FSPB GUIDANCE DOCUMENT ON SECTION 17A (5) MACC ACT 2009

October 2020

ABOUT THE FINANCIAL SERVICES PROFESSIONAL BOARD

The Financial Services Professional Board ("FSPB") is an industry-led voluntary initiative that was launched in Kuala Lumpur, Malaysia by Bank Negara Malaysia and Securities Commission Malaysia on 24 September 2014 and effective 1st January 2019, fully funded by the Association of Banks Malaysia, the Life Insurance Association of Malaysia and the General Insurance Association of Malaysia. It comprises a group of prominent individuals from the financial services industry ("FSI") and related industries. The aim of FSPB is to support a strong culture of professionalism and ethics across the FSI through the development and advocacy of professional and ethical standards that are applicable across the FSI, including banking, capital markets, insurance and Islamic finance.

TABLE OF CONTENTS

Credits: FSPB Working Group

1. Kelvin Yeow (HSBC Bank Malaysia Berhad)- Team Lead
2. David Lee (Hongkong and Shanghai Banking Corporation Ltd)
3. Haziruddin Hasan (Deutsche Bank (Malaysia) Berhad)
4. Radhihah Bt Naim (J.P. Morgan Chase Bank Berhad)
5. Kwan Keen Yew (CIMB Bank Berhad)
6. Idariah Mohd Idris (Manulife Insurance Berhad)
7. Vhinodhan Veerapalan (Sun Life Malaysia)
8. Alan Ho (Zurich Life Insurance Malaysia Berhad)

Introduction to FSPB Guidance Document on S17A (5) MACC Act

Section 17A(5) of the Malaysian Anti-Corruption Commission Act(MACC) came into force on 1st June 2020. Separately, the Prime Minister's Office (PMO) issued the Guidelines on Adequate Procedures ('Guidelines') to assist in "understanding what are the adequate procedures that should be implemented to prevent the occurrence of corrupt practices in relation to an organisation's business activities."

Bribery and Corruption is defined as offering (or agreeing to give), soliciting, or accepting (or agreeing to accept) bribes and other improper financial advantages.

Corporate Liability:
Liable whether or not top-level management and/or representatives had actual knowledge of the corrupt acts of its employees and/or associated persons.

Defence:
Implement adequate procedures protects both organization and top management from the corporate liabilities.

Employees and/or associated persons must not provide "***anything of value***" (financial or otherwise) to obtain or retain any business or advantage. It also applies to clients, suppliers and any person with whom the organization anticipates does or anticipates doing business.
"Anything of Value" extends beyond cash or cash equivalents to include:

- Improper gifts and entertainment
- Travel and/or lodging
- Charitable and political contributions
- Employment or internships for clients, government officials, or their related persons.

The Guidelines are provided in the form of five main principles. Implementing and ensuring the effectiveness of these policies, procedures and controls with reference to these principles would provide reasonable assurance to the Board and Senior Management to counter and resolve Bribery and Corruption risks arising in the organizations' business activities.

Purpose of the FSPB Guidance Document

The purpose of the FSPB Guidance Document is to provide guidance, support the effective implementation of "adequate and proportionate procedures" to Bribery and Corruption ("B&C") risks for financial institutions. The five FSPB Guidance Notes are aligned with the PMO Principles as follows:

1. **Top Level Commitment**
2. **Risk Assessment**
3. **Undertake Control Measures**
4. **Systematic Review, Monitoring and Enforcement**
5. **Training and Communications**

Objective

The FSPB Guidance Notes were prepared by an FSPB Working Group with representatives from participating financial institutions. The FSPB initiative on behalf of its stakeholders aims to set out best practices on policies, procedures and processes for each Principle which in aggregate would support the effective implementation of adequate procedures to prevent or mitigate the occurrence of B&C practices. Merely meeting the compliance test of having adequate procedures (ticking the boxes) should not be viewed as a full defence to corporate liability. Senior Management should be able to demonstrate that these policies, procedures and processes are implemented, practiced and enforced effectively throughout the institution and is proportionate to the B&C risks it would encounter in operating its business. The organizational culture must be consistent to an ethical environment where there is no tolerance for B&C at all levels within the organization.

Proportionality

In order to assess proportionality in B&C prevention procedures, a risk assessment which would include coverage of policies and implementation procedures should be conducted within the context of size of the business, its structure, the scope and nature of its activities, and the culture of its operating environment.

Voluntary and Non-Binding

Adherence to the FSPB Guidance Document in part or wholly is voluntary and non-binding. To assist in conducting an effective self-assessment, a checklist is attached as an Appendix IV. The checklist includes procedures discussed in the PMO's Adequate Procedures Principles (APP) Document and additional controls that are best practices in financial institutions.

How to Use the Guidance Document

This Document should be read in conjunction with the following FSPB Standards, applicable laws and regulations governing financial institutions:

1. **FSPB Professional Code for the Financial Services Industry**
2. **FSPB Standard on Conflict of Interest Management Framework**
3. **FSPB Standard on Whistleblowing for Financial Institutions**
4. **S17A(5) Malaysian Anti-Corruption Commission Act (MACC) 2009**
5. **Guidelines on Adequate Procedures to Section 17A(5) MACC 2009- Prime Minister's Department (PMO)**
6. **BNM's Guidelines on Minimum Audit Standards for Internal Auditor of Financial Institutions**

FSPB Guidance Note 1: Top Level Commitment

Ethical Culture and "Tone from the Top"

As the Board and Senior Management have full ownership of the organization's culture and the accountability of its results, they are in the best position to ensure the organization conducts its business without bribery and corruption. The success of a B&C program is mainly influenced by the ethical culture of an organization. The Board and Senior Management must therefore establish a strong 'tone from the top' to convey its commitment to zero tolerance for bribery and corruption.

The anti-bribery and corruption tone must be adopted equally by the middle- and first-line management. The tone from the top will only succeed where the leadership are seen to live by the standards they advocate.

PMO Guidelines on Adequate Procedures

Principle I: Top Level Commitment

The top-level management is primarily responsible for ensuring that the commercial organisation:

a. **practices the highest level of integrity and ethics;**
b. **complies fully with the applicable laws and regulatory requirements on anti-corruption;**
c. **effectively manages the key corruption risks of the organisation.**

Commitment

The commitment of the Board and its Senior Management to the organisation's stance on 'zero tolerance' for B&C is demonstrated through appropriate involvement in the development and/or enhancement and subsequent assessment of a governance structure that ensures the effective implementation of a B&C program encompassing the following:

- Bribery and Corruption risks management framework (policies and objectives to adequately address bribery and corruption risks)
- internal control system
- regular review and monitoring and
- regular training and communication

The effective implementation of a B&C program is also contingent on adequate resourcing of competent persons or functions that has the responsibility for the identification, assessment and mitigation of B&C risks. For example, in the 1st Line of Defence, Business Unit Heads and In-Business Control Units would be well positioned to address certain emerging B&C risks associated with Gifts & Entertainment, Travel Expenses, Agents & Third Parties, Commission Structures, Interaction with Customers, Business Partnerships, Government and Public Official Interactions, Procurement & Sourcing, Donations and Sponsorships.

In the 2nd Line of Defence, Human Resources could be well placed to address emerging B&C risks arising from People/HR risks. Such risks would include Hiring Practices of Interns, Temporary Staff, Contractors, Fulltime Employees and Third-party Vendors.

A single functional group such as Legal & Compliance Unit or Group Compliance would ensure

the overall compliance of the B&C program within the organisation in addition to undertaking the role of an internal consultant to the 1st and 2nd Line of Defence units. However, the responsibility and accountability of the B&C program would lie with the Business Unit Heads and Senior Management. The lines of responsibility must be clearly established and documented in individual performance appraisal forms and RCSA (Risk and Control Self Assessments).

The commitment to 'zero tolerance' for B&C including the consequences of such unacceptable behaviours must be regularly communicated in writing and made public internally throughout the organization and externally to third parties associated with the organization.

Keeping the Board and Senior Management informed

Organizations should consider mechanisms to demonstrate how the Board and Senior Management are aware of their B&C exposure and the effectiveness of its B&C program. Examples may include periodic confirmations (which could be part of a larger attestation, such as in connection with a code of conduct), as well as governance and oversight records (e.g., meeting packets and minutes of periodic risk management forums or committees).

Remedial activities and discipline

Organisations should have a framework by which individual deficiencies in B&C control execution are assessed and rectified. The framework to address B&C risks could be part of a larger risk management, human resources, or other employee disciplinary framework. The severity of any remedial actions (which can include informal notices) and consequences (which may include loss or rescission of pay, and termination) should be proportionate to the root causes including the severity of the deficiency, the job role of the individual (with the expectation that more senior professionals should be accountable for demonstrating proper awareness of B&C principles) and the relevant individual's intent. For example, an employee who does not complete mandatory B&C training within a specific time period may be subject to a different level of disciplinary action than an employee who intentionally subverts controls relating to the provision of gifts to government officials. Management should ensure that such disciplinary actions are taken and, for larger organisations, breach-related metrics may be incorporated into broader governance and oversight routines.

Internal whistleblowing mechanism

To promote a culture of integrity and transparent communication, organisations should review the FSPB Standard on Whistleblowing for Financial Institutions and adopt appropriate measures.

FSPB Guidance Note 2: Risk Assessment

Definition

Risk Assessment is a documented disciplined assessment methodology or process to evaluate the following:

- anticipated likelihood and possible impact of B&C
- analyse and prioritise identified B&C risks
- evaluate controls in place for their suitability and effectiveness to mitigate B&C risks

PMO Guidelines on Adequate Procedures

Principle II: Risk Assessment

A bribery and corruption risk assessment should form the basis of an organisation's anti-corruption efforts.

Scope

Organisations should consider whether B&C risk should be assessed as a standalone document, or whether the assessment should be part of a larger family of risks (e.g., non-financial risk, conduct risk, financial crime risk, etc.). Depending on factors which may include the size, complexity, and business/products of the organisation, B&C risk assessment may be for the organisation as a whole, or may be conducted based on business line/unit, function, or at the legal entity level.

Frequency

This could be done on a periodic basis, or a trigger basis, or a combination of both. Potential triggers include materially relevant audit findings, changes in underlying business, significant changes in control execution, etc. However, as a baseline, organisations should reassess the risk at least every three years, or if there is a material change in applicable law.

Risk Identification

A comprehensive review should be undertaken with inputs from all relevant stakeholders to identify all B&C risks that can occur within the FI's processes, client base or target market reached to market products and services and other third-party interactions. In the absence of appropriate controls or effective controls, the following inherent risk areas have been identified as having high and unacceptable B&C risks:

a. Staff Employment and Internships for Clients, Government Officials or their related persons
b. Gifts & Entertainment/ Business Hospitality
c. Cash and Manual Payments
d. Products and Business Transactions/Deals
e. Travel and /or Hotel Accommodation
f. Sponsorships and Donations (charitable and political)
g. Suppliers & Intermediaries
h. Clients & Business Strategy
i. M&A Activity

Assessment Methodology:

The assessment methodology shown below intends to serve as a guidance. Organisations should consider the most suitable risk assessment methodology assessment appropriate to the size, nature of business and complexity of its organisation. In most instances, B&C risks are assessed as part of the organisation's overall Operational Risk Framework.

a. Inherent risk

The inherent risk should reflect the B&C risk that the assessed unit is exposed to in the absence of specific B&C-related controls. In assessing inherent risk, organisations may find it appropriate to consider non-B&C day-to-day business controls (such as expense management, procurement, accounting, and fraud-related controls).

b. Appropriateness and effectiveness of controls

Organisations should consider whether there are relevant controls fit to mitigate the inherent risk, the existence and nature of any gaps in the design of or adherence to those controls, and the existence and nature of any other identified issues. Usually there are existing controls which are designed to mitigate another principal risk. Nonetheless they should be assessed for their effectiveness against B&C risks.

c. Residual risk, reflecting the impact of the controls against the inherent risk.

To this effect, appropriate risk measurement metrics should be established to compute the Residual Risk, taking into account Probability of Occurrence, Financial and Non-Financial Impacts and Control Effectiveness.

Risk Management Tools

The following are examples of risk management tools which could assist when assessing B&C risks within the Operational Risk Framework:

(a) Risk Taxonomy

A common taxonomy of sources of B&C risk types helps in ensuring consistency in risk identification and assessment activities, and articulation of the nature and type of inherent B&C risk to which the FI is potentially exposed.

(b) Risk and Control Self-Assessments (RCSAs)

Risk and control assessments are one of the primary tools typically used to assess inherent operational risks and the design and effectiveness of mitigating controls within the FI. RCSAs provide value through:

- including an assessment of business environment, inherent risks, controls, and residual risks, referencing the FRFI's operational risk taxonomy;
- encouraging proper alignment between the risk and its mitigating controls;
- being completed on a periodic basis (to support accurate and timely information); and

- having appropriate supporting activities and frequency of maintenance to remain current and relevant in the management of operational risk

RCSAs are completed by the first line of defence, including the various control groups, and should reflect the current environment but also be forward-looking in nature. Resulting action plans emerging from completion of an RCSA should be tracked and monitored to facilitate required enhancements being appropriately implemented. In addition, the second line of defence should review and provide objective challenge to the risk and control assessments, and the resulting action plans of the first line of defence.

PMO Guidelines on Adequate Procedures

Principle III: Undertake Control Measures

- appropriate controls and contingency measures which are reasonable and proportionate to the nature and size of the organisation
- to address any corruption risks arising from weaknesses in governance framework, processes and procedures.

FSPB Guidance Note 3: Undertake Control Measures

Policies and Procedures

Policies and Procedures are important tools to establish clear rules, guidelines and standard operating procedures to mitigate B&C risk. As organisations can vary in size, nature, and complexity, there is no "one size fits all" set of policies and procedures, even for organisations within the same industry.

For instance, an organisation with 100 employees may find it practical to require Legal or Compliance review of all gifts and hospitality, whereas a substantially larger organisation with an international footprint and multiple product lines may appropriately address relevant risks though a tier-based approach where (depending on factors such as the nature of the gift/hospitality, the per-person cost, and the intended recipients) different approvers may be required when certain thresholds or factors are met.

Examples of Anti-B&C Policies in Practice Today

1. Anti B&C Policy
2. Anti B&C Due Diligence Guidelines for Business Transactions/ Deals
3. Gifts and Entertainment Policy
4. Anti B&C Hiring Procedures
5. Anti B&C Advisor/Intermediary Procedures
6. Anti B&C Third Party Risk Management and Due Diligence Procedures

Elements of the Policies and Procedures

The following are some important elements of comprehensive B&C policies and procedures.

a. Definitions

Relevant terms and corresponding definitions should be identified in consideration of the Malaysian Anti-Corruption Act and other laws and regulations that apply to the organisation

and its Associated Persons. Organisations may also consider the definitions and principles of the UK Bribery Act and US Foreign Corrupt Practices Act, and relevant guidance as issued by respective courts and enforcement agencies. Key terms may include "Corruption," "Bribe" (or "Gratification"), "Facilitation Payment," "Public Official" (which may be defined to effectively include employees of Government Linked Companies as well as foreign officials) and "Associated Person."

b. Prohibitions

Organisations should prohibit the offer, promise, or payment of Bribes by the organisation, its employees, and its Associated Persons. Organisations should also prohibit the offer, promise, or payment of Facilitation Payments, although consideration may be given to circumstances of duress such as physical danger.

c. Gifts, entertainment, hospitality and travel (collectively, "G&E")

G&E can play an important and appropriate role in ordinary and customary business relations, including the opportunity to discuss business-related matters in less formal settings, the recognition of holidays and other cultural events, and the expression of ordinary social courtesies. Organisations may consider it appropriate to establish recording or approval requirements relating to the provision and acceptance of G&E.

Note:

- G&E should never be intended as a Bribe (or Gratification).
- Organisations may wish to consider whether certain types of gifts, such as festival money packets (in cash) may be offered or received as G&E and (where relevant) whether additional controls (or prohibition) may be needed.

d. Sponsorships/Charitable payments

The organisation's policies and procedures should be determined in consideration of payments to sponsorships or charitable organisations, to manage the risk that these may be used similarly to gifts, payments, or other things of value and therefore constitute a Bribe or Gratification.

e. Political contributions

Organisations should consider the circumstances under which it will make payments to support a political organisation or influence an election (including referendums), or allow others to make such payments on its behalf; similarly, organisations should consider the circumstances under which it will allow the use of its facilities and resources (including personnel) in connection with political contributions. Such circumstances should be consistent with applicable election laws, and should never be offered, promised, permitted or made as a Bribe or Gratification.

f. Use of Third Parties

i. Organisations should be aware of some of the ways in which third parties may introduce B&C risk including the following:

- Organisations might utilize a broad range of third-party categories (sales agents, distributors, introducers, joint ventures partners, consulting companies). in the course of its business. It is appropriate to engage third parties when there is a need for their services, and they are performed in an appropriate manner and at market rates. However, if a third party, offers a Gratification or improper benefit in the course of performing work for the organisation, this may expose the organisation itself (and its staff and management) to B&C enforcement.

- In some cases, the third party may be owned, controlled or closely connected to a Public Official. While the third party itself may not be obtaining or retaining business, it may have been improperly selected in order to provide a benefit to that Public Official.

ii. The organisation's B&C program should be designed and executed with the awareness of the above. Organisations should apply controls, including adequate due diligence, based on the third parties it utilizes. These controls may increase or decrease depending on the risk of a particular third party (or category of third parties), and may include (and/or may be part of the broader human resources, security, fraud and procurement controls):

- Measures to the confirm that there is a legitimate business need for the third party's services.
- Measures to confirm that the specific third party is selected based on appropriate business qualifications.
- Measures to review payments and confirm that they are reflective of market pricing, and the nature of the work performed (which may include due diligence to understand the mechanism by which the third party will perform its services). This would also include confirming that the work was actually performed as anticipated.
- Contractual provisions prohibiting the third party from making Bribes/Gratifications and other improper payments. Otherwise requiring the third party to agree to follow all applicable B&C laws
- Due diligence to identify the third party and/or its key personnel or ultimate beneficiary owner, and whether the same is (or is closely connected to) a Public Official.
- Due diligence to identify whether there is material negative B&C-related news relating to the third party and/or its key personnel or ultimate beneficiary owner.
- Due diligence to confirm that the third party is aware of B&C laws and regulations and, is subject to adequate policies and procedures to manage B&C risk.
- Questionnaires to support execution of the above.
- Periodic and ad hoc refresh of some or all the aforementioned controls.

g. Business partnership and opportunities

Organisations should consider circumstances under new business partnership or opportunities that might give risk to B&C risk for example:

- Projects, joint ventures involving government/public offices
- mergers and acquisitions
- high-value projects or projects involving many contractors or intermediaries.
- Contracts, transactions involving political exposed persons – where the proposed business relationship involves or is linked to a prominent public official.

Recordkeeping

Systems for recording the provision and receipt of G&E, charitable payments, and political contributions, including a description of cost and nature of the expenditure, the business purpose, the details pertaining to the giver and recipient and (where applicable) evidence of any approvals. Larger organisations should consider whether meaningful efficiencies can be achieved by integrating these systems with expense reimbursement systems.

Systems for recording material organisational developments that may impact B&C risk, such as the development of a new product, a meaningful change to business practices, entry into a new market, engaging in a partnership or joint venture, etc.

Institutions shall ensure proper record keeping is in place as per regulatory expectations, which include among others results of risk assessment, due diligence documents, reports, and other relevant documents in relation to bribery and corruption controls.

Relationship with other controls

The B&C policies and procedures may be designed to work with other control areas such as:

a. Code of Conduct
b. Finance and accounting systems designed to detect and deter fraud, misappropriation or other inaccurate recording of expenditures.
c. Procurement systems and records designed to reflect relevant details regarding the rationale for utilizing external vendors and service providers (including business need, competency of vendor, and pricing that reflects the market).

FSPB Guidance Note 4: Systematic Review, Monitoring and Enforcement

Organisations should establish a mechanism by which the Board and management have oversight of B&C risks and are able to take appropriate actions when needed. Such a mechanism can incorporate risk assessments, issue identification/management systems, and audit results.

This may be bolstered through the identification, provision and analysis of routine performance metrics or risk indicators. Examples can include metrics relating to the provision or approval of G&E, the utilization of third parties, or the identification of breaches.

The Three Lines of Defence (see Appendix III -sourced from IIA) may also conduct periodic reviews or exercise to assess the efficiency and efficacy of the B&C program, such as spot-testing adherence to procedures, analysing ad hoc metrics, checking due diligence quality and completeness, etc.

Some organisations have dedicated monitoring programs or procedures (which may include criteria for establishing scope, frequency, sampling methods, etc.) that is separate and apart from their audit function; In such cases, B&C controls should be incorporated into those programs.
The Three Lines of Defence may also, from time to time, provide subjective analyses (e.g., key or emerging risks, trends or anomalies, etc.) and papers (e.g., description of an enhanced G&E documentation system).

PMO Guidelines on Adequate Procedures

Principle IV: Systematic Review, Monitoring and Enforcement

The top-level management should ensure:

- **regular reviews are conducted to assess the performance, efficiency and effectiveness of the anti-corruption programme**
- **ensure the programme is enforced.**

Such reviews may take the form of an internal audit, or an audit carried out by an external party.

Internal Audit

B&C-related risks should be incorporated into an organisation's overall audit program, which should be designed with the particular organisation's needs, risks, and structure in mind, with due escalation to the outcome of the audits to the Board Audit Committee for oversight.
Regular reviews to assess the performance, efficiency and effectiveness of the anti-corruption programme, and ensure the programme is enforced may take the form of an internal audit, or an audit carried out by an independent party within the organisation or an external party. The review may be conducted at least once every three years to obtain assurance that the organisation is operating in compliance with its policies and procedures in relation to corruption.

FSPB Guidance Note 5: Training and Communication

Using training as a way to communicate policies and procedures

Relevant policies and procedures should be communicated throughout the organisation, including through periodic training for all directors, officers, relevant employees, and, where appropriate, agents and business partners. The content of the training may vary depending on the audience.

It may be appropriate for some organisations to adopt a multi-faceted approach to training. For instance, the organisation may require all employees to receive baseline B&C training (which could be part of a larger training program), while targeting certain employees for supplemental training, particularly if they have an elevate risk of encountering B&C scenarios, or have oversight responsibilities. The format/delivery of the training can depend on factors including the organisation's size, geographic disbursement, and other factors.

PMO Guidelines on Adequate Procedures

Principle V: Training and Communications

Develop and disseminate internal and external training and communications relevant to its anti-corruption management system, in proportion to its operation, covering the following areas:

- **policy**
- **training**
- **reporting channel**
- **consequences of non-compliance**

Customized training

Training content (including delivery language) should be developed in consideration of the audience and the particular reasons they should receive B&C training. For example, general training might include

(a) an overview of the core B&C principles and policy requirements,
(b) when and how to escalate, and
(c) the consequences – both individually and for the organisation – of a breach.

Where organisations provide tailored training for top management, training topics might include

(a) the importance of avoiding B&C,
(b) the key components of the potentially relevant laws, as they relate both to the financial organisation as well as the executive,
(c) how the financial organisation manages B&C risk, and
(d) the executive's role in the aforementioned.

Tailored training may also be appropriate for certain categories of individuals, such as those who engage Associated Persons; those who seek to influence governmental policy, regulation, or law-making; members of business units that have extensive governmental client base; individuals who advise on B&C matters; and (in some cases) key external parties (e.g., certain Associated Persons who present heightened risk and may not have otherwise received relevant training).

Applying and combining different modes of communication

Organisations should approach both training and communications from a variety of channels, and should consider a variety of media. Examples can include larger induction sessions, web-based programmed content, interactive classroom sessions (whether in person or electronically), or “town hall” or “all-hands” sessions. These may be supplemented or reinforced through periodic emails, printed materials (e.g., posters, quick reference cards, handbooks), video clips, etc. and on day-to-day routines such as team calls. In addition, organisations may incorporate B&C content or set aside B&C sessions into periodic business retreat or “offsite” events, as a means to reinforce the role of AB&C in the organisation’s operations.

APPENDIX I: Red Flags (Wolfsberg Group Guidance)

These are examples sourced from the Wolfsberg Group Guidance for financial institutions (https://www.wolfsberg-principles.com/wolfsberg-group-standards). The Wolfsberg Group consists of the following financial institutions: Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale, Standard Chartered and UBS.

Institutions could consider having in place triggers to identify the following for review and monitoring.

General

- Little to no relevant experience regarding the services to be provided
- Flawed background or reputation (including, for example, prior corruption or a negative reputation for integrity)
- Recent senior Public Official of the same government department or business responsible for the award of the contract or matter at issue or who worked in a procurement or decision-making position
- Transaction or Intermediary suggested by a Public Official, particularly one connected to the business or matter at issue
- Close business, personal or family relationship with a Public Official who has discretionary authority over the business or transaction at issue
- Party to a transaction or contract makes unreasonable/unsupported objections to ABC due diligence or representations or warranties being included in the agreement
- Party does not reside or have a significant business presence in the country where the service is to be provided
- Use of a shell company or some other non-transparent corporate structure
- Requires payment of a commission, or a significant portion thereof, before or immediately upon award of the contract
- Requests for unusual contract terms
- Requests for payment in cash, advance payments, payment to an individual or entity that is not the contracting individual/entity, or payment into a country that is not the contracting individual/entity's principal place of business or the country where the services are performed
- Anticipates payments that cannot plausibly be commercially justified vis-à-vis the role undertaken
- Adjustment of remuneration demand during the course of the engagement, particularly in close proximity to the award of business
- Vague or unsupported book -keeping
- Heavy reliance on cash

Associated Persons

Examples of red flags when dealing with associated persons include:

- the associated person insists on operating in anonymity
- inappropriate payment requests, e.g. requests for indirect payments made payable in a country other than one where the associated person operates, or to a separate entity
- due diligence identifies significant past allegations or incidents of corruption or illegality
- a public official recommended the associated person, particularly one with discretionary authority over the business at issue
- there are persons involved in the transaction who have no substantive commercial role
- the associated person objects to reasonable clauses in the contract regarding compliance with anti-bribery laws or other applicable laws
- the associated person does not reside or have a significant business presence in the country where the customer or project is located
- due diligence reveals the associated party is a shell company or has some other unorthodox corporate structure (e.g. a trust without information about the economic beneficiary)
- the associated person will not reveal its beneficial ownership, or is unwilling to provide documentary proof of ownership if asked
- the only qualification the associated person brings to the venture is influence over public officials, or the associated person claims that he can help secure a contract because he knows 'the right people'
- the associated person requests an increase in an agreed commission in order for the third party to:
    1. 'take care' of some people;
    2. circumvent a known requirement or cut some red tape; and
    3. to account for expenditure they must incur to obtain or retain business or a business advantage.

APPENDIX II: The Three Lines of Defence Model

The IIA (Institute of Internal Auditors) endorse the 'Three Lines of Defense' model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:

The first line of defence (functions that own and manage risks):

This is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of the company, its objectives, the environment in which it operates, and the risks it faces.

The second line of defence (functions that oversee or who specialise in compliance or the management of risk):

This provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line, conducts monitoring to judge how effectively they are doing it, and helps ensure consistency of definitions and measurement of risk.

The third line of defence (functions that provide independent assurance)

This is provided by internal audit. Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines are operating effectively and advise how they could be improved. Tasked by, and reporting to the board / audit committee, it provides an evaluation, through a risk-based approach, on the effectiveness of governance, risk management, and internal control to the organisation's governing body and senior management. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and are operating effectively.

Appendix III: Guidance Notes Checklist

The following checklist is intended to summarize the important elements of the Guidelines and is referenced to the PMO Guidelines on Adequate Procedures (PGAP). The checklist is by no means definitive or all-inclusive nor is it a minimal. It should serve as a tracking mechanism for FSPB members to utilize according to the requirements of the organization.

Item	Elements	Reference PGAP	Y/N	Target Date	Remarks
	TOP LEVEL COMMITMENT	P1			
1	**Establish "tone from the top":**	4.1.2			
	Statement issued by the Board of Directors and Senior Management on the following:				
	-Zero tolerance to B&C -Consequences of breach including disciplinary action for all levels				
2	**Appropriate Degree of Engagement**	4.1.2			
	There is a review mechanism for Board of Directors and Senior Management to assess effectiveness of:				
	B&C Risk Management Framework				
	B&C Internal Control System				
	B&C Review and Monitoring				
	B&C Training and Communication				
3	**Anti-bribery and corruption program could include the following:**	4.1.3			
	Clear policies and objectives that adequately address corruption risks	i			
	Promote a culture of integrity	ii			
	Communicate policies and commitments on anti-corruption to both internal and external parties	iii			
	Promote use of reporting (whistleblowing) channels for:	iv			
	any suspected and/or real corruption incidents				
	inadequacies in the anti-corruption compliance program				
	appoint a competent person or function to be responsible for all anti-corruption compliance matters	v			

	Ensure lines of authority for overseeing the anti-corruption compliance programme are appropriate	**vi**			
	ensure that the results of any audit, reviews of risk assessment, control measures and performance are reported to all top-level management, including the full Board of Directors, and acted upon.	vii			
	RISK ASSESSMENT	P2/4.2			
4	**Scope**				
	Are B&C risk assessed as a standalone document	4.2.3			
	Is the assessment part of a larger family of risks (e.g., non-financial risk, conduct risk, financial crime risk, etc.)?	4.2.3			
	Factors such as size, complexity, and business/products of the organisation should be considered if B&C risk assessment may be for the organisation as a whole, business line/unit, function, or at the legal entity level				
5	**Frequency**				
	This could be done on a periodic basis (at least every 3 years), or a trigger basis, or a combination of both.				
6	**Risk Identification**	4.2.2			
	Steps to identify include:				
	weaknesses in the governance framework and internal systems/ procedures	i			
	financial transactions that may disguise corrupt payments	ii			
	business activities in countries or sectors that pose a higher corruption risk	iii			
	non-compliance of external parties regarding legal and regulatory requirements related to anti-corruption	iv			
	relationships with third parties in its supply chain (e.g. agents, vendors, contractors, and suppliers) that can create exposure to B&C	v			
7	**Assessment Methodology**				

	B&C risks are assessed as part of the organisation's overall Operational Risk Framework using tools such as RCSA (Risk Control Self-Assessments)				
	B&C related Inherent Risks, Mitigating Controls and Residual Risks are identified by First Line of Defence and reviewed by the Second Line of Defence				
	First and Second Lines of Defence identifies B&C related risks and incorporate them in RCSA				
	UNDERTAKE CONTROL MEASURES	P3/4.3			
7	**Due diligence**	a			
	establish key considerations or criteria for conducting due diligence on any relevant parties or personnel (such as Board members, employees, agents, vendors, contractors, suppliers, consultants and senior public officials) prior to entering into any formalised relationships.				
	Methods may include background checks on the person or entity,				
	a document verification process,				
	conducting interviews with the person to be appointed to a key role where corruption risk has been identified.				
8	**Reporting Channel**	b			
	establish a whistleblowing channel For smaller organisations, the reporting channel can be a dedicated e-mail address;	i			
	encourage persons to report, in good faith, any suspected, attempted or actual corruption incidents	ii			
	Establish a secure information management system to ensure the confidentiality of the whistle-blower's identity and the information reported;	iii			
	prohibit retaliation against those making reports in good faith.	iv			
9	**Policies and Procedures**	4.3.2			
	Establish policies and procedures to cover:				

	anti-bribery and corruption policy or statement	**i**			
	conflicts of interest	ii			
	gifts, entertainment, hospitality and travel	iii			
	donations and sponsorships, including political donations	iv			
	facilitation payments	v			
	financial controls, such as separation of duties and approving powers or multiple signatories for transactions	vi			
	non-financial controls, such as a separation of duties and approving powers or a pre-tendering process	vii			
	managing and improving upon any inadequacies in the anti-corruption monitoring framework	viii			
	record keeping for managing documentation related to the adequate procedures	ix			
	Policies should be:	4.3.3			
	endorsed by top level management	i			
	kept up to date	ii			
	publicly and/or easily available	iii			
	suitable for use where and when needed	iv			
10	**SYSTEMATIC REVIEW, MONITORING AND ENFORCEMENT**	P4/4.4			
	The top-level management should ensure that regular reviews are conducted by internal audit, or an audit carried out by an external party to assess the performance, efficiency and effectiveness of the anti-corruption programme, and ensure the programme is enforced.	4.4.1			
	The reviews should form the basis of any efforts to improve the existing anti-corruption controls such as :	4.4.2			
	plan, establish, implement and maintain a monitoring programme, which covers the scope, frequency, and methods for review	4.4.3/ i			

	identify the competent person(s) and/or establish a compliance function to perform an internal audit, in relation to the organisation's anti-corruption measures	**ii**			
	conduct continual evaluations and improvements on the organisation's policies and procedures in relation to corruption	iii			
	consider an external audit (for example MS ISO 37001 auditors) by a qualified and independent third party at least once every three years	iv			
	monitor the performance of personnel in relation to any anti-corruption policies and procedures to ensure their understanding and compliance with the organisation's stance in their respective roles and functions	v			
	conduct disciplinary proceedings against personnel found to be non-compliant to the programme.	vi			
11	**TRAINING AND COMMUNICATION**	P5/4.5			
	develop and disseminate internal and external training and communications relevant to its anti-corruption management system, in proportion to its operation, covering the following areas:	4.5.1			
	policy	i			
	training	ii			
	reporting channel	iii			
	consequences of non-compliance	iv			
	Communication of Policies				
	The organization's anti-corruption policy should be made publicly available,	4.5.2			
	and should also be appropriately communicated to all personnel and business associates.				
	Communication Plan on anti-B&C	4.5.3			
	Key points should be communicated				
	Target audiences				

	how they will be communicated				
	timeframe for conducting the communication				
	Consider what languages the materials will be communicated in.				
	These may include, but are not limited to:	4.5.4			
	messages on the organisation's intranet or website	i			
	emails, newsletters, posters	ii			
	code of business conduct and employee's handbooks	iii			
	video seminars or messages	iv			
	town-hall sessions	v			
	Training				
	ensure employees and business associates have thorough understanding of the organization's anti-corruption position	4.5.5			
	The training may be conducted in a variety of formats, including but not limited to:	4.5.6			
	induction programs featuring anti-corruption elements	i			
	role-specific training, which is tailored to corruption risks the position is exposed to	ii			
	corporate training programs, seminars, videos and in-house courses;	iii			
	intranet or web-based programs	iv			
	town hall sessions	v			
	retreats	vi			
	out-reach programs	vii			

END OF FSPB GUIDANCE DOCUMENT