



**DISCUSSION PAPER  
COMPLIANCE WITH LAWS AND  
REGULATIONS: AUDITS AND  
ASSURANCE ENGAGEMENTS  
IN THE PUBLIC SECTOR**

**December 2007**

*The Fédération des Experts Comptables Européens (FEE) is the representative organisation for the accountancy profession in Europe. FEE's membership consists of 44 professional institutes of accountants from 32 countries. FEE Member Bodies are present in all 27 Member States of the European Union and three member countries of EFTA. FEE Member Bodies represent more than 500,000 accountants in Europe.*

## CONTENTS

Part One: Introduction.....	4
What is meant by compliance with laws and regulations?.....	4
Objectives and scope of this discussion paper .....	5
Structure of this paper .....	6
Part Two: What Are The Relevant Frameworks of Laws and Regulations .....	7
What are the relevant laws and regulations.....	7
Responsibility for compliance with laws and regulations.....	8
Applicable frameworks of laws and regulations .....	9
Integrity .....	9
Part Three: Principles Common to Audit and Assurance Engagements .....	10
Planning: Obtaining a preliminary understanding of the environment .....	10
Accepting the engagement and the engagement letter .....	11
Materiality – the nature of the assignment .....	12
Risk of non-compliance with laws and regulations .....	13
Part Four: An Audit of General Purpose Financial Statements .....	16
Controls testing .....	16
Substantive testing.....	17
Reporting.....	18
Part Five: Other Assurance Engagements.....	20
Testing.....	20
Reporting.....	21
Agreed-upon procedures engagements .....	21
Grant Claims made under the 7 <sup>th</sup> Research Framework Programme .....	22
Annex 1: Example Risks and Control Procedures .....	23

## PART ONE: INTRODUCTION

### *What is meant by compliance with laws and regulations?*

1. The term ‘compliance with laws and regulations’ as used in this paper has a very broad scope. This scope includes financial regulations as criteria with which an entity is required to comply when preparing financial information, and non-financial regulations as criteria with which an entity is required to comply at an operational level. For an audit of general purpose financial statements under a financial reporting framework, the practitioner often has to gather evidence to report on whether the audited entity has complied, in all material respects, with the legislation and regulations under which it is mandated to operate. For a special purpose assurance engagement, the practitioner may be required to gather evidence and report on whether a particular set of regulations or contractual requirements have been complied with.
2. In the public sector, an audit of financial statements generally has a broader compliance element than in the private sector. The consideration of compliance with laws and regulations in an audit of financial statements conducted under International Standards on Auditing (ISAs) is detailed in ISA 250 *The Auditor’s Responsibilities Relating to Laws and Regulations in an Audit of Financial Statements*<sup>1</sup>. This ISA requires the auditor to obtain sufficient appropriate audit evidence that the financial statements are not materially misstated due to non-compliance with laws and regulations, and to respond appropriately to identified or suspected non-compliance with those laws and regulations.
3. Auditors are engaged, in audit assignments, to form an opinion on a set of financial statements prepared by the management of an entity. In preparing those financial statements, the entity is making a series of assertions about the information contained within, and auditors are performing work to test whether those assertions hold true.
4. In the public sector, there is often an additional requirement for entities to comply with, and for auditors to test against. This paper refers to the additional requirement as compliance with laws and regulations which encompasses many additional matters. Often, this requirement will be to report on compliance with the legal framework under which the entity operates, or the wider requirement of regularity, where there is a requirement to operate within the boundaries of formally authorised or permitted procedures. A discussion of the relevant laws and regulations is given in Part Two of this paper.
5. Increasingly more monies allocated by government or other public authorities find their way to private sector entities with accountability arrangements and responsibilities on those entities. Hence, auditors of the private sector entity could find themselves having to undertake assurance procedures on aspects of the related expenditures and income and reporting the results of such procedures. Such procedures are likely to form part of a separate assurance engagement. This paper is therefore relevant to all auditors undertaking work where compliance with laws and regulations is relevant. This includes assurance engagements as well as the audit of financial statements, and includes both public and private sectors.

---

<sup>1</sup> All references to International Standards on Auditing in this discussion paper refer to the original titles of the respective ISAs.

### *Objectives and scope of this discussion paper*

6. This paper is intended as a discussion paper, to raise the issues which face practitioners in a public or private sector audit or assurance engagement in relation to compliance with laws and regulations. It does not seek to add to, or replace, any existing standards or guidance.
7. International Standards on Auditing (ISAs), issued by IFAC's International Auditing and Assurance Standards Board (IAASB), are the main source of guidance available for an audit of general purpose financial statements. The IAASB has also issued assurance standards (ISAEs) and reporting standards (ISRSs) which can be applied to assurance engagements. In an audit context, INTOSAI has developed Practice Notes which clarify and enhance the application of the ISAs in a public sector context. Some countries also have in place additional guidance for both audit and assurance engagements in the public sector.
8. This paper recognises that further discussion of compliance with laws and regulations would be useful as:
  - The scope of the compliance element in a public sector audit context is often broader than in the private sector audit context; and
  - There is an increasing range of assurance engagements being performed in the public sector, resulting from, for example, the increased focus and interest in the audit of European Union monies, such as the certification of grant claims, and the trend towards reporting of expenditure by programme category in annual accounts, such as EU Framework funds.
9. In addition, in deciding to publish this discussion paper, FEE recognised the following further developments in public sector accounting and auditing:
  - The growing incidence of compliance audit in the private sector, for example the certification of expenditures for a recipient of a publicly funded grant;
  - The increased trend in the use of private sector auditors in the examination of public sector expenditures;
  - The move towards introducing performance against budgets as part of a public sector entity's financial performance; and
  - That in some countries management are required to include a specific statement that they have complied with the relevant financial laws and regulations as a part of the general purpose financial statements, and that the practitioner's audit opinion covers that compliance statement as well as the financial statements, and that they give a true and fair view.
10. Given these developments, FEE feels that a paper discussing the principles of compliance with laws and regulations would be a useful addition to the material available to assist practitioners.
11. The paper will also briefly discuss assignments which fall under ISRS 4400 *Engagements to Perform Agreed-upon Procedures Regarding Financial Information*, including the certification of grant claims under the 7<sup>th</sup> Research Framework Programme.

### *Structure of this paper*

12. This paper is designed to cover both audit and assurance assignments where there is a requirement of the practitioner to examine whether the client has conformed to the applicable laws and regulations. It is structured as follows:
  - Part Two of this paper will discuss what is meant by laws and regulations, and what the relevant frameworks of laws and regulations are. It will also discuss the concept of integrity;
  - Part Three discusses some of the general principles which apply to both audits and assurance engagements. This will cover gaining the preliminary understanding and the decision as to whether to accept the audit or assurance engagement and in particular the importance of the engagement letter and the need to agree the nature and extent of the testing to be performed and the report to be made. It will also discuss the concepts of materiality and risk as applied to such an engagement;
  - Part Four discusses the principles as applied to an audit of general purpose financial statements in the public sector, including the nature of the testing, the evaluation of results and the nature of the report to be made, including where non-compliance is found; and
  - Part Five discusses the principles as applied to an assurance engagement. It will also briefly cover factual findings engagements, where the auditor is performing agreed-upon procedures so that the report recipient may form an opinion rather than the auditor, including a case study on the certification of grant claims made under the 7<sup>th</sup> Framework Programme.
13. FEE hopes that this paper will be a useful addition to the material available for those involved in an audit or assurance assignment which involves an element of testing for compliance with the applicable laws and regulations. Where this paper refers to the term ‘practitioner’, this should be read as including assurance providers engaged on other assignments as well as the auditors performing a statutory audit of general purpose financial statements. The paper is aimed at the external practitioner, although internal audit can be a key tool that management can use for ensuring their compliance objectives (see Part Two).
14. FEE would welcome any observations you may have on this Discussion Paper. Please submit them to Saskia Slomp: [saskia.slomp@fee.be](mailto:saskia.slomp@fee.be).

## **PART TWO: WHAT ARE THE RELEVANT FRAMEWORKS OF LAWS AND REGULATIONS**

### *What are the relevant laws and regulations*

15. The laws and regulations applicable to an engagement can take many forms. Some laws and regulations determine the form and content of an entity's financial statements. Other regulations set out the boundaries which management are required to stay within in the operation of their business. Some industries are highly regulated (e.g. banking), whereas others are subject to a standard set of operational regulations that they must comply with (e.g. health and safety).
16. In general, public sector entities are subject to a greater number of laws and regulations than private sector entities. The public sector entity is usually created by establishing legislation which will set out the nature and structure of the entity, together with its operational remit. This will create a legislative source for the control over the public funds that the entity receives, and the manner in which those funds have been used.
17. An audit of general purpose financial statements in the public sector is similar in its nature and scope to an audit in the private sector. In addition to an examination of whether the financial statements contain material misstatements as a result of the misapplication of the financial reporting framework, the practitioner has regard to whether the financial statements might be materially misstated due to non-compliance with laws and regulations. ISA 250 defines these as:
  - Those which determine the form of the financial statements; and
  - Those which are to be complied with by those charged with governance or set out the provisions under which the entity can carry out its business.
18. A separate opinion on whether the financial statements comply with statutory requirements may be given, as allowed under ISA 700, including that the transactions and operations of an entity have been in accordance with the relevant laws and regulations and the underlying legislation.
19. The terms of engagement of most public sector assurance assignments will include a similar requirement, to provide assurance on compliance with the laws and regulations which govern the client entity. The key issue will often be to determine if the income and expenditure has been used for the purposes, and only those purposes, intended by the authority which granted the funds used for the transactions. Whether this is a grant of European funds, or internal expenditures, there is likely to be a requirement of the practitioner to consider the nature of these transactions as well as their fair presentation and disclosure in the financial statements.
20. In general, there will be a hierarchy of laws and regulations under which the public sector entities (or the private entity recipient of public funds) operate. These will include, but are not limited to:
  - International law;
  - Constitution of the individual country;
  - Legislation enacted by the legislative bodies in the country;
  - Regulations made by the government;

- State, regional or municipal laws;
  - Ministerial directions operating over an individual entities; and
  - Provisions attached to certain transaction streams, such as grants.
21. For each audit or assurance assignment, the practitioner will be required to have regard to the specific set, or parts of, laws and regulations that are the specifically developed criteria relevant to the income and expenditures that form the subject matter of the engagement when planning and reporting on their work.

### ***Responsibility for compliance with laws and regulations***

22. It is the responsibility of the management of the entity to ensure that it has complied with the relevant laws and regulations. Such responsibility includes the identification of the relevant regulations, implementation of the required procedures to conform to the regulations, monitoring of performance against them, and taking appropriate action if non-compliance is determined. Under corporate governance rules, those charged with governance are formally responsible for the conduct of their businesses. In the public sector, this is often taken a stage further and the Chief Executive or equivalent of the public entity is formally accountable to the legislature for the performance of their entity.
23. It is not the practitioner's responsibility to ensure compliance with laws and regulations. However, if included within the audit or assurance engagement, the practitioner may have a responsibility to perform procedures on whether the entity is in compliance. Nevertheless, in many circumstances the practitioner cannot be expected to identify all instances of potential non-compliance as part of an assignment, even when the nature of the engagement requires 100 per cent testing for a certain assertion or transaction stream. The concept of materiality can also apply to compliance with laws and regulations, for example where the nature of the non-compliance might have no implications for the work done by the practitioner. The practitioner will determine materiality with regard to the particular circumstances at the entity and the nature of the assignment.
24. In discharging their responsibility for compliance with laws and regulations, management will seek to set up management information systems which ensure that compliance is embedded within the normal operating procedures of the entity. These systems would be set up such that they indicate to management that their operations are compliant, and highlight any procedures which are not.
25. In some countries (for example the Netherlands), management are required to make an annual financial compliance statement as a separate part of the general purpose financial statements confirming their responsibilities and that they have complied with those relevant financial laws and regulations. In these cases, the practitioner's audit opinion on the truth and fairness of the general purpose financial statements also covers the financial compliance statement. Internal Audit can play a key role for management in assessing whether the management information systems are fit for purpose, and whether they provide the required assurance such that management may make such a statement of compliance.



### *Applicable frameworks of laws and regulations*

26. It is for the practitioner to understand the relevant frameworks which apply to the engagement. As part of his planning the practitioner should identify those regulations which apply to the engagement and design appropriate procedures to gain the necessary amount of evidence to satisfy the terms of engagement. Part Three of this paper discusses in more detail the specific aspects of planning which are relevant to this process.

### *Integrity*

27. Integrity is less concerned with compliance with laws and regulations, and more with standards of conduct, behaviour and corporate governance. It is a related concept to the framework of laws and regulations, as management is expected to act in accordance with those laws and regulations, and with fairness, integrity and the avoidance of personal profit.
28. Integrity is not subject to objective verification and often is not covered by the opinion on a set of financial statements, although the specific scope of the audit or assurance engagement will vary according to the applicable framework of laws and regulations. It is up to the auditor to judge, if matters of integrity come to light during an assignment, the best way to proceed in raising the matter in the most appropriate way. In some jurisdictions (for example in Scotland), there are relevant laws and regulations setting out how the auditors are to proceed and report if matters of integrity are uncovered during the assignment.
29. If significant integrity matters are found, covering fraud or corruption, there is detailed existing guidance in ISAs as to how to proceed. Member States will also have their own procedures for taking such matters forward.

## **PART THREE: PRINCIPLES COMMON TO AUDIT AND ASSURANCE ENGAGEMENTS**

### ***Planning: Obtaining a preliminary understanding of the environment***

30. Planning is a key process of any job carried out by a practitioner. ISA 300 sets out the procedures that the practitioner should follow when planning an audit. In addition, ISAE 3000 sets out that obtaining an understanding of the subject matter and other engagement circumstances is an essential part of planning and performing an assurance engagement. This understanding provides the practitioner with a frame of reference for exercising professional judgement throughout the assignment. The planning process for an assurance engagement will often be less detailed than for an audit, as the purpose of the engagement and the use that will be made of the report will normally be clarified up front. Often, the request for an assurance engagement will be in addition to the audit engagement, and therefore the practitioner may well have knowledge of the environment that is relevant to the entity.
31. The guidance contained in ISA 300 is detailed and well-known to all practitioners, and will therefore not be repeated in this discussion paper. ISA 315 also contains a detailed treatment of understanding the entity and its environment. However, where compliance with laws and regulations plays a key role in the engagement, there are some special considerations which can be taken into account to fully understand the environment under which the engagement will take place:
- Identifying the specific laws and regulations that are relevant to the entity and to the scope of the assignment being planned. This can be researched through legislative / Internet searches. It should also be available through client documentation and through discussions with the entity itself. Where a third party is involved (e.g. if the assignment is certification of a grant claim), then the applicable regulations should be set out in the terms and conditions attached to the funding;
  - Understanding the business operations and transaction streams which are affected by those laws and regulations, and are relevant to the scope of the engagement being performed;
  - Understanding the need to address a separate compliance statement, as is mentioned in the International Framework for Assurance Engagements<sup>2</sup>;
  - Understanding the scope of the proposed engagement itself, in terms of the level of assurance being sought and the work required to reduce risk to an appropriate level based on that assurance; and
  - Identifying significant transactions which may be not in the normal course of the entity's business. This could be done by review of management accounts. Other material in the public domain relating to the entity could also be reviewed.

<sup>2</sup> The IAASB International Framework for Assurance Engagements

32. The planning process should also include gaining an overview of the procedures implemented by management to ensure compliance with laws and regulations. For this type of assignment, relevant procedures that the practitioner might conduct include:
- Review of policies and procedures in place at the entity;
  - Discussions with management on relevant control procedures;
  - Organisational structures and appointments procedures at the entity; and
  - Review of previous audits or assurance assignments for relevant results.
33. Having obtained an understanding of the framework of laws and regulations and the scope of the assignment to be performed, the practitioner must then consider whether to accept the engagement.

### ***Accepting the engagement and the engagement letter***

34. An examination of compliance with laws and regulations, either as part of an audit of general purpose financial statements or as a separate assurance engagement, is likely to involve a different set of skills from an audit of just the financial statements. There are two different types of engagement which are relevant:
- The audit of general purpose financial statements of a public sector entity, where there is an additional requirement to test and report on compliance with laws and regulations; and
  - A specific assurance engagement to look at a particular element or scheme (such as certification of a grant claim) which involves compliance with the laws and regulations which govern that scheme or grant.

Laws and regulations could also cover requirements on systems and processes.

35. ISA 210 contains guidance for accepting the terms of an engagement, and is applicable to both scenarios set out above. ISAE 3000 discusses the key elements to consider when deciding whether to accept an assurance engagement.
36. Practitioners will also need to consider whether they have the necessary competencies to perform the assignment appropriately. They should have regard to the requirements of ISA 220 *Quality Control for Audits of Historical Financial Information*. In particular, the practitioner should satisfy himself that he has the appropriate knowledge and skills, and that the work of the team is appropriately supervised and reviewed. For specific assurance engagements where the practitioner does not have a history of working in that environment, the practitioner will need to carefully assess whether he can satisfy the requirements of ISA 210, particularly given the information needs of the intended users.
37. The key issue is the information needs of the intended users, and the purposes to which the audit report will be used. As with all audit or assurance engagements, the practitioner and the recipient of the report must be clear as to the level of assurance required and the level of assurance obtained and given. A key risk is that the recipient of the audit report may be seeking 100 per cent assurance (e.g. over the certification of a grant claim), which is a level of assurance the practitioner cannot provide.

38. To avoid such an expectation gap being created over the interpretation of the audit or assurance report, the engagement letter is of paramount importance. The practitioner, before accepting the engagement, will need to ensure that both they, the client entity to be examined, and the user of the audit report (if different) are clear as to the scope of the work and the level of assurance to be provided. This should be clearly set out in the engagement letter and signed by all relevant parties.
39. In some cases, the appointment of the auditor and the reporting requirements may already be covered by existing legislation (such as a public sector audit in the UK, where the requirement to test for and report on regularity is set out in legislation). However, an engagement letter may still be prepared in order to set out the nature of the work, the relative responsibilities of the practitioner and management, and the nature and use to which the report or other output can be put.

### ***Materiality – the nature of the assignment***

40. Materiality is a well known concept. A misstatement can be said to be material if its omission or misstatement can influence the reader of a financial statement or other piece of financial information. Auditors test financial statements to determine if they are materially misstated, not whether they are 100 per cent accurate. Such absolute assurance cannot be provided.
41. Materiality for a specific engagement will depend on the applicable financial reporting framework, and / or on the laws and regulations applied. The practitioner, in setting the materiality level, will have regard to the nature of the engagement and use his professional judgement to determine the appropriate level. Following the audit testing, the practitioner will form an opinion as to whether the entity receiving funding under the applicable laws and regulations has complied with those laws and regulations in all material respects.
42. Materiality also reflects that fact that responsibility for compliance with laws and regulations remains with those charged with governance at the entity. The practitioner cannot be expected to detect all instances of potential non-compliance.
43. Materiality will be determined by the practitioner based on his understanding of the relevant framework of laws and regulations, and the associated risk assessment. For both audits and assurance engagements, materiality for compliance with laws and regulations work has two aspects – qualitative and quantitative.
44. Qualitative materiality will be a matter of judgement for the auditor, and will depend on the specific laws and regulations concerned. For example, the entity may be the recipient of public grants. There may be a risk of funding being claimed back at a particular level of non-compliance with the terms and conditions of the grant. That level of non-compliance would therefore be material, regardless of any other aspects of the amount of funds associated with the non-compliance, as it would affect decisions and the finances of the entity concerned.
45. Quantitative materiality will be assessed at the planning stage for both the audit of general purpose financial statements and for assurance engagements, and again will depend on the nature of the engagement and the assurance to be provided. With all engagements, materiality should be constantly reassessed as the engagement progresses.

46. Taken together, these two aspects will provide a framework for the practitioner to evaluate their testing and results. The evaluation of results to determine material non-compliance will be a matter of judgement for the practitioner and will be driven by the specific nature of the engagement. A breach of quantitative materiality is a fairly straight-forward concept. Some examples of potentially material non-compliance of a qualitative nature are as follows:
- Where amounts of expenditures are in excess of the amounts approved by the legislative body;
  - Where expenditure is incurred on an item not authorised by the regulations under which the entity operates;
  - Where receipts are generated from unauthorised sources, or where income is not charged for a service that it is required to charge for;
  - Where an entity exceeds the maximum amount it can receive or spend on a scheme or programme, where particular terms and conditions are attached to that scheme (e.g. giving or receiving a grant);
  - Where a grant recipient may be claiming back more than they have spent; and
  - Where integrity matters are involved, for example making payments to the trustees of a public sector entity.
47. The point at which non-compliance is determined by the practitioner to be material is a matter of judgement. The practitioner will have regard to the context of the non-compliance and the nature of the engagement. For example, non-compliance resulting from over spending of a grant may begin at €1 depending on the terms and conditions attached to the grant, whereas non-compliance with an applicable reporting framework may involve a different threshold.

### ***Risk of non-compliance with laws and regulations***

48. The concept of risk assessment applies to assurance engagements covering compliance with laws and regulations as much as for general purpose financial statement audits. The auditor will need to understand the entity's business and the relevant framework of laws and regulations, and document and test the controls that the entity might have in place to ensure their own compliance with those laws and regulations. The principles of ISA 315 *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment* applies equally to public sector engagements as to private sector ones.
49. Relevant factors on the nature of the framework of laws and regulations which might influence the level of inherent risk to the assignment may include:
- *The nature and extent of the laws and regulations.* Where there are complex regulations there is increased risk of non-compliance through misinterpretation or misapplication of those regulations. Practitioners may wish to assess the level of internal control for ensuring compliance with those regulations, and the level of post-review of transactions to ensure that controls are effective;

- *The existence of new or amended laws and regulations during the reporting period.* Where there are new regulations there is an increased risk that new procedures are not implemented in a timely manner to prevent transactions being entered into without authority in the transition period. There is also a risk that the new procedures are not fit for purpose. The practitioner will also need to consider whether the reporting period needs to be split into parts and different procedures performed for the periods where different frameworks of laws and regulations applied;
  - *The relevant hierarchies of the laws and regulations* (for example the existence of EU legislation operating over Member State laws and regulations). In particular whether there are competing regulations, for example where a central government entity operating under certain laws and regulations gives a grant to a local government entity which might operate under different laws and regulations;
  - *The extent to which transactions are made through third parties or as a result of claim declarations.* Where there is significant grant income or expenditures there is an increased risk that the conditions attached to the grants cannot be directly verified for compliance. Practitioners may wish to assess the controls over validation of such claims and determine if there is significant residual risk;
  - *The existence of unusual transactions for the entity concerned.* In particular where there is a large amount of revenue generated by the entity there is a risk that the entity does not have the legislative powers to raise such income, or that the income is not used for the purposes intended by the legislative body;
  - *Any conditions attached to funding.* For example, if the receipt of funding is linked to the performance of an entity, there may be a risk that performance indicators are manipulated in order to meet the conditions attached to that funding. This is increased if the performance measure is not well defined or easily manipulated. Practitioners will need to be aware that such non-financial measures might impact on the financial circumstances of the entity, and understand the relationship between the two; and
  - *Specific duties which may influence the financial statements.* For example, where an entity has a duty to break-even and would receive a qualified audit opinion if it overspends. There is a risk that the entity would under-estimate its accrued costs at the year end, or manipulate its accounting estimates, in order to ensure that its break-even duty is met.
50. Having identified the inherent risks, the practitioner would then identify controls at the entity to determine whether the entity has sufficiently controlled the risk to an acceptable level of residual risk. Examples of such controls which may be present include:
- Schemes of delegated authority in the entity;
  - Formal agreements between the entity and third parties (for example the grant conditions and the related authorised grant claim applications);
  - Formal control plans prepared, monitored and regularly reviewed by managers over transaction streams;
  - Suitable focus on management accounts; and

- Detailed, reviewed procedures for assessing grant claims and the subsequent control of that expenditure.
51. In the UK, the Auditing Practices Board has issued a Practice Note on audits in the public sector (Practice Note 10: Audit of Financial Statements of Public Sector Bodies in the United Kingdom). In the UK, public sector auditors are required to report on whether, in all material respects, the transactions have conformed to the authorities which govern them, in addition to reporting on the truth and fairness of the financial statements<sup>3</sup>. This additional requirement is known as regularity in the UK.
  52. As part of its Practice Note, the Auditing Practices Board issues guidance on the audit of regularity. It has included within its guidance an Annex on risks to regularity and possible control procedures. Whilst aimed at a UK audience, this has wider applicability for a more general compliance with laws and regulations engagement, and is reproduced as Annex 1 in this paper.
  53. Having assessed the inherent and control risk, the auditor can then determine the nature, timing and extent of the further procedures to be performed. Of particular relevance to an engagement with a compliance element is that risks may attach to the compliance elements which are not risks attached to the financial statements themselves. For example, there may be little risk that an income balance is materially misstated in the financial statements, but risk may attach to the authority of the entity to generate that income. The practitioner would need to assess whether, in this case, special audit consideration should be paid to the compliance element.

---

<sup>3</sup> In the UK, compliance with laws and regulations is encompassed by the term ‘compliance with authorities’.

## **PART FOUR: AN AUDIT OF GENERAL PURPOSE FINANCIAL STATEMENTS**

54. This section of the discussion paper will focus on the audit of public sector general purpose financial statements. Whilst practitioners will have regard to ISA 250 in planning and performing their work, this section will focus on some of the general principles where the compliance element is significant, and will discuss the reporting implications for the practitioner. As this section is concerned with an audit of financial statements, the practitioner will be referred to as the auditor and refers to the independent, external auditor performing the audit.
55. The auditor should plan and perform tests to gain sufficient appropriate evidence that the laws and regulations which govern the transactions have been complied with. The key determinant of the level of evidence required will be driven by the nature of the assignment as set out in the engagement letter. As with all engagements, the auditor needs to gather evidence to reduce the audit risk to an acceptably low level.

### ***Controls testing***

56. As described in Part Two of this paper, the entity is responsible for ensuring that all laws and regulations have been complied with. It would be expected that management had introduced procedures and systems to ensure that the organisation is in compliance, or to detect and correct any instances where non-compliance has occurred. During the planning phase, the auditor will have identified those controls operated by management, where the auditor has concluded that effective operation of that control will mitigate the risk of non-compliance.
57. Many public sector entities will have been established by legislation, and will have their operating procedures defined by that legislation. For example, the members of, and appointments to, the governing board may be set out in the establishing legislation, and the auditor can perform a direct check that this has been complied with.
58. Further suggested control procedures are set out in Annex 1 against their associated risks. In summary, these are:
- Review of the adequacy of formal procedures for the translation of regulations into operational procedures;
  - Test the effectiveness of the control plans prepared and monitored by scheme managers;
  - Review of work conducted by other assurance providers, such as by Internal Audit or internal management assurance plans;
  - Review management control and monitoring of third parties;
  - Examine results of inspection visits carried out by the entity to third party recipients of funds (for example, by Internal Audit) to review their systems and procedures;
  - Independent certification of claims by the third party's auditors; and
  - Review procedures for the application, validation and authorisation of grant claims, including physical inspections and financial assessments.



## ***Substantive testing***

59. For audits performed under International Standards on Auditing, some detailed substantive testing is always required when gaining evidence to support an opinion. For the compliance element of an assignment, the nature of the detailed testing will be driven by the terms of engagement and the judgement of the auditor, but it is highly likely that some transaction testing will be required.
60. The extent of the substantive testing to be performed will be determined by the auditor's assessment of the effectiveness of controls. For an audit, evidence gathered to support the standard financial statement assertions may also provide evidence over the entity's compliance with laws and regulations. However, there are circumstances where the auditor might want to perform additional procedures. This might include where the regulations set a limit on the amount of expenditures that the entity can incur in any given period. In this instance, the auditor may wish to review transactions around the year-end to ensure that they are recorded in the correct period and review managements' accounting estimates to ensure that they are based on reliable evidence. The auditor may also wish to carry out tests to ensure that expenditure is not being charged to the wrong programme.
61. The relevant laws and regulations may also set a limit on the types of transactions that the entity can enter into. For example, in the UK each central government department is voted funds by the Parliament, and the nature of the expenditures that can be incurred, and income received, is set out as part of the Act where the funds are authorised. Expenditure outside of this remit would be considered to be not in accordance with Parliament's intentions, and would be termed irregular. The auditor might wish to review management accounts and the financial statements for evidence of any transactions which are unusual to the entity and therefore potentially irregular. As part of detailed transactions testing, the auditor may also want to review the nature of the transaction against the permitted income and expenditure streams as laid out in the applicable laws and regulations.
62. Analytical procedures can also be used as an effective tool by the auditor in determining compliance with laws and regulations. For example, where an entity makes payments under a particular scheme where there is a payment cap, the auditor could consider the relationship between the total number of recipients and the total reported expenditure, in order to identify potential overpayments.
63. A common area of transactions where regulations operate is grants. Entities make grants to recipients on the basis of a valid, authorised and appropriate grant claim. The auditor may want to test that the entity has only made grant payments to valid claimants on the basis of complete, reliable evidence. The auditor will also want to assess what processes the entity has in place to gain appropriate assurance that the grant has been used by the receiving entity for purposes covered by the criteria under which the grant was awarded.
64. Auditors may also need to ensure that the balances and disclosures in the financial statements conform to governing laws and regulations. Such disclosures, including the required format of the accounts, will be determined by the applicable financial reporting framework and the auditor will need to ensure that all required disclosures have been made. In addition, certain transactions may require, as part of the laws and regulations which govern those transactions, additional disclosures to be made by the entity, and the auditor will need to ensure that the entity has complied with these additional requirements. The planning work undertaken to understand the relevant

framework of laws and regulations should allow the auditor to determine which disclosures are required.

## ***Reporting***

65. As with all audit assignments, the audit report will have regard to the provisions of ISA 700 *The Independent Auditor's Report on a Complete Set of General Purpose Financial Statements*. If appropriate, the auditor will also have regard to the requirements of ISA 705 *Modifications to the Opinion in the Independent Auditor's Report*, and ISA 706 *Emphasis of Matter Paragraphs and Other Matters Paragraphs in the Independent Auditor's Report*.
66. The form of the audit report will also be determined by the terms of the engagement and the applicable laws and regulations. There may be a separate opinion on compliance with the relevant laws and regulations within the audit report, or a separate compliance report may be required. The auditor should have regard when determining the most appropriate format of the audit report to:
- The applicable legislation or regulation governing the entity;
  - The intended recipients (e.g. the legislature, the audited entity or other parties); and
  - Any legislation governing the auditor (e.g. via the mandate of a Supreme Audit Institution).
67. Under ISA 700, the auditor's report will clearly set out the respective responsibilities of the management of the entity, and the auditor, as they relate to compliance with laws and regulations, the scope of the work and the standards applied, and whether the evidence gained provided sufficient, appropriate audit evidence to form an opinion on compliance with the applicable framework of laws and regulations.
68. The information set out in the auditor's report should be able to be clearly understood by the intended recipient of the report. Setting out the responsibilities, the scope of the work (including any specified criteria) and the evidence obtained should enable the risk of an expectation gap between the auditor and the recipient of the audit report to be minimised. Without such clarity, the usefulness of the audit report can be reduced as the report can be open to interpretation by the readers.
69. When auditors determine non-compliance with laws and regulations, these should be raised with management to see if corrective action can be taken. However, unlike errors found in a financial statements audit, it may not be that the entity can simply make an adjustment to regularise the position. Whilst in certain cases corrective action can be taken, such as the recovery of an overpayment of grant, the auditor must consider:
- Whether the non-compliant event cannot be reversed;
  - What the impact on the report or opinion might be;
  - Whether the event needs to be reported regardless of whether corrective action has been taken by the entity;

- 
- Whether management are implicated in the non-compliant event in a way that, in the auditors' judgement, needs to be reported to a supervisory body;
  - Whether there is a duty under ISA 250 to report to a regulatory body;
  - Whether there is indication of fraud, whether through misappropriation of assets or financial reporting fraud, and
  - Whether the event highlights weaknesses in control procedures at the entity that need to be reported to management or a third party.
70. Where the auditor concludes that the activities, financial transactions and related information disclosed in the financial statements are, in all material respects, in compliance with the relevant laws and regulations, an unqualified opinion would be given. Where material non-compliance is determined, a qualified opinion may be given and the auditor would consider the implications for the financial statements as a whole.
71. Auditors may also be required to prepare additional reports, depending on the relevant legislation or regulation governing the audit, to third parties such as the legislature. Depending on those regulations, the auditor may need to prepare such a report regardless of whether material non-compliance has been found. In other circumstances, the auditor may only be required to report by exception, detailing the circumstances which have led to the need for a report.

## **PART FIVE: OTHER ASSURANCE ENGAGEMENTS**

72. As has been discussed earlier in this paper, the special purpose assurance engagement is becoming increasingly common where public funds are used. In particular, it is becoming more commonplace where grants are concerned for assurance to be provided that the grant recipient has used the granted funds in accordance with the terms and conditions of the grant. The assurance engagement could also cover requirements on systems and processes.
73. With the expansion in the number of schemes that operate, this is becoming an increasing issue for the European Commission to gain some form of assurance that the funds it has granted under its Framework Programmes have been used appropriately under the terms and conditions of the grant agreements. There is also ongoing work where certifying entities of EU funds are required to provide assurance over the regular use of those funds, such as agricultural funds.
74. With these types of assurance engagement, there is a particular risk that an expectation gap is created between the assurance provided and the assurance expected. In some cases, the grantor may be expecting the practitioner's report to provide 100 per cent assurance over the expenditure which the grant has been used for. The practitioners can therefore be reluctant to sign assurance reports which may be interpreted in this fashion, as 100 per cent assurance cannot be obtained and to sign the report raises liability issues for the audit profession.
75. The principles outlined in Part Three of this paper are therefore of vital importance to an assurance engagement. In particular:
- To understand and clarify for whom the report is being prepared, the purpose for which it will be used and therefore the reliance that will be placed on it and by whom;
  - The type of engagement that is required (i.e. assurance or agreed-upon procedures), and thus the scope of work and procedures that will be carried out to provide the form of report requested; and
  - The format of the report itself.

### ***Testing***

76. The nature and extent of the procedures performed will be determined by the terms of engagement. In general, these can be broken down into two scenarios:
- Where the outcome is specified by the terms of engagement, but the practitioner can exercise judgement as to the best way to obtain sufficient, appropriate evidence to satisfy that outcome; and
  - Where the engagement includes agreed-upon-procedures, and if the practitioner performed just these procedures he is deemed to have satisfied the evidence requirements of the engagement. This is considered further in the section on ISRS 4400 engagements below.

77. Where the practitioner has judgement as to how the necessary evidence is obtained, the practitioner will have regard to the relevant ISAs or ISAEs in order to determine that sufficient, appropriate evidence has been obtained. The key to this judgement will be the level of assurance required by the report and the way in which the report will be used by the recipient.

### ***Reporting***

78. For an assurance engagement, the form of the report will be directly related to the terms of engagement, within the applicable legal and practice requirements, and should be agreed at the start of the engagement. Regardless of the form of the report, the practitioner will have regard to the provisions of ISAE 3000 when determining the nature and content of that report. Relevant reporting options will be specific to the particular engagement but may include:
- An additional opinion to sit alongside the financial statements;
  - An opinion specific to the nature of the assignment (e.g. on the certification of grant claims);
  - A written or long-form report on compliance with laws and regulations to the client entity or a third party; or
  - A report to a regulatory body.

### ***Agreed-upon procedures engagements***

79. Practitioners may also be asked to perform engagements where the required testing is based on agreed-upon-procedures, and a report on factual findings is prepared. Under these arrangements, the practitioner is not required to form an opinion on the engagement (and hence this is not an ‘assurance engagement’), but merely provides the agreed information to the recipient of the factual findings report. In these engagements, the recipient of the report uses it to form their own opinion on the subject matter of the engagement.
80. Such engagements are covered by ISRS 4400 *Engagements to Perform Agreed-upon Procedures Regarding Financial Information*. This discussion paper is primarily concerned with engagements where the practitioner is required to form an opinion on compliance with laws and regulations. It does not therefore go into further detail, other than to confirm that where the terms of engagement include agreed-upon-procedures and a specified format of the factual findings report (i.e. where no opinion is given), this should be followed by the practitioner.
81. For the certification of grant claims made under the 7<sup>th</sup> Research Framework Programme, FEE has been working with the European Commission and the audit profession to come up with a form of agreed-upon-procedures and factual findings report which satisfies both the Commission and the profession. The results of this work are highlighted in the following case study.

## *Case Study*

### ***Grant Claims made under the 7<sup>th</sup> Research Framework Programme***

The 7<sup>th</sup> Research Framework Programme (FP 7) is used to fund research projects at entities such as universities, public authorities, companies and small enterprises, and also individual researchers who participate in the research programmes. The funding is paid directly to the entities (the beneficiaries) by the European Commission based on claims made in accordance with the terms of the research funding and involves a total of some €3.2bn over seven years (2007-2013). Where the beneficiary is a consortium, the funding is paid via the coordinator.

The costs claimed under the 6<sup>th</sup> research framework programme have often been examined by private sector firms, usually the same firm which audits the general purpose financial statements. For FP 7, the European Commission was concerned to ensure it was able to reach a conclusion on compliance with the conditions of grant, whilst clarifying that the role of the auditor was not to provide that ‘conclusion’ via an ‘assurance’ opinion. Thus FP 7 is an example of where compliance assurance is not provided by the ‘auditor’, but rather the ‘auditor’ provides information that the Commission may use as a basis to form its own conclusions.

The grant agreement provisions require the beneficiary to engage with the ‘auditor’ to provide an independent report on factual findings on costs claimed under a grant agreement financed under FP 7. Beneficiaries can adopt a simplified approach to making claims by providing detailed information on their average personnel and overhead costing approaches; in this case the engagement of the ‘auditor’ by the grant recipient is for an independent report on factual findings on the ‘methodology’ concerning a grant agreement financed under FP 7. For example, for employee costs, the ‘auditor’ is asked to state the basis on which employees record their time (e.g. on a daily/weekly/monthly basis) and the records used (e.g. paper/computer-based system) and that the time records selected by the auditor were authorised by the project manager or other superior. If no time records are available which fit this description the ‘auditor’ is required to list this fact as an ‘exception’ in the covering report. For the ‘methodology’, an example is that the ‘auditor’ is required to state that for 10 employees selected at random, the time recording methodology includes separation of time between management / administrative and project time. Key information is thus effectively highlighted to enable the Commission to consider the matter further.

For both costs claimed and methodology used the auditor is not required to form any opinion, nor to extrapolate from any samples used, but rather to report the facts as required by the ‘terms of reference’ specified by the Commission for the engagement of the ‘auditor’ in respect of grant claims. The Commission will then form its own view on compliance with the grant conditions. The terms of reference state that as well as undertaking the work in accordance with the terms of reference, it shall be undertaken in accordance with ISRS 4400 *Engagements to perform Agreed-upon Procedures regarding Financial Information*.

## ANNEX 1: EXAMPLE RISKS AND CONTROL PROCEDURES

<i>Risk Factor</i>	<i>Description of Risk</i>	<i>Possible Control Procedures at Entity</i>
Complexity of regulations	The more complex the regulations the greater the risk of error. This may occur through a misunderstanding or misinterpretation of the regulation or through an error in application.	<p>Formal procedures for the translation of statutory requirements into operating instructions.</p> <p>Formal control plans prepared and monitored by scheme managers.</p> <p>Review of scheme control plans and operating manuals by Internal Audit or some other independent audit.</p>
New legislation	New legislation may require the introduction of new administrative and control procedures. This may result in errors to either the design or operation of controls designed to ensure regularity.	The above controls apply to the new procedures introduced.
European Union schemes	Where legislation is developed by the European Commission there is a risk that regulations and guidance may be misinterpreted or omitted from internal instructions.	The controls applied to complex regulations apply equally to EU funded schemes.
Services and programmes delivered through third parties	Where programmes are delivered by agents, departments lose a degree of direct control and may have to rely on agents to ensure compliance with authorities.	<p>Formal agreements between the entity and the agent defining control procedures to be applied in the administration of services, for example:</p> <ul style="list-style-type: none"> <li>• Management control and monitoring of third party activities;</li> <li>• Inspection visits by Internal Audit to third parties to review systems and procedures, including those relevant to regularity;</li> <li>• Independent certification of payment and receipts by the third party's auditor.</li> </ul>
Payments and receipts made on the basis of claims or declarations	An entity's ability to confirm compliance with authorities may be restricted where, for example, criteria specified for receipt of grant are not	Established criteria for making claims clearly set out in departmental guidance and instructions to claimants.

<i>Risk Factor</i>	<i>Description of Risk</i>	<i>Possible Control Procedures at Entity</i>
	subject to direct verification.	<p>Standard requirements for documentation evidencing entitlement to be submitted in support of claims (this may be a condition of payment of grant or a requirement once the activity supported by the grant has been completed).</p> <p>Physical inspection of claimant's records to confirm eligibility.</p> <p>Procedures for assessing the financial standing of claimants before awarding a grant and monitoring continued solvency.</p> <p>Independent certification of the application of grant by external auditor.</p>