General Principles for Financial Forensics

PREAMBLE

The Conference of International Investigators (CII) has endorsed 'Uniform Principles and Guidelines for Investigations' ("Investigation Guidelines").[1] As part of its function, an Investigative Office may conduct activities known as financial forensics.[2] Financial forensics is a field that, in the context of an Investigative Office, involves the application of specialised knowledge, experience, and investigative skills by qualified forensic accounting professionals to identify, analyse, quantify, interpret and communicate financial information and evidence in the conduct of the Office's investigations or other fact-finding activities.

The purpose of these General Principles is to provide common uses and principles for the conduct of financial forensics by Investigative Offices and the professionals conducting them. This document also applies to external service providers or other functions within the organisation conducting financial forensics on behalf of, or in collaboration with, its Investigative Office.

The General Principles for Financial Forensics supplements the CII's Investigation Guidelines and was endorsed by the CII at its 20th Conference.[3] The scope and nature of financial forensics, whether conducted by Investigative Offices or external parties, remain within the discretion of each organisation and are to be conducted by qualified professionals applying professional judgment within the framework of each organisation's own requirements, policies and procedures. These General Principles do not and are not intended to bind any Organisation; or confer, impose or imply any duties, obligations or rights on them; or affect their rights and obligations per its rules, policies and procedures including any privileges and immunities afforded to them by international treaty, customary international law and the laws of the respective member state.

THEMES AND OBJECTIVES

1. Investigative Offices conduct financial forensics including transactional data analytics to detect or to investigate possible prohibited practices or as proactive fraud detection and risk assessment measures. When conducted effectively, such activities can significantly enhance the impact and effectiveness of the Investigative Office's work, its reviews and investigations.

2. Indicators of prohibited practices, such as misappropriation, theft / embezzlement of funds or goods, misuse of funds, corruption, and conflicts of interest, may be revealed or substantiated by forensically reviewing finance and accounting-related documents and records and related supporting documentation of the organisation, its implementing agencies, project office and/or project suppliers.

3. Indicators may include but are not limited to (i) financial and accounting anomalies, such as irregular postings, unusual adjustments, misapplied expenses, duplicated payments, or atypical financial ratios; (ii) falsified financial reports and associated supporting documents and ledgers (such as vendor, payroll, cash and customer ledgers); (iii) questionable

[1] The 'Uniform Principles and Guidelines for Investigations' were originally endorsed by the 4th Conference of International Investigators in 2003. A revised set was endorsed by the 10th Conference in 2009.

[2] Consistent with the Investigation Guidelines, the term "Organisation" used herein includes reference to all institutions participating in the Conference of International Investigators. The term "Investigative Office" refers to the investigative units or function of each organisation with a mandate to investigate allegations of fraud and wrongdoing within their organisation or associated with its projects and activities.

[3] At its 20th Conference, the CII also endorsed 'General Principles for Proactive Integrity Risk or Fraud Detection Activities'.

expense patterns and unfamiliar suppliers; (iv) unexplained or unsupported revenues, expenses or accounting adjustments; or (v) inflated pricing and/or other indicators relevant to procurements and the various stages of a transaction or program activity life cycle.

4. The presence of the indicators may also signal intentional violations or circumvention of internal control processes and possible collusion either within the organisation or involving external parties. Investigating how this occurred and by whom provides critical information in support of any investigative conclusions as well as recommendations for additional fraud mitigation measures.

5. Financial forensics may be referred to by an Investigative Office or its external providers as "forensic accounting," "financial fraud inspections/investigations," "forensic audits," or "fraud audits" or other terms reflecting the scope and purpose of the underlying activities. The activities may apply to projects and programs administered or financed by the organisation, internal organisational activities and operations, or staff misconduct matters.[4]

USES AND ROLE

6. Financial forensics have multiple uses for Investigative Offices. The activities may be used within the scope of an investigation of alleged prohibited practices including staff misconduct. They may also be used in the context of allegations received or identified fraud indicators (i.e., 'red flags') that may not yet be the subject of a formal investigation and need further forensic review or assessment.

7. Additionally, financial forensics may be used as an integral part of the Investigative Office's fraud deterrence efforts or mandate to detect fraud or other prohibited practices in high integrity-risk situations. They may also be used to quantify the economic losses or impact of a prohibited practice or misconduct to the organisation for pursuing relevant restitution or sanctions.

CONDUCTING THE ACTIVITIES

8. The professionals conducting the work, whether investigators or other professionals within, or external to, the Investigative Office, should preferably[5] have the requisite professional credentials, qualifications, skills and experiences in accounting principles and processes, accounting systems and controls, and financial reporting. They should also be skilled in, as needed, applications of digital analytical tools and data analytics, forensic techniques and fraud schemes, evidence collection and interpretation, interviewing, and investigative report writing. The more skilled professionals are often referred to in the field as 'forensic accountants' or 'financial investigators.'

9. The professionals conducting the work should employ an investigative mindset in the identification, analysis and evaluation of financial, accounting and other information relevant to the activities contemplating that the information may be intentionally biased, false, misleading and/or incomplete.

10. The scope and extent of the work should be aligned with the purpose and objectives of the activities to be conducted, available resources, access to information and witnesses, and the relevant standard of proof; i.e., whether the objective of the work is for fraud detection or deterrence, the forensic assessment of red flags, the investigation of possible wrong-

[4] For staff misconduct matters, financial forensics may also include an examination of staff personal financial records and activities, as allowed by the organisation's internal rules and policies.

[5] The requisite professional credentials, qualifications and depth and breadth of skills and experience would vary based on the nature and complexity of the financial forensics work being performed (e.g., basic review of bank statements versus complex funds tracing) and the resources available.

doing, the pursuit of possible sanctions, the quantification of economic losses, or a combination thereof.

11. To the extent provided by the organisation's rules, policies and relevant agreements, the professionals conducting financial forensics shall have the authority to examine and copy for their work the relevant books and records including digital versions of projects, executing agencies, individuals or others participating or seeking to participate in the organisation's operations or financed activities.

12. To the extent provided by the organisation's rules, policies and relevant agreements, the Investigative Office may use financial forensics professionals to conduct data analytics on relevant financial, accounting and associated digital data (such as procurement tenders) as effective and timely detection measures to identify anomalies or other indicators of possible prohibited practices and to enhance the selection of transactions for further review or investigation.[6]

13. The review and analysis of financial, accounting and associated digital data records should include a review of digital extracts of accounting and other data,[7] where possible, to enhance and quicken the detection and clarification of issues. The data should be appropriately structured and formatted to facilitate analysis using digital tools such as sorting, filtering, grouping, summation, content queries, graphical display and for identifying critical patterns, links and trends.

14. Financial forensics may be accompanied by digital forensics and/or e-discovery activities on relevant data and/or digital devices where possible to gain additional relevant information not otherwise available, to validate source data or to detect falsified information, as relevant. For example, recovered emails and metadata may reveal that the true source of an external invoice submitted to the organisation was an employee of the organisation rather than the purported supplier.[8]

15. The work may require interviews of potential witnesses and alleged subject(s) and/or their associated documented communications to establish context, understand procedures and processes, and to clarify, corroborate, validate, substantiate or refute allegations or preliminary findings. The work may also require independent corroboration of information by third parties (e.g., banks and suppliers).

FINDINGS AND REPORTING

16. Findings and observations from financial forensics, whether alone or combined with information and findings from other investigative activities, may be used by the Investigative Office as relevant to: (i) inform the conduct of further review or investigative activities, case closure or referral; (ii) conclude and report on the outcome of a formal investigation including associated economic losses; or (iii) communicate findings and losses internally to the organisation, an implementing agency or supplier for information and action, as relevant, and/or (iv) communicate evidence and findings to an administrative or judicial authority in accordance with applicable rules, as appropriate.

17. Howsoever used, findings are to be substantiated and communicated in the context of the scope and purpose of the activities conducted, relevant standard of proof, and applicable

[6] Proactive detection techniques using data analytics are best applied on live or near-live digital data, when available and as relevant.

[7] Such as procurement data, supplier lists, shipment data including non-financial data from external or open sources, such as business registrations.

[8] The skills and experience of the professional conducting the digital forensics and analysis should be aligned with the scope and objectives of the work.

policies of the organisation and Investigative Office.[9] Findings should be well documented and supported, and the relevant supporting documentation and data should be maintained as part of the evidentiary record, as applicable. This includes, but is not limited to, copies of accounting ledgers and journals; transactional supporting documentation such as invoices, bank statements, payment documentation and delivery receipts; detailed analysis and worksheets; digital forensic and/or e-discovery analysis results; third party information and confirmations; open source search results, corporate registrations and filings; communications; and records or transcripts of interviews, as applicable.

18. The identification of root causes and control weaknesses from financial forensics and other investigative activities can form the basis for recommending fraud risk mitigation measures to the organisation or its implementing agencies. The quantification of economic losses or impacts can be used to support the organisation's pursuit of restitution, recoveries, fines and/or sanctions.

GENERAL CONSIDERATIONS

19. The same general principles as outlined in the Investigation Guidelines shall apply while conducting financial forensics as related to maintaining independence, objectivity, impartiality, fairness and integrity; maintaining the confidentiality of sensitive and non-public information; and disclosing potential conflicts of interest of the staff conducting the work.

20. Investigative Offices are further encouraged to consider sharing information from their financial forensics or performing joint activities with other Investigative Offices, within their existing arrangements and parameters for sharing information. For example, for implementing programs funded by two or more organisations, financial forensics could detect overlapping expenditures and duplicate claims made by the implementer to multiple organisations.

21. The general principles provided in this document may not be phrased to suit all possible circumstances arising from the conduct of financial forensics. Due to the unique nature of many activities conducted by Investigative Offices within their mandates and an organisation's specific rules and policies, professional judgment should be exercised when applying these General Principles.

IMPLEMENTING GUIDELINES

22. In addition to these General Principles, the CII may develop and publish detailed *Implementing Guidelines for Financial Forensics* to be used for reference as needed as further non-binding guidance for Investigative Offices conducting such specialised activities.

[9] Possible applicable standards may be reasonable basis, preponderance of evidence, beyond a reasonable doubt or other standard as is applicable to the scope and purpose of the work and as is required by the organisation's policies.