledge area was in the bottom five in the IAF research study. Once again, this represents a significant gap for internal audit departments but a tremendous opportunity for internal auditors who dive into this space. Technology cuts across the Pulse report's top three highest risk areas — cybersecurity, IT (not covered by cybersecurity), and third-party relationships (often including IT services and/or unique security concerns). Internal auditors who are not actively upskilling in the IT space quickly become irrelevant.

- **ESG**

  This is a rapidly evolving landscape with global standards under development and a number of big players influencing the direction of ESG reporting over time. It is important that internal auditors get up to speed on these pending requirements and standards and what processes within their organisations will be most impacted by what is to come. This is a great opportunity for internal audits to demonstrate value early on rather than wait and react later.

What should Internal Auditors do?

IPPF *Standard* 1210.A2 mentioned that internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organisation but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

IPPF *Standard* 1210.A3 mentioned that internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work.

IPPF *Standard* 1220.A2 mentioned that in exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

IPPF *Standard* 1230 – Continuing Professional Development mentioned that internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

In the short and medium-term, internal auditors must focus on these four areas to stay relevant. Of course, these are not the only skills internal auditors should be developing. Internal auditors shall keep abreast of current development, emerging risks, and potential areas of improvement.

Reference:

https://internalauditor.theiia.org/en/voices/blog/building-a-better-auditor/2022/march/building-a-better-auditor-four-skills-internal-auditors-should-develop-now/

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/.