Forensic Audit Standard

CONTENT

The purpose of this standard is to improve the quality of Forensic Audits by informing the users and suppliers of Forensic Audits of the conditions that may be imposed on the design and performance of a fraud investigation.

With this standard, the Institute of Fraud Auditors aims to ensure that recipients of reports on Forensic Audits can always assess the report in the same way.

1 Introduction

A Fraud Auditor is a professional whose activities are focused on the prevention, detection and/or investigation of fraud. The present standard is limited to the investigative activities which are hereafter referred to as a Forensic Audit.

A Forensic Audit is an investigation with often an important financial dimension that is generally carried out in a multidisciplinary context and whose findings may be used in legal proceedings.

From this definition, a number of elements can be derived that are important in the context of a quality standard and that will be further elaborated. A Forensic Audit distinguishes itself by its fraud-related character from other types of investigations and therefore makes high requirements on the performance and results of the investigation and on the auditors.

The person or persons executing the Forensic Audit is referred to as the Forensic Auditor.

This document has been prepared and is maintained by the IFA. If you believe that changes are necessary, we ask you to submit them to the IFA in a substantiated manner. We will then consider making the necessary changes as appropriate.

For guidance on privacy-related aspects of the Forensic Audit, we refer the reader to the IFA guidelines on GDPR.

In this document, the following verbal forms are used:

- "shall" indicates a requirement;
- "should" indicates a recommendation;
- "may" indicates a permission;
- "can" indicates a possibility or a capability.

This guide represents quality standards for Forensic Auditors and is not in anyway replacing any legal obligation applicable to the Forensic Auditor. Depending on the position of the Forensic Auditor (part of the internal audit department, private consultant, public sector auditor) the activities could differ on some points.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

- **Commissioning Organization**: the natural or legal person for whose legitimate interest the Forensic Audit is performed[1].
- **Forensic Auditor**: the natural or legal person charged with a Forensic Audit by the Commissioning Organization. The Forensic Auditor can be an internal department or an external service provider.
- **Team Member or Investigator**: an individual acting under the responsibility of the Forensic Auditor on a specific Forensic Audit assignment. The individual

[1] In some cases (e.g. within the public sector), the legitimate interest (of the Commissioning Organization) might be delegated – by law, regulations or other provisions – in a structural way to the Forensic Auditor.

preferably holds the quality certificate Registered Fraud Auditor.
- **Subject**: the natural or legal person who is, has been or is likely to become the subject of the Forensic Audit.
- **Open Source Intelligence (OSINT)** : the practice of collecting information from published or otherwise publicly available sources, especially in relation to physical persons, legal entities and the relation(s) between them.
- **Policy**: intentions and directions of an organization as formally expressed by its top management.
- **Structured versus Unstructured data** : Structured data is organized according a predefined data model e.g. a file, a database : Unstructured data lacks any predefined format or model e.g. text, mail, pdf, video, audio.

3 Identify

3.1 Identify the allegations / irregularities / whistleblowing notification

After receiving the initial information, the Forensic Auditor should:

- Assess the information and define the possible irregularities/allegations.
- Assess whether the received information can be investigated and whether the information could have been manipulated by the source.
- Assess the source of the information and its reliability.
- Assess the substantiating documentation/evidence.

3.2 Identify the (legal) persons involved

Based on the available information at stage, the Forensic Auditor shall:

- Determine the individuals /legal entities or other third parties involved in the potential irregularities.
- Evaluate any potential conflict of interest regarding the identified parties that would compromise the independence of the Forensic Auditor.

3.3 Develop the potential fraud theory

In order to be able to assess the appropriateness to proceed with a Forensic Audit, the Forensic Auditor should:

- Describe the potential fraud-scheme(s), based on the information provided by the source and the additional information.
- Determine a plan of action to investigate the potential fraud scheme(s) and the finality of the Forensic Audit and the investigative questions that need to be addressed.

3.4 Gather additional information if required

In case required for the purposes of the initiate phase, the Forensic Auditor may gather additional information from the following sources:

- Information from the Whistleblower
    - In case of an audit initiated by a whistleblower, the whistleblower can be

addressed for additional information[2].
    - The Forensic Auditor shall take into account the sometimes delicate position of the whistleblower. According to the specific context, this implies that the Forensic Auditor should take actions in order to guarantee the confidentiality of his/her identity.
- Open Source Intelligence
    - The Forensic Auditor can gather additional information obtained by OSINT.
    - This information gathering should be done very discreetly.

3.5 Decision to proceed

The Forensic Auditor should document the overall assessment of the compliant/allegation and the plan of action.

In function thereof the Commissioning Organization shall make the final decision whether to proceed with the Forensic Audit.[3]

NOTE: From the start, it is important to specify if the allegations are about possible criminal activity as described by penal law. The Forensic Auditor (or the Commissioning Organization) might inform the judicial agencies upfront, or later on, based upon the audit findings. We refer to the disclosure standard as foreseen in 5.8

4 Plan

4.1 Composition of the Forensic Auditor's team

4.1.1 Roles

There are a number of roles that could be present in the team of the Forensic Auditor in function of the nature, complexity and extent of the investigation and/or the experience of the Forensic Auditor. It is possible that a Team Member (also referred to as Investigator) can take on multiple roles.

Lead Investigator

The Lead Investigator is the Investigator managing and leading the operational activities of the Forensic Audit and must have a proven track record in Forensic Audits. The Lead Investigator prepares the Forensic Audit, defines the strategy, and signs off the Forensic Audit report.

Quality Assurance Responsible

The Quality Assurance Responsible role is performed by an Investigator with a proven expertise in Forensic Audits and performs quality checks of the Forensic Audit on a continuous basis. A formal quality check of the final report should be conducted by the Quality Assurance Responsible prior to sharing the report with the client. Depending on the

[2] In case of an anonymous whistleblower the information might be gathered by means of an online secured system allowing confidential interactions.
[3] In some cases, the Commissioning Organization might delegate the power to make the decision to the Forensic Auditor. This could for example be the case for the Forensic Audit departments of governmental entities.

size and complexity of the investigation, the role can be taken up by the Lead Investigator.

Investigator

The Investigator executes the Forensic Audit, establishes findings and writes the Forensic Audit report. Depending on the size and complexity of the Forensic Audit, there can be one or multiple Investigators; or the Lead Investigator can perform the role of Investigator.

4.1.2 Competencies

The competencies of the Investigators included in the team are dependent on the nature of the Forensic Audit and can include the following skills:

- OSINT
- Forensic Technology
- Data Analytics
- Financial analysis skills
- Interview skills
- Legal knowledge
- Report-writing skills

These competencies are not necessarily attributable to one unique profile. In case the required competencies do not exist amongst the Team Members, these competencies may be outsourced to a subcontractor.

4.1.3 Independence

The Forensic Auditor shall ensure that no Team Members have a conflict of interest. Each active Team Member shall internally disclose any independence issue or, in general, any situation where there is an indication of conflicting interests, for example, but not limited to:

- A relative or close acquaintance working at the Commissioning Organization or at the Subject;
- Performing other services for the Commissioning Organization or the Subject insofar those could compromise the independence of the Team Member; or
- Having a (financial) interest at the Commissioning Organization or with the Subject;

After deliberation, the Team Member who has conflicting interests, shall be excluded from the Forensic Audit and the necessary mitigating measures (e.g. Chinese walls) should be put in place.

4.1.4 License private detective

For some investigative activities in a Forensic Audit a license of private detective is needed.

This is the case when surveillance activities need to be carried out and/or information cannot be obtained from the interested party[4] and therefore third parties (other than the

[4] The Royal Decree of 30 July 1994 states that all collection and analysis activities related to information obtained from the interested party does not need be carried out by a licensed private detective. The interested party can be the subject of the Forensic Audit or the commissioning organization who has an 'interest' that a Forensic Audit will be caried out.

Commissioning Organization - including sources to which the Commissioning Organization has a legal or contractual right of access to -, the Subject, the Whistleblower and open sources) need to be approached. In practice, this implies that a private detective license is required for 'extra muros'[5] investigations.

4.2 Forensic Audit Plan

The Forensic Audit Plan is a document which should be drafted at the start of a Forensic Audit and can set out:

- Goal(s) of the Forensic Audit;
- Scope and limitations of the Forensic Audit;
- Relevant data sources;
- Forensic Audit strategy (investigative techniques);
- Anticipated timing; and
- Reporting protocols.

The objective of a Forensic Audit Plan is to ensure a fair, balanced and thorough Forensic Audit.

The Forensic Audit Plan – and all of its' elements discussed in the below subparagraphs – is not a one-time event. The Forensic Auditor should continuously evaluate the Forensic Audit Plan and update the Forensic Audit Plan when deemed necessary.

4.2.1 Data sources & collection

The Forensic Auditor should determine which data sources will be consulted. Defining beforehand the relevant data sources will allow the Forensic Auditor to use the available time and resources in an appropriate manner. Data sources are generally of three types:

- **Testimonial evidence**: statements made by witnesses or suspects during interviews;
- **Digital evidence**: information in electronic form; and
- **Hardcopy evidence**: physical records produced by individuals or organizations such as notes, memoranda, letters, minutes of meetings, financial records, receipts etc.

The Forensic Auditor should reflect on how the relevant data will be collected. For example, but not limited to:

- Use of forensic technology;
- Administrative considerations;
- Legal considerations; or
- Access considerations.

The identification, preservation and collection of data is further discussed in chapters 5.1.1 and 6.1.

4.2.2 Investigative techniques

The Forensic Auditor should reflect and set out in the Forensic Audit Plan which investigative techniques will be used and what are the most efficient techniques for the

[5] OSINT is not considered to be an extra muros – investigation as it relates only to publicly available information.

Forensic Audit at hand taking into account the principles of proportionality and subsidiarity.

4.2.3 Timing

The Forensic Audit Plan can include the anticipated timing of the Forensic Audit and amongst other, the following elements:

- A prior agreed-upon timeline;
- Deadline for the deliverables such as the final report, supporting documents or recommendations to management; and
- Frequency of the status updates during the Forensic Audit, if any.

4.2.4 Reporting protocols

4.2.4.1 Updates

The Forensic Auditor should, define the protocol of providing updates. This can include, but is not limited to:

- Confidentiality
- Frequency;
- Format;
- Language; and
- Recipients of the update(s).

4.2.4.2 Final reporting

The Forensic Auditor should agree with the Commissioning Organization on the reporting protocol for the final report. The reporting protocol for the final deliverable can include elements such as:

- Confidentiality
- Timing;
- Format;
- Language;
- Recipients of the final deliverable.

4.2.4.3 Attorney privilege

Insofar the report, draft or final, falls under the legal privilege of attorneys the Forensic Auditor should apply the reporting and communication protocols defined by the involved attorney.

4.3 Assess legal implications

The Forensic Auditor shall acknowledge the need for checks and balances and by consequence segregation of duties in the process of fact finding and legal assessment. The role of the Forensic Auditor should lie in the fact-finding process.

For that reason, he shall in principle waive any obligation of partiality imposed on him and shall not advocate a legal position or pass judgment on the facts as established during the Forensic Audit he conducts.

However, the Forensic Auditor should be aware at all times that his factual findings will, if necessary, be used in a legal context. He therefore should take into account the relevant procedural and substantive legal framework when determining the timing and focus of his

Forensic Audit and formulation of any recommendations (if necessary, in general terms) at the end of his assignment.

4.4 Engagement letter

The engagement letter entered into between the Commissioning Organization and the Forensic Auditor should at least cover the following topics:

- Background and reason of the Forensic Audit
- Objectives
- Scope
- Investigative activities planned
- Limitations

5 Initiate

5.1 Hidden actions

The Forensic Auditor may consider to undertake some hidden actions that allow to take certain steps without alerting people.

5.1.1 Preserving and securing evidence

The Forensic Auditor should take the appropriate measures to ensure that (i) useful sources of information are identified, (ii) the information is preserved from alteration or deletion and (iii) critical data is collected without any further delay.

5.1.1.1 Identify data

The Forensic Auditor should identify all potential data sources which could contain information relevant to the Forensic Audit. The following data sources should be considered:

- Desktops, laptops
- Email servers
- Instant Messaging servers (Teams, Skype,..)
- File servers
- Archives
- Back-ups
- Portable devices
- Intranet, extranet, social networking
- Databases
- Legacy systems
- Network shares, home drives
- Applications, structured data
- Paper documents
- …

The Forensic Auditor should make the following considerations before commencing to preserve and collect evidence:

- Understand the objective and background of the collection

- Determine the mode of operation, the authority for the collection, employee consent granted (if required) and key onsite contact(s)
- Determine the physical location of the (electronical and hardcopy) information, e.g.:
  - Are there paper documents or objects in employee's offices that may be relevant?
  - Are potentially relevant paper documents or objects stored centrally? (libraries, file cabinets, warehouses, etc.)
  - How and where is electronic information stored?

The scope of data potentially subject to preservation and disclosure may be uncertain in the early phases and may change as the Forensic Audit progresses. The Forensic Auditor should anticipate change and have a procedure in place for capturing any newly identified information.

5.1.1.2 Preserve data

After all potential sources of relevant information have been identified, the Forensic Auditor should take steps to ensure that those data sources are protected from any form of alteration or deletion.

5.1.1.3 Collect critical data

Data which is considered as vital for the objectives of the Forensic Audit is considered as 'critical data'. The Forensic Auditor may collect such data in this phase of the Forensic Audit without any further delay.

Reference can be made to chapter 6.1 for further details on the collection of data.

5.1.1.4 Prepare for securing & restricting accesses (IT, building, bank account)

The Forensic Auditor should consider restricting the Subject's physical access as well as access to IT- or financial systems in order to prevent data destruction/alteration or further financial losses. Any such restrictions shall be authorized by the Commissioning Organization before applying them.

5.1.2 Surveillance

Surveillance activities shall only be performed by licensed private detectives (list available at the website https://vigilis.ibz.be/).

The Forensic Auditor should make the following considerations regarding the involvement of surveillance activities:

- The use of surveillance shall be considered thoroughly. Surveillance should only be used when no other audit activities suffice to confirm or disprove suspicions of fraud.
- The surveillance shall be followed up strictly and shall not be used longer than needed, taking into consideration subsidiarity, proportionality.
- Observations - also in public – which take place long-term and systematically (dynamic tracking) are only permitted under special circumstances
- All legal rules and instructions concerning private detectives shall be followed and

the general privacy rules should be taken into account, e.g:

- The immunity of the residence, garden and driveway must be respected
- Stalking and harassment must be avoided
- Spying on and making visual recordings of persons in places not accessible to the public is punishable if a device is used (camera, binoculars, heat cameras, etc.) intentionally and without permission
- The use of cameras on the work floor is only permitted if the employer has clearly informed the employees about the use of the cameras and their exact location

5.2 Announce the investigation

Before starting the actual analysis of the collected data, the Forensic Auditor should assess the need and the opportunity to announce the Forensic Audit on a need-to-know basis. Such announcement may after careful consideration also be given to the Subject.

5.3 Interview the 'Subject'

At the start of the Forensic Audit and depending on the case, the Subject can be given the opportunity to present his/her version of the facts and to supply information.

Complementary, an in-depth interview with more detailed questions and/or confrontation with factual elements can take place later on.

In this context we refer to 5.2. and 6.3.

6 Execute

6.1 Data collection

6.1.1 Preliminary considerations

The Forensic Auditor should make the following considerations before the actual collection of data:

- The objectives of the Forensic Audit dictate the type of collection: This may be forensic images of physical devices, extracts of emails, or extracts from transactional systems
- Consider the authority to collect certain data sources and whether the Subject's consent is required.
- Consider privacy implications when collecting data from phones, tablets,…

6.1.2 Structured data

The Forensic Auditor should apply the following principles for the collection of structured data:

- Ensure the completeness and integrity of the collected or received data. For this purpose, the Forensic Auditor may create forensic images, copy full databases, calculate hash values or validate check sums.
- Apply a tier-3 approach on the data handling: original copy, backup copy and working copy.
- The subsequent analysis should be performed on the working copy version only.
- Document the audit trail (e.g. data request / data collection / data processing / data validation / approach applied).

6.1.3 Unstructured data

The Forensic Auditor should apply the following principles for the collection of unstructured data:

- Minimum handling of the original data source: the Forensic Auditor should avoid to make any changes to the original data source, e.g. by physically removing a hard disk to create a forensic image or applying a read-only access to the original data source.
- Account for any change: any actions that could impact the original data source, should be clearly documented.
- Validate the integrity of the collected data, e.g. through hash values or screenshots of the applied extraction techniques.
- Make use of Data Collection forms and Chain of Custody forms.

6.2 Interviews

6.2.1 Subject

6.2.1.1 Spontaneous declarations

If the Subject wants to make a spontaneous declaration, the Subject shall be beforehand informed that he or she is entitled to be advised by a legal counsel, a trade union representative or a confidential advisor and the Subject should confirm in written that he or she does not want to be assisted by a legal counsel, a trade union representative or a confidential advisor.

6.2.1.2 Organized interviews

The Forensic Auditor should apply the below principles when organizing and conducting an interview with a Subject:

- The Subject shall be formally invited for the interview.
- The invitation document should contain:
  - the reason/cause for investigation
  - the names of the Forensic Auditor, the Investigators (Team Members) that will conduct the interview and the Commissioning Organization
  - the practical details of the interview
  - the voluntariness of the interview and the right to be silent, except in the case that he/she must attend the interview based on legal provisions
  - the fact that he/she may be assisted by a legal counsel, a trade union representative or a confidential advisor

- the fact that he/she can request that the answers will be written in a statement, whenever requested in the interviewee's own words
- the fact that he/she will have the possibility to read this statement and to ask for adjustments
- the fact that he/she can provide additional information or evidence
- the fact that he/she can suggest additional research steps
- the fact that he/she can request a copy of the interview
- the fact that the statement and the information provided can be used in the report and, if necessary, as evidence in court

- The questionnaire shall be structured in such a way that next to the focus on confirmation/refutation and explanations of suspicions or findings, the Subject should also get the opportunity to (additionally) declare what he/she wants to declare
- If needed/requested, the interview shall be paused
- In the written statement, the Forensic Auditor should use question and answer format as much as possible
- The interviewee should be given (i) sufficient time to read the statement and (ii) the opportunity to ask for adjustments/additions
- In the case the interviewee refuses to sign the statement, the Forensic Auditor may confirm this refusal by signing off the statement as drafted at the moment of the refusal
- The following formal aspects should be applied:
  - The interview is carried out by 2 Investigators
  - Recording is only possible after the explicit consent of the interviewee and will not eliminate the need for a written statement
  - The written statement contains the date, time (start and end time) and place of the interview, the name of the Forensic Auditor and the Commissioning Organization, the names of the Investigators, the name and the function of the interviewee and/or any other person present during the interview

6.2.2 Witness

The Forensic Auditor should apply the below principles when organizing and conducting an interview with a witness:

- The Forensic Auditor should only interview persons as a witness if the witness can not be considered as a Subject at that moment. In case the status would change during the interview, the interviewee will be informed about (i) this change of status and (ii) the rules of play applicable under 6.2.1.
- The Forensic Auditor should seek for a good balance between an open mind to the statement while ensuring sufficient focus and detail.
- The Forensic Auditor shall take into account the possible vulnerable, uncertain situation of the witness/whistleblower and should bring this to the attention of the

Commissioning Organization with regard to protection from negative consequences

- The witness should be informed about the possibility his statement might be known to the suspect, e.g. in court proceedings

6.3 Investigative techniques

The Forensic Auditor should use the investigative techniques relevant for the Forensic Audit. Those techniques may include:

- OSINT
- Forensic Technology
- Data Analytics
- Forensic Accounting
- Interviews
- Surveillance
- …

The Forensic Auditor should select the appropriate investigative techniques based on the principles of legality, proportionality and subsidiarity and should take into account the latest technological possibilities.

6.4 Compliance with policies and procedures

In the case an external regulatory framework is not available nor applicable, the Forensic Auditor should use internal policies and/or procedures as a reference for his factual findings.

7 Close

7.1 Validation of findings

The Forensic Auditor shall validate that all findings are supported by reliable and verifiable evidence before drafting the investigation report (chapter 7.2) and before the confrontational interview (chapter 7.3).

The Subject should have the opportunity to comment and provide additional documentation in order to safeguard the right of defence. This validation by the Subject can take place after the confrontational interview (chapter 7.3).

Findings shall be validated internally as part of a quality review procedure.(chapter 4.1).

7.2 Drafting the Forensic Audit report

The following elements should be included in the Forensic Audit report:

- Background, reason and objectives of the Forensic Audit
- Scope of the Forensic Audit
- If relevant: limitations of the investigation
- Available information

- Timeline of actions and investigative techniques applied
- Factual findings

The following elements can be included additionally:

- Executive summary
- Recommendations to prevent future fraud and strengthen internal control within the Commissioning Organization. Recommendations can also be part of a separate recommendation letter
- List of the individuals that will receive a (numbered) copy of the report. Assigning numbered copies to each recipient will facilitate researching any leaks (it also deters recipients from sharing the received information)
- Annexes

The Forensic Audit report shall be factual and impartial. The Forensic Auditor shall not make any conclusions regarding the legal / criminal qualifications of the facts.

7.3 Reporting to bodies/persons authorized to make final decisions

From the onset, the Forensic Auditor should identify the potential recipients of the report.

These will typically include roles within the Commissioning Organization:

- Board of directors
- CEO, CFO, legal counsel
- Audit committee

7.4 Disclosure

Without prejudice to his obligations regarding independence and impartiality, the Forensic Auditor performs activities, that serve the determination of the legal position of the Commissioning Organization, although the Forensic Auditor will neither determine nor advocate a legal position . By consequence the Forensic Auditor shall be obliged to preserve the confidentiality of all information regarding the existence and the results of the Forensic Audit he conducts or has conducted.

The foregoing implies that the Forensic Auditor shall not (unless prior and written agreement by the Commissioning Organization) communicate about the existence and/or results of the Forensic Audit he conducted other than to Commissioning Organization, its' representative and/or its' highest governing body as the Forensic Auditor deems it necessary.[6]

The Forensic Auditor shall assess any judicial or government-related instruction to disclose information in accordance with the on him applicable legal, deontological and/or contractually agreed legal framework.

7.5 Archiving

The Forensic Auditor should apply the following principles for archiving the data related to a Forensic Audit:

- All data should be centralized
- All data (digital + hard copy) should be stored at a central, secure place with

[6] Some Fraud Auditors – e.g. within the public sector – might be subject to additional reporting or disclosure obligations.

restricted access

- All original hard copy data and data storages should be returned to the Commissioning Organization
- In accordance with the (privacy) laws concerning the storage of information, data has to be deleted after a specific period of time. We refer to the rules imposed by the GDPR legislation and the IFA code of conduct on privacy.
- On the one side, information, especially personal data, should not be stored longer than needed. On the other side, data from cases referred to judicial authorities might be needed later.
- Data should be deleted definitively (shredding hard copies; deleting digital data and/or destruction of data storages) as soon as possible.