COMPLIANCE AUDIT MANUAL

(CAM)

AFROSAI-E

CONTENTS

COMPLIANCE AUDITING – WORKING PAPERS
1. IC1 Identifying the subject matter
2. IC2 CA Establishment of the audit team (competence, team and resources)
3. IC3 CA Code of ethics declaration (independence)
4. IC4 CA Code of ethics conclusion
5. CAP1 Audit strategy and audit plan for subject matter
6. CAP2 CA Engagement letter
7. CAP3 CA Minutes of entry meeting
8. CAP4 CA Quality control questionnaire planning phase
9. PCP1 Performing compliance audit procedures
10. ECA1 Evaluating audit evidence and concluding on the subject matter
11. ECA2 CA Code of ethics compliance
12. ECA3 CA Management representation letter
13. ARC1 Compliance audit report – a) Direct reporting b) Attestation
14. ARC2 CA Management letter
15. ARC3 CA Minutes of exit meeting
16. ARC4 CA Quality control questionnaire (execution and reporting phase)

PREFACE

Compliance audit is an assessment of whether the provisions in the applicable laws, rules and regulations made thereunder and various orders and instructions issued by the competent authority are being complied with. This audit by its very nature promotes accountability, good governance and transparency. It is imperative that compliance audits are planned, conducted and reported in a structured manner.

This compliance audit manual has been written to facilitate the performance of compliance audits as per the International Standards of Supreme Audit Institutions (ISSAIs) and provides guidance on how to conduct a compliance audit.

The manual aims to:

1. Explain the main concepts of compliance audit and link it to the audit practice;

2. Provide guidance on and illustrations of the process, tools and working papers that may be used in planning, conducting and reporting on a compliance audit based on the ISSAIs;

3. Guide strategic considerations in implementing the compliance audit standard in the SAI.

Compliance audit can be conducted as a stand-alone audit, or as an audit combined with financial audit and/or performance audit. This manual will mainly contain and explain compliance audit as a stand-alone activity according to requirements and explanations in ISSAI 4000. The Compliance Audit Standard ISSAI 4000 is based on the fundamental principles in ISSAI 100 and 400.

In this manual, the two types of engagement, attestation and direct reporting, are explained. However, the focus will be on direct reporting as per the ISSAIs. The manual includes several recommendations on how SAIs should proceed when implementing compliance audit. The member SAIs that choose to adopt the manual are encouraged to customise both the manual and working paper templates according to their needs, taking into account requirements in their mandates and national legislation.

This manual will cover all aspects of the compliance audit process (initial considerations, planning, gathering and evaluating evidence, forming conclusions, reporting and follow-up).

1. INTRODUCTION TO COMPLIANCE AUDIT IN THE PUBLIC SECTOR CONTEXT

There are three main types of public sector auditing: financial audit, compliance audit and performance audit. It is important to understand the differences between the three audit types. The objective(s) of the audit to be conducted will determine the applicable standards to follow. In this chapter, we aim to explain the three audit types so that it is clear how compliance audit is different from the other audit types.

1.1. The three audit types in the public sector

Public sector auditing can be described as a systematic process of objectively obtaining and evaluating evidence to determine whether information or actual conditions conform to established criteria.[1]

Compliance audit

The definition of compliance audit builds on the definition of public sector audits with a specific focus on assessing compliance with criteria derived from authorities. Authorities are the parliamentary decisions, laws, legislative acts, established codes or norms, and agreed-upon terms that a public sector entity is expected to comply with in the execution of its roles and responsibilities.

In compliance auditing, you identify a subject matter, which is the area of the entity's work that the audit will address, for example the entity's procurements, their reporting on non-financial information, and their adherence to the freedom of information law or the staff's compliance with their codes of conduct.

Compliance audit is the independent assessment of whether a particular subject matter is in compliance with applicable authorities identified as criteria. As auditors, we assess whether activities, financial transactions and information are, in all material respects, in compliance with the authorities which govern the audited entity.[2] Auditors performing compliance audit look for material deviations or departures from criteria that could be based on laws and regulations, principles of sound financial management, or propriety, which is the observance of the general principles governing sound financial management and the conduct of public officials.

Parliament appropriates public funds to activities for the benefit of the citizens in a country. Public sector auditing is essential to evaluate if public sector administration is managing to allocate the funds as decided by those that appropriated the public funds. The officials are expected to act in the best interest of the public by spending the funds for the intended purposes, and in line with the authorities (laws and regulations etc. that govern them).

It is the responsibility of the public sector entities and their appointed officials to be *transparent* about their actions and *accountable* to citizens for the funds with which they are entrusted, and to exercise *good governance* over such funds.[3] Compliance audit plays an important role in ensuring that the principles of transparency, accountability and good governance are actually met.

---

[1] ISSAI 100/18
[2] ISSAI 400/12
[3] ISSAI 400/16

Compliance auditing promotes transparency by providing reliable reports as to whether funds have been administered, management exercised and citizens' rights to due process honoured, as required by the applicable authorities. It promotes accountability by reporting deviations from and violations of authorities, so that corrective action may be taken and those accountable may be held responsible for their actions. It promotes good governance both by identifying weaknesses and deviations from laws and regulations and by assessing propriety where there are insufficient or inadequate laws and regulations. Fraud and corruption are, by their very nature, elements that counteract transparency, accountability and good stewardship. Compliance auditing therefore promotes good governance in the public sector by considering the risk of fraud in relation to compliance.[4]

Financial audit

Financial auditing is determining whether an entity's financial information is presented in accordance with an applicable financial reporting and regulatory framework.[5]

During a financial audit, auditors look for misstatements and errors that can have a material impact on the information presented in the financial statements. Misstatements or errors are considered material if they impact the decisions of the intended users of the financial statements.

Compliance in financial auditing is limited, and it is described in ISSAI 1250 par. 10 that the objectives of the audit are:
(a) To obtain sufficient appropriate audit evidence regarding compliance with the provisions of those laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements;
(b) To perform specified audit procedures to help identify instances of non-compliance with other laws and regulations that may have a material effect on the financial statements; and
(c) To respond appropriately to non-compliance or suspected non-compliance with laws and regulations identified during the audit.

Normally, considerations of compliance with laws and regulations in the public sector has a broader scope than that set out in ISSAI 1250. This may, for example, include additional responsibilities for expressing a separate opinion or conclusion as to the entity's compliance with laws and regulations. Public sector auditors with such additional responsibilities should consider ISSAI 4000 instead of trying to include this as part of financial audits.

Performance audit

Performance auditing is an independent, objective and reliable examination of whether the government undertakings, systems, operations, programmes, activities or organisations are operating in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvements. Performance auditing seeks to provide new information, analysis or insights and, where appropriate, recommendations for improvement.[6]

---

[4] ISSAI 400/17

[5] ISSAI 100/22

[6] ISSAI 300/9-10

Performance audit's 3 E's seek to examine, for example, if the government is using resources economically while handling a subject matter; if the ratio of input to output is optimal in government operations (efficient); and if the government entity is able to deliver the intended result and impact on society (effective).

1.2. The objective of a compliance audit

The main objective of compliance auditing is to provide the intended user(s) with information on whether the audited public entities follow parliamentary decisions, laws, legislative acts, policy, established codes and agreed-upon terms. These form the relevant authorities governing the subject matter/entity that is going to be audited. The authorities are the sources of audit criteria. Regardless of the source of criteria, you perform the audit and form a conclusion with the selected level of assurance, in accordance with the requirements in ISSAI 4000. The audit criteria might already be defined by the national legislation and/or the remit of the audited entity. In these cases, a SAI will not always have ability to influence the scope of the audit work. The SAI promotes good governance by identifying and reporting deviations from criteria, so that corrective action may be taken and so that those responsible are held accountable for their actions. Compliance audits are carried out by assessing whether activities, financial transactions and information comply, in all material respects, with the authorities that govern the audited entity.[7]

A compliance audit may be concerned with regularity or with propriety. While regularity is the main focus of compliance auditing, propriety may also be pertinent given the public sector context, in which there are certain expectations concerning financial management and the conduct of officials. Depending on the mandate of the SAI, and the nature of laws and regulations in the public sector context of the SAI, the audit scope may therefore include aspects of propriety. Suitable criteria are needed both in audits focusing on regularity and in audits focusing on propriety.[8]

This manual provides guidance mainly on the regularity aspect of compliance auditing.

1.3. Compliance audit as a stand-alone activity or as combined audit

A compliance audit is a stand-alone audit and may be conducted on a regular or ad-hoc basis, as distinct and clearly defined audits each related to a specific subject matter.[9] ISSAI 4000 explains key considerations that are applicable when SAIs conduct compliance audits as a stand-alone engagement, which will be explained in detail in this manual.

The combined audit approach is not covered in this manual. However, if you are required to conduct a combined financial and compliance audit, you must report it separately as stated in ISSAI 4000, paragraph 16. *"For combined audits, the auditor assesses which standard to refer to. When a compliance audit is combined with a financial audit, the conclusion/opinion on the aspect of compliance should be clearly separated from the opinion on the financial statements."*

---

7 ISSAI 4000/23-26

8 ISSAI 400/32

9 ISSAI 400/25

2. KEY CONCEPTS IN COMPLIANCE AUDIT

The purpose of this chapter is to introduce the key concepts of compliance audit. They are the basis for a high-quality compliance audit. By understanding these concepts thoroughly, you will be able to design an audit with a clear understanding of:

- ➢ What is going to be audited (the subject matter);
- ➢ The sources for the criteria (authorities);
- ➢ How you assess the subject matter using criteria;
- ➢ Who are the parties involved in the audit (three parties model);
- ➢ What assurance you are providing as an auditor (limited or reasonable); and
- ➢ Determining the type of engagement (direct reporting or attestation).

2.1. Subject matter and subject matter information

The *subject matter* depends on the mandate of the SAI, the relevant authorities governing the entity and the scope of the audit. Therefore, depending on the mandate and authorities, the content and scope of compliance audit and the subject matter may vary widely.

Subject matter refers to the information, condition or activity that is measured or evaluated against certain criteria. An appropriate subject matter is identifiable and capable of consistent evaluation or measurement against the criteria, such that it can be subjected to procedures for gathering sufficient and appropriate audit evidence to support the audit opinion or conclusion. It can take many forms and have different characteristics depending on the audit objective and audit scope. For attestation engagements on compliance it is more relevant to identify the subject matter information, which may be a statement of compliance prepared in accordance with an established and standardised reporting framework.[10]

The subject matter and relevant audit criteria might already be defined, by the mandate of the SAI or national legislation. Some SAIs have mandated requirements or must perform audits on request from Parliament, while other SAIs have discretion to select the coverage of compliance audits.

The scope depends on the needs of the intended user(s), the decided level of assurance, the risk and materiality that have been assessed and the competence and resources available in the SAI.[11]

The subject matter can often be broad, and therefore it is necessary to narrow it down to make it auditable. For example, when your subject matter is procurement, it can be narrowed down to:

- a. The entity's planning of a procurement within an area; or
- b. The entity's sourcing of goods and services within an area; or
- c. The contract management process within the entity.

---

[10] ISSAI 100/26 and ISSAI 400/33
[11] ISSAI 4000/43-44

The *subject matter information* refers to the outcome of evaluating or measuring the subject matter against the criteria. It can take many forms and have different characteristics depending on the audit objective and audit scope.[12]

In an attestation engagement, where the auditor attests that the given subject matter information is correct, the audit criteria are implicitly given by the presentation of the subject matter information. In these cases, you need to identify relevant audit criteria to draw conclusions on the correctness of criteria implicitly given in the subject matter information by the responsible party.[13]

In an attestation engagement, the responsible party (the entity) measures the subject matter against the criteria and presents the subject matter information, on which you (the auditor) then gather sufficient and appropriate audit evidence to provide a reasonable basis for forming a conclusion. The conclusion is expressed in the form of findings, conclusions, recommendations or an opinion.[14]

Examples of subject matter and subject matter information:

Subject matter: National Department of Health's procurement sourcing practices with special emphasis on the procurement of medical equipment.

Subject matter information: Tenders/contracts that form the basis for selection.

The entity should have information (the criteria govern the information that is needed) on which suppliers have been chosen, and what contracts have been signed. What do the contracts contain? Is the exact amount paid to suppliers? Is a contract registry maintained and updated? Is confirmation of the payment of medical kits given? Is budget control satisfactory? Are funds made available for the purchase of medical kits used for other purposes, thus resulting in incomplete supply of medical kits?

Subject matter: Expenditures related to training activities of a government entity.
Subject matter information: Financial information and reports on training activities.

Other examples of subject matter information:
The description of internal control, KPIs (key performance indicators), sustainability reports and performance information reports are examples of subject matter information.

2.2. Authorities and criteria

Authorities are the source of criteria and the relationship between the authorities and criteria is explained below.

Authorities

Authorities are the most fundamental element of compliance auditing, since the structure and content of authorities furnish the audit criteria and therefore form the basis of how the audit is to proceed under a specific constitutional arrangement. Authorities are relevant acts or resolutions of the legislature or other statutory instruments, directions and guidance issued by the public sector bodies

---

[12] ISSAI 100/28
[13] ISSAI 4000/113
[14] ISSAI 4000/40

with powers provided for in statute, with which the audited entity is expected to comply. Authorities may include laws, policies, rules, regulations and other instruments that people/organisations must follow to be compliant.

The extent of your work in obtaining a sufficient understanding of the legal and regulatory framework will depend on the nature and complexity of the laws and regulations and the subject matter that is going to be audited.

Conflicting authorities

If you identify conflicting authorities, it is important to consider the hierarchy of the authorities; the higher level of authority will prevail over subordinate authorities. For example, if something has been defined in the law about a subject matter, the internal regulations of an entity has to be in line with this law. If they are not, auditors should point out the contradiction and, if their mandate allows, recommend a change in subordinate regulation.[15]

Criteria

Criteria are the benchmarks deriving from authorities, which are used to evaluate the subject matter consistently and reasonably;[16] for example, if the subject matter is the procurement of medical equipment within a department in the Ministry of Health, the authorities can be laws concerning procurement, health laws regulating procurement within the area etc. The criteria can be a specific paragraph in a law regulating the way an entity is supposed to procure medical equipment. Criteria can be specific or more general, and may be drawn from various sources, including laws, regulations, standards, sound principles and best practices.

Auditors are expected to carry out proper risk assessment to determine which compliance requirements are likely to be violated and, based on that, design and perform procedures to detect such instances. Auditors use professional judgement in determining and applying criteria, and professional scepticism to assess if the criteria are suitable and exhibit the characteristics that are mentioned below.

ISSAI 400 and 4000 emphasise the need for applying suitable audit criteria when assessing regularity and propriety aspects of an entity. The reason is that the quality of audit opinion and conclusion in compliance audits largely depends on how auditors assess and apply corresponding audit criteria to the subject matter in their work.

Characteristics of criteria

Suitable audit criteria, either regularity or propriety, exhibit the following characteristics:[17]

   i)   Relevance: The criteria point out how the subject matter should be; for example, a paragraph in a procurement law determines that you must have a plan before sourcing any goods or services.
   ii)   Completeness: The criteria provide a comprehensive picture; for example, the criteria contain all matters that are important for procurement planning.

---

[15] ISSAI 400/30 and ISSAI 4000/117
[16] ISSAI 400/31
[17] ISSAI 4000/118

iii) Reliability: The criteria are correct; for example, the quoting from a paragraph in the procurement law is correct, and the source of the authority is reliable.

iv) Neutrality: The criteria are not biased; for example, find a balanced way to present the text in a paragraph on planning in a procurement law.

v) Understandability: It is easy for the reader to understand the connection between the criteria and the audit question; for example, which paragraph to use in a procurement law to measure performance.

vi) Usefulness: It is easy to understand why this particular criterion is used here to benchmark the evidence.

vii) Comparability: The criteria are used in other similar audits; for example, when the SAI audits procurement planning in different areas, the same paragraphs in a procurement law can be used.

viii) Acceptability: The criteria are well understood and generally agreed to and can be used as a benchmark among experts in the field, audited entity, legislature, media and general public; for example, certain paragraphs in a procurement law that are important for planning purposes.

ix) Availability: The criteria are easy to understand and available to the users; for example, a paragraph in a procurement law is put into context when using it to assess the evidence, and the user has access to the criteria.

The relative importance of each of the above characteristics when assessing the suitability of criteria to a particular subject matter is a matter of professional judgement. The suitability of criteria is not affected by the level of assurance; that is, if criteria are unsuitable for a reasonable assurance engagement, they are also unsuitable for a limited assurance engagement, and vice versa.

Once suitable criteria have been identified based on the characteristics set out above, they then must be appropriately operationalised for the particular circumstances of each audit to be able to reach meaningful conclusion(s) and should be understandable for the intended user.

2.3. The three parties in public sector auditing

Public sector audits involve three separate parties: the responsible party, the auditor (SAI) and the intended user(s).

The responsible party in compliance auditing is responsible for the subject matter or the subject matter information of the audit and is usually the executive branch of the central or local government. The intended user(s) may be legislative or oversight bodies, those charged with governance, the public prosecutor or the general public. The auditor prepares the compliance audit report for the intended users.

The role of information in understanding the three parties
The relationship between the parties in the public sector can be explained by the principal-agent model. When one person (the principal) agrees with or hires another person (the agent) to perform tasks on his/her behalf, a relationship is established.
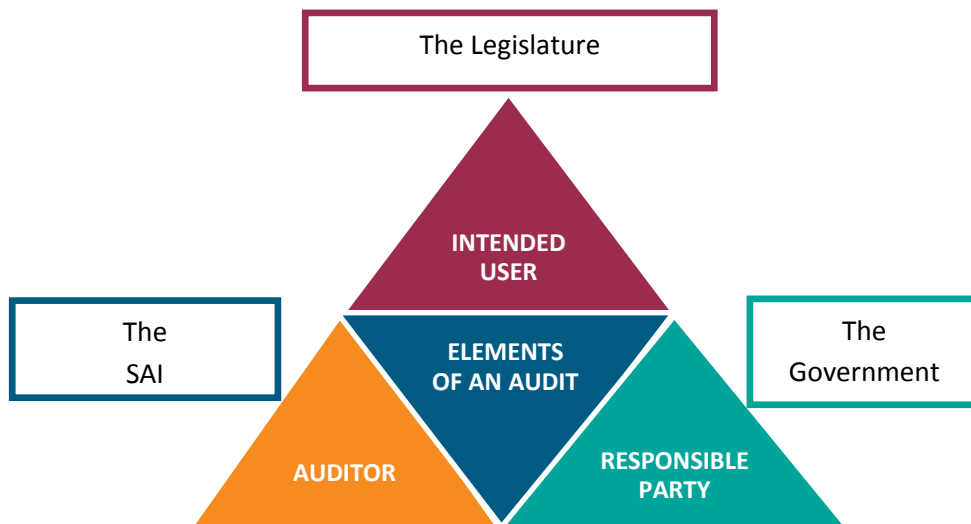
Figure 1: The three parties' relationship

In the public sector, there are many layers of principal-agent relationships; such as, the principal is the public and the agent is Parliament; Parliament (intended user) is the principal and the agent is the government (responsible party); the government is the principal and the agent is the minister. This model is very useful to explain the role of audit. Auditors play a crucial role in balancing the information asymmetry between the principal and the agent. SAI reports provide an independent assessment of the activities of agents, so that they can be held accountable by the principals.

When one person (the principal) agrees with or hires another person (the agent) to perform tasks on his behalf, a relationship is established. The principal will then delegate the necessary authority and resources to the agent to conduct the tasks. Now the principal needs to ensure that the agent is performing the tasks and using the resources according to the agreement. However, there is an imbalance in this relationship; although the principal holds the power, it is very difficult to monitor the decisions and performance of the agent. The principal cannot simply rely on the good intention of the agent, since the agent is likely to have a different agenda and priorities than the principal. The principal needs information to monitor the agent, but all information about the activities is in the hands of the agent, or is produced by the agent.

2.4. Assurance level

Every compliance audit is an assurance engagement. Assurance level may be determined at SAI level or team level, but must be based on the needs of the intended user(s). The audit report provides either reasonable or limited assurance.

Reasonable and limited assurance
In compliance auditing there are two levels of assurance: reasonable assurance and limited assurance. In reasonable assurance the audit conclusion is expressed positively, conveying that, in the auditor's opinion, the subject matter is or is not compliant in all material respects, or, where relevant, that the

subject matter information provides a true and fair view, in accordance with the applicable criteria.[18] In limited assurance, the audit conclusion states that, based on the procedures performed, nothing has come to the auditor's attention to cause the auditor to believe that the subject matter is not in compliance with the criteria.[19] Both reasonable and limited assurance is possible in both direct reporting and attestation engagements in compliance audit.

Levels of assurance are examined further in planning the audit, since the decision to provide a limited or reasonable assurance will have a strong impact on the design and results of the audit.

2.5. Types of engagements

Each assurance engagement is either an attestation engagement or a direct reporting engagement. A direct reporting engagement and attestation engagement differ based on who prepares and measures/evaluates the subject matter. The subject matter can either be set out in the mandate or selected by the SAI.

Direct reporting engagement

In a direct reporting engagement, it is the auditor who measures or evaluates the subject matter against the criteria. The auditor is responsible for producing the subject matter information. The auditor selects the subject matter and criteria, taking into consideration risk and materiality. By measuring the subject matter evidence against the criteria, the auditor is able to form a conclusion. The conclusion is expressed in the form of findings, answers to specific audit questions, recommendations or an opinion.[20]

In a direct reporting engagement performed with reasonable assurance, the audit conclusion expresses the auditor's view that the subject matter is or is not compliant, in all material respects, with the applicable criteria.

When providing limited assurance, the conclusion conveys that nothing has come to the auditor's attention indicating that the findings are not in compliance with the audit criteria. When the auditor has been aware of instances of non-compliance, the conclusion needs to reflect this.

Attestation engagement

In an attestation engagement, the responsible party (the entity) measures the subject matter against the criteria and presents the subject matter information, on which you, the auditor, then gather sufficient and appropriate audit evidence to provide a reasonable basis for forming a conclusion. The conclusion is expressed in the form of findings, conclusions, recommendations or an opinion.[21]

In an attestation engagement with reasonable assurance the auditor's conclusion expresses the auditor's view that the subject matter information is/is not in accordance with the applicable criteria.

---

18 ISSAI 4000/33

19 ISSAI 4000/35

20 ISSAI 100/29 and ISSAI 4000/37

21 ISSAI 100/29 and ISSAI 4000/40

In an attestation engagement with limited assurance the auditor states whether, based on the procedures performed, anything has come to her/his attention to cause the auditor to believe that the subject matter is not in compliance, in all material respects, with the applicable criteria. The procedures performed are limited compared with what is necessary to obtain reasonable assurance.[22]

Levels of assurance and engagement types

To understand the relationship between assurance level, engagement type and the form of conclusion or opinion to give, it is necessary to understand the link between assurance levels and types of audit shown in Table 1. Conclusion and opinion are described in detail in chapter 5.5.

Assurance level \ Engagement type	Direct reporting engagement	Attestation engagement
Reasonable assurance	Conclusion	Conclusion/ Opinion
Limited assurance	Conclusion	Opinion

Table 1: Levels of assurance and types of engagements in compliance auditing

The table describes both the relationship and recommendation in this manual. For example, if the engagement type is direct reporting, you should provide a conclusion with reasonable assurance and if it is attestation, you may provide either a conclusion or an opinion and aim for reasonable assurance. It is important to remember that an opinion requires even more audit work than a conclusion. The other argument is that opinions are standardised, but conclusions give more room to formulate according to the subject matter.

---

[22] ISSAI 4000/42-42

3. GENERAL PRINCIPLES AND REQUIREMENTS OF COMPLIANCE AUDITING

ISSAI 400 describes the general principles of compliance auditing. These principles are fundamental to the conducting of a compliance audit. As the nature of the audit is iterative and cumulative, you should consider these principles prior to the commencement of any audit and at more than one point during the audit process i.e. planning and designing, gathering and evaluating evidence and reporting.

The fundamental principles are grouped by principles related to the SAI's organisational requirements, which are the general principles,[23] and they are related to specific steps in the audit process, e.g. planning, conducting and reporting.

The general principles of compliance auditing are briefly described in this chapter. You are required to exercise professional judgement and scepticism throughout the engagement while considering the other elements of the general principles.

3.1. Professional judgement and scepticism

Auditors must plan and conduct the audit with professional scepticism and exercise professional judgement throughout the audit. The auditor's attitude should be characterised by professional scepticism and professional judgement, which are to be applied when forming decisions about the appropriate course of action. Auditors should exercise due care to ensure that their professional behaviour is appropriate.[24]

Professional judgement

To exhibit professional judgement, the auditor attends relevant training and uses knowledge and experience within the context provided by auditing and ethical standards, so that well considered decisions can be made at all stages of the audit process. The professional judgement is used when assessing risk and materiality, defining the subject matter, scope and the corresponding audit criteria and determining the level of assurance. Professional judgement is also used to assess procedures necessary to gather sufficient and appropriate audit evidence and the evaluation thereof. The use of professional judgement is crucial when analysing the audit evidence and forming conclusions based on the findings.[25]

Professional scepticism

Professional scepticism is an attitude that includes maintaining an open and objective mind by being alert to conditions that may indicate possible non-compliance due to error or fraud. Professional scepticism is important when evaluating audit evidence contradicting other audit evidence already obtained, and information that brings into question the reliability of audit evidence, such as documents and responses to inquiries. Exercising professional scepticism is necessary to ensure that you avoid personal bias and to make sure that you are not overgeneralising when drawing conclusions from

---

23 ISSAI 100/34 and ISSAI 400/42

24 ISSAI 100/37

25 ISSAI 4000/72-73

observations. In addition, the auditor will act rationally based on a critical assessment of all the evidence collected.[26]

3.2. Quality control

This refers to processes in place whereby the overall quality of a compliance audit is reviewed to ensure that the audit was in compliance with applicable governing standards and that the audit report's conclusion or opinion issued, is appropriate in the circumstances. The quality control procedures can be supervision, reviews, consultation and adequate training and might cover the planning, execution and reporting stage. Some SAIs have already established quality control/assurance units for the purpose of reviewing selected audit reports before they are issued, or providing assurance to management that quality control is functioning well.

Quality control at engagement team level

The engagement team members for every audit should perform quality control procedures as per the SAI policy. Team members at different levels, including the person with delegated responsibility for the audit, perform quality control procedures. They are designed to ensure that each team member takes part in the responsibility for the overall quality of the audit assignment. Team members are also responsible for providing SAI management with relevant information to enable the functioning of that part of the SAI's system of quality control relating to independence.

Role of the person responsible for the audit

In the public sector, the Auditor-General is usually the statutory auditor responsible for all audits. However, practicalities dictate that other (high-level) suitably qualified audit staff with the appropriate competence and capabilities may be delegated or appointed to take over the responsibility for an assignment. Such delegation should preferably be in writing and communicated for each engagement to all relevant personnel.

The person with delegated responsibility for the audit should take overall responsibility for the quality on the audit assignment and observe evidence of non-compliance of the audit team with ethical requirements. If any non-compliance is observed, appropriate action must be taken. For each audit assignment, the person responsible for the audit should form a conclusion on compliance with requirements that apply to the audit engagement. This entails the following:

- Evaluating the information on identified breaches, if any, of the SAI's independence policies and procedures to determine whether they create a threat to independence for the audit engagement;
- Taking appropriate action to eliminate such threats or reduce them to an acceptable level by applying safeguards. The person responsible for the auditor's report should promptly report to the SAI any failure to resolve the matter for appropriate action; and
- Documenting conclusions on independence and any relevant discussions with the SAI that support these conclusions.

The person responsible for the audit should, throughout the audit:

---

26 ISSAI 4000/78-79

- Remain alert, take note and document any non-compliance with relevant ethical requirements and ensure that appropriate actions are taken;
- Take responsibility for the direction, supervision and performance of the audit engagement;
- Take responsibility for the performance quality reviews throughout the audit. In terms of this, review the audit documentation and discussions with the audit team to confirm if the audit evidence is sufficient and appropriate;
- Take responsibility for ensuring that appropriate consultation is taking place on difficult or contentious matters, including the fact that conclusions are reached and implemented. Such consultation should be documented; and
- Take responsibility for issuing a report, which is appropriate in the circumstances.

In addition, the person responsible for the audit should consider the results of the SAI's quality control monitoring processes as per the latest information circulated and the effect this may have on the audit. Additional guidance on quality control is given in ISSAI 40, *Quality Control for SAIs*. How to conduct the detailed review at first, second and third level is described in section 4.3.

3.3. Audit team management and skills

The SAI shall ensure that the audit team collectively has the necessary professional competence to perform the audit. The person with delegated responsibility for the audit is the person signing the plan that safeguards this. Quality control includes considering whether the audit team has sufficient and appropriate competence to conduct the audit, is capable of selecting criteria free from bias, has methodological competence to conduct the different techniques, has general access to accurate information, has considered available information, and has had sufficient time to complete the audit assignment. The audit team is assembled to collectively have the necessary competence, knowledge, skills and expertise to perform the audit in accordance with professional standards. Refer to chapter 5.1 for more details on the team's competence.

3.4. Audit risk

Audit risk is the risk that the auditor's report, conclusion or opinion may be inappropriate, meaning that the information that is given to the intended user is not correct. A compliance audit shall be performed where the audit risk is reduced to an acceptably low level in the circumstances of the audit. This is done by selecting procedures to collect information from different sources (triangulation of methods) to ascertain the correctness of the information, refer to chapter 5.2.5. For example, you start by first reading documents produced by the entity, followed by analysing statistics if available and then ask employees about your evidence. By this methodological triangulation, you have different sources of the same information, or you may use information from one source as base to get a more comprehensive picture. The auditor performs different procedures to reduce or manage the risk of reaching inappropriate conclusions, recognising that the limitations inherent in all audits mean that an audit can never provide absolute certainty of the condition of the subject matter.[27]

---

27 ISSAI 100/40

Reducing audit risk includes the following aspects: anticipating the possible or known risks of the work envisaged and consequences thereof, developing procedures to address those risks during the audit and documenting which risks will be addressed and how. You need to evaluate whether the scope of the work performed is sufficient. In addition, when concluding, you need to evaluate whether you have sufficient and appropriate audit evidence when assessing subject matter against criteria to form conclusion(s), based on the level of risk involved.[28] The higher the level of risk, the greater the extent of audit work that will be required to lower detection risk sufficiently to achieve the acceptable level of audit risk.

Risk of fraud

You need to identify and assess the risk of fraud and obtain sufficient and appropriate audit evidence regarding the assessed risks, through designing and implementing appropriate responses. Due to the inherent limitations of an audit, there is an unavoidable risk that unlawful acts, including fraud, may occur and not be detected. The risk of not detecting an unlawful act resulting from fraud is higher than the risk of not detecting one resulting from error. This is because fraud may involve organised schemes designed to conceal it, deliberate failure to record transactions, or intentional misrepresentations being made to the SAI. Such attempts at concealment may be even more difficult to detect when accompanied by collusion. You are responsible for maintaining professional scepticism throughout the audit and recognising the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud.[29]
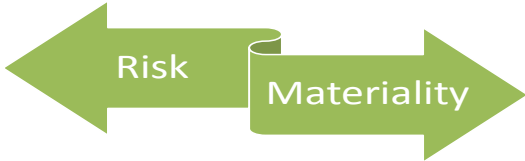
Figure 2: Risk and materiality

In compliance auditing, you need to assess both the risk and materiality. The concept of materiality in a compliance audit is different from the traditional thinking in financial audits.

3.5. What is materiality?

The concept of materiality recognises that some matters, either individually or in the aggregate, are relatively important, and in compliance auditing we relate this to whether an instance of non-compliance is material. In this regard, you need to answer one of the most important questions and that is how material would that instance of non-compliance be to the intended users of the compliance audit report and how would this affect their decisions based on it.

Materiality is relevant in all audits. A matter can be judged material if knowledge of it would be likely to influence the decisions of the intended users. Determining materiality is a matter of professional judgement and depends on your (the auditor's) interpretation of the users' needs. This judgement may

---

28 ISSAI 4000/53

29 ISSAI 4000/59-61

relate to an individual item or to a group of items taken together (instances of non-compliance). Materiality is often considered in terms of value, but it also has other quantitative as well as qualitative aspects. The inherent characteristics of an item or group of items may render a **matter** material by its very nature. A matter may also be material because of the context in which it occurs.[30]

You need to ask these questions:

- Who is /are the intended user(s)?
- What is the objective of the audit?
- Is the «matter» significant enough irrespective of whether the findings are negative or not?

The qualitative aspect of materiality generally plays a greater role in public sector audits and especially in compliance audit. Materiality shall be considered for the purposes of planning, evaluating the evidence obtained and reporting. An essential part of determining materiality is to consider whether reported cases of non-compliance could reasonably be expected to influence decisions of the intended users. The assessment of materiality requires comprehensive professional judgement on the part of the auditor and is related to the audit scope.[31] Refer to chapter 5.2.4 for details on how to assess and determine materiality.

3.6. Documentation and communication

Sufficient audit documentation is important within all steps of the compliance audit. This is to ensure that all steps taken and decisions made during an audit are properly justified and documented in such a way that an experienced auditor who does not have any prior knowledge or connection with the audit, will be able to understand the audit conducted by reviewing the audit documentation.

Communication takes place at all stages of the audit: before the audit starts, during initial planning, during the gathering and evaluating of evidence, at the reporting phase and at the follow-up phase. It is essential that the audited entity together with the SAI is kept informed of all matters relating to the audit. This is a key to develop a constructive working relationship between you and the entity and within the audit team. This would help keep all parties informed of the audit's progress and would really assist in resolving any matters that may obstruct the audit and could cause delays.

Any significant difficulties encountered during the audit, as well as instances of material non-compliance, should be communicated to the appropriate level of management or those charged with governance. The auditor should also inform the responsible party of the audit criteria.[32]

Documentation
Audit documentation is the written record of the basis on which auditors draw their conclusion(s) or opinion(s). Thus, documents prepared during the planning, conducting, reporting or follow-up stage of a compliance audit can be examined to see whether auditors have carried out a compliance audit as per the ISSAIs.

---

30 ISSAI 100/41

31 ISSAI 400/47
32 ISSAI 400/49

Preparing sufficient and appropriate audit documentation on a timely basis helps to enhance the quality of the audit and facilitates the effective review and evaluation of the audit evidence obtained and conclusions reached before the audit report is finalised. Documentation prepared after the audit work has been performed is likely to be less accurate than documentation prepared at the time such work is performed. The auditor should prepare relevant audit documentation before the audit report is issued, and the documentation should be retained for an appropriate period of time.[33]

Documents should contain sufficient information to enable an experienced auditor, having no previous connection with the audit, to be able to understand the audit conducted, including:

- The relationship between the audit objective, the subject matter, the criteria and audit scope;
- A clear understanding of the criteria used;
- Risk assessment, assessment of materiality and audit strategy;
- Audit plan and the explanation and reasoning for the methodology/procedures;
- Explanation of conclusion(s)/opinion(s) given;
- A plan for follow-up;
- The reasoning behind all significant matters that required the exercise of professional judgement and professional scepticism.

Audit documentation should be prepared in sufficient detail to provide a clear understanding of its purpose, source and the conclusions reached. The documentation should also be appropriately organised to provide a clear link to the significant findings or issues. Office memoranda, confirmations, correspondence, schedules, audit programmes and letters of representation are some examples of documents. Audit documentation may be in the form of paper, electronic files or other media.

Document retention

Some SAIs may have policies and procedures consistent with their laws and auditing standards to maintain documentation of their work. Document retention policies ensure that the relevant record is available for use for a certain number of years after an audit. These policies and procedures usually describe (a) documents covered in their scope; (b) the form in which the documents would be kept/archived; (c) the period for which the documents would be retained; and (d) how these documents can be accessed when needed. SAIs should see whether policies and procedures exist for document retention and, in case they have such policies, they should see if these are adequate. In case of inadequacies, SAIs may consider establishing documentation requirements through policies and procedures for the retention of audit documentation. These requirements may be due to the historical significance of certain types of documents, which, for example, may require indefinite retention in the country's national archives. There may also be additional requirements related to national security classifications, including how documentation is stored. Public sector auditors familiarise themselves with the applicable legislation regarding retention of documentation.[34]

---

[33] ISSAI 400/48
[34] Practice Notes ISSAI 1230

Confidentiality and transparency issues

SAIs need to establish and ensure that auditors comply with ethical requirements to observe at all times the confidentiality of information contained in audit documentation, unless specific authority has been given by the entity to disclose such information, or there is a legal or professional duty to do so. There is an ongoing need in the public sector to balance confidentiality with the need for transparency and accountability. The balance between confidentiality and transparency requires professional judgement to ensure that documentation of a confidential nature is clearly identified and treated as such, while at the same time granting access as appropriate. It is therefore important to be familiar with the SAI's policies and procedures addressing confidentiality. Such procedures might include types of audit documentation to be considered confidential, types of audit documentation to be made available to the public, clearly defined lines of responsibility for authorising disclosure of audit documentation and routines for making such information available if required. Furthermore, public sector auditors may have additional statutory responsibilities related to confidentiality. These responsibilities may be based on the mandate of the SAIs or legislation related to official secrets or privacy. Such legislation, for example, could relate to audits of defence, health, social service or tax agencies. Public sector auditors familiarise themselves with the particular local requirements related to confidentiality to which they are bound.

As a matter of principle, when the audited entity has a statutory obligation to gather and retain certain information, requests from outside parties for such information are normally referred to the audited entity. In situations where public sector auditors consider granting access to audit documentation, they normally consult with relevant parties (such as the audited entity to whom the request relates) prior to the information being disclosed.

Communication

Instances of material non-compliance shall be communicated to the appropriate level of management and (if applicable) those charged with governance. Other significant matters arising from the audit that are directly relevant to the entity shall also be communicated. Findings that are not deemed material, or do not warrant inclusion in the auditor's report, may also be communicated to management during the audit. Communicating such findings may help the audited entity to remedy instances of non-compliance and avoid similar instances in the future.[35] Good communication with the audited entity throughout the audit process may help make the process more effective and constructive. Effective two-way communication is important in assisting:[36]

  a) The auditor and those charged with governance in understanding matters related to the audit in context, and in developing a constructive working relationship. This relationship is developed while maintaining the auditor's independence and objectivity;
  b) The auditor in obtaining information relevant to the audit from those charged with governance. For example, those charged with governance may assist the auditor in understanding the entity and its environment, in identifying appropriate sources of audit evidence and in providing information about specific transactions or events.

---

[35] ISSAI 4000/99-100
[36] ISSAI 1260/4

The communication process

SAIs need to have a visible system in place that requires you to evaluate whether the two-way communication between you and those charged with governance has been adequate for the purpose of the audit. If the two-way communication is not adequate, it is advised that you take appropriate action. In the public sector, appropriate action may include communicating with the legislature or the appropriate regulators, or funding agencies.

Laws or regulations may restrict the auditor's communication of certain matters to those charged with governance. For example, laws or regulations may specifically prohibit a communication, or other action, that might prejudice an investigation by an appropriate authority into an actual or suspected illegal act. In some circumstances, potential conflicts between the auditor's obligation of confidentiality and obligation to communicate may be complex. In such cases, you may consider obtaining legal advice.[37]

4. OVERALL COMPLIANCE AUDIT PLANNING

Compliance with rules and regulations is the primary and the most important requirement for ensuring accountability of the public executive. Decision makers need to know whether relevant laws and regulations are being complied with, whether they have achieved the desired results, and whether the accepted standards are being adhered to; and if not, what corrective action is necessary. It is imperative that compliance audits are planned to achieve adequate coverage at an acceptably low level of audit risk, and that audit processes are carried out efficiently and result in a high-quality audit report.

4.1. Overall compliance audit plans

An overall risk assessment process will seek to identify and assess risks at a high level. It can be connected to a sector, an area of responsibility of a particular ministry or entity. To identify and assess risks, the SAI must have a systematic approach to gathering data about the government's management of its areas of responsibility and its methods of implementing the policies.

Where the SAI has the mandate to conduct compliance audits and has the discretion to select the subject matter, it performs the procedures necessary to identify significant areas and/or areas with a potential high risk of non-compliance. In performing these procedures, the auditor may take into consideration any of the following:[38]

a) Public or legislative interests or expectations;
b) Impact on citizens;
c) Projects with significant public funding;
d) Beneficiaries of public funds;
e) Significance of certain provisions of the law;
f) Principles of good governance;
g) Roles of different public sector bodies;

---

[37] ISSAI 1260.7
[38] ISSAI 4000/64-67

h) Rights of citizens and of public sector bodies;

i) Potential breaches of applicable laws and other regulations, which govern the public entity's activity, or the public debt, public deficit and external obligations;

j) Non-compliance with internal controls, or the absence of an adequate internal control system;

k) Findings identified in previous audits; and

l) Risks of non-compliance signalled by third parties.

When examining these factors, and identifying risks, the SAI may determine if the high-level risks can be addressed by defining a subject matter, on which it then performs a compliance audit. Another factor to consider in planning the compliance audit can be the urgency of the need for information on a particular subject matter by the intended users.

4.2. Preparing annual overall compliance audit plans

The exercise, as described above, would help in creating risk profile of the entities. Based on their risk profile and initial risk assessment, the audits/subject matters should be prioritised for planning and conducting compliance audits. The risk profile should be considered in conjunction with the audit capacity in terms of availability of competence and resources, and an annual overall audit plan including compliance audits to be taken up and completed during the year should be prepared.

The annual overall audit plan of the SAIs should therefore be prepared by adopting a holistic approach of covering entities for each type of audit and leveraging common processes. This plan would therefore also indicate entities for which compliance audits would be conducted. The risk profile of the audit units would have to be reviewed and updated periodically to assess continued maintenance or to consider revision of the risk profile assigned to the entities based on new intervening developments, changes and increase/decrease in irregularities noticed by various stakeholders, etc.

Components of annual compliance audit plan

a. Selection of entities where there is high risk of non-compliance in certain areas, for example procurement and/or where the subject matter is significant to the intended users, for example health, housing, education or projects with significant public funding;

b. Determination of specific subject matter, where considered necessary; and

c. Allocation of audit resources for the audits to be undertaken.

Determine and prioritise subject matters at SAI level

Depending on the practice in the SAI, the subject matter should either be identified by the individual audit teams, or the topics may be identified in a sector group prior to the audit year. The identified topics/subject matters should then be presented to the top management of the SAI, who then prioritise the subject matters at the SAI level and rank them.

Compliance audit is risk based and you need to bear in mind that a risk-based approach should be applied to identify the subject matters. It is essential that the SAIs rather spend the scarce resources on the audits where the risk is high and that the subject matter is significant/material to the intended user(s). Therefore, it is recommended that, where the SAI has discretion to select the subject matter, compliance audits based on ISSAI 4000 should be carried out only where there is high risk or the subject

matter is significant, and these should be prioritised at the SAI level. It is not necessary to carry out compliance audit for the same subject matter annually for each entity unless it is a requirement in the SAI's mandate. When the subject matter is prioritised/ranked at the SAI level, it is also possible to avoid audits that have low impact and that are immaterial to the intended users.

Implementation of the plan

The biggest test of any plan is in how it is implemented. What needs to be done is usually well defined in these plans but there is often a need for further guidance on how to make the provisions operational. Plans at business unit level or work-plans should include more detail on how each activity is going to be carried out. Please refer to the AFROSAI-E guidance on *Annual Overall Plan* for more details.

4.3. Audit review process

The SAI must ensure that the process of reviews of the audits is established through a quality control system and is functioning well. The recommended review process is described below.

The audit review process

The review process can be divided into the following levels:

- First level – lowest level of review, e.g. assistant manager/audit manager or equivalent;
- Second level – reviews may be done by the responsible senior manager or equivalent person; and
- Third level – review by the senior manager or higher. This level of review includes the person who will sign off the auditor's report.

All three levels of review should consider the following fundamental issues when reviewing a compliance audit file:

- All required working papers and procedural steps have been adequately completed, signed by preparer and reviewer, dated and cross-referenced. When a working paper on procedural steps is omitted adequate reasons are supplied;
- The subject matter, criteria and audit questions (and other relevant audited information) have been identified and clearly linked to the audit;
- Knowledge obtained in understanding the entity is adequate to inform the auditor's decision relating to the audit approach and the audit scope;
- Conclusions were adequately drawn and supported by appropriate and sufficient audit evidence;
- Significant deviations from the overall audit plan and any changes in the subject matters or scope of the audit have been documented;
- An adequate level of audit coverage has been obtained for material areas;
- All significant professional judgements made have been documented and are supported by appropriate audit evidence;
- The compliance audit was conducted in accordance with the relevant audit approach, guidelines and other directives;
- All significant audit matters have been resolved or have been appropriately reported in the compliance audit report;
- The work performed and results obtained have been adequately documented;

- Based on the underlying audit work and findings, the correct audit conclusion has been expressed; and
- Reported findings are supported by adequate and sufficient audit evidence.

The working papers should be reviewed as far as possible immediately after the work has been completed. Timely review provides better control over the quality of work and the time consumed in its performance. Normally the reviewer will be on a higher level than the preparer. Quality control questionnaires have been included after the planning, conclusion and reporting phase of the audit, to facilitate timely reviews.

First level (audit supervisor/audit manager)
Depending on the size of the audit, the audit supervisor or manager will conduct the first level of review. In the case of larger audits, there may be more than one first-level reviewer. In such cases, the reviewers should focus on the sections that have been allocated to them. First-level review should be performed on an ongoing basis; for example, each time a working paper is finalised by the preparer it should be reviewed. All working papers, conclusions drawn, professional judgements made and the related audit evidence on the audit file should be reviewed. This includes the review of the following:
- Adequate and sufficient completion of working papers including clear and understandable language and spelling;
- Consistency of documented information and decisions made between different working papers;
- Significant decisions made and audit evidence supporting decisions and findings;
- The planning of the audit, balancing audit risk, evaluating the sample sizes, conclusions, management letter issues, audit findings (exceptions), auditor's report issues etc.; and
- The audit procedures performed, ensuring that all the criteria and audit questions were addressed.

Second level (audit manager/audit director)
The second level of review is almost as detailed as the first, but some reliance can be placed on the review work already performed. The experience and seniority of the first reviewer will influence the reliance placed on the first review conducted.

The second reviewer will still concentrate on detailed work, but to a lesser extent. Focus will be placed on documentation of key working papers, including as a minimum:
- Audit strategy and audit plan, including the engagement letter;
- Appropriateness of the nature and extent of the audit work performed;
- Confirming that there is adequate audit evidence supporting the findings and conclusion;
- Confirming that all audit questions and criteria have been addressed; and
- Compliance audit report with supporting audit evidence for the findings.

The second reviewer should also review the work performed by the first reviewer.

Third level (audit director and all subsequent reviewers)
The third-level review should be performed by the person who has delegated responsibility for the compliance audit report. In certain instances, the review will be performed by more than one person within the SAI. For example, when the first-level review is performed by the audit manager and the second-level review is performed by the senior manager, the third-level review may be performed by

the business executive or equivalent who may still not be responsible for signing off the report. In this case, the person signing off the report will perform another third-level review.

The person performing a third-level review should be, as far as possible, involved in major decisions relating to the audit. The audit strategy should be approved by the third-level reviewer before the execution phase starts, i.e. performing procedures (fieldwork). If this is not possible, the third-level reviewer should at least be consulted to obtain his or her inputs regarding the audit plan and scope. This is to ensure that the correct audit approach is followed and that the person who is responsible for signing the report is aware of the aspects covered in the audit plan.

The third-level reviewer's review should focus on the following aspects:
- Work performed by the second-level reviewer;
- Appropriate and sufficient audit evidence exists to support the audit findings and conclusion;
- Issues are correctly raised in the management letter and the compliance audit report;
- Compare the work performed with the audit strategy to ensure that all risk areas have been addressed and deviations from the strategy have been documented with reasons;
- Aspects relating to finalising the audit including working papers under Audit conclusion and Reporting; and
- The audited subject matter aiming to ensure that the audit sufficiently covered all criteria, audit questions and risks identified.

The scope of the third-level reviewer should be increased, if he or she identifies other possible risk areas, or if there is any indication that the audit file does not meet the required technical standards, and requirements in ISSAI 4000.

Documenting reviews
Working papers must be signed off and dated by the person who has "prepared" and the one who has "reviewed" the audit work. Reviews of audit work are performed on three levels, with the result that some working papers are reviewed more than once. When a review is complete, the reviewer should initial the working paper template and provide comments on the review sheet.

5. COMPLIANCE AUDIT – STEP-BY-STEP APPROACH

The subject matter is determined and prioritised at the SAI level as described in chapter 4. The audit team needs to follow the step-by-step compliance audit approach when carrying out the audit. The diagram below gives an overview of the entire compliance audit process at a glance and shows how the phases, the audit steps and the working papers are linked together.

AUDIT PHASE	AUDIT STEPS	WORKING PAPAERS
Initial considerations	• Conduct initial risk assessment to identify subject matter • Consider principles with ethical significance (e.g. independence and objectivity) • Team engagement (with discussions around clarification of expectations)	• Identify subject matter • Establishment of the team • Code of ethics • Conclusion on ethics
Planning the audit	• Identify intended user(s) • Define the subject matter and the corresponding audit criteria • Determine the level of assurance • Determine materiality • Carry out risk assessment of the subject matter at entity level • Understand the entity and its control environment related to the subject matter • Develop an audit strategy and audit plan • Assess the audit risk • Plan audit procedure to enable reasonable assurance	• Audit strategy and audit plan • Engagement letter • Minutes of entry meeting • Quality control questionnaire (planning phase)
Performing the audit procedures to obtain audit evidence	• Gather sufficient and appropriate evidence through various methods and procedures • Continually update planning and risk assessment • Consider non-compliance that may indicate suspected unlawful acts	• Gathering evidence and performing audit procedures (execution) • Management representation letter
Evaluating audit evidence & forming conclusions	• Evaluate whether sufficient and appropriate evidence is obtained • Consider materiality for reporting purpose • Form conclusions	• Evaluating evidence and concluding on the subject matter • Code of ethics compliance
Reporting Follow-up	• Prepare report • Include recommendations and responses from entity as appropriate and finalise • Decide follow-up as appropriate, including a follow-up plan	• Management letter • Compliance audit report • Minutes of exit meeting • Quality control questionnaire

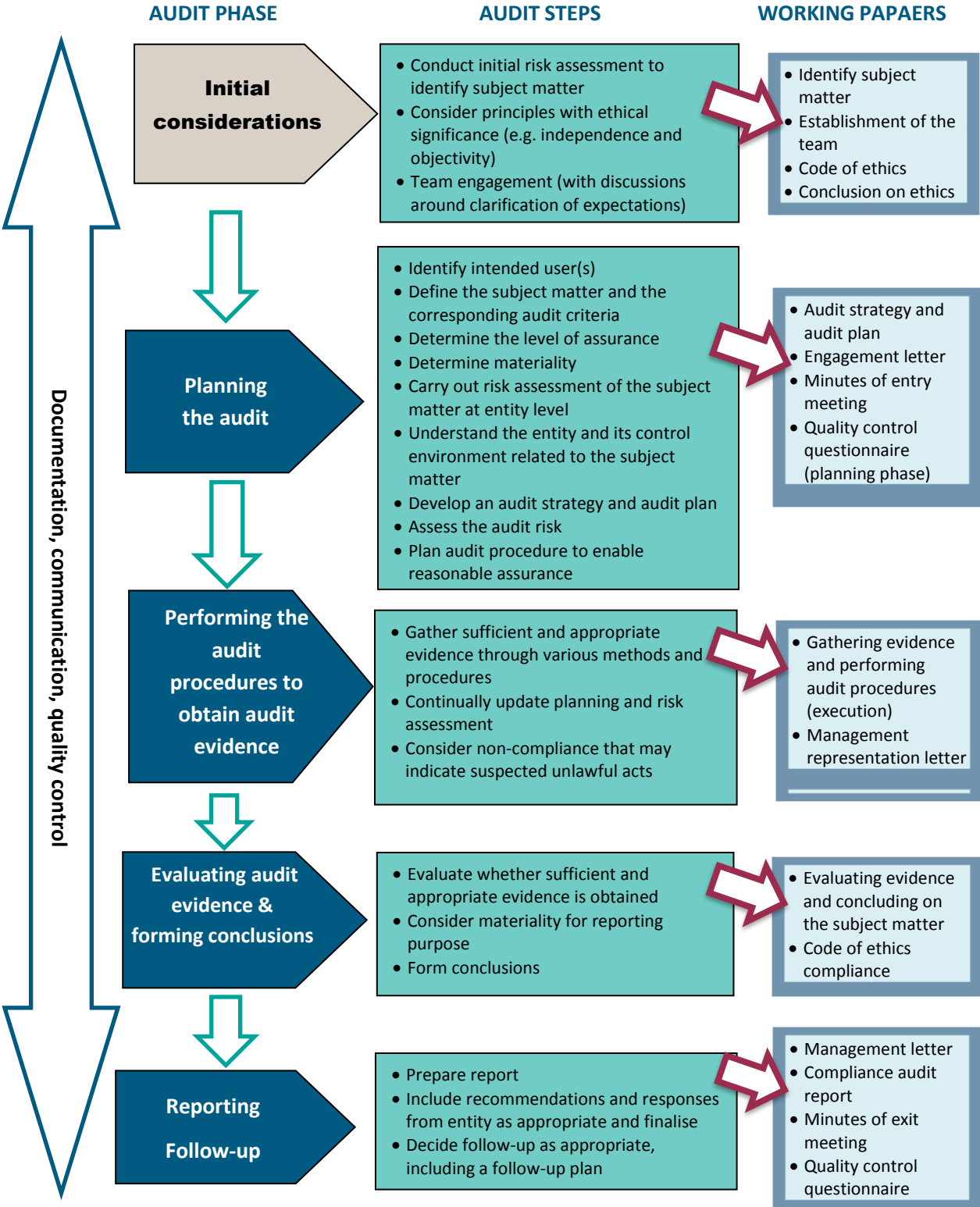*Documentation, communication, quality control*

Figure 3: Compliance audit process

5.1.   Initial considerations

It is a requirement that the auditor shall comply with the relevant procedures relating to objectivity and ethics, which in turn shall comply with the related ISSAIs on objectivity and ethics. The auditor is to demonstrate professional behaviour and integrity, be objective, possess the required professional competence, and exercise due care. S/he is also to maintain independence in fact and appearance and confidentiality regarding all audit matters.

You, the auditor, shall take care to remain objective so that findings and conclusions will be impartial and shall be seen as such by third parties.[39]

You need to go through the following audit steps and working papers to meet the requirements of the initial considerations phase:
1. Identifying the subject matter
2. Consider principles with ethical significance (e.g. independence and objectivity)
3. Team engagement and assessment of competence

5.1.1.   Step 1 – Identifying the subject matter

The very first step in compliance audit is to identify the subject matter and relevant corresponding/suitable criteria. The process of identifying the subject matter requires initial risk assessment in order to determine whether there is a high risk of non-compliance. A risk matrix may be applied to assess the risk of non-compliance in a subject matter. Once the subject matter has been approved by the senior management/at SAI level, the compliance audit may commence at the team level by following the process described in the rest of chapter 5.

To conduct the initial risk assessment, you will have to carry out some risk assessment procedures, refer to working paper IC1. *Identifying the subject matter*. To get started with the risk assessment you may base it on the knowledge you have obtained from prior years' audit findings, signals from Parliament, development in the sector or matters from the media, and/or how significant it is for the citizens of the country.

You need to describe/answer the following:
1. Is the audit of this subject matter required by the SAI's mandate? If not, does the SAI have discretion to select the subject matter?
2. Describe the risks of non-compliance that are related to the subject matter.
3. How significant is the subject matter to the intended user(s)?
4. What is the objective and scope of this subject matter?
5. Does the SAI have sufficient resources to conduct this audit?
6. Does the SAI have the required competence, or would there be a need to engage an expert?

This working paper should be approved at senior management level and the audit prioritised and ranked at SAI level.

---

[39] ISSAI 4000/45-48

Applying a risk chart/matrix to identify high-risk areas

In the process of risk assessment, it is useful to apply a risk chart to place the risks in the right category as follows:

Critical	High	Moderate	Low

You need to ask what is the likelihood that there is a risk of non-compliance with xyz requirements and what would be the impact if that risk occurs. Asking these questions related to the risks of non-compliance in a subject matter would help you to see a clear picture of the risks that are critical or high and in this manner, help you to prioritise if the risks are significant and whether you should pursue the subject matter further and conduct a compliance audit.
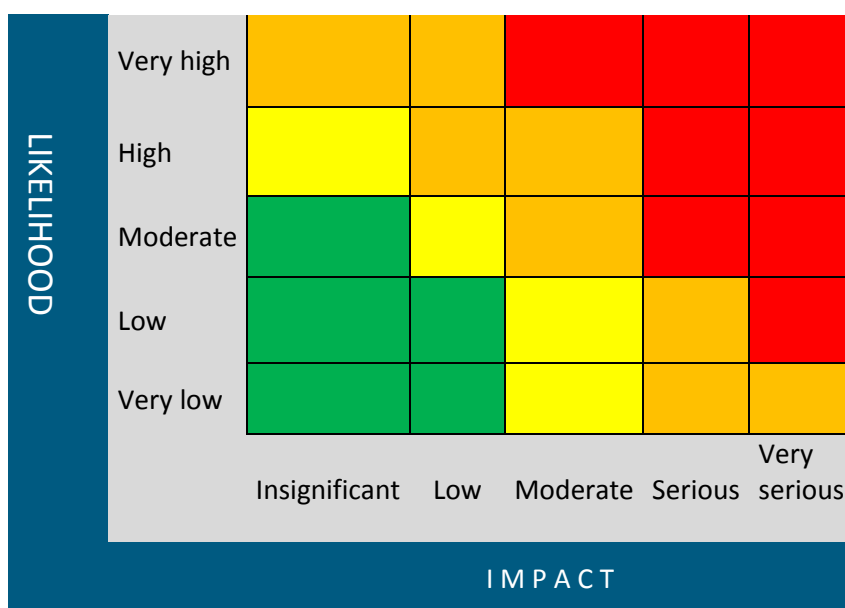
Figure 4: Risk chart/matrix

In this risk assessment approach, it is not necessary to address the risks that are insignificant or low. You should also assess the risks carefully in the moderate category and identify whether or not there is really a need to conduct a compliance audit. This model will, hopefully, help you to avoid low impact audits and prioritise the subject matter that is significant to the intended users (Parliament, citizens, donors, etc.) or where the risk of non-compliance is high.

Risk charts such as the one given above are good tools for classifying risk areas. However, it should be noted that when using such models, you should be aware of the strengths and weaknesses of the model being used. For example, whilst the risk-chart model is a rationale-based model of assessment, it lacks in intuition. As such, when you use it you should consider the intuitive aspects of the assessment as mentioned earlier in 5.1.1.

5.1.2. Step 2 – Consider principles with ethical significance

You need to demonstrate professional behaviour and integrity, be objective, possess the required professional competence, and exercise due care. You are also to maintain independence in fact and appearance and confidentiality regarding all audit matters. You can find additional guidance in ISSAI 10. *Mexico Declaration on SAI Independence* as well as ISSAI 30. *Code of Ethics*.[40] The SAIs need also to consider that ethical requirements apply to all the levels and ensure that senior management is also included.

5.1.3. Step 3 – Team engagement and assessment of competency

The SAI shall ensure that the audit team collectively has the necessary professional competence to perform the audit. Quality control includes considering whether the audit team has sufficient and appropriate competence to conduct the audit, is capable of selecting criteria free from bias, has general access to accurate information, has considered available information, and has had sufficient time to complete the audit assignment. The audit team is assembled to collectively have the necessary competence, knowledge, skills and expertise to perform the audit in accordance with professional standards.

Depending on the subject matter, this may include:
a) Auditing skills and skills regarding data collection/analysis;
b) Legal competence;
c) An understanding and practical experience of the type of audit being undertaken;
d) Knowledge of the applicable standards and authorities;
e) An understanding of the audited entity's operations and appropriate experience for the type of entity and operations being audited;
f) The ability and experience to exercise professional judgement; and
g) Producing an auditor's report that is appropriate in the circumstances.

The team should have team discussions to discuss the subject matter, how significant and material it is to the intended users and the initial risk assessment of non-compliance related to the subject matter, and clarify that the entire team has the same understanding of the subject matter and work allocation.

The SAI also determines whether their work is adequate for the purposes of the audit. Even if external experts perform audit work on behalf of the SAI, the SAI is still responsible for the conclusion(s).[41]

Availability of other resources
Reasonable assurance audits usually require more time and resources, compared to a limited assurance audit conducted on the same subject matter with the same scope. Therefore, a SAI with limited resources would be more inclined to conduct a limited assurance audit. However, this should

---

[40] ISSAI 4000/46-47
[41] ISSAI 4000/85-88

be considered carefully by giving precedence to user needs, and by considering other factors such as materiality and risk.

Working papers to complete

W/P ref.	Working paper	Objectives of the working paper
IC1	Identifying the subject matter	Identify and determine the subject matter through carrying out initial risk assessment where the risk of non-compliance is high, or the subject matter is significant to the intended users.
IC2	Establishment of the audit team	Record the names of the audit team allocated to the compliance audit and their respective competencies in relation to the specific subject matter. Include the planned budgeted hours (or days) as estimated including activities that relate to the audit.
IC3	Code of ethics declaration	Consider the compliance of the audit team members with the principles of the code of ethics. Document conflicts of interest and actions taken in response.
IC4	Code of ethics conclusion	Conclude on the audit team's compliance with code of ethics.

5.2. Audit planning process

Adequate planning helps to devote appropriate attention to important areas of the audit, identify potential problems on a timely basis and properly organise and manage the audit to respond to users' needs efficiently and effectively. Adequate planning also assists the auditor to properly assign work to the team members, and facilitates the direction, supervision and review of their work. Further, it assists, where applicable, the coordination of work done by auditors and experts, if required. The nature and extent of planning activities will vary with the circumstances of the audit; for example, the complexity of the underlying subject matter and criteria. Examples of some of the main matters that may be considered in planning include:

- The characteristics of the audit that define its scope, including the characteristics of the underlying subject matter and the criteria;
- The expected timing and the nature of the communications required;
- Whether knowledge gained on other audits performed by the auditor for the responsible party is relevant;
- The audit process;
- The auditor's understanding of the responsible party and their environment, including the risks that the subject matter may not be in compliance with the criteria;
- Control environment and internal control of the entity;
- Identification of intended users and their information needs, and consideration of materiality and the audit risk;
- The extent to which the risk of fraud is relevant to the audit;

- The nature, timing and extent of resources necessary to perform the audit, such as personnel and expertise requirements, including the nature and extent of experts' involvement; and
- The impact of the internal audit functions on the audit.

The auditor may decide to discuss elements of planning with the responsible party to facilitate the conduct and management of the audit. Although these discussions often occur, the overall audit strategy and the audit plan remain the auditor's responsibility. When discussing matters included in the overall audit strategy or audit plan, it is important not to compromise the effectiveness of the audit. For example, discussing the nature and timing of detailed procedures with the responsible party may compromise the effectiveness of the audit by making the procedures too predictable.

In smaller or less complex audits, the entire audit may be conducted by a very small audit team. With a smaller team, coordination and communication between team members is easier. Establishing the overall audit strategy in such cases need not be a complex or time-consuming exercise; it varies according to the size of the entity, the complexity of the audit, including the underlying subject matter and criteria, and the size of the audit team.

The auditors should also establish legal elements for their work by understanding the mandate of the SAI, the responsibilities of public sector auditors, and the constitutional status and responsibilities of the audited entity as well as the expectations of the intended users. This understanding provides public sector auditors with a reference to be used in applying professional judgement throughout the entire audit process.

The necessary planning phase audit steps are illustrated in figure 5, and are as follows:

1. Identify intended user(s) and responsible party;
2. Define the subject matter and the corresponding audit criteria;
3. Determine the level of assurance;
4. Determine materiality;
5. Carry out risk assessment of the subject matter at entity level;
6. Understand the entity and control environment related to the subject matter;
7. Develop audit strategy and plan; and
8. Documentation and communication.
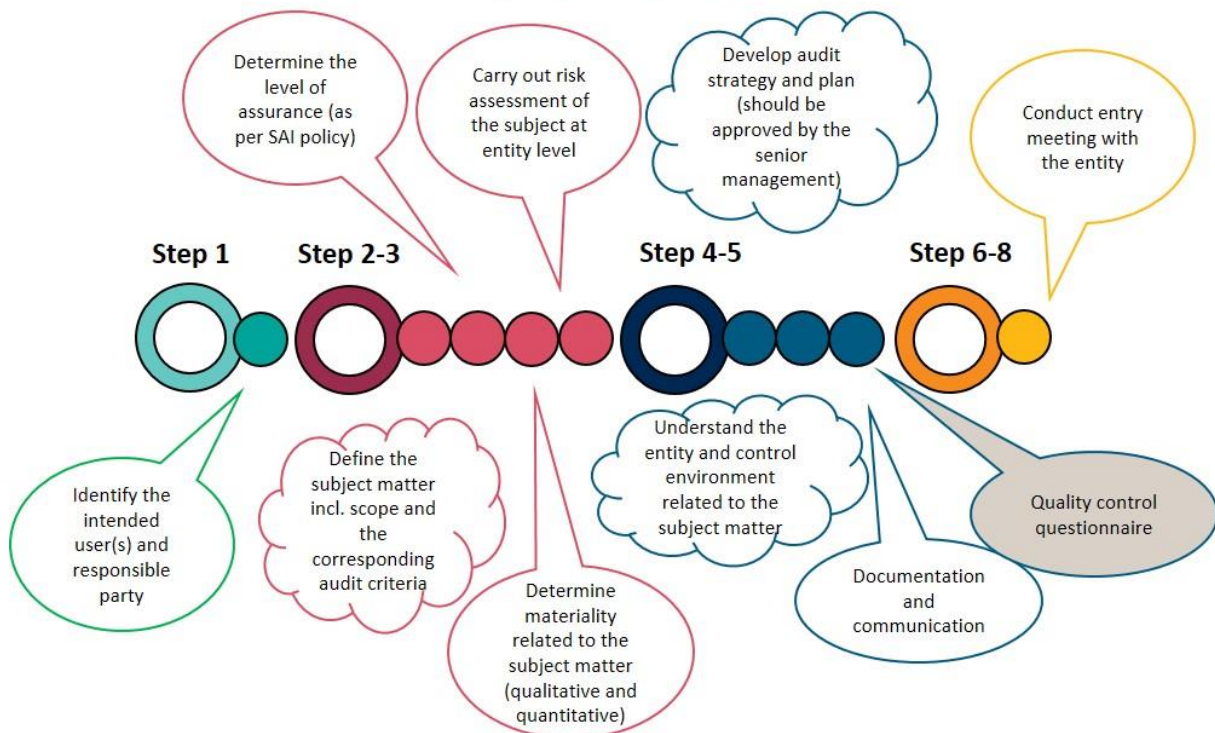
Figure 5: Planning the compliance audit – step-by-step approach

5.2.1. Step 1 – Identifying intended user(s) and responsible party

You must identify the intended users and responsible party and consider the implication of their role.

The intended user(s) are the persons for whom the auditor prepares the compliance audit report. The intended user(s) may be legislative or oversight bodies, those charged with governance, the public prosecutor, media, the general public and donors. The responsible party is responsible for the subject matter, and is as such the subject of the audit.

Identification of the responsible party is important when setting the audit criteria. The responsible party needs to comply with criteria deriving e.g. from laws, regulations, budgetary laws and financial regulations. Depending on the subject matter, you must choose the relevant audit criteria. You need to communicate with the responsible party.

5.2.2. Step 2 – Define subject matter and the corresponding audit criteria

Some SAIs have mandated requirements or have to perform audits on request from Parliament, while other SAIs have discretion to select the coverage of compliance audits. The way in which the subject matter is selected, has an impact on the audit approach when it comes to audit evidence and resources.

The concepts of subject matter, criteria and scope are interrelated. Auditors need to appreciate that these concepts influence each other as illustrated in the figure below.
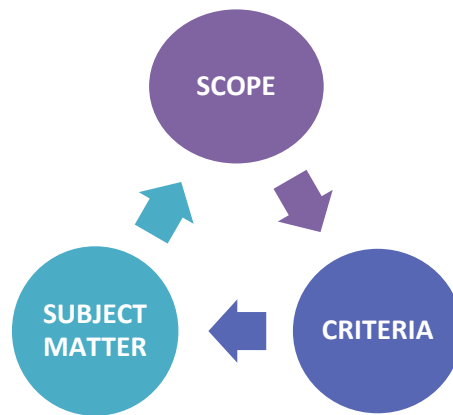
Figure 6: Interrelationship between subject matter, scope and criteria

You need to exercise professional judgement while reviewing the relationship depicted in the figure above. The objective of this review is to properly identify the scope of a compliance audit for planning purposes. It is important here to note that the scope of a compliance audit may change while conducting the audit if you identify material information that makes it necessary to reconsider scope accordingly. Some examples of audit areas for identifying subject matter are mentioned below as reference:

- Financial performance:
  - use of appropriated funds (budget execution)
  - revenue collection, e.g. council taxes, application of fines and penalties
  - use of grants and loans
- Procurement
- Expenditure
- Service delivery – medical, education, etc.
- Public complaints
- Heritage protection
- Propriety of auditee's officials/decision making
- Health and safety
- Environmental protection
- Internal control framework
- Payment of social benefits, pensions
- Physical characteristics, zoning density, access to government buildings etc.
- Extractive industries – contracts, etc.

An example of a subject matter in the audit area of procurement can be

"Procurement of services for road construction for the Ministry of Transport"

By this we mean that the Ministry of Transport is responsible for procuring services for construction of roads in the country, but does not and cannot construct the roads in its own capacity. Therefore, they must ensure awarding of the contracts for road construction to suppliers according to the requirements of the Procurement Act. We will follow this subject matter throughout the manual to demonstrate understanding in certain areas of the compliance audit process.

Audit objective

The audit objective establishes the main focus of the audit formulated in a neutral way, providing direction to the auditors/team in determining the audit scope, audit questions, audit criteria, strategy and methods. The objective is clearly linked to the audit questions, and answering the audit questions should lead to the achievement of the audit objective.

Audit scope

The scope defines the subject matter, and what is going to be audited. The scope depends on the needs of the intended user(s), the determined level of assurance, the risk that has been assessed and the competence and resources available in the SAI.[42] Determination of subject matter and criteria is one of the very first steps to be carried out in planning and performing compliance audit. In some situations, the scope and nature of the compliance audit does not follow directly from the audit mandate or relevant legislation of the SAI and, instead, it is based on the public sector auditor's professional judgement.

The audit scope is a clear statement of the focus, extent and limits of the audit in terms of the subject matter's compliance with the criteria. The scoping of an audit is influenced by materiality and risk, and it determines which authorities and parts thereof will be covered. The audit process as a whole should be designed to cover the entire audit scope,[43] i.e. the audit scope is the boundary of the audit and is directly linked to the audit objective. In the process of scoping the audit you need to specify further and set a limit to what you are going to audit. The scope in compliance audit may include one or several financial years, but cannot be limited to only that. Scope should include more than time period, as is mentioned above, so that the link to audit objective is clear.

Example of the audit objective and scope
The **objective** is to verify that the Ministry of Transport has planned, conducted and monitored the process of procurement of road construction projects as per requirements of the Procurement Act.   **Scope:** Road construction projects in the Ministry of Transport for 2017, will be covered in this audit and evaluated against the criteria, para. 2 of the Procurement Act, which requires that the entity must include projects worth USD 3 million and above in the procurement plan. Irregularities in the process of awarding contracts, such as tailoring of bid specifications, will also be covered and evaluated against Sec. 1 para. 3, requiring an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective.

Formulate audit questions

When you have determined the subject matter, there is a need to define it further by breaking it down into audit questions. The main function of the audit question(s) is to organise and concretise the audit. The questions should be thematically adequate in relation to the audit objective, unambiguous and clearly formulated, and they should not overlap. Each question must have significant importance for the audit. The audit questions will guide you and with the coverage defined in the audit scope, all

---

[42] ISSAI 4000/43-44
[43] ISSAI 400/50

aspects of the audit objective should be covered by the audit questions. It is recommended that you do not formulate too many questions and perhaps limit them to 3-6 in order to maintain a clear focus. You may also have a few overall questions and detail them into sub-questions.

The audit questions should be:

- Short and clear, unambiguous and easy to comprehend;
- Relevant and logically linked to the subject matter and the audit objective; and
- Sufficient to answer the problems/risks of non-compliance identified in the subject matter.

Example of audit questions and criteria
Audit question #1: Has the ministry included the road construction projects in the annual procurement plan? **Criteria:** Section 3 para. 2 of the Procurement Act requires that the Ministry of Transport must include projects worth USD 3 million and above in the procurement plan. **Audit question #2:** Has the method of procurement been fair, equitable and transparent? **Criteria:** Section 1 para. 3 requires that an accounting officer must ensure that a ministry maintains an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective.

Derive criteria from the authorities

When you have defined the subject matter, the corresponding criteria must be identified and must be linked to the audit questions in the working paper CAP1. *Audit strategy and plan*. As mentioned earlier, criteria are the benchmark against which the subject matter is evaluated to measure if the subject matter is or is not in compliance with the identified criteria. You must use professional judgement in determining and applying criteria, and professional scepticism to assess if the criteria are suitable and exhibit the characteristics as mentioned in chapter 2.2. For regularity, the criteria are derived from laws, regulations, policies etc. The quality of audit conclusion or opinion in compliance audits largely depends on how you assess and apply corresponding audit criteria to the subject matter in your work.

You must identify the relevant audit criteria prior to the audit to provide a basis for a conclusion or an opinion on the subject matter. Suitable audit criteria must be relevant, complete, reliable, neutral, understandable, useful, available, comparable and acceptable, refer to chapter 2.2 and ISSAI 4000/118.

Once suitable criteria have been identified based on the characteristics, they then must be appropriately operationalised for the particular circumstances of each audit to be able to reach meaningful conclusion(s). In general, it is not possible to conduct a compliance audit if you have not been able to identify suitable criteria. If you discover, after the commencement of the compliance audit, that some or all of the applicable criteria are unsuitable or are not appropriate for the relevant subject matter, you (the auditor/SAI) should reconsider that audit. If it is not possible under applicable law or regulation, you (the auditor/SAI) continue with the compliance audit, and express a modified conclusion, or a disclaimer, as appropriate in the circumstances.

5.2.3. Step 3 – Determine the level of assurance

The level of assurance to be provided in an audit, needs to be considered when the scope and subject matter of an audit is being identified. Conducting a limited or reasonable assurance audit is a strategic decision, which needs to be made at the entity level, by the SAI, after considering:

- Needs of the intended user(s);
- State of internal control environment and system of the audited entity;
- Availability of and access to information;
- Existing competencies of the auditors/team; and
- Availability of resources.

The list given above is not exhaustive. SAIs may consider other factors in addition while deciding on the level of assurance to be provided in an audit.

Needs of intended users

User needs are the most important factor to consider in determining the level of assurance to be provided by the audit. A SAI has to assess the needs of the intended users to determine which type of engagement is more appropriate. This requires an understanding of the decisions made by the users, and the type of information they need for their decision-making purposes.

It can be said that if the decision-making process of the users requires sophisticated information on the subject matter and its functioning, a reasonable assurance audit would be more appropriate. This assurance level provides an insight into the systems of the subject matter and their reliability.

Availability of information

Although access to information is a fundamental aspect of an audit and SAIs usually have strong powers to ensure necessary access, a SAI can still face situations where information available for the audit is limited; some information may not even exist, or the auditor may not have sufficient access to existing information. Due to the specific nature of the public sector audit, in such cases, the SAI may not be in a position to decline conducting the audit. However, this factor would have an impact on the level of assurance to be provided. Reasonable assurance audits require the auditor to have access to the systems and processes utilised by the responsible party (e.g. internal controls of an entity), and therefore necessitate more information compared to a limited assurance audit. Therefore, limitations on information would likely lead to a limited assurance audit.

Determination of assurance may be set at SAI level in the policy documents, where it indicates what kind of assurance the SAI would like to give for compliance audits considering the nature and risk of the subject matter of the entities. In general, for direct reporting engagements, reasonable assurance with conclusions can be considered and for attestation engagements, reasonable assurance with opinions.

5.2.4. Step 4 – Determine materiality

You must determine materiality to form a basis for the design of the audit and re-assess it throughout the audit process. The concept of materiality includes nature, context and value. The majority of instances of non-compliance will be material by nature in compliance audit and therefore qualitative materiality is more relevant in compliance audit than quantitative materiality. Determination of

materiality requires you to understand and assess what factors might influence the decisions of the intended users. For example, when the identified criteria allow for variations in the presentation of the subject matter, you should consider how the adopted presentation might influence the decisions of the intended users.

Materiality is applied in planning and executing the audit, and in evaluating the effect of instances of non-compliance. In the planning phase, assessing materiality helps you to identify the audit questions that are of importance to the intended user(s). In performing the audit, you are to use materiality in deciding on the extent of audit procedures to be executed and the evaluation of audit evidence. In evaluating and concluding the audit, the materiality is used to evaluate the scope of work and the level of non-compliance to determine the impact on the conclusion or opinion.

Qualitative and quantitative factors in determining materiality
The relative importance of qualitative factors and quantitative factors when considering materiality in a particular audit is a matter of professional judgement. In some cases, the qualitative factors are more important than the quantitative factors. Public expectations and public interest are examples of qualitative factors that may affect the determination of materiality. Instances of excess spending over appropriations authorised by the legislature or introduction of a new service not provided for in the approved appropriations, may be instances of non-compliance that are not material but may still warrant communication to the auditee due to their nature.

Qualitative factors may include such things as:
- The interaction between, and relative importance of, various components of the subject matter information when it is made up of multiple components, such as a report that includes numerous performance indicators;
- The wording chosen with respect to subject matter information that is expressed in narrative form;
- The nature of an instance of non-compliance; for example, the nature of observed deviations from a control when the subject matter information is a statement that the control is effective;
- Whether an instance of non-compliance affects compliance with laws or regulations;
- Whether an instance of non-compliance is the result of an intentional act or is unintentional;
- When the subject matter information relates to a conclusion on compliance with laws or regulations, the seriousness of the consequences of non-compliance; and
- When the underlying subject matter is related to a particular aspect of the programme or entity and is significant regarding the nature, visibility and sensitivity of the programme or entity.

Examples of qualitative materiality

*Example 1 – **Road construction project not included in the procurement plan***
It is qualitatively material that the road construction project is not included in the procurement plan as this might lead to construction of roads that were not needed most to be constructed,

---

according to the public needs and expectations, and the infrastructure might not be developing in the desired direction for the community/region/nation.

*Example 2 – **False diplomas***
In the case of employment of new employees, **it is qualitatively material that the entity verifies that the submitted diplomas are genuine documents**. In this case it would mean that a person is hired on a false background and receiving a salary on wrong terms. It is not important to check whether the salaries are correct**, but what is material is that people are employed based on the right qualifications**. For instance, if a person is employed as a medical doctor and has a false degree/diploma, and has been employed based on that. It would have serious consequences for the patients if the "doctor" prescribed wrong medicines. Employment of unqualified personnel based on false diplomas not only has economic effects for the entity, but also consequences for society since the qualifications are not right, and this is affecting service delivery to the citizens.

*Example 3 – **IT access control***
It is qualitatively material if unauthorised persons/entities have access to the IT-systems. For example, for the HR/payroll system, it is crucial that only those who are processing the information have access. If unauthorised persons have access, even though it is read-only access, and the persons cannot manipulate the information, there will be a breach of confidentiality. Another example is if unauthorised persons get access to classified information, for example to the database of the Ministry of Defence or Ministry of External Affairs. This information can be misused when/if it falls into the wrong hands, which may have serious implications for the nation.

Quantitative factors relate to the magnitude of non-compliance relative to the reported amounts for those aspects of the subject matter information which may be:
- The number of persons or entities affected by the particular subject matter, or the monetary amounts involved; and
- The number of observed deviations from a control may be a relevant quantitative factor when the subject matter information is a statement that the control is effective.

Quantitative materiality is determined by applying a percentage to a chosen benchmark as a starting point. This involves the exercise of professional judgement and reflects, in the auditor's judgement, that which user(s) of the information are most likely to consider important. Quantitative materiality is mostly used in attestation engagement.

Concluding on the materiality of the non-compliance identified as a result of the procedures performed requires the auditor's professional judgement. Professional judgements about materiality are made in the light of surrounding circumstances, but are not affected by the level of assurance; that is, for the same intended users and purpose, materiality for a reasonable assurance engagement is the same as for a limited assurance engagement because materiality is based on the information needs of intended users.

5.2.5. Step 5 – Carry out risk assessment of the subject matter at entity level

In assessing the risks of material non-compliance, you may consider the following factors:
- The complexity of the applicable compliance requirements;

- The susceptibility of the applicable compliance requirements to non-compliance;
- The length of time the entity has been subject to the applicable compliance requirements;
- The auditor's observations about how the entity has complied with the applicable compliance requirements in prior years;
- The potential effect on the entity of non-compliance with the applicable compliance requirements; and
- The degree of judgement involved in adhering to the compliance requirements.

Some examples of situations in which there may be a risk of material non-compliance that is pervasive in the entity's non-compliance are:

- An entity that is experiencing financial difficulty and for which there is an increased risk that grant funds will be diverted for unauthorised purposes; and
- An entity that has a history of poor recordkeeping of its programmes.

Examples of non-compliance

Example 1
The government agency has not performed inspections for the past five years. This non-compliance may be significant due to qualitative aspects such as safety implications. Although no particular monetary amounts are involved, the non-compliance may be material due to the potential consequences it may have for the safety of the building's occupants. In the event of a disaster, there is also a risk that the non-compliance may result in significant liability claims which could have material financial implications for the government agency as well.

Example 2
The terms of a funding agreement state that the recipient of the funds must prepare financial statements and send them to the donor organisation by a certain date. The financial statements had not been prepared and sent by this date. The non-compliance may or may not be material depending on whether or not the financial statements were subsequently prepared and sent, the extent of the delay, the reasons for the delay, any consequences that may arise as a result of the non-compliance, etc.

Performing risk assessment procedures

Obtaining an understanding of the entity, the applicable compliance requirements, and the entity's internal control over compliance establishes a frame of reference within which you, the auditor, plan the compliance audit. Within this frame of reference, you exercise professional judgement about assessing risks of material non-compliance and responding to those risks throughout the compliance audit.

The nature and extent of the risk assessment procedures you will perform may vary from entity to entity and are influenced by factors such as:

- The newness and complexity of the applicable compliance requirements;
- Your knowledge of the entity's internal control over compliance with the applicable compliance requirements obtained in previous audits or other professional audits;

- The nature of the applicable compliance requirements;
- The services provided by the entity and how they are affected by external factors; and
- The level of oversight by the government.

Risk assessment regarding controls requires you to examine whether:
- Managers/key officials of the entity clearly understand key compliance objectives. Also, if they are able to detect instances of non-compliance and initiate processes necessary to fix the underlying cause of non-compliance;
- Organisational structure identifies risks of non-compliance. A large and complex organisation typically has a dedicated unit for risk management. It continuously examines compliance and other risks facing the entity, reviews controls, and recommends changes therein to ensure that the entity complies with applicable compliance requirements;
- Key managers/officials of the audited entity have been given responsibility to communicate changes. An entity operating in a dynamic environment needs to respond quickly to the changes in environment. If the entity has assigned official(s)/manager(s) to communicate information on changes in procedures/controls across the entity, it decreases the risk of non-compliance;
- Key managers/officials have a clear understanding of complex parts of its operations. When key managers/officials lack such understanding, they are not likely to implement or oversee compliance with requirements, as they need to. The risk of non-compliance is likely to be higher in that situation; and
- The entity's management views audit findings/recommendations seriously and takes appropriate corrective measures. An institutional body, e.g. committee/board, meets periodically to review compliance issues arising from audits.

The procedures related to understanding how management has responded to audit findings and recommendations that could have a material effect on the entity's compliance with the applicable compliance requirements, are performed to assist you in understanding whether management responded appropriately to such findings. Examples of *external monitoring* include regulatory reviews, programme reviews by government agencies and reviews by oversight bodies. Examples of *internal monitoring* include reports prepared by the internal audit function and internal quality assessments.

Performing risk assessment procedures to obtain an understanding of the entity's internal control over compliance includes an evaluation of the design of controls and whether the controls have been implemented.

Internal control consists of the following five interrelated components:
- The control environment;
- The entity's risk assessment;
- Information and communication systems;
- Control activities; and
- Monitoring.

Considering the risks of fraud
As auditors, we know that fraud and corruption pose serious risks to the public sector. The potential damage of fraud and corruption extends well beyond any financial loss, as it also causes substantial

negative effects on the entity's reputation and internal working environment. Several cases of fraud and corruption can also severely reduce people's trust in the public sector as a whole. Fraud risks and assessments of materiality in relation to fraud are considered in the context of the broader scope of public sector auditing.

It is important to have a clear understanding of what fraud and corruption means. The distinguishing factor between fraud and error is whether the underlying action that results in the non-compliance is intentional or unintentional. Fraud and corruption are intentional acts involving the use of deception to obtain an unjust or illegal advantage. The ones responsible for a fraudulent act may be members of the management, those charged with governance, employees, or third parties.

Depending on their mandate, this may be an appropriate starting point for auditors when looking for indicators of possible acts of fraud and corruption. Much can be done to prevent fraud and corruption by addressing weak internal controls.

Managing public property is also a vulnerable area. Valuable property is vulnerable to theft or loss. This includes money, goods or real estate, human capital and also information as a valuable public asset.

5.2.6. Step 6 – Understand the entity and control environment related to the subject matter

Understanding the audited entity is crucial for compliance audit as it might be used to define the subject matter and the criteria in more detail, audit materiality and assess the risk of non-compliance at all levels. Risk assessment is an iterative process and understanding of the entity related to subject matter might lead to revising the assessed risks of non-compliance or updating them with more details. Likewise, you might also have to revise or update criteria.

You need, therefore, to examine the following factors in understanding the audited entity in the light of relevant authorities. In some cases, compliance audit can cover more than one entity and in such cases, auditors should obtain an understanding of all the entities of which activities will be audited by determined scope. For example, some SAIs conduct compliance audit on the proper utilisation of a fund that is used by more than one entity.

To achieve these, you may need to consider the following aspects of the audited entity:
- Strategies, operations and good governance of the entity;
- Understand and evaluate whether the fundamental goals and objectives and measures to implement as outlined in the strategic plan of the audited entity are aligned to the mandatory coverage and standards required;
- The goals specified in the strategic action plans and programmes are linked to the results;
- Activities and operations are directed towards attainment of the goals and objectives of the audited entity which should in turn respond to all compliance requirements of the entity; and
- Legal acts applied to the operations of the audited entity and other authorities, like administrative policies, internal procedures and instructions/orders, do not contradict the normative legal acts.

You may use the following sources of information to develop a proper understanding of the nature of the audited entity, including:
1. Laws and regulations;

2. Budgetary legislation/approved budget;
3. Code of ethics, code of conduct;
4. Internal policies, strategic plans, operational plans, procedures manuals;
5. Contracts;
6. Grant agreements;
7. Media reports;
8. Annual report; attestation and direct reporting audits, and internal or external monitoring that directly relates to the objectives of the compliance audit;
9. Minutes of meetings (Board of Directors, management minutes);
10. Internal audit reports;
11. Knowledge from previous audits;
12. National statistics; and
13. Visiting the entity's website.

Control environment sets the tone of an organisation influencing the control consciousness of its employees. The audited entity establishes internal controls with the aim of fulfilling compliance requirements in its operations. You need to understand:
a. What these controls are;
b. Whether the controls are adequate and can detect, prevent, and correct instances of non-compliance; and most importantly,
c. Whether the controls are working as intended.

In the context of compliance audits, an internal control system is composed of policies, structure, procedures, processes, tasks and other tangible and intangible factors that help the audited entity to respond appropriately to risks of non-compliance with the compliance requirements. An effective system should safeguard the audited entity's assets, facilitate internal and external reporting and help the audited entity to comply with relevant legislation. You need to have considerable insight into the internal functioning of the subject matter through assessment of the control environment and internal controls of the audited entity.

Assessing control environment related to the subject matter
In general, the auditors examine whether management has created and maintained a culture of honesty and ethical behaviour, whether the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control and whether those other components are not undermined by deficiencies in the control environment. You can carry out control assessment by gathering and analysing the following information of the entity:[44]
- Policies and procedures including a code of conduct are clearly written and communicated;
- Duties are properly segregated between performance, review, and record keeping of tasks;

---

[44] The text given for control assessment and risk management is based on the guidance provided by the General Accountability Office, USA for Internal Control Assessment for auditors. It has been adapted to fit in the requirements as mandated in the ISSAIs. Additional details on how internal control assessment can be carried out may be seen on the website http://www.gao.gov/special.pubs/ai00021p.pdf

- Organisational arrangement (board/committee) is in place for reviewing audits/communication of auditors. Proceedings of the board/committee are properly documented/followed up;
- Management has responded positively to the audit findings/recommendations in the past;
- Responsibilities of key officials/managers are clearly defined;
- Key managers/officials have adequate knowledge and experience to discharge their responsibilities;
- Staff is properly educated/trained about compliance requirements and has the responsibility to point out instances of non-compliance to management;
- Management supports adequate information and reporting systems;
- Computer and program controls include data entry controls e.g. edit checks, exception reporting, access controls, reviews of input and output data; and
- You can determine how to analyse the information depending on the subject matter. For example, if the subject matter relates to assets, whether assets are secured and physically counted periodically and compared with recorded amounts.

The particular type of controls evaluated depends on the subject matter, and the nature and scope of the particular compliance audit. In evaluating internal control, public sector auditors assess the risk that the control structure may not prevent or detect material non-compliance. The internal control system in an entity may also include controls designed to correct identified instances of non-compliance. In these cases, you need to obtain an understanding of internal control relevant to the audit objective, and test controls on which you expect to rely. The result of the internal control assessment will help you to determine the confidence level and hence, the extent of the audit procedures to perform.

Based on the evaluation of internal control, you will be able to decide on the appropriate audit approach and identify the audit evidence required in conducting the audit. If you have identified risks of material non-compliance, you should develop an overall response to such risks. Then you should design further audit procedures, including tests of details (which may include tests of transactions) to obtain sufficient appropriate audit evidence about the entity's compliance with each of the applicable compliance requirements in response to the assessed risks of material non-compliance.

Linking identified risks to audit strategy
An important aspect of compliance audit planning is that you practically consider the linkage of identified risks to the audit strategy. On the basis of the value of detection which is acceptable for the evaluation of internal controls, you can then decide on the audit strategy to follow. You should also perform walkthroughs of identified controls in order to gain a degree of confidence in the operating effectiveness of these controls. During walkthroughs, you need to exercise professional judgement in determining what could potentially go wrong and how to collect sufficient and appropriate evidence to test this assumption.

5.2.7.   Step 7 – Develop audit strategy and audit plan
For developing an audit strategy and the audit plan, you need to follow these audit steps:

- ✓ Develop an audit strategy and the audit plan;
- ✓ Assess audit risk;
- ✓ Plan audit procedures to enable reasonable assurance; and
- ✓ Documentation and communication.

Develop an audit strategy and the audit plan

Finalisation of the audit strategy and the audit plan is the last step of the planning process. Planning the audit so that it will be performed effectively involves discussions with the audit team, and developing an overall audit strategy and an audit plan. The standard emphasises the need for an audit strategy and audit plan because this helps SAIs in determining how the audit will proceed from start to end. All critical aspects of a compliance audit are examined thoroughly, and an understanding reached on what would be done (audit strategy) and how (audit plan). Both the audit strategy and the audit plan should be documented in writing and updated as necessary throughout the audit. Planning also involves considerations related to the direction, supervision and review of the audit team.

The purpose of the audit strategy is to devise an effective response to the risks of non-compliance. It specifies and sets the planned extent, timing and direction of the audit and guides the development of the audit plan. The audit strategy will show how auditors would respond to risk, and changes may be made to the scope of the audit when additional information becomes available on the subject matter, criteria or controls, thereby changing the risk profile of the audited entity.

The purpose of the audit strategy is to document/design the overall decisions, and the strategy may contain the following:[45]
   a) The subject matter, scope, criteria and other characteristics of the compliance audit taking into account the mandate of the SAI;
   b) Audit questions;
   c) The type of engagement (attestation engagement or direct reporting engagement);
   d) The level of assurance to be provided;
   e) Composition and work allocation of the audit team, including any need for experts, and the dates of quality control;
   f) Communication with the auditee and/or those charged with governance;
   g) Reporting responsibilities, as well as to whom and when such reporting will take place, and in what form;
   h) The entities covered by the audit; and
   i) The materiality and risk assessment.

Once you have understood the compliance requirements applicable to a subject matter and the internal controls affecting it, you are able to identify the risk that something can go wrong and accordingly plan necessary audit procedures that would allow you to arrive at an appropriate conclusion or opinion considering that risk.

Assess audit risk

Auditors should manage the risk of providing a report that is inappropriate in the circumstances of the audit. The audit risk is the risk that the audit report – or more specifically the auditor's conclusion or

---

[45] ISSAI 4000/139

opinion – will be inappropriate in the circumstances of the audit. Consideration of audit risk is relevant in both attestation engagement and direct reporting engagement audits.

You need to consider audit risk throughout the audit process. In addition, the audit should be conducted in such a way that it would manage the audit risk, or reduce it to an acceptably low level. The relative significance of the dimensions of audit risk depends on the nature of the subject matter, whether the audit is to provide reasonable or limited assurance.

Plan audit procedures to enable reasonable assurance

In preparing an audit plan, SAIs review, rearrange and document every step of the audit process in sufficient detail. Thus, audit plans eventually work as benchmarks against which the flow of compliance audit activities is appraised.

Planning audit procedures involves designing procedures to respond to the identified risks of non-compliance. The exact nature, timing and extent of the audit procedures to be performed may vary widely from one audit to the other. Audit procedures will be discussed in the chapter on performing compliance audits and gathering evidence, refer to chapter 5.3.

You must develop an audit plan for the compliance audit. The audit strategy is an essential input to the audit plan. The audit plan may include:
- Nature, timing and extent of the planned audit procedures and when they will be performed;
- An assessment of risk and of internal controls relevant for the audit;
- The audit procedures designed as a response to risk; and
- The potential audit evidence to be collected during the audit.

Example of risk of non-compliance linked to the audit question, criteria and planned procedures			
Audit question	**Criteria**	**Risk of non-compliance**	**Planned procedure (inspection/inquiry)**
Has the ministry included the project in the annual procurement plan?	Section 3 para. 2 of the Procurement Act requires that the entity must include projects worth USD 3 million and above in the procurement plan.	Risk that the project was not included in the annual procurement plan resulting in unauthorised expenditure as it was not part of the budget.	Inspect the procurement plan to confirm if the project was included. Inspect the budget estimates and enquire with the budget and implementation officials if the project was budgeted for.

5.2.8. Documentation and communication

You are advised to **document**:
  a. The risk assessment procedures performed, including those related to gaining an understanding of the internal control system;

b. Responses to the assessed risks of material non-compliance, the procedures performed to test compliance with the applicable compliance requirements, and the results of those procedures, including any tests of controls;

c. Materiality, qualitative and quantitative, and the basis on which they were determined; and

d. How the audit team complied with the specific public sector audit requirements (if any) that are supplementary to the auditing standards.

The auditor's documentation of evidence regarding identified or suspected non-compliance with authorities may include, for example:

a. Copies of records or documents; and

b. Minutes of discussions held with management, those charged with governance, or other parties inside or outside the entity.

In determining the nature and extent of the documentation for a typical compliance audit, you are advised to consider the following factors:

- Risks of material non-compliance with the applicable criteria;
- Auditor's response to the assessed risks through planned audit procedures;
- Methods for gathering evidence;
- Extent to which professional judgement was applied in audit work, especially in the context of materiality consideration; and
- Materiality of the evidence obtained against criteria.

Working paper CAP 1. *Audit strategy and plan* is designed to assist you in the documentation of your work at the planning stage and by completing this you will be able to fulfil the requirements in the standard. Below is a snapshot of CAP1 where you link audit questions, criteria, risks and planned procedures and base the audit work on this in the next phases.

CAP1: Audit Strategy and Plan

Assurance Level: Reasonable (explain which level of assurance is chosen and why)
It can be set by the SAI in policy documents, ref. your SAI Policy if any

Audit question ref. ISSAI 4000/128	Audit Criteria, ref. ISSAI 4000/110	Risk related to this audit question and corresponding criteria	Planned audit Procedure (s)	Methods for gathering evidence	Expected Audit Evidence
Audit question No. 1					
Audit question No. 2, etc.					

Communication

An engagement letter should be issued to the audited entity when the audit team has defined the subject matter properly and identified the corresponding criteria. It is important to include this information in the engagement letter and discuss especially the criteria with the entity in the entry meeting. It is desirable that the entity agrees with the criteria that the team has identified; however, it is not a requirement in the standard. Auditors should still pay attention to management's comments

as it might provide the team with valuable information regarding the subject matter and the criteria. You may also discuss the audit strategy at a high level and the risks that have been identified.

Working papers to complete

Complete the working papers for the planning phase as mentioned in the table below. It is important to go through all the steps in these working papers. Describe them in such a manner that other auditors and reviewers who are not familiar with the subject matter are able to understand the reason why the subject matter was determined, why the criteria are relevant, what audit questions you have defined, what the risks for non-compliance and materiality are and the reason for determining level of assurance etc.

W/P ref.	Working paper	Objectives of the working paper
CAP1	Audit strategy and audit plan for subject matter	Examine all critical aspects of the compliance audit thoroughly and understand what to do (audit strategy). Determine/define subject matter, derive criteria, determine audit objective and audit scope, understand the entity's control environment, determine materiality and assess risk at entity level, determine assurance level and engagement type. Plan the audit and consider audit risk, how to respond to audit risk, what kind of procedures to perform, timeline for the audit and when to report. Planning also involves considerations related to the direction, supervision and review of the audit team.
CAP2	Engagement letter	Issue an engagement letter to the responsible party. If the financial audit team has completed planning for the same entity at the same time and it is the same team that is carrying out financial and compliance audit, the team may produce one engagement letter to the entity and include paragraphs where at least the subject matter, criteria and timeline are mentioned. Otherwise, consider issuing a separate engagement letter where subject matter, criteria, engagement type, audit objective, audit scope and the timeline for carrying out the audit and reporting are mentioned as a minimum.
CAP3	Minutes of entry meeting	You are required to conduct an entry meeting and document it in the minutes of the entry meeting; the entity should be informed about the subject matter, criteria, audit questions, the objective and scope of the audit.
CAP4	Quality control questionnaire – planning phase	Carry out quality control of the subject matter after the planning phase has been completed. This should be approved by a level-3 reviewer before the auditor proceeds and starts performing procedures.

5.3. Performing the audit procedures to obtain audit evidence

In this phase, you the auditor primarily gather and document evidence to form a conclusion or opinion as to whether the subject matter, in all material respects, complies with established criteria. The nature and sources of the necessary audit evidence shall be determined by the desired level of assurance, the criteria, materiality, the subject matter and the scope of the audit. Sufficient audit evidence is related to the decision about the level of assurance. To form a conclusion with reasonable assurance, you need

to obtain more evidence than in a limited assurance engagement. The nature of audit evidence is also different for the two types of audits. For limited assurance engagements, the audit evidence is mostly analytical procedures and inspections while for reasonable assurance engagements, you would normally need to perform mostly all the audit techniques.[46]

Follow these steps for gathering sufficient and appropriate evidence:
1. Gather evidence through various methods and perform procedures;
2. Consider non-compliance that may indicate fraud;
3. Re-assess risk and gather more evidence; and
4. Documentation and communication.

5.3.1. Step 1 – Gather evidence through various methods and perform procedures

Audit evidence is the information used by the auditor to analyse a subject matter against established criteria to arrive at findings for forming a conclusion(s) or an opinion. You need to design and apply appropriate audit procedures to obtain sufficient and appropriate audit evidence.

You must select a combination of audit techniques to be able to form a conclusion with the selected level of assurance, and perform effective audit procedures in line with the audit plan to gather audit evidence and fulfil audit objectives. **You will often need to combine and compare evidence from sources using different techniques/methods in order to meet the requirements for sufficiency and appropriateness.**[47]

When the risks of non-compliance are significant, and you plan to rely on the controls in place, such controls are required to be tested. When controls are not considered reliable, you must plan and perform substantive procedures to respond to the identified risks. You should perform additional substantive procedures when there are significant risks of non-compliance.

Evidence-gathering methods
The effectiveness of an evidence-gathering process is dependent on a realistic planning of this part of the audit process using proper evidence-gathering techniques. SAIs may be using different tools for this purpose. The standard provides guidance on how to gather and evaluate audit evidence. Some of the techniques of gathering audit evidence are mentioned below.

Observation
Auditors look at processes or procedures being performed. In performing compliance audit, this may include looking at how a bid tendering process is carried out, observing how benefit payments are processed, or observing if performance of any kind is in line with laws and regulations.

Inspection
Inspection may include:
- Examining the books and records to determine how project funds have been accounted for, and the completeness of recording;

---

[46] ISSAI 4000/145-146
[47] ISSAI 4000/158-159

- Comparing actual project accounting records to the terms of the project agreement;
- Review of case files/relevant documents to determine if recipients of benefits met eligibility requirements; and
- Examining an asset, such as a bridge or a building, to determine if it meets the applicable building specifications.

You should consider the reliability of any documents inspected and keep in mind the risk of fraud and the possibility that documents inspected may not be authentic. In cases of fraud, sometimes two different sets of books and records have been kept. You may conduct additional audit procedures e.g. also inquire of different persons in the entity to ascertain the source of the documents, or the controls over their preparation or maintenance.

Inquiry

This involves seeking information from relevant persons, both within and outside the audited entity, and may include:

- Formal written inquiries;
- Informal oral discussions;
- Interviewing and asking questions of relevant persons, including experts; and
- Preparing and sending questionnaires or surveys.

Inquiry is generally used extensively throughout an audit and complements other audit procedures. For example, when observing processes being performed, such as the benefits payment process within a country/state, inquiries could be made of officers regarding how relevant legislation, including changes and updates, is identified and interpreted. Results of inquiries may indicate that the processes are performed in different ways in different locations; which is a frequent cause of non-compliance.

To get a better understanding, inquiries are often made of persons outside the particular function subject to audit. For example, in addition to making inquiries of accounting personnel at a line ministry, it may also be relevant to make inquiries of the ministry's legal or technical departments. Generally, the further a person is from the subject of audit, the greater the probability that they will be objective in their response, although their experience with the audit area is likely to be in a narrow area. Those external to the audited entity – such as banks, contractors, media – are more likely still to be objective. In this case, you need to be mindful of potential relationships between the audited entity and personnel of the external body.

Inquiry can be a weak form of audit evidence and it alone cannot provide sufficient appropriate evidence for audit purposes. To obtain sufficient appropriate evidence, inquiry should be performed together with other types of procedures. Inquiry is most effective when conducted with relevant and knowledgeable persons, i.e. persons in positions of authority who are authorised to speak or give opinions on behalf of the entity.

Confirmation

This is a formal type of inquiry and involves obtaining a reply from a third party, independently from the audited entity, regarding some particular information. In compliance audits, confirmation may involve obtaining feedback:

- Directly from grant beneficiaries that they have received the grants or other funds that the audited entity asserts have been paid out;
- Directly from grant beneficiaries that funds have been used for the particular purpose set out in the terms of a grant or funding agreement;
- Directly from suppliers that they have provided assets to the audited entity on a certain date and free of damage; and
- Receiving guidance from the legislature as to how a specific piece of legislation is meant to be interpreted.

Written confirmations may also be obtained from management regarding oral representations made during the audit. Examples of written management representations may relate to:
- Management's assertion of compliance with a relevant section of legislation, the terms of an agreement, etc.;
- Management's disclosure of all instances of non-compliance of which it is aware; and
- Management having provided the auditor with complete information about the subject matter.

By their very nature, management representations are a weak form of assurance, but where the audited entity's management is privy to confidential information, this may be the only source of evidence.

Re-performance

This can be a very important technique to use to determine if the results of your work detect deviation from the entity/auditee's work. The auditor is independently carrying out the same procedures already performed by the audited entity. The data systems that are used by the entity/auditee can demand special qualifications that have to be considered before starting the re-performance. You must consider this, and assess the need to engage an expert who understands the system if needed; for example, re-performance of pension calculations, recipients of hospital treatment or engineering models etc. Re-performance may be done manually or by using computer-assisted audit techniques. Some examples of re-performance are:
- Review of individual case files to test whether the audited entity made the correct decisions or provided the appropriate service in accordance with the relevant criteria;
- Process steps re-performed to test the appropriateness of visas or residence permits issued;
- Re-computation of taxation deductions on the audited body's staff payroll to confirm the correct amounts payable in taxation;
- Confirming the correct application of criteria for making benefit payments involving payments to persons meeting specific requirements;
- Where elderly benefit payments (pension or assistance) involve payments to persons over a certain age, the audited entity's selection of recipients from a public database may be re-performed by public sector auditors using computer-assisted audit techniques to test the accuracy of the entity's process; and
- Re-performing the tender selection process using the selection criteria to test that the correct bids (tenders) have been selected.

Combination of techniques

In the process of gathering sufficient and appropriate evidence, you will have to apply various techniques/methods together, such as inquiries, observations and inspection, for certain procedures to meet the requirements of sufficiency and appropriateness[48].

Figure 7: Example of combination of various techniques for evidence gathering

The reason is that more assurance is ordinarily obtained from consistent evidence gathered from different sources, or of a different nature, than from items of evidence considered individually. In addition, obtaining evidence from different sources or of a different nature may indicate that an individual item of evidence is not reliable. For example, corroborating information obtained from a source independent of the appropriate party(ies) may increase the assurance you will obtain from a representation from the appropriate party(ies). Conversely, when evidence obtained from one source is inconsistent with that obtained from another, you need to determine what additional procedures are necessary to resolve the inconsistency.

Substantive testing involves testing detailed transactions or activities against the audit criteria. Substantive testing is mostly used in attestation engagements and must always be included as an audit technique in such engagements. However, performing only substantive testing is only effective in rare cases and this audit technique will normally be combined with other audit techniques.[49]

Tests of key controls involves testing the controls that management has put in place to reduce the risk of non-compliance or the risk that the subject matter information is materially misstated. For most subject matters, testing key controls is an effective way to collect audit evidence.[50]

Analytical procedures can be used both as part of the risk analysis and when collecting audit evidence. Audit evidence can be collected either by comparing data, investigating fluctuations or identifying relationships that appear inconsistent with what was expected, either based on historical data or the auditor's past experience. Regression analysis techniques or other mathematical methods may assist public sector auditors in comparing actual to expected results. Analytical procedures can never be the only technique used. In a limited assurance engagement, analytical procedures and inspections are

---

[48] ISSAI 4000/159
[49] ISSAI 4000/167
[50] ISSAI 4000/168

normally enough to form a conclusion with limited assurance while a conclusion with reasonable assurance must be formed on the basis of a combination of the audit techniques.[51]

In compliance auditing, opportunities for analytical procedures may be limited, and their usage will depend upon the availability of reliable financial and operational information and statistics. An example would be comparing increases and decreases in benefits payments (pension allowance) from one year to the next, with demographic information such as the number of citizens having reached retirement age within the last year. If the pension benefits payments, having been in the range of 5%-6% of government spending during 2005 to 2013, have increased to 11% in 2014, auditors should examine whether this change is due to non-compliance in computing pension liabilities etc.

Compliance audit sampling

The standard states that the auditor shall use audit sampling, where appropriate, to provide a sufficient number of items to draw conclusions about the population from which the sample is selected. When designing an audit sample, the auditor shall consider the purpose of the audit procedure and the characteristics of the population from which the sample will be drawn. Audit sampling is defined as the application of audit procedures to less than 100 per cent of items within a population of audit relevance. A sample may be quantitative or qualitative depending on the audit scope, and the need for information to illuminate the subject matter from several angles. [52]

The standard states that audit sampling shall be used where it is appropriate, and it indicates that it is not required for every subject matter and audit procedure. Therefore, you need to assess whether or not it is appropriate to use sampling for a particular subject matter and selected procedures. When you have assessed that you need to use sampling, you must assess if it requires use of statistical or non-statistical sampling methods. In case you have determined that non-statistical methods are more appropriate, you may apply judgemental sampling and apply professional judgement in this regard.

Once you have designed an audit procedure, it is possible to vary the sample size from one to all the items in the population being tested. The sample size usually depends on the following factors:
- a) Effectiveness of internal control;
- b) Risk involved in the subject matter; and
- c) Materiality of the subject matter.

Qualitative sampling

Qualitative sampling is a selective procedure conducted as a deliberate and systematic process to identify the factors of variation in the subject matter. The auditor might sample on the basis of characteristics of individuals, groups, activities, processes or the audited entity as a whole. Qualitative sampling always requires careful assessment and sufficient knowledge of the subject matter.[53]

➤ *Judgemental sampling*

Judgemental sampling is a non-statistical method that may be used in case you are not able to determine the sample size through statistical method or you have assessed that judgemental sampling

---

[51] ISSAI 4000/169
[52] ISSAI 4000/172-174
[53] ISSAI 4000/176

is the best approach for certain procedures in your subject matter. You may then use the table below as a guideline. Before you can determine the sample size, you need to conclude on the reliance you will place on the controls. You will be able to conclude on reliance when you have assessed the internal controls related to the subject matter. For example, if you have assessed that the internal controls are not functioning properly and therefore you have assessed the reliance on controls as low, your sample size in this regard will be higher than if your control reliance is high. In addition to control reliance you are required to apply professional judgement when you are determining sample size based on judgemental sampling.

Recommended sample size

Level of reliance on controls	Sample size
Low reliance	40-60
Moderate reliance	20-40
High reliance	10-30

Table 2: *Sample size (range from min-max)*

Another example of qualitative sampling is filtering of data according to certain criteria, in order to narrow down the population you would draw your samples from. You may use Excel for this purpose and this technique is described in more detail in appendix 1.

Quantitative sampling

Quantitative sampling is used when the auditor seeks to draw conclusions about the whole population by testing a sample of items selected from it. In quantitative sampling, the sample risk must be reduced to an acceptably low level. However, the technical approach to quantitative sampling may require statistical techniques.[54] One of the quantitative sampling techniques, attribute sampling, is explained briefly below.

➤ *Attribute sampling*

In compliance audit, we will normally have a test where the result is either "the part of the subject matter we are examining is in compliance with the criteria" or "the part of the subject matter we are examining is not in compliance with the criteria". In such an instance, we make an assessment with a binary result: compliant or non-compliant. "Compliance" can be considered an attribute. We therefore recommend using attribute sampling in most instances when carrying out quantitative sampling in compliance audit. This technique is also recommended by the Institute of Internal Auditors for examining compliance. Please refer to appendix 1 for more explanation and a hyperlink to the iaonline-website for a sampling table.

When to perform the procedures

An audit procedure is the detailed instruction for the collection of a type of audit evidence that needs to be obtained at some time during the audit. In designing the audit procedures, it is important to consider the audit approach and decide whether the audit requires tests of controls, substantive tests or analytical review.

---

[54] ISSAI 4000/175

This involves the timing of the audit evidence that needs to be collected. The timing decision is affected by many factors, such as:

- Timeline of the audit;
- When the entity needs the audit to be completed;
- When you believe collection of evidence will be most effective;
- The availability of the staff to conduct the audit; and
- Deadline for the audit report.

Which audit procedure(s) to use

The exact nature, timing and extent of procedures will vary from one audit to the other. Both reasonable assurance and limited assurance engagements require the application of assurance skills and techniques and the gathering of sufficient and appropriate evidence as part of an iterative, systematic engagement process that includes obtaining an understanding of the subject matter and other circumstances regarding the audit. For limited assurance engagements, the audit evidence is normally obtained by performing analytical procedures and inspections, while for reasonable assurance engagements, you normally need to perform mostly all the audit techniques.[55]

You need to plan appropriate responses to assessed risks (refer to working paper CAP1). Responses to assessed risks include designing audit procedures that address the risks.[56] Determining the nature, time and extent of procedures is a matter of professional judgement and will vary from one engagement to the next. When you are planning audit procedures they must also be designed in such a way that they form the basis for answering the audit questions.

However, when reaching this stage in the audit, you are expected to have finished the work related to:

- Risk assessment procedures and in that regard to have applied analytical procedures and inquiries;
- The process of understanding the control environment related to the subject matter and to have performed procedures, and have a view on whether or not you will rely on the controls related to the subject matter. How much work needs to be done will depend on how broad the subject matter is and the assurance level that will be provided; and
- If you intend to rely on the operating effectiveness of controls, you need to obtain evidence that the controls are operating effectively when determining the nature, timing and extent of substantive procedures. The design and implementation of key controls relevant to the subject matter might be evaluated as adequate.

Procedures for a reasonable assurance engagement

- ➢ Based on your understanding of the underlying subject matter and other circumstances, identify and assess the non-compliance and compliance deviations in the subject matter information;
- ➢ To obtain reasonable assurance, you need to perform effective procedures in line with the audit plan and gather audit evidence, fulfil audit objectives and support the conclusion;

---

[55] ISSAI 4000/146
[56] ISSAI 4000/149

- You will often need to combine and compare evidence from sources using different techniques/methods in order to meet the requirements of sufficiency and appropriateness. For example, by interviewing management and employees, you may obtain an understanding of how management shares its views on the entity's practices and ethical behaviour with staff. You may then determine whether controls have been implemented by considering, for example, whether management has a written code of conduct and whether it is followed in practice. A survey submitted to the employees could for example illuminate to what extent the management acts in accordance with the code of conduct.[57] Based on the scope, you will gather quantitative and qualitative audit evidence, or a combination; i.e. in this case you would have tested key controls, inspected documents, observed and used inquiries;
- If it is appropriate, you should use sampling both for assessing control reliance and when performing substantive procedures;
- Substantive testing is mostly used in attestation engagements and must always be included as an audit technique in such engagements. However, performing procedures based only on substantive testing is not sufficient and you would need to combine it with other audit techniques;[58] and
- Evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and, if necessary in the circumstances, obtain further evidence.

A limited assurance engagement

The nature, timing and extent of procedures for gathering sufficient appropriate evidence in a limited assurance engagement are limited relative to a reasonable assurance engagement. The procedures may or may not primarily be analytical, inspections and inquiries, and will vary with the circumstances of the engagement; in particular, the underlying subject matter, and the information needs of the intended users and the engaging party, including relevant time and cost constraints.

- Analytical procedures and inspections are normally enough to form a conclusion with limited assurance engagements;[59]
- In the process of performing procedures, you should identify areas where non-compliance of the subject matter information is likely to arise, based on your understanding of the underlying subject matter and other engagement circumstances;
- You should design and perform procedures to address those areas and to obtain limited assurance to support the conclusion; and
- If you become aware of a matter that causes you to believe the subject matter information may be non-compliant, design and perform additional procedures to obtain further evidence.

Professional scepticism and judgement in gathering audit evidence

Professional scepticism is necessary to the critical assessment of evidence gathered by the auditor. This includes questioning inconsistent evidence and the reliability of documents and responses to inquiries. It also includes consideration of the sufficiency and appropriateness of evidence obtained in the light of the circumstances. The distinguishing feature of the professional judgement expected of

---

[57] ISSAI 4000/159
[58] ISSAI 4000/167
[59] ISSAI 4000/169

an auditor is that it is exercised by an auditor whose knowledge and experience have assisted in developing the necessary competencies to achieve reasonable judgements.

5.3.2. Step 2 – Consideration of non-compliance indicative of fraud and unlawful acts

Auditors use different techniques for gathering evidence as explained in the previous section. Some of the same techniques are extensively used in identifying fraud as explained below.

i. Observation: Auditors may observe the extent to which the management and staff are complying with policies, procedures, and internal controls. Observation may reveal a deficient control environment including a lack of ethics and integrity on the part of top management. This implies a higher fraud risk for the entity.

ii. Inspection: Auditors may examine the record for journal entries involving large rounded amounts at or near the close of accounting.

iii. Interviews: Auditors may interview top managers and key officials and note changes in management and employee behaviour indicating deception, corruption, red flags, and other abnormal occurrences that indicate fraud. Interviews would become more meaningful if auditors suspect fraud during their observation/inspection.

iv. Analytical reviews: Auditors compare financial information from period to period to identify abnormal financial data relationships. An unexpected increase in expenditure or revenue may be a sign of fraud.

v. Walkthrough: Auditors may trace an original source document through recording processes to test reliability of the internal control systems and discover points of opportunity for fraud.

You need to be aware of how the management of the audited entity responds to audit findings and report on it. This is an indicator of the entity's seriousness toward compliance issues. In cases where the management does not give due importance to the irregularities identified, which would be reflected in documents without any information as reference to corrective actions being taken, the risk of fraud in that kind of environment is going to be higher. You need to be alert to such signals while carrying out risk assessment in conducting the audit.

While gathering audit evidence, if you come across suspected unlawful acts or fraud, you should assess if the evidence complies with laws and regulations. In cooperation with the management of the SAI, you need to consider the SAI's mandate and internal reporting policies. When you have assessed that there is suspected fraud, you must consider how to inform the relevant authorities, and follow up to ensure that relevant action has been taken.

5.3.3. Step 3 – Re-assessment of risk and gathering more evidence

Gathering of sufficient and appropriate audit evidence is a systematic and iterative process as it involves:
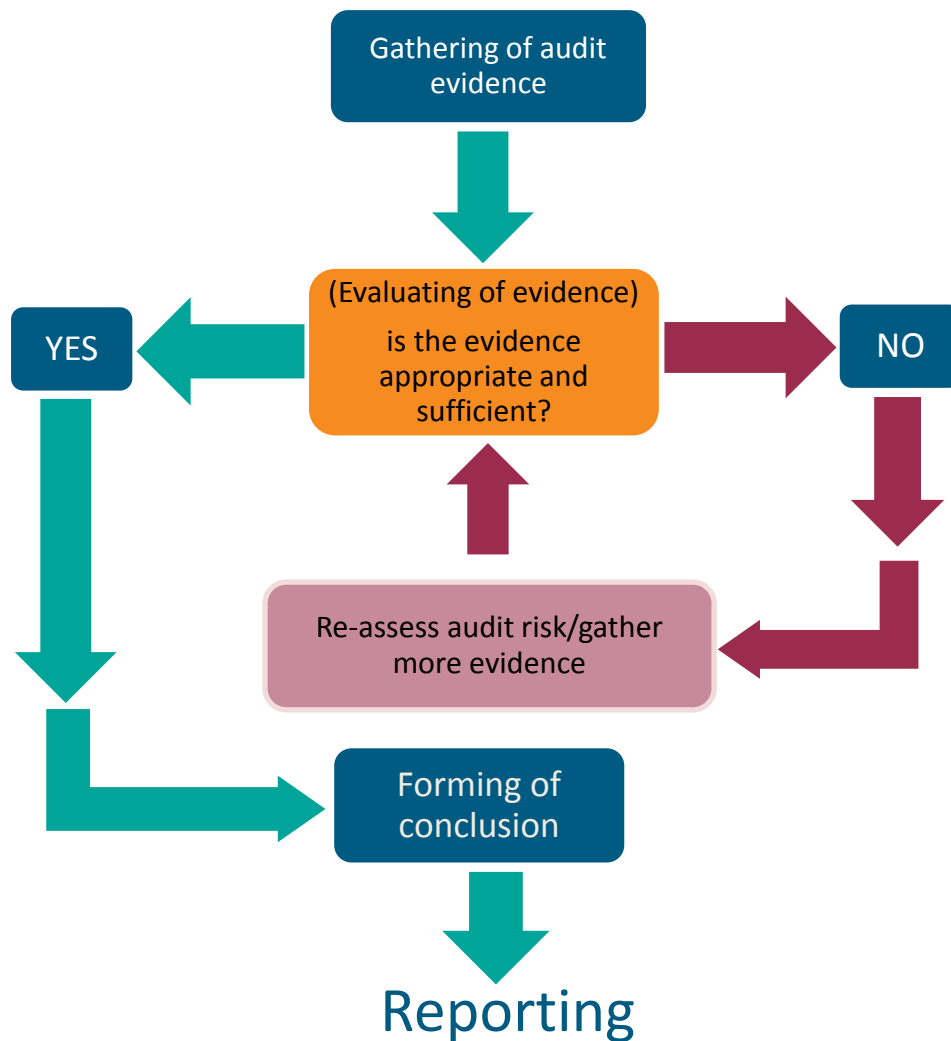
i. Gathering evidence by performing appropriate audit procedures;

ii. Evaluating the evidence obtained as to its sufficiency (quantity) and appropriateness (quality); and

iii. Re-assessing risk and gathering further evidence as necessary.

As you perform planned audit procedures, the audit evidence obtained may lead to modifying the nature, timing or extent of other planned audit procedures. Information may come to your attention that differs significantly from the information on which the risk assessments were based at the outset. For example, the extent of deviation that you detect by performing audit procedures may alter your judgement about the risk assessments and may indicate a material weakness in internal control. In such circumstances, you should re-evaluate the planned audit procedures based on revised considerations of assessed risks.

In some circumstances, you may not have obtained the sufficiency or appropriateness of evidence that you had expected to obtain through the planned procedures. In these circumstances, you need to consider that the evidence obtained from the procedures performed is not sufficient and appropriate to be able to form a conclusion on the subject matter information. You may then either extend the work performed, or perform other procedures that are necessary in the circumstances. Where neither of these is practicable in the circumstances, you will not be able to obtain sufficient appropriate evidence to be able to form a conclusion.

The diagram below illustrates the iterative process of evidence gathering, evaluating the evidence and whether it is sufficient and appropriate, re-assessing the risk and forming the conclusion, which eventually will be included in the compliance audit report.

```
                    ┌─────────────────────┐
                    │  Gathering of audit │
                    │      evidence       │
                    └─────────────────────┘
                              │
                              ▼
    ┌───────┐        ┌─────────────────────┐        ┌──────┐
    │  YES  │ ◄───── │ (Evaluating of      │ ─────► │  NO  │
    └───────┘        │  evidence)          │        └──────┘
        │            │ is the evidence     │            │
        │            │ appropriate and     │            │
        │            │ sufficient?         │            │
        │            └─────────────────────┘            │
        │                     ▲                         │
        │            ┌─────────────────────┐            │
        │            │ Re-assess audit     │ ◄──────────┘
        │            │ risk/gather more    │
        │            │ evidence            │
        │            └─────────────────────┘
        │            ┌─────────────────────┐
        └──────────► │  Forming of         │
                     │  conclusion         │
                     └─────────────────────┘
                              │
                              ▼
                         Reporting
```

Figure 8: The iterative process of evidence gathering and re-assessment of risk

5.3.4. Documentation and communication

When performing procedures, you should only gather evidence that is relevant for your procedures. The evidence must be retained in the audit file together with the working papers to support your findings and conclusions. All the evidence types have been mentioned already in the previous sections.

Communication at the evidence-gathering phase

While gathering evidence for the findings, your interaction with the audited entity becomes critical. As stressed above, the quality of the audit depends on the sufficiency and appropriateness of the audit evidence. Auditors maintaining good communication with the audited entity are better placed to review initial findings with the relevant officials in the audited entity, firm up their findings, and gather sufficient appropriate evidence in support.

For the audited entity as well, continuous interaction helps in identifying weak areas and taking steps toward rectification. Any significant difficulties encountered during the audit, as well as instances of material non-compliance, are promptly communicated to the appropriate level of management, or to those charged with governance. Though different SAIs may have different approaches to

communication with the audited entity, it may be desirable to communicate all identified instances of non-compliance to management so that the management can take appropriate actions.

Working papers to complete

W/P ref.	Working paper	Objectives of the working paper
PCP1	Performing compliance audit procedures	You may use this working paper for audit questions and for all the related audit procedures. If, for example, you have 3-5 audit questions, you are advised to use this template 3-5 times at this phase. For comprehensive procedures, we recommend that you use this working paper for only one procedure at a time. You must answer each audit question, assess findings against materiality, evaluate if the evidence gathered is sufficient and appropriate and conclude on whether the subject matter was in compliance with criteria or not.

5.4. Evaluating audit evidence and forming conclusions

At the end of the audit, you examine evidence for sufficiency and appropriateness with a view to forming a conclusion or opinion as to whether the subject matter is, or is not, in compliance with the established criteria. At this stage, you consider materiality for reporting purposes. The conclusion or opinion is presented in the form of a report to the intended user(s) and you may include the recommendations and responses from the entity as appropriate.

In the previous phase, we have discussed the audit evidence, the key concepts such as the sufficiency and appropriateness of evidence, and professional scepticism. More importantly, we have discussed in detail the various techniques that can be used in the process of gathering audit evidence. Once audit evidence has been gathered, you must evaluate the evidence for its sufficiency and appropriateness in order to form the audit conclusion.

In this chapter, we will discuss the process of evaluating audit evidence, assessing the materiality of the issues identified and the circumstances under which different audit conclusions are arrived at.

Follow these steps to evaluate evidence and form the conclusion:
1. Evaluate whether sufficient and appropriate evidence has been obtained;
2. Consider materiality for reporting purposes;
3. Form conclusions; and
4. Documentation and communication.

5.4.1. Step 1 – Evaluate whether sufficient and appropriate evidence has been obtained

You must evaluate the evidence obtained and determine whether it is sufficient and appropriate to reduce the audit risk to an acceptably low level. Evaluation of evidence includes exercising professional judgement and professional scepticism, which involves considering the relationship between the cost of obtaining evidence and the usefulness of the information obtained. You must apply professional judgement and exercise professional scepticism in evaluating the quantity and quality of evidence, and thus its sufficiency and appropriateness, to support the assurance report.

An audit is a cumulative and iterative process. As you perform the planned procedures, the evidence obtained may lead to changing the nature, timing or extent of other planned procedures. Information may come to your attention that differs significantly from that expected and upon which planned procedures were based. For example:

- ➢ The extent of non-compliance that you identified may alter your professional judgement about the reliability of particular sources of information;
- ➢ You may become aware of discrepancies in relevant information, or inconsistent or missing evidence; and
- ➢ If analytical procedures were performed towards the end of the engagement, the results of those procedures may indicate a previously unrecognised risk of non-compliance.

In such circumstances, you may need to re-evaluate the planned procedures.

Having gathered all audit evidence, you should take the necessary steps to form conclusion(s). When evaluating the audit evidence, review documentation to determine whether the subject matter has been sufficiently and appropriately examined. Based on the audit procedures performed and the audit evidence obtained, you should evaluate whether the assessments of the risks of non-compliance or compliance deviation remain appropriate or whether they need to be revised.

The evaluation process entails considering evidence that both supports and seems to contradict the audit report, conclusion or opinion on compliance or non-compliance. If audit evidence obtained from one source is inconsistent with that obtained from another, or if there are any doubts about the reliability of the information to be used as evidence, you should determine what modifications or additions to the audit procedures would resolve the matter and consider the implications, if any, for other aspects of the audit.

Have you obtained sufficient and appropriate evidence?

An engagement designed to provide a high level of assurance, both positive observations or conclusions and "reservations" (negative observations or conclusions, or modifications of opinion), must be able to withstand critical examination. In determining whether you have gathered evidence of sufficient quantity and appropriate quality, you need to be certain that, in your judgement, there is a low risk of making erroneous observations, faulty conclusions, or inappropriate recommendations.

Example of evaluating evidence and exercising professional judgement and scepticism

In a compliance audit of procurement, where one of the procedures was to check if specification of acquired goods for the construction of the building was the same as provided in the contract, the auditor found that the specifications differed. The responsible officers from the audited entity explained that the specifications were changed in accordance with new requirements for construction. By exercising professional scepticism, the auditor did not stop at this explanation and required and checked extra documents. By exercising professional judgement, the auditor assesses if these documents which show the improved changes were necessary, if the changes were made in compliance with the contract, if they complied with the procurement law and if the auditee did not incur any material loss due to this decision.

In considering whether you have obtained sufficient appropriate audit evidence, you should consider the level of assurance being provided and the assessment of significance and risk. For example, audits

that provide a high level of assurance generally have a higher threshold for what is sufficient appropriate evidence. Similarly, a high-risk or a significant/material audit component will typically have a higher threshold for what is sufficient and appropriate evidence than a lower-risk audit component.

The manager/team leader needs to ensure that the initial or revised risk assessment applied in the engagement remains valid. This is necessary since the risk assessment helps direct audit strategy, planned audit procedures, and the level and extent of evidence gathered.

The audit teams must consider all relevant evidence, regardless of whether it appears to corroborate or contradict audit criteria. Teams should approach the analysis of audit evidence not only with an objective frame of mind, but also with a level of scepticism.

In making the judgement of whether sufficient appropriate audit evidence has been obtained, the audit team considers the following questions:

➢ Has the team obtained audit evidence regarding all relevant criteria?
➢ Has the team, as part of executing the audit procedures, identified instances where further evidence was required? If yes, has it obtained, documented, and appropriately linked this further work?
➢ Has the team considered the impact of identified issues and/or misstatements on the nature, timing and extent of further procedures?
➢ Has the team identified and appropriately addressed any significant matters and, where appropriate, has it consulted and documented the results of these?
➢ Has the team addressed all required audit procedures?

Determine whether more evidence is required

When the evidence does not point clearly to whether a criterion has been met – for example, if some positive and some negative evidence exists – the team may need to investigate further to gain the required level of assurance.

This may be required, for example, to:
➢ Determine whether an issue is an isolated instance or represents a systemic problem;
➢ Determine who is affected by the issue (e.g. other units in the entity, central agencies, or third parties);
➢ Determine whether the issue can be addressed by the audited entity or whether it results from circumstances beyond its control; and
➢ Determine whether the entity's management is aware of the issue and whether it has taken corrective action.

If additional evidence needs to be gathered, this may involve additional interviews or review of additional files.

Confirming the absence of evidence

If evidence is not found in an area where the auditor expects to find it, this could be a finding in itself. The auditor first needs to confirm that the evidence should exist. For example, if project X is a capital project over a certain size, government policy requires that a business case be prepared. Therefore, a

documented business case should exist. If the auditor requests a copy of the document and the entity cannot provide it, this should be stated in writing.

Fact verification

For compliance audit, as the audit team gathers and analyses audit evidence during the examination phase, it meets with entity officials to communicate emerging findings and seek confirmation and validation of facts to ensure the accuracy and completeness of the evidence, and it is important that the team does this before providing the draft report to the entity.

5.4.2. Step 2 – Consider materiality for reporting purpose

While drawing a conclusion or opinion, you evaluate evidence in relation to identified materiality to identify potential instances of material non-compliance. Determining the significance of findings is based on the concept of materiality. What represents a material compliance deviation is a matter of professional judgement and includes considerations of context as well as quantitative and qualitative aspects of the transactions or issues concerned. The list below identifies some of the factors that you must consider in applying professional judgement to determine whether an instance of non-compliance is material.

➢ Importance of amounts involved (monetary amounts or other quantitative measures such as number of citizens, entities or organisations involved, pollutant emission levels, time delays in relation to deadlines, etc.);
➢ Circumstances;
➢ Visibility and sensitivity of the criteria or programme in question (for example, is it the subject of significant public interest, does it affect vulnerable citizens, etc.);
➢ Needs and expectations of the legislature, the public or other users of the audit report;
➢ Nature of the relevant authorities; and
➢ Extent or monetary value of the non-compliance.

In a compliance audit, the entity may have complied with nine provisions of the relevant law or regulation, but did not comply with one provision. Professional judgement is needed to conclude whether the entity complied with the relevant law or regulation. For example, you may consider the significance of the provision with which the entity did not comply, as well as the relationship of that provision with the remaining provisions of the relevant law or regulation.

While evaluating audit evidence, you consider whether material non-compliance is ***pervasive*** or not. If you are unable to obtain sufficient and appropriate audit evidence due to an ***uncertainty or scope limitation,*** you evaluate whether it is both material and pervasive.

Example of findings evaluated against materiality and conclusion				
Audit question	**Criteria**	**Audit findings**	**Evaluation against materiality**	**Conclusion**
Has the ministry included the project in the	Section 3 para. 2 of the Procurement	It was discovered that the road	The finding is qualitatively material as the	Road construction projects above USD 3 million must be

annual procurement plan?	Act requires that an entity must include projects worth USD 3 million and above in the procurement plan.	construction project was not included, resulting in non-compliance as stipulated in Sec. 3 para. 2 of the Procurement Act, and the amount of this project exceeded the threshold by far.	project was not part of the budget plan and resulted in the construction of roads that deviated from national plans, and also resulted in enormous unauthorised expenditure.	included in the procurement plan according to Sec. 3 para. 2 of the Procurement Act. The Ministry of Transport did not comply with this requirement as the audit finding shows that the project of Road Construction was not included in the plan.

5.4.3. Step 3 – Form conclusions

In evaluating the evidence, you can conclude that the audit evidence is conflicting. Some evidence supports the subject matter information, and other evidence appears to contradict it. You need to weigh the extent and credibility of conflicting evidence to determine the true situation. This is where you can use the hierarchy of evidence reliability, so that, for example, written external evidence is more credible than an informal management representation to the contrary. After evaluating whether the evidence is sufficient and appropriate given the assurance level of the audit, you should consider how best to conclude in the light of the evidence. When you are forming conclusions, you must also aim at answering the audit question in the working papers PCP1 and ECA1 and evaluate if the objective of the audit has been met. You should also conclude on the related criteria, whether or not the subject matter is in compliance with the criteria.

You need to properly document all significant activities that you have carried out while gathering and evaluating evidence. You need to revise the audit strategy and audit plan considering the results of the audit work in this phase. Frequently, additional information comes to your attention that requires you to re-examine a subject matter, criteria, scope, controls, risk assessment, and materiality consideration as explained above. You may, during compliance testing, come across instances that indicate fraud risk within the audited entity. How to address these issues is explained in chapter 5.3.4.

During this phase, you also need to engage with management to seek clarification on some issues that have bearing on how you are looking at the subject matter, criteria, scope, audit risk and materiality. This interaction helps you to make proper adjustments in the audit strategy and audit plan. Further, it also helps management to identify control weaknesses and other systemic weakness that you can begin to tackle promptly.

The conclusions you form at this stage are related to the audit questions, and criteria where you assess the findings against criteria and conclude on instances of non-compliance. Finally, you need to conclude on the overall subject matter and if it is compliant or non-compliant with the criteria. In case the conclusion is non-compliance, you need to describe the basis for the conclusion or opinion

(whether unmodified or modified/qualified) and this should be included in the audit report with the conclusion or opinion.

Types of audit conclusions and opinions

The type of compliance audit conclusions largely depends on the material nature of non-compliance issues identified during the audit and the effect those non-compliant issues have on the subject matter. Depending on the type of audit engagement, the wording of the conclusion may differ. The wording and content of the compliance audit conclusion and opinion is dealt with in chapter 5.5 on reporting.

5.4.4.   Step 4 – Documentation and communication

Auditors exercise professional judgement and scepticism in determining whether audit evidence is sufficient and appropriate throughout the audit. Factors that the auditors have to consider in the audit to evaluate evidence and form conclusions are discussed in this chapter. You should always prepare relevant audit documentation for the particular audit before the audit report is issued. You should also exercise professional judgement to determine the form and content of the communication. Written communication is preferred as it facilitates proper documentation of the interaction.

Individual procedures form the basis for the final overall conclusion on the subject matter and you document this work by using working paper ECA1, which is for evaluating compliance audit evidence, and concluding on the subject matter. In the process of evaluating evidence you are also supposed to evaluate the procedures performed and base these on each of the working papers (PCP1).

Although it is not a requirement in the standard, at this final stage of the audit you should also require a management representation letter from the audited entity, so that they can verify that relevant controls related to the subject matter are in place to avoid non-compliance and if such instances occur, what measures are taken. You should ask management to verify specifically issues that you have identified during the audit and this management letter will also be part of the audit evidence you have gathered and audit documentation.

In the next chapter on reporting a compliance audit, we will show how the results of gathering and evaluating evidence are reflected in compliance audit reports.

Working papers to complete

W/P ref.	Working paper	Objectives of the working paper
ECA1	Evaluating compliance audit evidence and concluding on the subject matter	In this working paper, you are required to form an overall conclusion for the entire subject matter, taking into consideration findings, risks and materiality. You need to assess that all the audit questions have been answered, and that there is a conclusion for each criterion. The conclusion should reflect whether or not the entity has complied with the applicable criteria for the particular subject matter. There is a section for *Summary of findings* where you summarise all the findings and then you assess the findings in terms of materiality. Finally, you must

		conclude on whether the determined level of assurance for this subject matter is supported by sufficient and appropriate evidence.
ECA2	Code of ethics compliance	This working paper is a follow-up on the code of ethics to ensure that the team is still independent after conducting the compliance audit.
ECA3	Management representation letter	You should require a management representation letter from the audited entity/responsible party stating that they have complied with xyz criteria to their best knowledge, and that the internal controls are in place to avoid instances of non-compliance, and if instances occur, what measures are taken. This together with conclusion on other procedures will form a basis for your final assessment of whether the subject matter is compliant or non-compliant with the applicable criteria.

5.5. Reporting

Reporting is the last, but not the least, essential part of any audit, as through this process the results of the audit are presented to the intended users on the responsible party's compliance with the stated criteria. Compliance audits involve reporting the deviations from the applicable criteria and violations of the applicable rules, regulations etc., so that corrective actions may be taken, and those responsible for such deviations or violations could be held accountable for their actions.

In the reporting phase, you should follow these steps:
1.   Prepare the compliance audit report;
2.   Include recommendations and responses from the entity as appropriate and finalise the report; and
3.   Decide follow-up as appropriate, including a follow-up plan.

5.5.1.   Step 1 – Prepare the compliance audit report

To ensure the objectivity of the audit findings and conclusions of the compliance audit report, confirmation of facts and figures by the entity and incorporation of responses of the responsible party is crucial. You must therefore ensure that facts and figures are accepted by the entity and pursue the responses from the entity.

The standard states that the auditor shall prepare an audit report based on the principles of completeness, objectivity, timeliness, accuracy and contradiction.[60]

   ➢   The principle of completeness requires the auditor to consider all relevant audit evidence before issuing a report;

   ➢   The principle of objectivity requires the auditor to apply professional judgement and scepticism to ensure that the report is factually correct, and that findings and conclusions are presented in a relevant, fair and balanced manner;

   ➢   The principle of timeliness implies preparing the report in due time to be relevant for the intended user(s); and

---

[60] ISSAI 4000/202 and 205-209

> ➤ The principle of contradiction implies incorporating responses from the responsible entity as appropriate and answering and assessing the responses.

Decide on report structure

The audit report must include the following elements (although not necessarily in this order):[61]

In the table below both direct reporting and attestation engagement reporting requirements are listed, but you must decide which one to apply depending on the engagement type.

	Direct reporting	Attestation engagement
a)	Title	Title
b)	Identification of the auditing standards	*Addressee
c)	Executive summary	Description of the subject matter information and when appropriate the underlying subject matter
d)	Description of the subject matter and the scope (extent and limits of the audit)	Extent and limits of the audit including the time period covered
e)	Audit criteria	Responsibilities of the responsible party and the auditor
f)	Explanation and reasoning for the methods used	Audit criteria
g)	Findings	Identification of the auditing standards and level of assurance
h)	Conclusion(s) based on answers to specific audit questions (or opinion)	A summary of the work performed, and methods used
i)	Replies from the audited entity (as appropriate)	Opinion/conclusion
j)	Recommendations (as appropriate)**	Replies from the audited entity (as appropriate)
k)	*Report date	Report date
l)	*Signature	Signature

* We recommend that the compliance audit report for direct reporting should also include the addressee and be dated and signed, even if this is not listed in the standard, ref. ISSAI 4000/210.

** Recommendations are normally only included in direct reporting engagements.

The content of the report

The report should have an introduction where the background to the audit is mentioned. In the next part the subject matter, audit objective and scope must be described so that the intended user is able to follow through the audit report. This information already exists in the audit strategy working paper. You may use the same information in the audit report, but it is important to bear the reader in mind, and formulate accordingly so that it is understood by readers who do not have prior knowledge of the sector, the entity and the subject matter.

---

[61] ISSAI 4000/210 and 218

➢ Executive summary

The report must contain an executive summary of the work performed and methods used as it helps the intended user(s) to understand the conclusion in the report. It is important that the summary be written in an objective way that allows intended users to understand the work done as the basis for the auditor's conclusion. In most cases, this will not involve detailing the entire work plan, but on the other hand, it is important for it not to be so summarised as to be ambiguous, nor written in a way that is overstated or embellished. The reason for having an executive summary is that many readers will only be reading the executive summary. This may also be the case for the main recipients in the Public Accounts Committees, Parliaments and top management of the audited entity. The executive summary should enable the reader to understand what questions were raised, how the audit was conducted, the main findings, conclusions and recommendations.

It is crucial that the information is given in a summary form that only contains the most important information of the report. The executive summary will typically be 1-2 pages, but it depends of course on how broad the audit is. You should only start writing the executive summary after the other chapters of the report and the recommendations have reached a certain level of quality. For many teams, the first review by the operational manager is necessary to establish a proper structure and clarity on what is presented in the report. Audit teams who start writing the executive summary before the rest of the report has reached a certain level of quality, will typically have to make substantial adjustments to the executive summary, which is not efficient. There is also a risk that important final adjustments to the findings chapter(s), the conclusions and recommendations are not properly reflected in the final version of the executive summary.

➢ Audit criteria and findings

The audit criteria section should state the laws, legislation, rules and regulations that were used in the audit, and the criteria should be explicitly identified in the audit report.

The findings section comprises the auditor's comparison of the obtained evidence against the stated criteria and how this comparison has led to the audit findings.

➢ Conclusion or opinion[62]

The auditor shall communicate the conclusion in an audit report. The conclusion can be expressed either as an opinion, conclusion, and answer to specific audit questions or recommendations.

In a reasonable assurance engagement, the auditor gathers sufficient and appropriate audit evidence to conclude whether the subject matter complies in all material respects with identified suitable criteria, and provides a report in the form of a positive assurance.

In a limited assurance engagement, the auditor gathers sufficient and appropriate evidence to address the engagement objective; however, the procedures are limited compared to what is necessary in a reasonable assurance engagement. The auditor then concludes, if appropriate, that nothing has come

---

[62] ISSAI 4000/191 and 200-201

to the auditor's attention to cause the auditor to believe that the subject matter is not in compliance with the applicable criteria.

i) *Conclusion*

In a direct reporting engagement, the auditor can provide assurance:[63]

(a) by making a clear statement of the level of assurance, through conclusion(s) which explicitly convey the level of assurance; or

(b) by explaining how findings, criteria and conclusions were developed in a balanced and reasoned manner and why the combinations of findings and criteria result in a certain overall conclusion or recommendation.

Conclusion with reasonable assurance as in alternative a) above may include the following information:
The mandate of the SAI on compliance audit, for example, that the SAI has discretion to conduct compliance audit according to the mandate's provision xx. The SAI has conducted a compliance audit of the [entity's name], on the xyz subject matter and evaluated compliance with [applied criteria]. The evidence obtained is sufficient and appropriate to provide a basis for our conclusion that the subject matter is compliant, in all material respects, with the applicable criteria.

If the subject matter is not compliant with the applicable criteria, you may also include the basis for the conclusion or refer to the paragraph *Basis for conclusion* in the report.

In a direct reporting engagement, it should generally be sufficient to provide a conclusion that the subject matter is or is not in compliance with the applicable criteria, i.e. unmodified or modified. However, if the SAI does not have the discretion to select a certain subject matter because it is given in the SAI's mandate, and the SAI is required to report on non-compliance instances, the SAI may also consider including a scope limitation or disclaimer in the conclusion.

Disclaimer for direct reporting may be expressed as follows:
"Because of the significance of the matter described in the *Basis for disclaimer of conclusion* section of our report, we have not been able to obtain sufficient appropriate evidence to form a conclusion on the [responsible party's] subject matter. Accordingly, we do not express a conclusion on that subject matter."

An unmodified/modified conclusion for limited assurance may be expressed as follows:
a) "Based on the procedures performed, nothing has come to our attention to cause us to believe that the subject matter is not, in all material respects, in compliance with the applicable criteria."

b) A modified/qualified conclusion for limited assurance engagements may be expressed as follows:
"Based on the procedures performed and the evidence obtained, except for the effect of the matter described in the *Basis for qualified conclusion* section of our report, nothing has come to our attention that causes us to believe that the subject matter, in all material respects, is not in compliance with applicable criteria."

---

[63] ISSAI 4000/199

ii)   Opinion[64]

An opinion is a clear written statement of the auditor expressed in a standardised format, either unmodified or modified. It is stated in the audit report whether instances of non-compliance are pervasive. *An opinion is normally used in an attestation engagement*.

Where no material instances of non-compliance have been identified, the opinion is unmodified. An example of the form of an unmodified opinion, for a reasonable assurance engagement (where appropriate wording is inserted in the brackets as applicable) may be as follows: "In our opinion [the audited entity's subject matter] is in compliance, in all material respects, with [the applied criteria]."

The auditor modifies the opinion in cases of:
a) Material instances of non-compliance. Depending on the extent of the non-compliance, this may result in: i) a qualified opinion or ii) an adverse opinion.

b) Scope limitation. Depending on the extent of the limitation, this may result in: iii) a qualified opinion or iv) a disclaimer.

In a limited assurance engagement, an example of an **unmodified opinion** may be: "Based on the work performed described in this report, nothing has come to our attention that causes us to believe that the subject matter is not in compliance, in all material respects, with the [applied criteria]".

A modified opinion can state that: "Based on the work performed described in this report, except for [describe exception], nothing has come to our attention that causes us to believe that the subject matter is not in compliance, in all material respects, with the [applied criteria]".
The wording of the opinion should reflect the mandate of the SAI. The auditor may therefore use terms such as "is legal and regular", "is regular" or "has been applied to the purposes intended by the Parliament."

In a reasonable assurance engagement with an unmodified opinion, the auditor states that the audit evidence obtained is sufficient and appropriate to provide a basis for the opinion.

> ➤ *Where the SAI has discretion to select subject matter we recommend that the auditor/SAI provide reasonable assurance for direct reporting engagements and provide a conclusion.*
>
> ➤ *When the SAI is conducting a compliance audit and has selected attestation engagement, we recommend that an opinion be provided.*

5.5.2.   Step 2 – Include recommendations and responses from entity as appropriate

The principle of contradiction implies incorporating responses from the responsible entity as appropriate and answering and assessing the responses. Incorporating responses from the audited

---

[64] ISSAI 4000/192-197

entity provides an indication of agreement to act on the matter reported. Discussing the draft report findings with the audited entity helps ensure that these are complete, accurate and fairly presented.

Where significant compliance deviations are reported, recommendations are provided in cases where there is potential for significant improvement. It may be helpful to user(s) that the auditor highlights ongoing corrective actions. While constructive and practical recommendations assist in promoting sound public sector management, the auditor is careful not to provide such detailed recommendations as to be taking on the role of management and thereby risk impairing his or her own objectivity. Recommendations might be issued separately from the report as they are usually written mainly for the management of the audited entity. In these instances, the recommendations might be issued separately in a letter to management.

In some SAIs the results from the compliance audit are reported together with the audit on the financial statement. The SAI then makes sure that the requirements are covered either through separate compliance audit elements or as part of the financial audit elements. Normally recommendations are not included in the attestation engagement reports. Recommendations might be issued separately in a letter to the management.[65]

5.5.3.   Documentation and communication

The content in the final compliance audit report must be supported by the documentation in the previous sections, and should cover all the phases from initial considerations to evaluating evidence and overall conclusion on the subject matter. It should be possible for an experienced auditor and/or reviewer to follow the common thread throughout the compliance audit that has been conducted. It cannot be emphasised enough that the conclusion should be aligned with the actual audit that has been carried out and not differ from the findings.

Communication

It is important that the entity get an opportunity to read the draft report and respond to it. You should send the report to the entity and set a deadline to obtain management's view. This will depend on the SAI policy. In the absence of a SAI policy, we recommend a response period of 2-3 weeks. If you do not require this, you may run the risk that management might not prioritise responding to the audit report, perhaps due to other tasks they deem more important. You must also ensure that the report is sent to the correct level at the audited entity to ascertain that they have the mandate to respond to the SAI on behalf of the audited entity.

Some SAIs can, according to their audit mandate, order the audited entity to correct identified instances of non-compliance. In doing so, public sector auditors determine whether their independence and objectivity will be impaired, and take appropriate action to avoid such impairment.

To document the reporting phase, working papers listed in the table below should be completed.

---

[65] ISSAI 4000/219-220

Working papers to complete

W/P ref.	Working paper	Objectives of the working paper
ARC1	Compliance audit report a) Direct reporting b) Attestation	We have developed a template with focus on a) direct reporting as we assume this will be the main engagement type that will be relevant for most SAIs for stand-alone compliance audits. b) We have also developed a template where we provide additional guidance on attestation engagement. The audit report must follow the structure that is provided in the standard and as a minimum, but there are various options that the SAI may choose. The SAIs can customise the templates according to their reporting practice and mandate requirements.
ARC2	Management letter (as appropriate)	Issues or findings that are relevant for management to be aware of, but are not relevant for the auditor's report may be mentioned in the management letter. Issues or findings that are very sensitive and that cannot be mentioned in the audit report should also be included in the management letter so that proper measures can be taken. It is important to remember that a management letter is not a replacement of the compliance audit report and that these two documents have a different purpose and structure.
ARC3	Exit meeting minutes	You shall conduct an exit meeting with the entity and communicate as a minimum the findings and conclusion in the audit report.
ARC4	Quality control questionnaire (Reporting phase)	The audit report and the working papers must be reviewed. The report must be approved by a level-3 reviewer before the draft report is sent to the entity for verification of facts, and to fulfil the requirements of the principle of contradiction.

The SAI's reporting to the Parliament/intended user, etc.

Most of the SAIs have specific mandated requirements on how to report to the Parliament, Public Accounts Committee or President. The SAIs may either table the compliance audit report to Parliament if the mandate provides for that, or include the findings and conclusion from the compliance audit report in the annual report in case that is the reporting requirement. In any case, the SAIs need to identify what kind of reporting practice is most appropriate according to their mandate and establish the reporting of compliance audits accordingly.

5.5.4.   Step 3 – Decide follow-up as appropriate, including a follow-up plan

The auditor shall decide follow-up on opinions/conclusions/recommendations of instances of non-compliance in the audit report when appropriate.[66]

An important role for a SAI in monitoring the action taken by the responsible party is to follow up on the matters raised in an audit report. A plan for a follow-up is written after the report has been published, containing questions on whether the audited entity has adequately addressed the matters

---

raised. Insufficient or unsatisfactory action by the audited entity may call for a further report by the SAI.

A follow-up process facilitates the effective implementation of corrective action and provides useful feedback to the audited entity, the user(s) of the audit report, the general public and the auditor for future audit planning.

The need to follow up previously reported instances of non-compliance will vary with:
- the nature of the subject matter; and
- the non-compliance identified and the particular circumstances of the audit.

Other follow-up processes may include reports, internal reviews and evaluations prepared by the audited entity or others and a follow-up audit.

Follow-up processes may be set out in the mandate of the SAI. Such processes may be constructive for the audited entity.

When following up on an audit report, you should concentrate on findings related to instances of non-compliance and, where appropriate, recommendations that are still relevant at the time of the follow-up, and adopt an unbiased and independent approach.

Follow-up may include the following activities:
- Determine if the nature of the subject matter and instances of non-compliance are of such nature that a follow-up is necessary;
- If there is a need for follow-up, the SAI should have a follow-up plan that has been written after the report was published. The follow-up plan should contain questions on whether the audited entity has adequately addressed the matters raised in the compliance audit report;
- Arrange a meeting with the audited entity after a certain time period after the compliance audit, to find out what actions have been taken to improve compliance with the laws or regulations (criteria) that were violated, and where appropriate, check whether recommendations have been implemented;
- Request the audited entity to inform the SAI in writing on what actions the entity has taken to address the matters raised in the report; and
- Insufficient or unsatisfactory action by the audited entity may call for a further report by the SAI.

Appendix 1: Guidance on CA sampling

Audit sampling is defined as the application of audit procedures to less than 100 per cent of items within a population of audit relevance. A sample may be quantitative or qualitative depending on the audit scope, and the need for information to illuminate the subject matter from several angles.

Qualitative sampling
Qualitative sampling is a selective procedure conducted as a deliberate and systematic process to identify the factors of variation in the subject matter. The auditor might sample on the basis of

characteristics of individuals, groups, activities, processes or the audited entity as a whole. Qualitative sampling always requires careful assessment and sufficient knowledge of the subject matter.

The auditor can get a lot of assurance from performing qualitative sampling; for example, filtering data based on different features or dividing data into strata and performing procedures on the different sub-populations. This could, for example, result in many small sub-populations that collectively give sufficient evidence to conclude with reasonable assurance. A challenge with qualitative sampling is that the auditor has to use judgement to determine that the sample meets the required level of assurance. This requires strong qualitative arguments, because you do not have the benefit of statistical inference to help determine that sufficient evidence has been gathered. If using the qualitative sampling, the auditor should justify why this gives sufficient evidence in a robust manner.

Example 1

In this simplified example we have a data set with five different cost categories: ice cream, beer, chips, furniture and computers. By filtering the data, we can do some analyses on them, and use that as a basis for sampling.

One way of filtering the data is to use the filter function and selecting the data we want. However, for the purpose of analysis it may be useful to use formulae.

We can apply formulae =COUNT.IF (COUNTIF) and =SUM.IF (SUMIFS) like this:

No. of records

ice cream	=COUNT.IF(B2:B1133;"ice cream")
beer	=COUNT.IF(B2:B1133;"beer")
chips	=COUNT.IF(B2:B1133;"chips ")
furniture	=COUNT.IF(B2:B1133;"furniture")
computers	=COUNT.IF(B2:B1133;"computers")

Totals

Ice cream	=SUMIFS(Demonstration!C2:C1133;Demonstration!B2:B1133;"ice cream")
Beer	=SUMIFS(Demonstration!C2:C1133;Demonstration!B2:B1133;"beer")
Chips	=H13/10

Furniture	=SUMIFS(Demonstration!C2:C1133;Demonstration!B2:B1133;"furniture")
Computer	=SUMIFS(Demonstration!C2:C1133;Demonstration!B2:B1133;"computers")
	=SUMMER(H10:H14)

We then get the results:

No. of records

ice cream	227
beer	227
chips	226
furniture	226
computers	226

Totals

Ice cream	227,00	0 %
Beer	2 270,00	0 %
Chips	22 600,00	1 %
Furniture	226 000,00	9 %
Computers	2 260 000,00	90 %
	2 511 097,00	

Here we see an equal number of records for each cost category. However, when we examine the proportion that each purchase represents of the total, the picture is very different. In this case a qualitative sample may be to select only computers. In a procurement audit, it may be useful to select only purchases that are above the threshold for tendering. For example, if the threshold for tendering is 50 000, you would only select computers and furniture.

Of course, the challenge with qualitative sampling is that it does not allow you to make inferences about the parts of the population you are not testing, so if you use this method, you have to accept that there is residual risk for the remaining population. If you selected computers and furniture for testing, the remaining population would make up 1% of all purchases, so that residual risk may be acceptable.

Quantitative sampling
Quantitative sampling is used when the auditor seeks to draw conclusions about the whole population by testing a sample of items selected from it. In quantitative sampling, the sample risk must be reduced to an acceptably low level. However, the technical approach to quantitative sampling may require statistical techniques.

Once an audit procedure has been selected, it is possible to vary the sample size from one to all the items in the population being tested. The sample size usually depends on the following factors:
a) effectiveness of internal control b) risk involved in the subject matter and
c) materiality of the subject matter.

Attribute sampling

We recommend using attribute sampling in most instances when carrying out quantitative sampling in compliance audit. This is also the technique that the Institute of Internal Auditors recommends for examining compliance (see hyperlink below).

Attribute sampling is designed for testing records that exhibit a certain attribute that is binary in nature. Typically, in financial audit, attribute sampling is used for tests of controls. The binary result of such tests is: 1. The control is functioning. 2. The control is not functioning.

We can apply similar logic in compliance auditing where compliance can be considered to be an attribute:

1. The documentation examined is not in compliance.
2. The documentation examined is in compliance.

However, it is a little trickier to quantify what an acceptable level of compliance is. If 5% of records examined are not in compliance, is that an acceptable rate? In compliance auditing a lot can depend on the nature of the finding, which means that qualitative factors may weigh more heavily. For example, if the government has selected a supplier of medication, where it turns out that the supplier cannot deliver the medication because it is not qualified to do so, it would have disastrous consequences for the citizens who need that medication. However, if there was an error in the procurement process for furniture at the office, it would be a problem for the entity, but not a disaster for the stakeholders in an audit.

This is an area where the auditor must exercise professional judgement, but it is difficult to prescribe solutions or rules of thumb in a manual. Each case must be assessed individually on its merits.

Attribute sampling is a quantitative technique that uses statistical tables to determine sample sizes based on a confidence interval, an expected error rate and a tolerable error rate.

We can relate these factors to the sample size in the following way:

Sample size determinants	Impact on sample size
Confidence interval is a metric that reflects how confident you are that the sample will reflect the population.	The higher the confidence level, the larger the sample.
Tolerable error rate: Materiality in sampling is often referred to as tolerable error rate. This percentage reflects how much deviation you will accept before it impacts your conclusion, or you modify your conclusion/opinion.	The higher the tolerable error rate, the smaller the sample.
Expected error rate: If you have determined that there is a risk of misstatement, the higher that risk, the higher the error rate you expect.	The higher the expected error rate, the larger the sample.

Determining these three parameters is challenging for auditors. It requires judgement and thinking about what is sufficient to provide the level of assurance that the auditor is aiming for. The following will give some guidance:

Confidence interval: Typically, a confidence level of 95% is acceptable to achieve a representative sample that allows for conclusion with reasonable assurance. It can be adjusted up to 99%, if the auditor requires minimal residual risk. It can also be adjusted down, typically to 90%, if the auditor determines that he or she can accept some more residual risk. For example, if the auditor is only providing limited assurance, a lower confidence level can be acceptable.

Tolerable error rate (TE): This is a reflection of materiality. In financial audit, we set this equal to, or below our defined performance materiality. In compliance audit, the auditor needs to determine a tolerable error rate based on his or own determination of materiality related to the subject matter. In other words, how large a proportion of non-compliance findings the auditor can find before he or she determines that there is material non-compliance.

Expected error rate (EER): The expected error rate reflects the auditor's judgement about the likelihood of errors, which is a component of risk. This parameter has one important rule: it has to be lower than the tolerable error rate. The intuition behind this is that if you expect the error rate to be higher than materiality, you are assuming a very high risk, which would imply very large samples. A simplified version of the mathematics also demonstrates this logic: (Sample size = Population adjusted for confidence level/Tolerable error-Expected error). The closer TE-EER gets to zero, the larger the sample size will be, but if EER>TE, you get a negative sample, which doesn't make sense. The difference between EER and TE is often referred to as the level of precision. The smaller the difference, the more precise the test, because the sample size will be larger.

A useful rule of thumb for setting EER is to use the error rate observed in a previous audit. However, compliance audits are often discretionary, and not performed repeatedly, meaning that the auditor may be unable to observe previous error rates. It may therefore be advisable to start with a relatively high error rate (one close to tolerable) and adjust it lower once an observable error rate has been identified.

Performing tests of compliance on a sample
To perform an audit procedure on a sample the auditor must:
- Define a test objective;
- Define the population to be tested;
- Determine the sampling unit and control items to be tested;
- Determine the sample size and draw the sample;
- Evaluate the sample against relevant criteria;
- Project the sampled error rate on the population; and
- Conclude on the results of the procedure and determine if errors are material.

The test objective is a precise formulation of what you aim to conclude by performing the test. The population is the total of records that you are going to conclude on after performing the test. The sampling unit is the item you are selecting to test. The control items are the other documentation you will use to confirm the sampling unit; from which you can confirm compliance with criteria.

There is an important connection between the test objective, the population and the sampling unit and control items, as it is important to be sure that the population being tested will help meet the test

objective. For example, if you are testing for accuracy, the population you draw from will be the final place the information is recorded, and the control items will be documentation that was fed into this final report. If you are testing for completeness, you will sample from the source documentation and find control items in the final place the information is reported.

Example 2 – Quantitative sampling

To determine sample size, in attribute sampling, we use a computer-assisted auditing tool such as IDEA or ACL or a statistical table, such as the one found here: https://iaonline.theiia.org/attribute-sampling-plans

We will use SAI X as an example, which as we have seen purchases ice cream, beer, chips, furniture and computers.

1. The test objective here will be to inspect the documentation for any procurement that has been carried out by SAI X and determine if the appropriate procurement procedure has been followed.
2. The population to be tested has been isolated as the complete list of procurements carried out in 201x (see attached Excel spreadsheet).
3. The sampling unit will be the list of transactions in the Excel worksheet. The control items will be the procurement documentation related to the transactions we draw from the population.
4. The sample size will be determined IDEA, ACL or the table found here:
   https://iaonline.theiia.org/attribute-sampling-plans
   For the purposes of this exercise we will assume the following parameters:
   Confidence interval: 95% (if using the iaonline-table, this is the only option as it is generated with a 95% confidence interval).
   Tolerable error rate: 5%
   Expected error rate: 2%
   That gives us a sample size of 181.
   (If the tolerable error rate is 6 % and EER 1 %, the sample size will be 78)

   Please note that this is the result from the table. IDEA/ACL may give slightly different results, but should be in the same area.

   To draw the sample in Excel you need to assign a random number to each row. This is done by using the formula =RAND(). Write the formula in the first available column next to the dataset like this:

Then copy the formula for the whole dataset by double-clicking on the little square at the bottom right side of the cell. Hold the cursor over it until it turns into a **+**-sign and double-click.

You have now assigned each record with a random number. You will notice that the numbers change every time you change something in Excel. To avoid this, copy the whole column in the next column, pasting only values. You can then replace the first column you created with your new column of fixed random numbers.

Now you are ready to draw your sample. In the column next to your random numbers, make a new column with the numbers 1-181:

This is going to identify your sample.

Finally, in order to draw your sample, select all the columns, except the last one you created (with the numbers 1-181). Click on the Sort button.
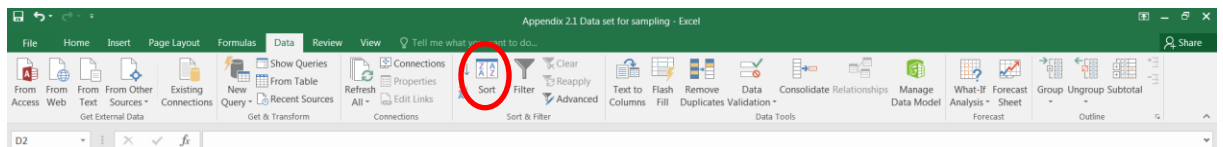
Sort the data in the random number-column, it doesn't matter if you choose ascending or descending. The records will now have been placed in a random order; the first 181, which you have already numbered, are your sample.

You are now able to perform the remaining steps.

Non-statistical techniques

The SAI can apply non-statistical quantitative techniques, such as a rule of thumb. An example is calculating the sample size based on the account balance (A), with a reliance factor for risk adjustment (RF) and the tolerable misstatement (TM): Sample size = (A/TE*RF). Such techniques can be efficient if they save the auditor time and they are commonly used in financial audit. But, to provide sufficient assurance, they need to be tested to give similar sized samples as the tables for the statistical technique.

A technique like this is also easier to apply to quantitative data: the example above requires an account balance. In many potential topics in compliance audit, there may not be an account balance available, or it may not make sense to use the account balance as the population from which you select a sample.

In summary, this type of technique will only be efficient if there is a type of compliance audit that is repeated often, so that there is a benefit from saving time in drawing samples. The time saved also needs to outweigh the time spent developing the technique and testing that it actually produces representative sample sizes.