Organisation for Economic Co-operation and Development

GOV/SIGMA(2019)1

Unclassified

English - Or. English

17 June 2019

PUBLIC GOVERNANCE DIRECTORATE

SIGMA - Support for Improvement in Governance and Management

Guidelines for assessing the quality of internal control systems

SIGMA Paper No.59

Public sector organisations across the world are increasingly using advanced management concepts. One such concept, internal control, is a set of management arrangements designed to achieve an organisation's objectives on time, to appropriate performance standards, within budget, efficiently, effectively and in compliance with the law. These Guidelines explain in detail how to develop internal control in public sector organisations and how to assess the quality of existing systems. They are intended to guide ministries of finance and public sector managers in EU candidate countries and potential candidates, but could also be used by other administrations interested in assessing or improving their management and control systems.

JT03448998

Guidelines for assessing the quality of internal control systems

SIGMA Paper No. 59

Authorised for publication by Marcos Bonturi, Director,
Public Governance Directorate, OECD

2 Rue André Pascal
75775 Paris Cedex 16
France

mailto:sigmaweb@oecd.org
Tel: +33 (0) 1 45 24 82 00

www.sigmaweb.org

This document has been produced with the financial assistance of the European Union (EU). It should not be reported as representing the official views of the EU, the OECD or its member countries, or of partners participating in the SIGMA Programme. The opinions expressed and arguments employed are those of the authors.

Table of contents

List of abbreviations and acronyms

CHU	Central Harmonisation Unit
EC	European Commission
EU	European Union
ECA	European Court of Auditors
FMC	Financial management and control
IA	Internal audit
IC	Internal control
PIC	Public internal control
PIFC	Public internal financial control

Foreword

Good public administration has become a key precondition for European Union (EU) accession. The EU expects future member countries to have strong institutions and effective public administrations. High quality and proportionate management systems help institutions achieve their aims. The concept of internal control (IC) helps managers in the public sector set management arrangements that deliver objectives on time, to performance standards, within budget, efficiently and effectively. The existence of efficient and effective management systems based on this concept is currently an integral part of EU accession negotiations.

Developing and maintaining efficient management and control systems, based on the principle of decentralised managerial accountability, remains a challenge for public sector managers in the EU candidate countries and potential candidates (hereafter referred to as 'the administrations'). They look to their ministries of finance for advice and feedback. The ministries of finance, as part of their co-ordination role, are active in developing the IC system. They do this not only by setting the legal framework and organising training and awareness-raising events, but also by providing additional opinions and reporting on the quality of existing systems.

Over the years, SIGMA has assisted a number of administrations with designing and implementing their IC systems. It has prepared these guidelines as a response to the increased demand from ministries of finance for comprehensive guidance on harmonising and adapting the implementation of sound IC across the public organisations for which they are responsible.

The guidelines provide practical advice on how to assess the quality of management and control systems, how to report on this and how to identify which elements are crucial for enhancing their integrity, efficiency and effectiveness. They target the central co-ordinating institutions and managers responsible for management systems in their organisations.

The guidelines are based on the leading practices in IC, which are published by the European Commission in the *Principles of Public Internal Control.*[1] They are intended to facilitate the transition from reporting on compliance with formal IC requirements to reporting on efficiency, effectiveness and economy based on IC quality assessments. They provide a thorough explanation of how to use different sources for annual reporting and offer sound proposals for further improvements.

They are also intended to increase awareness and understanding of the underlying concepts, the practical implications of applying the concepts in the administrations and the functioning of IC.

The administrations are encouraged to embed and apply these guidelines in accordance with their national administrative traditions, arrangements and preferences, as they work towards complying with EU accession requirements.

[1] EC (2015), *Public Internal Control Systems in the European Union: Principles of Public Internal Control,* Position Paper No. 1. "Public Internal Control, An EU approach." Ref. 2015-1. http://ec.europa.eu/budget/pic/lib/docs/2015/CD02PrinciplesofPIC-PositionPaper.pdf

Introduction

To ensure high-quality management and control systems, governments need efficient feedback mechanisms. In mature systems, providing this feedback is the sole responsibility of the managers of public organisations, usually through management declarations or assurance statements on internal control (IC), based on self-assessment. Before a candidate country is ready to join the EU, it needs to have a centralised body that monitors and assesses the state of play and the progress made in enhancing efficient IC systems, as well as in organising the reporting system.

External IC quality assessment provides valuable feedback on the potential weaknesses and risks in the functioning of the organisation's IC system. During the assessment, units in charge of central harmonisation and co-ordination for IC (CHUs) should not only summarise the results of the institutions' IC reports on an annual basis for the government, but also provide information and additional scrutiny on the validity and accuracy of information reported by the public organisations.

Regular IC quality reviews in the individual public organisations provide an important source for such insights.

The reviews undertaken by the CHUs are considered crucial at the current stage of implementation of IC in candidate countries or potential candidates (hereafter referred to as "the administrations"). It is expected that they will contribute to further strengthening public management and control systems.

As understanding of IC concepts evolves, the role of the CHUs should diminish and management should play an increasingly important role in ensuring the quality of IC, eventually taking full responsibility for IC quality reviews.

The methodology outlined in these guidelines can be applied by the CHUs and by heads of public organisations when monitoring or evaluating the functioning of IC in their organisations, which they are required to do on a continuous basis in order to assess effectiveness.

These guidelines are divided into two main parts, which are complemented by related annexes. The parts can be read and used separately.

Part A is addressed mainly to the CHUs, as they are responsible for external co-ordination, development, establishment and implementation of IC. It will help with designing and implementing a harmonised and standardised methodology for the review of IC quality in all public organisations across the administrations. It provides step-by-step guidance through the process, from the planning stage to implementation and then reporting. Together with the easy-to use checklists and suggestions for the legal framework, it creates a sound basis for developing tailored national methodologies

Part B principally targets heads of institutions and public managers responsible for the continuous assessment of the effectiveness of their management and control systems. This methodology should be applied when internally monitoring or evaluating the functioning of their organisations. It also gives a structured set of examples of mechanisms for implementing different elements of management and control systems.

The guidelines should also be used by other actors involved in IC quality assessment within the public sector, as they aim to raise awareness and understanding of IC concepts. Internal

auditors, in particular, could use the checklists as a complementary tool when auditing IC systems.

Acknowledgements

Miroslawa Boryczka of the SIGMA Programme, Daria Bochnar and Andra Larin led the development of these guidelines. The team would like to thank colleagues from the European Commission (EC), the Public Governance Directorate of the OECD, as well as CHUs and managers from administrations across the region, who reviewed the guidelines and provided invaluable comments and suggestions.

1. Part A. Internal control quality assessment: Guidelines for central harmonisation units

The minister of finance (and the CHU on their behalf) is in charge of co-ordination of development, establishment, implementation and maintenance of IC. This includes the responsibility of monitoring the functional state of IC systems in the administration and presenting the results in an annual report for the government.[2] SIGMA recognises the principle that sound IC is best achieved when embedded within an institution's operations and regularly assessed in terms of its quality.[3] To monitor and assess the quality of the IC systems and to draw conclusions on whether the principles of sound financial management have been respected in the administration, the CHU should use various tools and sources of information. One of these tools is the sample-based IC quality review, which supports the regular assessment of the overall quality of the IC system in the public sector.

This Part of the guidelines explains the three pillars the CHU should build upon when preparing its annual report on IC to the government. It is intended to provide guidance to the CHUs on how to organise the process of the sample-based IC quality reviews and how to use the findings. Annex 1 is an essential component of this guidance, containing the Model Checklist for IC quality assessment. Annex 2 provides some additional guidance on how to build the legal framework for the assessments.

IC systems in the administrations are expected to be in line with the Committee of Sponsoring Organisations of the Treadway Commission (COSO) model[4] and the guidelines explain how to assess the quality of implementation of each COSO component and principle. The administrations should adapt the scope of their assessments to the current stage of maturity of their systems.

1.1. Building blocks for internal control quality assessment

The CHU's annual report to the government should aim to provide a conclusion on the soundness of financial management in public organisations, in terms of both operations (economy, efficiency and effectiveness) and compliance with legislation and regulations. It can also be the vehicle for highlighting any weaknesses that may exist in the IC of the

[2] Based on *The Principles of Public Administration*, the CHUs in the EU candidate countries and potential candidates should organise at least one annual review of progress across the public organisations with regard to aligning financial management and internal controls to the established legal and operational requirements. OECD (2017), *The Principles of Public Administration*, OECD Publishing, Paris: http://www.sigmaweb.org/publications/Principles-of-Public-Administration_Edition-2017_ENG.pdf

[3] In the 2017 SIGMA Monitoring Reports, the average value of the indicator 6.6.1 'Adequacy of the operational framework for internal control' in the administrations is 3 (out of 5) and 6.7.1 'Functioning of internal control' is 1.

[4] The COSO principles were originally drafted to apply to private sector companies.

public organisation. The results of the IC sample-based quality assessment enable the government to draw conclusions on the quality and the functional state of IC systems in the administration. They form one of the key pillars in its annual report to the Parliament, but they should not be considered the only one.

The following primary sources of information should form the building blocks for the CHU consolidated annual report on the IC quality to the government:

1. Management control outcomes concerning key results and progress towards the achievements of general and specific objectives

The establishment of a strong IC system requires management effort and commitment - starting with development of an IC framework with regard to compliance requirements and progressing to assessment of the efficiency and effectiveness of the IC systems. As the management of the public organisation is responsible for setting objectives to meet the organisation's mission, strategic plan, goals and legal requirements, strong IC shall provide assurance that those objectives are in place and achieved. The management presents objectives in the form of annual work plans.[5] They should be defined in specific and measurable terms to enable management to identify, analyse and respond to risks related to them.

These aims are grouped in the following categories of objectives:

- Operational - Effectiveness and efficiency of operations
- Reporting - Reliability of reporting (financial and non-financial) for internal and external use
- Compliance - Compliance with applicable laws and regulations.

IC quality assessment is a primary responsibility for the public organisation's management. This should not only consist of the evaluation of overall conformity with the established regulatory framework, but rather focus on how the functioning of IC enhances the operational efficiency and effectiveness of the public organisation and the achievement of its objectives.

Practical suggestions for CHUs

The management control outcomes concerning key results and progress towards the achievements of general and specific objectives are the primary source of information that should be used by the CHU. Particular focus should be placed on the results of operational controls and indicators commonly used by management to monitor the activities, reinforced by periodical self-assessments and reports.

Moreover, any significant observations reported by the External Auditors or other supervisory bodies provide additional evidence on the IC quality (legality, regularity and sound financial management).

[5] The annual work plan refers to various management and planning documents establishing the objectives at the governmental, organisational and / or unit level.

The CHU should establish and agree with the public organisations the reporting lines guaranteeing smooth communication on the results of management controls and any significant observations reported by the External Auditors or other supervisory bodies. This information, provided to the CHU on timely basis will enable the CHU to accurately analyse the IC quality in the administration and form an opinion on it.

2. Internal audit observations and recommendations

The establishment of the internal audit (IA) function in public organisations was an important step forward in strengthening the overall IC. Currently, IA is expected to deliver new or wider-ranging services, focusing on economy, efficiency and effectiveness, and on the provision of information and assurance with regard to system operations. A well-designed and independent IA helps public organisation managers accomplish their organisation's objectives by bringing a systematic, disciplined approach to evaluating and making recommendations for improving the effectiveness of risk management, IC and governance processes.[6]

Practical suggestions for CHUs

Although the CHU and IA have differing and clearly-defined roles, their collective purpose is to promote high-quality IC systems by increasing transparency in and accountability for the use of public resources, as well as promoting sound financial management.

The CHU should discuss and agree with the heads of the IA units the methods to be used for co-operation and knowledge sharing. The annual opinion and report of the IA, containing the results of the IA work and a particular focus on areas at risk, should be the primary source of interest and analysis for the CHU. If it is considered constructive, the CHU should have access to the IA reports

3. CHU IC quality review results

In the early stages of establishing the IC system, strong co-ordination enhanced by external IC quality review (mostly performed by the CHU) is a common practice and has proved to be a helpful mechanism in reaching higher levels of IC maturity. However, CHU (or IA) IC quality reviews are not a substitute for the management's responsibility, but rather support the managers in fulfilling their responsibilities.

Practical suggestions for CHUs

Section 1.2 presents the description of the IC quality review process to be conducted by CHUs.

[6] The Institute of Internal Auditors (IIA) defines internal auditing as an "independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes"- IIA (2013), *International Professional Practices Framework* (IPPF)®, The Institute of Internal Auditors Inc,, Altamonte Springs, Florida, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

1.2. Internal control quality review process

1.2.1. Annual preparation for IC quality assessment

Annual planning

To ensure the efficient use of CHU resources and the proper planning of activities to assess the quality of IC in the public sector and, eventually, to report on the quality and functional state of the IC systems in the administration, it is recommended that the CHU should design an Annual IC Quality Assessment Plan that is tailored to the specifics of the IC system of the administration concerned and the risks related to its public organisations. The plan should foresee the activities to be undertaken under each of the three pillars: (i) collection and analysis of the management's self-assessment questionnaires and other available sources of evidence on the functioning of the IC systems; (ii) collection and analysis of the IA observations and recommendations; and (iii) IC quality reviews performed by the CHU.

The Annual IC Quality Assessment Plan should indicate the following with regard to the IC quality reviews:

- the institutions to be subjected to review during the given budgetary year;
- the timing of the reviews;
- the CHU personnel assigned to conduct the reviews.

Selection of public organisations for IC quality review

IC quality review should focus on detecting likely sources of error, deficiency and risk in a given organisation's IC system. Accordingly, the CHU shall identify critical public organisations that shall be subject to CHU IC quality review during the given year.

The IC quality reviews should provide additional verification to that obtained from the other sources of evidence and relate only to the entities being reviewed. It is not necessary or economically justified to carry out detailed IC quality reviews of all public organisations. The entities to be reviewed should be selected through a risk-based selection, and, as IC quality reviews are not intended for drawing general conclusions on the entire public sector, statistical sampling is not appropriate.

These guidelines does not provide comprehensive details on how to perform a risk assessment. There are many risk assessment methodologies and tools available.[7] The CHU should perform a risk assessment to identify and understand the nature, sources, and potential causes of risks that could affect the functioning of the IC systems in the public organisations as well as the quality of the information provided in those organisations' IC self-assessment reports.

Risk identification for quality review purposes should generally consider the following risk factors, although this list is not exhaustive:

[7] Examples of the use of risk assessment methods in specific areas: OECD (2016), *Risk Management by State-Owned Enterprises and their Ownership*, Corporate Governance, OECD Publishing, Paris, https://doi.org/10.1787/9789264262249-en. OECD (2018), *National Risk Assessments: A Cross Country Perspective*, OECD Publishing, Paris, https://doi.org/10.1787/9789264287532-en.

- the size of the budget managed by the public organisation;
- the objectives and the scope of activities of the public organisation;
- the issues identified by internal and external auditors;
- the results of previous CHU quality assessments;
- the risk of fraud;
- the proportion of irregular expenditure within the overall budget of the public organisation;
- information emanating from the treasury or other relevant unit of the MoF responsible for the general oversight of the financial operations of the public organisation;
- IC self-assessment reports.

The identified risks should be assessed and prioritised by considering the following:

- the likelihood of risks materialising against the achievement of objectives;
- the impact of such risks on the information reported in their annual activity report to the government, self-assessment reports to the CHU or other relevant report;
- the extent to which misstatements in the self-assessment reports would be detectable.

The CHU should use the results of the risk assessment to select those organisations most at risk for its quality review exercise.

Some types of risk are more important than others; for example, the level of achievement of objectives, the size of budget managed by the public organisation and the ratio of irregular expenditure detected. If irregular expenditure amounts are higher than the materiality level determined by the CHU, they should always be subject to quality review by the CHU. The same applies to the institutions with lower than expected ratio of achievement of objectives.

It is also acceptable that the CHU occasionally reviews IC quality in those organisations recognised as front-runners in the implementation of IC systems. This type of review can support better understanding of the most efficient IC examples and promote good practices throughout the administration.

1.2.2. Conducting the IC quality review

Preparatory activities

IC quality review includes a mixture of desk-based and on-site practices.

Preparation for on-site visits should include the following:

1. Identification of the key actors and oversight bodies responsible for IC in the public organisation (including the head of the institution or his/her representative, the head of finance, the internal auditor, financial management and control (FMC) and risk managers if there are any); arranging a date and time for the on-site visit.
2. Ensuring the review team has basic information about the public organisation and the established management and control framework (legal basis, duties and

responsibilities, size and scope of the budget, structure, sub-ordinate bodies of the public organisation etc.).

3. Collection of key IC documents which are publicly available or in the possession of the CHU, such as self-assessment reports, annual plans, annual activity/implementation reports, risk registers, internal procedural rules (where in place), internal audit reports and supreme audit institution (SAI) reports.
4. Examination of the latest self-assessment report of the public organisation, comparing it with the one from the previous year and analysing the changes and justifications provided.
5. Analysing the information available on the functioning of IC (in particular, the internal audit and SAI reports, other independent external audit assessments, for example by the EC, or ECA audits, addressing any serious management and control weaknesses identified in the IC but also, if possible, information coming from the Treasury and/or relevant unit of the MoF responsible for the general oversight of the financial operations of the institution).
6. Adjusting the approach and preparing the checklist for the on-site visit (see Annex 1 for further guidance); arranging interviews with the relevant representatives of the public organisation.
7. Preparing the initial list of additional information to be presented by the interviewees during the visit (if it is only necessary to check whether it exists) or sent to the CHU (if it needs to be analysed).

In preparing the checklist, the CHU should establish the depth and scope of the checks to be performed during the IC quality review. The scope should correspond to the current maturity of the IC system in place and the stage of its development in the administration concerned. The context in which the administration operates (legal framework, political arrangements, economic conditions etc.) should always be taken into consideration and the decision on whether to conduct a full or partial IC quality review should be undertaken accordingly. The CHU should decide on which principles or attributes are applicable and should be reviewed by applying its professional judgement and its understanding of the situation using various sources (including the legal basis, the maturity of the IC system in the administration and in the given public organisation and the IC mechanisms expected to be in place).

When establishing its review methodology, the CHU may include in its checklist the evidence it expects to collect and the type of review activities to be conducted, both for planning purposes and to support and further facilitate the review process. The review techniques for obtaining evidence may include enquiry, inspection, observation, confirmation, re-calculation, re-performance and analytical procedures, often in combination. The CHU shall decide on the most appropriate technique (or combination) when designing respective checks for gathering evidence. The CHU shall apply professional judgment in establishing the depth of its approach, including which and how much supporting documentation to request / review as well as which and how many interviews to conduct. The objective is to design and perform IC quality review procedures in such a way as to enable the CHU to obtain sufficient and appropriate evidence to be able to draw reasonable conclusions on the compliance with sound financial management principles:

- **Sufficiency** is the measure of the quantity of evidence needed to support the findings and conclusions. In assessing the sufficiency of evidence, the CHU needs to determine whether enough evidence has been obtained to persuade a knowledgeable person that the findings are reasonable.
- **Appropriateness** is the measure of the quality of evidence; it encompasses relevance, validity and reliability.
    - **Reliability** refers to the extent to which the evidence has been gathered and produced with a transparent method that can be reproduced.
    - **Validity** refers to the extent to which the evidence is a meaningful or reasonable basis for measuring what is being evaluated. In other words, validity refers to the extent to which the evidence represents what it is purported to represent.
    - **Relevance** refers to the extent to which the evidence has a logical relationship with, and importance to, the issue being addressed. Relevance of information used as evidence may be affected by the direction of testing. A given set of review procedures may provide evidence that is relevant to compliance with several requirements, but not with some other rules. On the other hand, evidence from different sources or of a different nature may often be relevant to the same tested item.

Annex 1 illustrates the possible checks for all principles, and attributes under these principles, which can be verified. In designing its checklist, the CHU may consider the review questions provided therein. However, the questions should be adjusted to the specifics of the administration / organisation (especially the principles under the control activities). Furthermore, the list of possible evidence as well as the data collection and analysis methods in Annex 1 are illustrative in nature and shall not be binding. However, they may provide valuable insights as to how to design the review approach for establishing sufficient appropriate evidence.

Carrying out the IC quality review

During the IC quality review, the CHU shall verify, according to the established checklist, the IC system's state of play, including whether sufficient appropriate evidence exists on the applicable principles / attributes, and document the results in the checklist. Both on-site and desk-based checks should be used.

Evidence may take many forms, such as electronic and paper records of transactions, written and electronic communication with outsiders, observations by the reviewer, and oral or written testimony by the public organisation.

Annex 1 is an integral part of this chapter. It guides the IC quality review by providing potential sources of evidence, methods and approach.

The CHU should inform the public organisation under review who it expects to conduct interviews with and the nature of documentation it expects to review. It may request that some of the documentary evidence be provided to the CHU in advance of the on-site visit.

The CHU should use its professional judgment to assess whether sufficient appropriate evidence has been obtained. In the review process, the CHU should consider all relevant evidence, regardless of whether it appears to corroborate or to contradict the compliance with the respective requirements. Accordingly, at any stage of the IC quality review, the

CHU may discover that additional documentation or clarification is needed to what was planned, whereby further information might be requested or further interviews arranged.

CHU should document the IC quality review results. CHU documentation (including the checklist and working papers) should generally include the following:

- a conclusion on the level of implementation of the different attributes of each IC principle reviewed (e.g. implemented - partially implemented - not implemented or effective-partially effective-ineffective);
- a summary of the data or processes reviewed;
- the date of the activity and the individual(s) conducting and participating in it;
- a description of any noncompliance, potential noncompliance, data irregularities, or other deficiencies identified, supported by robust evidence;
- classification of the importance of the IC deficiencies or weaknesses (e.g. high - medium - low);
- recommendations for improvement.

Documentation of the review results should include sufficient detail to allow verification of the audit trail, demonstrate that the annual IC quality assessment plan was followed, and allow re-performance.

The CHU should provide feedback on the results of its review to the management of the public organisation in a timely manner so that the management can review and follow-up.

1.2.3. Feedback on the quality of IC

Drawing conclusions as to the quality of the IC system and reporting to management

Although the CHU's primary responsibility is to report to the government on the state of play of the IC systems in the administration, it is equally important to provide feedback to the public organisations' managers.

Upon each review, the CHU should draw conclusions as to the effectiveness and efficiency of the IC system in place in the public organisation, with regard to whether it helps the organisation achieve its objectives relating to operations, reporting and compliance as well as sustaining and improving performance. The CHU should provide feedback to the public organisation and advise them on suggested improvements.

In assessing the overall quality of the IC system, the conclusions reached with regard to each principle and the relevant attributes reviewed (i.e. the level of implementation and relative importance of any deficiencies) shall be considered, focusing on its effectiveness.

The CHU IC quality review may result in the conclusion that the public organisation's IC system is effective, partially effective or ineffective:

- The IC system shall be considered **effective** where no or only low-level weaknesses and deficiencies were detected.
- The IC system shall be considered **partially effective** where the detected weaknesses and deficiencies are assessed as medium and/or low-level, and no significant weaknesses or events harmful to reputation were detected. In this case,

the overall conclusion of the CHU on the IC system should include standard information on the nature, scope and impact of the detected weaknesses together with recommendations for improvement.

- The IC system shall be considered **ineffective** where a major deficiency is detected the absence or failure of a component or relevant principle, or where the components do not operate in an integrated manner.

The CHU may apply a quantified approach (e.g. using ratings on a scale of 1 to 5 or 1 to 3, where the lowest rating corresponds to an ineffective system and the highest to an effective IC system).

A rating as to the level of efficiency could be also applied to each of the questions addressed in the checklist; and summary assessments should be made at the level of each principle, the five COSO components and, finally, at the level of the whole public organisation.

Drawing conclusions at any level (question, principle or organisation) assumes the application of professional judgment, supported by as much evidence as available and known to the CHU. The use of ratings, despite giving a sense of greater objectivity or comparability, does not change this approach.

CHU recommendations should not determine what must be done but seek to advise the public organisation. Recommendations should be action-oriented, convincing, well-supported, and cost-effective. When appropriately implemented, they should achieve the desired beneficial results.

The CHU should determine the form of the feedback provided to the public organisation. It may be in the form of a letter with observations or a report, supported, if needed, by a checklist. The main objective of this communication is to provide an overall conclusion on the functioning of the IC system and a summary of key observations and recommendations to the high-level management. Prior to issuing the final recommendations, the CHU may consider holding a dialogue with the management of the public organisation on the suggested actions.

The management of the public organisation should ensure that the CHU recommendations are implemented and inform the CHU when they have been completed.

In more advanced IC systems, where the management would issue the annual assurance statements, the results of the CHU IC quality review and the organisation's respective follow-up should be taken into account in making the reservations in the annual assurance statement.

1.2.4. Annual reporting on the quality of the IC system to the government

Annual reporting to the government should provide feedback as to the quality and functional state of the IC system in the administration. The aim of this section is to explain how the conclusions deriving from the IC quality review should be incorporated in the annual report.

The administrations have already implemented annual reporting by the CHU to the government. The reports to the government are structured according to the three pillars of

PIFC – the FMC system, internal audit and central harmonisation unit.[8] The information on the quality and state of play of the IC systems concerns the first pillar. The annual report chapter dedicated to the CHU activities (the third pillar), should provide information on IC quality reviews performed (including, for example, the list of public organisations subject to IC quality reviews and their timing).

Although the format of the annual reports may vary across administrations according to the regulatory framework and the government's information needs, the CHU should provide, along with a summary based on the public organisations' self-assessment reports, its conclusions on the functional state of the IC system in the administration, including the qualitative aspects. The conclusions should be based on the three pillars of the quality assessment (see also Section 1.2.1), including analysis of:

- the management's self-assessment questionnaires;
- matters identified by internal and external auditors;
- various progress reports on implementation of PIFC strategies or IC development plans;
- reported cases of fraud and irregularities;
- information emanating from the treasury or other relevant unit of the MoF responsible for the general oversight of the financial operations of the public organisation.

Moreover, such analysis should be supported by the results of the CHU's IC quality reviews conducted over the given year.[9] These reviews should give the CHU a basis for identifying any systematic issues detected at the level of the entire public sector, i.e. those cases when the weaknesses or the deficiencies of the IC systems cannot be eliminated at the level of the individual organisation.

The conclusions of the annual report on the state of play of the IC systems in the administration should include:

- the overall functioning and state of play of the IC system in the administration, including the existence of any systematic issues;
- an overview of improvements that should have been implemented over the previous year and are still outstanding;[10]

[8] It is common that for the first two sections, the CHU annual reports consolidate statistical information from the self-assessment reports of those public organisations which have submitted the reports to the CHU. In the third section concerning the CHU, the reports provide the statistical overview of CHU activities over the year as well as summary on conducted monitoring activities of the administration's IC system (if performed).

[9] As IC quality reviews are not intended to be used to facilitate conclusions concerning the entire public sector, extrapolation of the review results is not appropriate.

[10] Though it is the responsibility of the management of any public organisation to ensure an effective IC system and to implement the CHU recommendations accordingly, in cases where the management has not taken timely action, the government may issue a special decision based on the CHU annual report obliging the specific public organisations to take further action on improving the IC systems in their organisations.

- CHU follow-up actions on previous years' reports and recommendations implemented over a given year or still outstanding.[11]

It is not expected that the annual report should include the results of the individual, on-site IC quality reviews of the public organisations undertaken during the year.

[11] In order to provide feedback on the status of recommendations issued by the CHU over the previous years, the CHU should regularly receive information from the relevant public organisations on the actions taken. The CHU may need to carry out additional, follow-up activities prior to issuing its annual report to the government. The follow-up would normally be in the form of a formal, written request on the status of open recommendations.

2. Part B. An internal control system based on the COSO model: a principle-by-principle guide for managers

Public internal financial control (PIFC) is an internal control framework for the public sector, composed of three pillars: the financial management and control (FMC) system, internal audit (IA), and the central harmonisation unit (CHU). In particular, the *acquis* requires the existence of effective and transparent management systems, including accountability arrangements for the achievement of objectives; a functionally independent IA; and relevant organisational structures, including central co-ordination of PIFC development across the public sector. Part B of these guidelines also covers the protection of the EU's financial interests against fraud in the management of EU funds and the protection of the euro against counterfeiting.[12]

Internal control (IC) encompasses more than financial and budgetary control and more than compliance checks. It is a set of management arrangements that enhances the efficient and effective delivery of the organisation's objectives on time, in line with the performance standard and within the established budget. IC is based upon the COSO model. Both PIFC and IC should apply across the entire public sector, and are applicable for the management and implementation of both national and EU funds.

For an individual public organisation, public internal control (PIC)[13] is defined as an integral process, effected by the organisation's management and personnel, designed to address risks and pursue opportunities and to provide reasonable assurance regarding the achievement of results in pursuit of the public interest and the organisation's mission, through:

- executing orderly, ethical, economical, efficient and effective operations;
- ensuring the relevance, reliability and integrity of information;
- fulfilling external and internal accountability obligations;
- complying with applicable laws and regulations;
- safeguarding resources against loss, misuse and damage;

[12] European Commission (2017), European Neighbourhood Policy and Enlargement Negotiations, Chapters of the *acquis* https://ec.europa.eu/neighbourhood-enlargement/policy/conditions-membership/chapters-of-the-acquis_en

[13] Public Internal Control (PIC) is a description of the rich variety of IC systems used in the public sectors of the EU-28.

- meeting other criteria of good public governance, including good policy preparation and implementation, good budgeting and financial solidity and sustainability.[14]

The management of the public organisation sets objectives to meet the organisation's mission, strategic plan, goals and requirements of the applicable laws and regulations. These objectives are presented in the form of annual work plans and should be defined in a specific and measurable terms to enable management to identify, analyse, and respond to risks related to achieving those objectives.

Strong IC provides assurance that objectives are in place and achieved. The IC quality assessment should support the managers in achievement of the agreed objectives. The objective of the IC quality assessment should not just be the evaluation of the overall conformance with the established regulatory framework, but should rather focus on how the functioning of IC enhances the operational efficiency and effectiveness of the public organisation and the achievement of its objectives.

IC applies to all public organisations. Although implementing IC is a complex and challenging task, well-established arrangements are essential to ensuring public resources are utilised efficiently, effectively and in compliance with established rules. Moreover, these arrangements should ensure the administrations achieve value for money in a legal, appropriate, ethical and financially responsible way and slowly move away from a purely compliance-based to objective-based systems. IC should facilitate managerial accountability and the delegation of authority to different levels of management with appropriate accountability reporting.

This Part of the guidelines presents a short description of key elements of efficient IC systems, organised by 17 COSO principles15 and followed by a set of self-checking questions. The questions are designed to help understanding and to assess the current state of play for subsequent attributes of a particular principle, mirroring its points of focus and the IC mechanisms expected to be in place. Annex 3 provides some additional background information about IC, the roles and responsibilities related to it, and its quality assessment. Annex 4 gives some practical examples of the implementation of different COSO principles in EU Member States.

Heads of public organisations and managers are encouraged to use these guidelines for improving and assessing the IC systems in their organisations.

2.1. Control environment

The control environment is the foundation for an IC system. It provides the discipline and structure that affect the overall quality of IC. It influences how objectives are defined and

[14] EC (2015), *Public Internal Control Systems in the European Union: Principles of Public Internal Control,* Position Paper No. 1. "Public Internal Control, An EU approach." Ref. 2015-1. Chapter 2, PIC defined and characterised. http://ec.europa.eu/budget/pic/lib/docs/2015/CD02PrinciplesofPIC-PositionPaper.pdf

[15] The description of the principles, points of focus, attributes and examples of mechanisms align with or are taken from the eBook developed by COSO, 'Internal Control - Integrated Framework', of which the executive summary is available online.
COSO (2013), *Internal control - integrated framework: executive summary*. http://www.coso.org/documents/990025p_executive_summary_final_may20_e.pdf

how control activities are structured. The oversight body and management establish and maintain a positive attitude towards IC throughout the public organisation.

Principle 1: The public organisation demonstrates a commitment to integrity and ethical values

Point of focus:

Leading by example on matters of integrity and ethics.

The public organisation's high-level, key members of management articulate and demonstrate the importance of integrity and ethical values across the organisation.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- tone at the top
- standards of conduct
- adherence to standards of conduct
- addressing deviations in a timely manner

Examples of mechanisms:

- Communications from senior management that support the expected standards of conduct and remain consistent as they spread throughout the public organisation.
- Public organisations at the national, regional and local level [16]:
  - establish and enforce regulations that reduce opportunities for conflicts of interest,
  - consider instituting mandatory registries that require lobbyists to publicly and regularly disclose their clients, issue areas, targets, techniques and financial information,
  - create transparency in decision-making processes by facilitating open hearings on policies and consultative decision-making processes to ensure that citizens' inputs are included, and transparently and proactively disclose conflicts of interest,
  - Inquire into and investigate in a timely manner any alleged conduct that is inconsistent with the public organisation's standards of conduct.
- Corrective action is taken when deviations from expected standards of conduct occur.

[16] Transparency International (2009), *Controlling Corporate Lobbying and Financing of Political Activities,* Policy Position # 06 / 2009, http://transparency.ee/cm/files/lisad/corporate_lobbying.pdf

Set of questions for this principle:

1.1 Is the management's commitment to integrity and ethical behaviour communicated effectively throughout the public organisation, both in words and actions?
1.2 Does the high-level management lead by example?
1.3 Is the tone set by the high-level management communicated through to the various operating units?
1.4 Is there a code of conduct and/or ethics policy and has it been adequately communicated to all levels of the public organisation? If yes, does it provide standards to guide the public organisation's behaviours, activities and decisions?
1.5 Does the public organisation have the training programme dedicated to integrity and ethical behaviour?
1.6 Do dedicated complaints mechanisms exist for corruption?
- Do these systems offer adequate levels of anonymity and protection to complainants?
- Is whistleblowing broadly defined? Can disclosures be made with a reasonable belief that the information is true at the time it is disclosed?
- Are protections for whistle-blowers clear and comprehensive?

1.7 Does the public organisation have a process to evaluate the performance of personnel and teams against its code of ethics?
1.8 Does the high-level management determine the tolerance level for deviations from certain expected standards of conduct? [17]

Principle 2: The public organisation exercises oversight responsibility

Point of focus:

The oversight body[18] exercises oversight of the development and performance of IC.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- oversight body exercises oversight responsibilities
- members of the oversight body have relevant expertise
- independence of the oversight body
- oversight of all the components of the IC system.

Examples of mechanisms:

[17] See also: OECD (2005), *Public Sector Integrity: A Framework for Assessment*, OECD Publishing, Paris, https://doi.org/10.1787/9789264010604-en.

[18] The oversight body is used in the following context:

- Within the public sector, it is the first-level budget user (e.g. the ministry of agriculture) which oversees their subordinate structures or organisations (e.g. the land agency);
- Within public organisations, the oversight body may be a board of directors (e.g. for state-owned enterprises), an audit or risk committee or other body, which is independent from the management of a public organisation.

The oversight body exercises oversight responsibilities:

- Identifies and accepts its responsibilities in relation to established requirements and expectations through the use of appropriate working arrangements and communication channels and reporting.
- Defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask pertinent questions of senior management and take commensurate actions.
- Has a sufficient number of members who are independent from management and objective in evaluations and decision-making.
- Provides oversight for the IC system, in particular for:
  - the control environment - establishing integrity and ethical values, developing expectations of competence, and maintaining accountability to all members of the oversight body and key stakeholders.
  - risk assessment - overseeing management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management overrule of IC.
  - control activities - providing oversight to management in the development and performance of control activities.
  - information and communication - analysing and discussing information relating to the public entity's achievement of objectives.
  - monitoring - scrutinising the nature and scope of management's monitoring activities as well as management's evaluation and corrective actions of identified deficiencies.

Set of questions for this principle:

2.1 Does the oversight body exercise oversight responsibilities, independently of management?

2.2 Does the oversight body consist of members from sufficiently diverse, complementary backgrounds and specialised skills to enable discussion, constructive criticism of management, and appropriate oversight of IC?

2.3 Do the members of the oversight body understand the public organisation's objectives, its related risks, and the expectations of its stakeholders?

2.4 Does the oversight body oversee the management's design, implementation, and operation of the public organisation's IC system (all components)?

2.5 Are the activities of the oversight body sufficiently focused on high-risk areas? (e.g. complex operations; transactions of high monetary value; low control consciousness among personnel; lack of experienced or skilled personnel; reorganisation or significant modification of operating activities; new IT systems; potential conflicts of interest or influence from external parties; and activities of a politically sensitive nature)

2.6 Is there systematic follow-up of significant issues identified?

2.7 If the subordinate organisations are responsible for carrying out corrective actions, has appropriate supervision or follow-up been established by the responsible first-level budget users?

2.8 Is the oversight of operational performance based on the public organisation's objectives and related performance indicators?

2.9 Are all reported internal control weaknesses properly analysed and addressed where necessary?

2.10 Does the oversight body provide input to management's plan for corrective actions when deficiencies in the IC system appear?

Principle 3: The public organisation establishes structures, reporting lines, authorities and responsibilities

Point of focus:

The public organisation's management should establish an organisational structure, assign responsibility, and delegate authority to achieve the organisation's objectives.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- organisational structure
- establishment of reporting lines
- definition, assignment and limitation of authorities and responsibilities

Examples of mechanisms:

The public organisation's management:

- Establishes the organisational structure necessary to enable the public organisation to plan, execute, control, and assess the core functions of the public organisation /budget user and its set operating objectives.
- Establishes authorities and responsibilities, tasks and reporting obligations concerning the achievement of objectives and budget resource management, which are clearly defined for each section of the organisational structure in writing and communicated to the personnel.
- Delegates authority only to the extent required to achieve the public organisation's objectives. As part of delegating authority, management evaluates the delegation for the proper segregation of duties within the units and in the organisational structure.
- Periodically evaluates the organisational structure so that it meets the public organisation's objectives and if necessary adapts to any new objectives for the organisation, such as a new law or regulation.
- Develops reporting lines in parallel with the development of lines of authority and accountabilities

Set of questions for this principle:

3.1 Does the organisational chart of the public organisation define the lines of authority and responsibility?
3.2 Is the organisational chart up to date?
3.3 Have the management responsibilities for the implementation of the public organisation's objectives and risk management been defined?

3.4 Does the public organisation's management delegate authority? Does it use appropriate processes and technology to assign responsibility and segregate duties as necessary, at the various levels of the public organisation?

3.5 Are the nature and scope of delegated functions and powers clear to all persons concerned?

3.6 Are the risks associated with the delegated functions and powers sufficiently analysed?

3.7 Has the public organisation's management established and evaluated the reporting lines within the public organisation and with the other organisations to enable the execution of authority, fulfilment of responsibilities, and flow of information?

3.8 Does the public organisation evaluate the organisational structure to assess how it supports the achievement of its objectives?

Principle 4: The public organisation demonstrates commitment to competence

Point of focus:

The public organisation demonstrates a commitment to attract, develop, and retain competent personnel in alignment with its objectives.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- human resource management policies and practices
- evaluation of competence and addressing of shortcomings
- attracting, developing and retaining competent personnel
- planning and preparing for succession.

Examples of mechanisms:

- Management establishes expectations of competence to carry out assigned responsibilities. This requires having the relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and certifications.
- Management evaluates the competence of personnel across the public organisation in relation to established policies. If needed, it addresses any shortcomings. The oversight body evaluates the competence of management as well as the overall competence of public organisation personnel.
- The management of the public organisation should develop and retain the following procedures:
  - Recruitment - to determine whether a particular candidate fits the public entity's needs and has the competence for the proposed role.
  - Training – to enable personnel to develop the competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role. An effective personnel development plan should take into account not only individual training requests but also the collective skills and competences needed to meet the public entity objectives. Carrying out analysis to detect significant gaps between required and available skills and competences in the entity can be an effective means of improving personnel development.
  - Mentoring – to provide feedback on the individual's performance based on standards of conduct and expectations of competence, align the individual's skills and expertise with the public organisation's objectives, and help personnel adapt to an evolving environment.
  - Evaluating and retaining – measuring the performance of personnel in relation to the achievement of objectives and demonstration of expected conduct. Measuring the performance against service-level agreements or other agreed-upon standards for recruiting and compensating outsourced service providers.

Providing incentives to motivate and reinforce expected levels of performance and desired conduct.

- Management defines succession and continuity plans for key roles to help the public organisation to continue achieving its objectives. These plans should address the organisation's need to replace competent personnel over time. The importance of the key role in the IC system and the impact on the public organisation in the event of its vacancy dictates the formality and depth of the continuity plan.

Set of questions for the principle:

4.1 Have the competences for key roles in the public organisation (regarding the relevant knowledge, skills, and abilities) been defined to enable the personnel to carry out assigned responsibilities?

4.2 Has the existing level of knowledge and skills of personnel been aligned with the public organisation's strategy/ objectives? Are they capable of coping with the everyday challenges and possibilities associated with the given assignments?

4.3 Have the recruitment procedures been established in such a way as to determine whether a particular candidate fits the public organisation's needs and has the competence for the proposed role?

4.4 Are there any issues or problems related to the recruitment and allocation of personnel that significantly affect the public organisation's performance?

4.5 Are sufficient training opportunities provided to personnel? Has an overall training strategy or plan that is aligned to the public organisation's objectives been developed?

4.6 Has the public organisation established cross-unit training for significant changes in personnel?

4.7 Are sufficient measures taken to analyse and develop the skills of the personnel and to plan for future human resource (HR) needs and skill requirements?

4.8 Are relevant training statistics available? If yes, is there evidence that personnel is taking the necessary courses in order to build their skills?

4.9 Does the environment of the public organisation motivate the personnel to channel their competencies and efforts towards the achievement of the organisation's strategic objectives?

4.10 Are sufficient measures taken to ensure flexible and dynamic organisation, for example via targeted training programmes, re-organisation or other measures?

4.11 Does the management measure:

- the performance of personnel in relation to the achievement of objectives and demonstration of expected conduct,
- the performance against service-level agreements or other agreed standards for recruiting and compensating outsourced service providers?

4.12 Are adequate arrangements in place to ensure effective personnel planning and allocation?

4.13 Does management have sufficient and relevant information about the priorities and workload of personnel as well as the skills required and available?

4.14 Is personnel turnover sufficiently monitored and analysed? Have the specific indicators for "excessive" and "insufficient" personnel turnover been defined? Are the root causes of any abnormal personnel turnover sufficiently analysed and addressed?

4.15 Has management defined the succession and continuity plans for key roles to help the public organisation continue achieving its objectives?

Principle 5: The public organisation enforces accountability

Point of focus:

The public organisation holds personnel accountable for their IC responsibilities in the pursuit of objectives.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- enforcement of accountability using the appropriate structures, authorities and responsibilities
- establishment and evaluation of performance measures, incentives and rewards
- considering excessive pressures

Examples of mechanisms:

The public organisation's management:

- Defines clear roles and responsibilities and holds personnel and subordinate organisations accountable for the performance of IC responsibilities across the organisation and for the implementation of corrective action as necessary.
- Conducts appraisal of the personnel on a regular basis. Assesses efficiency, abilities and performance of the personnel annually against expected standards of conduct and set objectives. Cases of underperformance are appropriately addressed.
- Promotes eligible personnel based on comparative merit, taking into account the results of their appraisal reports.
- Adjusts excessive pressures on personnel in the public organisation in order to help them fulfil their assigned responsibilities in accordance with the organisation's standards of conduct.

Set of questions for the principle:

5.1 Has the accountability for the strategic objectives been defined?
5.2 Has the accountability of the heads of internal organisational units been formally defined in the public organisation's internal regulations and rules (e.g. an internal organisation rulebook or internal rulebook on systematisation)?
5.3 Does the accountability of the heads of internal organisational units cover in particular:
- achievement of objectives in line with the approved budget,
- definition of performance indicators to enable them to report to higher management on the outputs and outcomes;

- supervision over the implementation of programmes, projects and activities under their responsibility;
- identification and management of risk within their scope of competence;
- management of the efficiency and effectiveness of the processes for which they are responsible,
- management of human, material and financial resources under their responsibility in a legal, regular, economic and effective manner;

5.4 Does the oversight body conduct appraisals of the management accountable for the IC responsibilities?

5.5 Are the personnel's annual objectives meaningful, sufficiently challenging and accepted by the management?

5.6 Are the personnel's appraisals used effectively by both managers and personnel as a means to improve performance?

5.7 Does the management appropriately address cases of both outstanding performance and underperformance?

5.8 Does the personnel receive concrete, useful feedback that helps them to improve?

5.9 Is the promotion process properly documented and based on the comparative merits of eligible personnel, taking into account the results of their appraisal reports?

5.10 Does management evaluate the pressure on personnel and adjust excessive pressures (e.g. by re-balancing workloads or increasing resource levels) to guarantee that the assigned responsibilities are fulfilled in accordance with the organisation's standards of conduct?

2.2. Risk assessment

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the public organisation are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the public organisation. Management should specify objectives with sufficient clarity to be able to identify and analyse risks to those objectives. Management should also consider the suitability of the objectives for the public organisation. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own mission and responsibilities that may render IC ineffective.

Principle 6: The public organisation specifies suitable objectives

Points of focus:

The establishment of objectives forms the basis on which risk assessment approaches are implemented and performed and subsequent control activities are established.

Management specifies objectives and groups them within broad categories at all levels of the organisation, in relation to operations, reporting and compliance.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

Operations objectives:

- reflect management's choices
- consider risk tolerance
- include operations and financial performance goals
- form a basis for committing resources

External financial reporting objectives:

- comply with applicable accounting standards
- consider materiality
- reflect the public organisation's activities

External non-financial reporting objectives:

- comply with externally established standards and frameworks
- consider the required level of precision
- reflect the public organisation's activities

Internal reporting objectives

- reflect management's choices
- consider the required level of precision
- reflect the public organisation's activities

Compliance objectives

- reflect external laws and regulations
- consider risk tolerance

Examples of mechanisms:

- The public organisation's management sets out several clear and well-conceived objectives, each supported by initiatives and criteria (e.g. implement three public engagement activities for greenhouse gas reduction within the next twelve months). The public organisation's objectives may have less financial emphasis, but still pursue goals related to revenue, liquidity and spending.
- Operations objectives are driven by public policy and priorities, public organisation's mission and strategy.
- External reporting objectives are driven primarily by laws, rules, regulations, and standards established by the regulators, standard-setting or accounting bodies.
- Internal reporting objectives are driven by the public organisation's strategic directions, and by reporting requirements and expectations established by management to support decision making and monitoring of the organisation's activities and performance.
- Compliance objectives integrate the minimum standards of conduct established by the laws and regulations.

Set of questions for the principle:

6.1 Has the public organisation specified the objectives with sufficient clarity, distinguishing between the strategic and operational objectives, to enable the identification and assessment of risks that threaten the achievement of objectives? Are entity-level objectives and associated sub-objectives specific, measurable, attainable, relevant and time-bound (SMART)?

6.2 Are entity-level objectives linked to more specific sub-objectives that cascade throughout the organisation?

Operations objectives:

6.3 Are the operational objectives of the public organisation aligned with the national / sector strategies and policies as well as the organisation's vision and mission? Is the strategic plan of the public organisation consistent with the overall medium-term budgetary framework?

6.4 Do the operations objectives reflect the level of operations and financial performance required by the public organisation?

6.5 Does the management consider what levels of variation relative to the achievement of operations objectives are acceptable?

6.6 Does management use its operations objectives as a basis for allocating the resources needed to attain the desired operations and financial performance?

External financial and non-financial reporting objectives:

6.7 Does management establish external reporting objectives consistent with laws and regulations, or standards and frameworks of recognised external organisations?

6.8 Are the financial reporting objectives consistent with the accounting principles suitable and available for that public organisation? Are the accounting principles selected appropriate in the circumstances?

6.9 Does the management consider materiality in its financial statement presentation?

6.10 Does management reflect the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in non-financial reporting?

6.11 Does external reporting reflect the underlying transactions and events within a range of acceptable limits?

Internal reporting objectives:

6.12 Does internal reporting provide management with accurate and complete information regarding management's choices and information needed in managing the public organisation?

6.13 Does management reflect the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives?

6.14 Does internal reporting reflect the underlying transactions and events within a range of acceptable limits?

Compliance objectives:

6.15 Are laws and regulations which establish minimum standards of conduct integrated into the public organisation's compliance objectives?

6.16 Does management consider what levels of variation relative to the achievement of compliance objectives are acceptable?

Principle 7: The public organisation identifies and analyses risk

Point of focus:

The public organisation identifies risks to the achievement of its objectives across the organisation and analyses these risks to determine how they should be managed.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- risk identification and analysis at public organisation, division, operating unit, and function levels
- analysis of both internal and external factors
- involvement of appropriate levels of management
- estimation of the significance of the risks identified
- determination of how to respond to risks.

Examples of mechanisms:

- Responsibility and accountability for risk identification and analysis processes reside with management at organisational and subunit levels.
- The public organisation establishes effective risk assessment mechanisms that involve appropriate level of management and expertise. Furthermore, the organisation nominates the risk panels and function responsible for risk management, puts in place entity-wide internal procedures and reporting lines to ensure that identification and analysis of risks is an ongoing iterative process conducted to enhance the public organisation's ability to achieve its objectives.
- Risk identification is comprehensive and considers all significant interactions – of goods, services and information – internal to a public organisation and between the entity and the applicable external players, including creditors, suppliers, actors in procurement process, employees, other public bodies, the EC etc.
- Management considers risks at all levels of the organisation, including identifying the risks related to the strategic objectives and the operational objectives.
- The organisation establishes a methodology for risk analysis. This process usually includes assessing the likelihood of the risk occurring and estimating its impact.
- Performance measures / indicators are used to determine the extent to which objectives are being achieved, and normally the same or a congruent unit of measure is used when considering the potential impact of a risk on the achievement of a specific objective (e.g. number of complaints, number of reported irregularities, etc.)
- Management takes the necessary actions to respond to risks by applying judgement based on assumptions about the risk and reasonable analysis of costs associated

with reducing the level of risk. Risk responses fall into the following categories: acceptance, avoidance, reduction, sharing. Typically, control activities are not needed when a public organisation chooses to accept or avoid a specific risk.

- Risk identification, analysis and selected risk management activities are documented in the risk registers and action plans.

Set of questions for the principle:

7.1 Has an organisation established risk assessment mechanisms, including a risk management function and risk panels?

7.2 Does the public organisation identify and assess risks at the entity, division, operating unit, and functional levels relevant to the achievement of objectives? Are both management and the various structural units involved in the process? Are the risks properly documented?

7.3 Is risk identification and analysis a regular process embedded in the public organisation's activities? Are there personnel allocated to follow up on the reported risks?

7.4 Is the risk register regularly updated and used in daily management? Do the identified risks mirror the organisation's objectives? Are the critical risks clearly distinguishable?

7.5 Does risk identification consider both internal and external factors and their impact on the achievement of objectives?

7.6 Are identified risks analysed through a process that includes estimating the potential significance of the risk?

7.7 Have the performance measures / indicators been used to determine the extent to which objectives are being achieved and potential impact of a risk on the achievement of a specific objective?

7.8 Is the management / risk panel assessing at reasonable intervals the risks that have been identified by various organisational structures throughout the year?

7.9 Does risk assessment include considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk?

7.10 Has the management established accountabilities for controlling specific risks? Are action plans developed to ensure the risks are appropriately managed?

7.11 Have the reporting lines been established for various stakeholders on identified risks, their mitigation or realisation?

7.12 Is appropriate monitoring of the results of actions taken to mitigate risk in place? Is the management held accountable for identifying and managing the risks to the achievement of objectives?

Principle 8: The public organisation assesses fraud risk

Point of focus:

The public organisation considers the potential for fraud in assessing risks to the achievement of objectives.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- consideration of various types of fraud
- assessment of incentive and pressures
- assessment of opportunities
- assessment of attitudes and rationalisations.

Examples of mechanisms:

- Risk assessment includes management's assessment of risks relating to the fraudulent reporting and safeguarding of assets. Possible acts of corruption, both by the public organisation's personnel and outsourced service providers (including the various actors participating in the public procurement process) are considered.
- As part of the risk assessment process, management considers various ways fraudulent reporting can occur:
  - management bias and ability to manipulate information,
  - degree of estimates and judgements used in reports,
  - fraud schemes and scenarios common in the industry,
  - incentives for fraudulent behaviour,
  - unusual and complex transactions subject to significant management influence,
  - vulnerability to management overrule and potential schemes to circumvent existing control activities, etc.
- With regard to risks relating to the safeguarding of assets, the following shall be considered: inappropriate use of the public organisation's assets and other resources, including intellectual property, and preventing loss through theft, waste or neglect.
- The risks considered in relation to corruption include incentives and pressures to achieve objectives while demonstrating adherence to expected standards of conduct and the effect of the control environment (especially Principles 4 and 5).

Set of questions for the principle:

8.1 Is fraud risk assessment an integral part of the regular risk assessment process?

8.2 Does the public organisation periodically carry out an assessment of its exposure to fraudulent activity and how operations could be impacted? Does this assessment include each of the public organisation's structural units?

8.3 Does the assessment of fraud consider:

- fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur;
- incentives and pressures;
- opportunities for unauthorised acquisition, use, or disposal of assets, altering of the public organisation's reporting records, or committing other inappropriate acts?

8.4 Does assessment of fraud risk consider how management and other personnel might engage in or justify inappropriate actions?

8.5 Is regular reporting and monitoring in place in the public organisation on its exposures to fraud?

Principle 9: The public organisation identifies and analyses significant changes

Point of focus:

The organisation identifies and assesses changes that could significantly impact the system of IC.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- assessment of changes in the external (regulatory, economic, physical) environment
- assessment of changes in the public organisation's mission and structure
- assessment of changes in leadership.

Examples of mechanisms:

- Management establishes a process to identify and assess those internal and external factors that could significantly affect the public organisation's ability to achieve its objectives, including putting in place controls to identify and communicate significant changes that could affect the organisation's objectives. This process operates either in parallel, or as part of, the public organisation's risk management process.
- The risk identification process considers:

  - changes to the regulatory, economic and physical environment in which the public organisation operates;

  - potential impacts of new organisational structures, significant alterations of old organisational structures, new subordinate organisations;

  - changes in management and respective attitudes and philosophies on the IC system.
- Management puts in place early warning systems to signal new risks that could have a significant impact on the public organisation. There are controls in place to identify and communicate such changes.
- The management assesses the risks associated with the significant changes. Analysis of significant changes includes identifying potential causes of achieving or failing to achieve an objective, assessing the likelihood that such causes will occur, evaluating the probable effect on achievement of the objectives, and considering the degree to which the risk can be managed.

Set of questions for the principle:

9.1 Does the public organisation have mechanisms in place to identify and react to risks presented by changes to the government, regulatory, economic, and physical environment in which the public organisation operates? Does it consider the expectations of the various stakeholders?

9.2 Does the organisation consider:
- the potential impacts of reorganisation, new organisational units and / or dramatically altered compositions of existing structures on the system of IC;
- changes in management and respective attitudes and approach to the system of IC?

9.3 Are controls and an early warning system in place to identify information signalling new risks that could have a significant impact on the public organisation?

9.4 Does the organisation assess the risks associated with significant changes? Has the public organisation assessed the likelihood and impact the significant changes may have on achievement of objectives and IC? Have the causes and effects on the achievement of objectives due to the significant change been identified and evaluated?

2.3. Control activities

Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the IC system, which includes the public organisation's information system.

Principle 10: The public organisation selects and develops control activities

Point of focus:

The public organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- integration with risk management
- consideration of entity-specific factors
- determination of relevant processes
- evaluation of a mixture of control activity types
- design of control activities at various levels
- addressing the segregation of duties.

Examples of mechanisms:

- Along with assessing the risks, the management identifies and puts in place control activities in order to respond to specific risks.
- The control activities support the meeting of objectives, the safeguarding of assets and ensuring completeness, accuracy and validity of information collected and reported by the public organisation.
- When determining what actions to put in place to mitigate risks, all aspects of the public organisation's IC components and processes, information technology, and locations where control activities are needed, are considered.
- The control activities are in general classified under the following categories:

  - Transaction control activities may be preventive or detective and may include, but are not limited to: authorisations and approvals, verifications, physical controls, controls over standing data, reconciliations and supervisory controls.

  - Performance (or analytical) reviews include comparison of operating or financial data, and may include performance review of the procurement process, reviews of actual performance versus budgets, forecasts, prior periods, financing needs, loans etc.

  - Segregation of duties generally entails dividing the responsibility for recording, authorising and approving transactions, and handling the related asset.

Set of questions for the principle:

10.1 Has management established a system where the personnel is systematically selecting and developing appropriate control activities?

10.2 Has management determined which relevant processes require control activities? Are both operational processes (those aligning with public organisation's mission) and horizontal processes (including budgeting, investment and public procurement, payment and treasury functions, asset management, accounting, and human resource management) considered?

10.3 Regarding the control activities:

- Have they been documented in the form of process maps and / or internal procedures (addressing the organisation's own processes for fulfilment of its mission and objectives)?
- Are they aligned with applicable legislation and guidelines from external oversight bodies (including budget and treasury departments, budget inspection, central procurement office, etc.)?
- Do they consider the effect of the environment, complexity, nature, and scope of the organisation's operations, as well as the specific characteristics of the organisation, and control activities have been selected and developed accordingly?
- Do they include a range and variety of controls, considering both manual and automated controls, and preventive and detective controls?
- Are they established at various levels of the public organisation?
- Are they regular? If ad hoc, have they been authorised by the responsible management?

10.4 Do the control activities help ensure that risk responses that address and mitigate risks are carried out?

10.5 Before any transaction is authorised or report/communication approved, are the aspects of this transaction verified by at least one member of personnel other than the one(s) who initiated the transaction? (For the same file the same person cannot do initiation and verification – the 'four eyes' principle).

10.6 Is there evidence of active and regular supervision by the management?

10.7 Are incompatible duties segregated, and where such segregation is not practical, are alternative control activities selected and developed?

Principle 11: The public organisation selects and develops general control activities over technology

Point of focus:

The public organisation selects and develops general control activities over technology to support the achievement of objectives.

Attributes:

The following contribute to the design, implementation, and operational effectiveness of this principle:

- design of appropriate control mechanisms for the public organisation's information technology system
- design of control activities for the information technology infrastructure
- design of security management process control activities
- design of information technology acquisition, development, and maintenance process control activities.

Examples of mechanisms:

- Processes are put in place to select, develop, operate, and maintain the public organisation's technology.
- General technology controls include control activities over the technology infrastructure, security management, and technology acquisition, development and maintenance. They apply to all technology from information technology applications, to desktop and mobile device environments, to operational technology (such as manufacturing robotics).
- Technology infrastructure (e.g. communication networks, electricity to power the technology) is actively checked for problems and corrective action taken when needed.
- Security control activities are in place to limit access to the system to only those who need it, reducing the possibility of unauthorised edits to the files. They generally cover access rights to the data, operating system (system software), network, application, and physical layers. While user access to technology is generally controlled through authentication control activities, general technology controls are designed to allow only authorised users on an approved list. These control activities generally employ a policy of restricting authorised users to the applications or functions commensurate with their job responsibilities and supporting an appropriate segregation of duties. A periodic review of access rights against the policy is often used to check if access remains appropriate.
- General technology controls over the acquisition and development of technology are deployed to help ensure that automated controls work properly when first developed and implemented and to help IC continue to function properly after they are implemented. For example, technology development methodology provides a

structure for system design and implementation, outlining documentation requirements, approvals and checkpoints with controls over acquisition, development and maintenance of technology.

- For maintaining technology, backup and recovery procedures as well as disaster recovery plans are used, depending on the risks and consequences of a full or partial outage.
- Control activities over any changes to the technology help ensure that it continues to function as designed.

Set of questions for the principle:

11.1 Does management understand and determine the dependency and linkage between the public organisation's processes, automated control activities, and general technology controls?

11.2 Does management select and develop control activities:

- over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing?
- that are designed and implemented to restrict technology access rights (both physical access and electronic access) to authorised users at all levels commensurate with their job responsibilities, and to protect the public organisation's assets from external threats?

11.3 Does management select and develop control activities over the acquisition, development and maintenance of technology and its infrastructure to achieve management's objectives?

11.4 Are adequate security procedures (IT and otherwise) in place so that assets and data are kept secure from unauthorised interference and physical damage?

11.5 Are the procedures for continuity of operations in place to ensure that significant risks to continuity (e.g. concerning loss of data, absence of individuals etc.) are identified and contingency plans put in place?

Principle 12: The public organisation deploys control activities through policies and procedures

Point of focus:

The public organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

Attributes:

The following contribute to the design, implementation, and operational effectiveness of this principle:

- documentation of responsibilities through policies
- periodic review of control activities

Examples of mechanisms:

- The public organisation may first establish a policy describing management's views of what should be done to effect control. Accordingly, the procedures consist of actions that implement that policy.
- Control activities specifically relate to those policies and procedures that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. For example, a policy (e.g. business continuity policy) might indicate the fields that trigger control activities. The procedure is the description of how the control activity is performed in a timely manner and with attention given to the factors set forth in the policy.
- The public organisations' policies and procedures may be communicated orally or in written and should consider the minimum requirements set out in the legislation.
- Policy and procedure must establish clear responsibility and accountability, which ultimately resides with the management of the public organisation and subunit where the risk resides, as well as providing clear responsibilities for personnel performing the control activity.
- The procedures should include the timing of when a control activity and any follow-up corrective actions are performed.
- In conducting a control activity, matters identified for follow-up should be investigated and, if appropriate, corrective action taken. In cases where the controls are described in the form of a checklist, the results of any control activity and corresponding corrective actions shall be described in the checklist.
- To conduct a control activity, the personnel should be competent and have sufficient authority to perform the control activity.
- When performing a control activity, the personnel should focus on the risks to which the policy is directed.
- Significant changes (in people, process, and technology) should be evaluated through the risk assessment process as they may reduce the effectiveness of control

activities or make some control activities redundant. Management should reassess accordingly the relevance of the existing controls and refresh them when necessary.

Set of questions for the principle:

12.1 Has management established control activities that are built into the processes of the public organisation and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions?
12.2 Has management established responsibility and accountability for control activities with the management (or other designated personnel) of the organisational units in which the relevant risks reside?
12.3 Do responsible personnel perform control activities in a timely manner as defined by the policies and procedures?
12.4 Do competent personnel with sufficient authority perform control activities with diligence and continuing focus?
12.5 Do responsible personnel investigate and act on matters identified as a result of executing control activities?
12.6 Has management periodically reviewed control activities to determine their continued relevance, and refreshed them when necessary?

2.4. Information and communication

The management of a public organisation uses quality information to support the IC system. Effective information and communication are vital for a public organisation to achieve its objectives. The management needs access to relevant and reliable communication related to internal as well as external events.

Principle 13: The public organisation obtains, generates and uses relevant, quality information

Point of focus:

The public organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- identification of information requirements
- capture of internal and external sources of data
- process relevant data into information
- maintenance quality throughout processing
- consideration of costs and benefits

Examples of mechanisms:

The public organisation management:

- defines the identified information requirements at the relevant level and necessary specificity for appropriate personnel,
- identifies information requirements in an iterative and ongoing process that occurs throughout an effective IC system,
- obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements,
- evaluates both internal and external sources of data for reliability,
- evaluates if the information provided is of the required quality, in particular whether it is: appropriate, current, complete, accurate, accessible, and provided on a timely basis.

Set of questions for the principle:

13.1 Has the management of the public organisation defined and identified the information requirements at the relevant level and necessary specificity for appropriate personnel?
- Are these requirements defined based on the results provided by the IC system (e.g. information on the mechanism of controls, risk, system deficiencies;
- Where possible, is there a clear link to the public organisation's objectives?

13.2 Does the management of the public organisation receive relevant information/data from reliable internal and external sources in a timely manner, based on the identified information requirements?

13.3 Does the management of the public organisation evaluate whether the information provided by both internal and external sources is:

- reliable,
- of good quality, and in particular if it is: appropriate, current, complete, accurate, accessible, and provided on a timely basis.

Principle 14: The public organisation ensures proper internal communication

Point of focus:

The public organisation internally communicates the information, including objectives and responsibilities for internal control, needed to support the functioning of IC.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- communication of IC information
- communication with the oversight body
- provision of separate communication lines
- selection of the relevant method of communication

Examples of mechanisms:

The public organisation management:

- receives quality information about the public organisation's operational processes that follows the reporting lines to help management achieve the public organisation's objectives,
- selects appropriate methods to communicate internally considering a variety of factors including:
  - audience - the intended recipients of the communication,
  - nature - the purpose and type of information being communicated
  - availability - information readily available to the audience when needed
  - cost - the resources used to communicate the information
  - legal or regulatory requirements - laws and regulations that may impact communication
- The oversight body receives quality information from the management and the personnel that flows up the reporting lines,
- The personnel can use alternative reporting lines to go around upward reporting lines when these lines are compromised (e.g. whistle-blower and ethics hotlines, for communicating confidential information).

Set of questions for the principle:

14.1 Have the current arrangements used for internal communication been analysed?

14.2 Are arrangements in place to ensure that the management and personnel of the public organisation are informed of other units' decisions/projects/initiatives that may affect their responsibilities and tasks?

14.3 Are there any recent examples where flaws in internal communication have caused problems or impacted on the public organisation's performance?
- Have the underlying causes been analysed?
- Have measures been taken to prevent similar communication issues in the future?

14.4 Does the oversight body receive the quality information that flows up the reporting lines from management and personnel?

14.5 Can the personnel use an alternative reporting line to go around upward reporting lines when these lines are compromised (e.g. whistle-blower and ethics hotlines, for communicating confidential information)?

14.6 Are the management and personnel of the public organisation sufficiently aware of the information systems security policy?
- Is information system security a regular topic at management meetings?
- Are objectives for information security established and monitored?
- Do results of the regular supervision of IT systems, audit findings or information from other sources suggest that there may be IT-security-related issues?
- Are these issues escalated to and discussed at the appropriate management level?

14.7 Is feedback from IT users regarding system performance collected and analysed to detect the potential effectiveness and efficiency deficiencies?
- Are statistics on IT system performance indicators regularly analysed?
- Are IT system performance issues reported to the appropriate management level?

Principle 15: The public organisation ensures proper external communication

Point of focus:

The public organisation communicates with external parties regarding matters affecting the functioning of IC.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- communication with external parties
- facilitating inbound communication
- communication with the oversight body
- provision of separate communication lines

Examples of mechanisms:

The public organisation management:

- communicates with, and obtains quality information from external parties, using established reporting lines on the achievement of the public organisations objectives and the risks associated with them,
- receives and assesses the information from concerned parties on significant matters relating to risks, changes, or issues that impact the pubic organisation's IC system,
- selects appropriate methods to communicate internally considering a variety of factors such as:
  - audience - the intended recipients of the communication,
  - nature - the purpose and type of information being communicated
  - availability - information readily available to the audience when needed
  - cost - the resources used to communicate the information
  - legal or regulatory requirements - laws and regulations that may affect communication
- The oversight body receives the quality information from external parties concerning any significant matters relating to risks, changes, or issues that impact the public organisation's IC system.

Set of questions for the principle:

15.1 Have the current procedures and methods used for external communication been analysed to identify their strengths and weaknesses, including cost-benefit aspects?

15.2 Does the public organisation's management receive and assess the information from concerned parties about significant matters relating to risks, changes, or issues that impact the pubic organisation's IC system?

15.3 Does the public organisation's management seek and analyse feedback from target audiences (e.g. main stakeholders, citizens, business partners) regarding the impact of its communication?

- is the information obtained reliable and pertinent?
- is relevant feedback escalated to the appropriate level and used to adapt ongoing communication strategies?

15.4 Does the oversight body receive the quality information that flows up the reporting lines from management and personnel?

2.5. Monitoring activities

Monitoring of the IC system is essential to ensure that IC remains aligned with changing objectives, environment, laws, resources, and risks. IC monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews.

Corrective actions are a necessary complement to control activities in order to achieve objectives.

Principle 16: The public organisation selects, develops and performs ongoing and/or separate evaluations

Point of focus:

The public organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of IC are present and functioning.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- consideration of a mixture of ongoing and separate evaluations
- consideration of the rate of change
- establishment of a baseline understanding
- use of knowledgeable personnel
- integration with business processes
- adjustments to scope and frequency
- objective evaluation

Examples of mechanisms:

The public organisation's management:

- Establishes a baseline against which to monitor the IC system. Once established, the management can use the baseline criteria to evaluate the IC system and make changes to reduce variances from these. The management can reduce these variances in one of two ways: either by changing the design of the IC system to better address the objectives and risks of the organisation or by improving the operational effectiveness of the IC system.
- Monitors the IC system through ongoing monitoring and separate evaluations. Ongoing monitoring is built into the public organisation's operations, continuous, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring. They may also include audits and other evaluations that might include the review of control design and direct testing of IC.
- Evaluates and documents the results of ongoing monitoring and separate evaluations to identify IC issues, in particular deficiencies.
- Identifies changes in the IC system that either have been carried out or are needed because of changes in the organisation and its environment.
- The IA function is carrying out regular specific assessments to provide senior management with an independent review of the subordinate systems.

Set of questions for the principle:

26.1 Are evaluation activities appropriately organised and resourced to meet their purposes?

26.2 Does the public organisation's management plan the evaluation activities in a transparent and consistent way so that relevant evaluation results are available in due time for operational and strategic decision-making and reporting needs?

26.3 Do evaluation activities provide reliable, robust and complete results?

- Are the evaluation reports used by management in practice, i.e. do they have a real impact on the public organisation's decision-making or the policy and legislative proposals prepared? If not, why?
- is development and performance of on-going and specific monitoring ensured, to ascertain that the components of IC are present and functioning at all levels?

26.4 Are evaluation results communicated in such a way that they ensure maximum use of the results and that they meet the needs of decision-makers and stakeholders?

26.5 Do the public organisation's managers and personnel participating in self-assessments of the organisation's IC systems have a sufficient understanding of IC and risk management?

- If not, what is done to avoid misinterpretations or misunderstandings that could affect the results and conclusions they reach?

26.6 Is the self-assessment well organised, pragmatic and value adding (or is it regarded as a "bureaucratic burden")? Is it sufficiently supported by senior management of the public organisation ("tone at the top")?

26.7 Is the self-assessment focused on the public organisation's main activities, objectives and risks?

26.8 Are the self-assessment results and conclusions sufficiently supported by reliable and accurate evidence, for example via references to other relevant sources?

26.9 Does the public organisation's management identify changes in the IC system that have either taken place or are needed because of changes in the organisation and its environment?

26.10 Is the IA function carrying out regular specific assessments to provide senior management with independent review of the subordinate systems?

Principle 17: The public organisation evaluates and communicates deficiencies

Point of focus:

When the IC deficiencies are identified, the management of the public organisation should take corrective action and communicate this to the appropriate level of authority in a timely manner.

Attributes

The following contribute to the design, implementation, and operational effectiveness of this principle:

- assessment of results
- communication of deficiencies
- monitoring of corrective actions

Examples of mechanisms:

- Personnel report IC issues through established reporting lines to the appropriate internal and external parties in a timely manner to enable the public organisation to promptly evaluate those issues.
- Management evaluates issues identified through monitoring activities or reported by personnel to determine whether any of the issues constitute an IC deficiency.
- Management evaluates and documents IC issues and determines appropriate corrective actions in a timely manner.
- Management completes and documents corrective actions to correct IC deficiencies in a timely manner.
- Management, with oversight from the oversight body, monitors the status of corrective actions taken so that they are completed in a timely manner and bring the expected result.

Set of questions for the principle assessment:

27.1 Does the personnel report IC issues through established reporting lines to the appropriate internal and external parties in a timely manner to enable the public organisation to promptly evaluate those issues?

27.2 Does the public organisation's management take adequate and timely actions to analyse and correct deficiencies reported by the personnel, IA function, financial and non-financial internal and external monitoring activities?

27.3 Does the public organisation's management monitor the status of corrective actions taken so that they are completed in a timely manner and bring the expected result (e.g. the recommendations of the IA or results of monitoring activities)?

Annex 1: Model checklist for IC quality assessment for central harmonisation units

The list of questions, sources of evidence and methods for assessing IC quality presented in this Annex is comprehensive but not exhaustive. It should be adjusted to the specific circumstances of the administration, in particular, the strategic and operational objectives, the stage of implementation and maturity of the IC system, specificities of the sector and public organisation, the results of risk assessment conducted and the available resources.

CHUs are encouraged to use the Model Checklist for developing the self-assessment questionnaires and the IC quality review checklist. The scope of the self-assessment questionnaires and IC quality review checklists should correspond to the current maturity and stage of development of the IC system in the specific administration.

Control environment

Principle 1: The public organisation demonstrates a commitment to integrity and ethical values

No.	Questions for the principle assessment	Main sources of evidence	Data collection and analysis methods
1	Is the management's commitment to integrity and ethical behaviour communicated effectively throughout the public organisation, both in words and actions?	- evidence confirming that the senior management supports the expected standards of conduct and that they are consistent throughout the public organisation; - examples of awareness meetings and sessions with staff on the subject of integrity and ethical behaviour , - written contribution by management in the form of a clear statement of commitment to ethical behaviour and to	- interviews with the senior management, stakeholders and staff of the public organisation, - staff survey on integrity and ethical behaviour in the public organisation, - review of the related internal and external communication; - assessment of reputational events, cases of the policy violations and other dubious-sounding statements.
2	Does senior management lead by example?		
3	Is the tone set by the high-level management communicated through to various operating units?		

		promote awareness of fraud, - documentation of the reputational events and their consequences,	
4	Is there a code of conduct and/or ethics policy and has it been adequately communicated to all levels of the public organisation? If yes, does it provide standards to guide the public organisation's behaviours, activities and decisions?	- The public organisation's code of conduct, - Database/ register listing the employees and the date of their review and acceptance or non-acceptance of the code of conduct and/or ethics policy , - record of training, briefings and awareness sessions, - Q&A page regarding the code of conduct and/or ethics policy, good practice examples, - Information on cases/ incidents regarding e.g.: use of the public organisation data for personal gain, receiving bribes and improper gifts, giving favours to suppliers, problematic family member-employee relationships, conflicts-of interests, improper influence, - Information on cases/ incidents regarding e.g.: misuse of the public entity assets, data and information, - Human resource procedures regarding violations of the code of conduct and/or ethics policy	- Structured interviews with the senior management, stakeholders and staff of the public organisation, - interviews with HR and training units, - staff survey on integrity and ethical behaviour in the public organisation, - review of training materials and presentations, - qualitative and quantitative analysis of reputational events, cases of the code of conduct and/or ethics policy violations, - analysis of the register for sensitive posts e.g the one responsible for contracts with, purchases from or sales to Government Departments/Offices), - discussion on the information security incidents,

5	Does the public organisation have a training programme dedicated to integrity and ethical behaviour?	- Training records, plans/ programmes, targeted audience, - Training materials and presentations	- interviews with the senior management, stakeholders and staff on the quality of training, - qualitative and quantitative assessment of the number, frequency, scope and coverage of the training programme dedicated to integrity and ethical behaviour
6	Do dedicated complaints mechanisms exist for corruption, if yes: - Do these systems offer adequate levels of anonymity and protection to complainants? - Is whistle-blowing broadly defined? - Can disclosures be made with a reasonable belief that the information is true at the time it is disclosed? - Are protections for whistle-blowers clear and comprehensive?	- Code of conduct and/or ethics policy, documentation on the reporting lines regarding the complaints for corruption, - Documentation of the communication and training efforts regarding internal whistle-blower and compliance programmes, - Evidence demonstrating the public organisation's ability to conduct a thorough and fair internal investigation (e.g., being able to present written guidelines for conducting an investigation and maintaining records regarding the timeliness of, and conclusions reached in, prior investigations);	- Review the public organisation code of conduct to address any potential inconsistencies with the whistle-blower rules (e.g., provisions for possible disciplinary action in the event employees do not report all violations of law in the first instance to the public organisation, protection of whist-blowers); - comprehensive review of all existing whistle-blower and compliance programmes, including any up-the-line financial reporting process, to confirm that they are effective and result in timely reports of possible violations of law to management and to the audit or other oversight body,
7	Does the public organisation have a process to evaluate the performance of personnel and teams against its code of ethics?	- Human resource procedures regarding the performance and potential cases of violations of the code	- interviews with management, HR and business units,

8	Does the high-level management determine the tolerance level for deviations from certain expected standards of conduct?	of conduct and/or ethics policy	- analysis of the cases of deviations and the corrective actions introduced.
Principle 2: The public organisation exercises oversight responsibility			
1	Does the oversight body[19] exercise oversight responsibilities independent from the management?	- The internal regulations on the oversight responsibilities - The charter/ procedures of the institution that exercises the oversight responsibilities	- Review of the composition, structure and activities of the institution that exercises the oversight responsibilities, - Analysis of the professional background and experience and training records of the members of the institution that exercises the oversight responsibilities, - Interviews with the public organisation management, internal audit and members of the institution that exercises the oversight responsibilities on its the scope of work and annual objectives,
2	Does the oversight body consist of members that have diverse, complementary backgrounds and specialised skills to enable discussion, offer constructive criticism to management, and make appropriate oversight on the internal control?	- The charter/ procedures of the institution that exercises the oversight responsibilities, including the requirements regarding its composition, the competency framework of its members and letters of appointment, and defined role of the Chair.	
3	Do the members of the oversight body understand the public organisation's objectives, its related risks, and the expectations of its stakeholders?		
4	Does the oversight body oversee the management's design, implementation, and operation of the public organisation's internal	- The charter/ procedures of the institution that exercises the oversight responsibilities	- Review of the reports and communications of the institution that exercises the oversight responsibilities,

[19] The oversight body is used in the following context:

- Within the public sector, it is the first-level budget user (e.g. the ministry of agriculture) which oversees their subordinate structures or organisations (e.g. the land agency);
- Within the public organisations, the oversight body may be a board of directors (e.g. for the state-owned enterprises), an audit or risk committee or other body, which is independent from the management of a public organisation.

	control system (all components)?	defining its role and scope, - Annual work plans, minutes of the meetings, implementation reports, reports on the follow up actions, annual report to the head of the public organisation.	- Interviews with the main stakeholders on the actual performance of the oversight conducted, in particular focused on: - Membership, procedures and resources, - Roles and responsibilities, - Relations with the head and management of public organisation, - Skills and understanding, - Analysis of the performance of the institution that exercises the oversight responsibilities, based on the review of the minutes of its meetings, reports and recommendations produced, reporting and communication to the head and management of the public organisation, - Analysis of the summary reports of the follow up actions provided by internal and external auditors, - Analysis of the Annual reports of the of the institution that exercises the oversight responsibilities, - Interviews with the members of the institution that exercises the oversight responsibilities on the significant deficiencies in the internal control system of the public organisation and the corrective actions taken,
5	Are the activities of the oversight body sufficiently focused on high-risk areas? (e.g. - complex operations; - transactions of high monetary value; - low control consciousness among personnel; - lack of experienced or skilled personnel; - reorganisation or significant modification of operating activities; new IT systems; - potential conflicts of interest or influence from external parties; - activities of a politically sensitive nature)		
6	Is there systematic follow-up of significant issues identified?	- Agendas, minutes of meetings and follow up notes, of the institution that exercises the oversight responsibilities, - Annual reports, reports on the deficiencies in the internal control system of the public organisation, risk registers, - Oversight body self-assessment questionnaires,	
7	If subordinate organisations are responsible for carrying out corrective actions, has appropriate supervision or follow-up been established by the responsible budget users?		
8	Is the oversight of operational performance based on the public organisation's objectives and related performance indicators?		
9	Are all reported internal control weaknesses properly analysed and addressed where necessary?		

10	Does the oversight body provide input to the management's plan for corrective actions when deficiencies in the internal control system appear?		
Principle 3: The public organisation establishes structures, reporting lines, authorities and responsibilities			
1	Does the organisational chart of the public organisation define the lines of authority and responsibility?	- Organisational chart - Internal and external rules and laws, - Minutes of the management meetings, - Procedures and laws change register ,	Analysis of the organisation chart to conclude if it clearly defines the lines of authority and responsibility, in particular if it: - Sets out assignments of authority and responsibility, - Ensures that duties are appropriately segregated, - Establishes reporting lines and communication channels, - Defines the various reporting dimensions relevant to the public organisation, - Identifies dependencies for roles and responsibilities involved in financial and non-financial reporting, Assessment of the potential overlaps in the responsibilities of the subsequent units in the public organisation. Review of the procedure change register to check of the delegated and sub-delegated budget users have received and acknowledged the organisational chart and assigned responsibility.
2	Is the organisational chart up to date?		
3	Have the management responsibilities for the implementation of the public organisation's objectives and risk management been defined?	- Organisational chart - Job descriptions - Risk management policy	Analysis of the KPIs and BPIs. Minutes of the management meetings concerning the discussion on the risk of the achievement public organisation objectives. Analysis and the comparison of the management plan and the

			annual implementation reports (including the annual cctivity reports).
4	Does the public organisation's management delegate authority? Does it and use appropriate processes and technology to assign responsibility and segregate duties as necessary, at the various levels of public organisation?	- Organisational chart - Management Plans and objectives - Annual and mid-term financial and operational reporting,	Assessment of the internal rules of procedures. Review of the delegation of the authority and the reporting lines.
5	Are the nature and scope of delegated functions and powers clear to all persons concerned?		Analysis of the extent of delegation and the confirmation of its acceptance.
6	Are the risks associated with the delegated functions and powers sufficiently analysed?		Review of the risk registers. Mapping in a matrix format of the controls identified during the audit
7	Has the public organisation's management established and evaluated the reporting lines within the public organisation and with the other organisations to enable the execution of authority, fulfilment of responsibilities, and flow of information?		Analysis of the internal rules regarding the responsibility, timelines, accuracy and reliability of the reporting.
8	Does the public organisation conduct an evaluation of the organisational structure to assess how it supports the achievement of its objectives?	- Self-assessment questionnaire (organisational efficiency) - Staff satisfaction survey - Internal and external audit reports	Collection of data through interviews, walkthrough with the public organisation's management and personnel to examine if this kind of evaluation is conducted and what the results are.
Principle 4: The public organisation demonstrates commitment to competence			
1	Have the competences for key roles of the public organisation (regarding the	- Laws on public service (law on civil service/	Interviews with the senior management, staff of the public organisation and HR unit,

	relevant knowledge, skills, and abilities) been defined to enable the personnel to carry out the assigned responsibilities?	civil servants and public employees); - Internal rules defining the competency framework for the employees, job descriptions defining roles and responsibilities, - Strategic and annual management plans, documents defining the operational objectives, - Staff satisfaction surveys, HR profiles and gap analysis. .	Interviews with the representatives of staff organisations, Comparison of staff profiles with the objectives of the public organisation, Analysis of the job descriptions, Interviews with the managers and staff representatives on how the profile and experience of staff employed support the achievement of the public organisation's objectives. Analysis of the staff survey results.
2	Has the existing level of knowledge and skills of the personnel been aligned with the public organisation's strategy/ objectives? Is personnel capable of coping with the everyday challenges and possibilities associated with the given assignments?		
3	Have the recruitment procedures been established to determine whether a particular candidate fits the public organisation's needs and has the competence for the proposed role?	- Recruitment procedures, competency framework, job descriptions.	Assessment of the process of definition of staff needs, Analysis of the recruitment process, its timeline, compliance and effectiveness, Analysis of the evolution of recruitment, age of staff, post and grade categories.
4	Are there any issues or problems related to personnel's recruitment and allocation that significantly affect the public organisation's performance?	- Annual reports on the staff costs and budgetary appropriations, - HR statistics, - Information the staffing levels, staff recruited, - Recruitment files	Analysis of the recruitment process, its timeline, compliance and effectiveness Review of the workforce projections produced by HR units used as a source of information for the planning of future recruitment competitions. Determining the room for manoeuvre in the allocation of human resources. Analysis of significant delays or decreases in the public organisation's performance. Interviews with the senior management and the HR unit of the public organisation.
5	Are the sufficient training opportunities provided to personnel?	- Internal and external rules/procedures	Interviews with the senior management and staff of the

	Has the overall training strategy, aligned to the public organisation's objectives been developed (training plans)?	regarding the training of public servants, - Strategic and annual training/ staff development programme, - Training budget and statistics, - Trainings files and databases, - Annual report on the staff training /development programme	public organisation and the HR training unit, Analysis of the training records and statistics, Assessment of the training availability, Analysis of the staff survey results,
6	Has the public organisation established cross-unit training for significant changes in personnel?		
7	Are sufficient measures taken to analyse and develop personnel's skills and to plan for future HR needs and skill requirements?		
8	Are relevant training statistics available? If yes, is there evidence that personnel is taking the necessary courses in order to build their skills?		
9	Does the public organisation have an environment in place that motivates the personnel to direct their competencies and work towards the achievement of the organisation's strategic objectives?	- Talent, learning and development programmes, - Career management procedures and plans, - Conditions of employment including flexible working arrangements - The results of the staff survey	Analysis and the assessment of the measures introduced by the public organisation to guarantee attractive and motivating environment for staff. Assessment of the career path in the public organisation. Interviews with the management and the staff members on the conditions of employment (e.g. part-time and teleworking possibilities), career path and the learning and development programmes.
10	Are sufficient measures taken to ensure flexible and dynamic organisation, for example via targeted training programmes, re-organisation or other measures?	- Staff mobility arrangements, - Knowledge management programmes, - Job screening documents, - Analysis of any significant gaps between required and available skills and	Comparative analysis of the staff profiles, the public organisation's objectives and the staff development programme, Interviews with the management and staff members.

		competences in the public organisation,	
11	Does the management measure: - the performance of personnel in relation to the achievement of objectives and demonstration of expected conduct, - the performance against service-level agreements or other agreed-upon standards for recruiting and compensating outsourced service providers?	- Annual management plans - Document describing the personnel's annual objectives - Implementation reports/ personnel appraisal reports - SLA agreements with service providers	Analysis of the management practices with regards to performance management Interviews with senior and middle management on performance management Assessment of a sample of the documents describing the personnel's annual objectives and evidence of their implementation Review of the SLA implementation for a sample of outsourced service providers (e.g. for projects of greatest value or reputational risks associated)
12	Are adequate arrangements in place to ensure effective personnel planning and allocation?	- Annual reports on the staff costs, budgetary appropriation, - HR data and statistics, - Information on the staff level, establishment plan post. - Analysis of the workloads	Analysis of the recruitment process, its timeline, and effectiveness Review of the workforce projections produced by HR units used as a source of information for the planning of future recruitment competitions. Analysis of the proportion of the total workforce to check the potential for moving available staff to front-line/ priority activities Review of the HR policies to capture if they promote, implement and monitor staff mobility (e.g. publication of vacant posts, list of specialist posts) in order to ensure that the right person is in the right job at the right time and, where feasible, to create career opportunities, Interviews with the senior management and HR unit of the public organisation.
13	Does management have sufficient and relevant information about priorities and staff workload as well as the required and available skills?		
14	Is staff turnover sufficiently monitored and analysed?	- HR statistics e.g. overall workload data,	Analysis of the HR data,

	Have the specific indicators for "excessive" and "insufficient" personnel's turnover been defined? Are the root causes of any abnormal personnel's turnover sufficiently analysed and addressed?	the overtime data for staff, - Staff survey results - Management reports	Analysis of ratios for "excessive" and "insufficient" staff turnover per unit. Review of the management reports focused on the potential recommendations Review of the staff survey results to capture, in particular, staff perception of organisational efficiency,
15	Has the management defined the succession and continuity plans for key roles to help the public organisation continue achieving its objectives?	- Succession plans, business continuity plans	Review of the HR policies to capture if they promote, implement and monitor staff mobility, Analysis of the succession plans and the business continuity plans. Interviews with the senior management and HR unit of the public organisation.
Principle 5: The public organisation enforces accountability			
1	Has the accountability for the strategic objectives been defined?	Public organisation's internal regulations and rules (e.g. internal organisation rulebook,iInternal rulebook on systematisation), Authorisation for delegation of duties Organisational chart Strategic and operational plans of the public organisation Management plans, KPIs Implementation reports, Annual activity reports	Analysis of the public organisation's internal regulations and rules in order to conclude on how the accountability framework has been defined and if it is transparent, Interviews with the personnel and management of the public organisation on the accountability framework, Comparison of the management plan's objectives, KPIs, with the outcomes and achieved results presented in the implementation, annual activity reports.
2	Has the accountability of the heads of internal units been formally defined in the public organisation's internal regulations and rules (e.g. Internal organisation rulebook, internal rulebook on systematisation)?		
3	Does the accountability of the heads of internal units cover in particular: • achievement of objectives in line with the approved budget, • definition of performance indicators to enable them to report to higher management on the outputs and outcomes and outcomes;		

	• supervision over the implementation of programmes, projects and activities under their responsibility; • identification and management of risk from their scope of competence; • management of the efficiency and effectiveness of the processes they are responsible, • management of human, material and financial resources under their responsibility in a legal, regular, economic and effective manner.		
4	Does the oversight body conduct the appraisals of the management accountable for the internal control responsibilities?	- Minutes of the meetings and the annual reports of the institution that exercises oversight responsibilities	Analysis of the minutes of the meetings and the annual reports of the institution that exercises oversight responsibilities , interviews with its members
5	Are the personnel's annual objectives meaningful, sufficiently challenging and accepted by the management?	- Post and job descriptions, - Internal policies and procedures on the staff appraisal process, - Documents/ information concerning the staff's annual objectives	Analysis of the sample of the staff's annual objectives, Interviews with the management and the staff on the process of defining the objectives and operational indicators Staff survey review concerning the definition of the staff objectives and the management quality.
6	Are the personnel's appraisals used effectively by managers and staff as a means to improve performance?		
7	Does the management appropriately address the cases of both outstanding and underperformance?	- Lists of promotions - Documents concerning the dismissal cases	Taking stock of the staff promotion/ dismissal cases and the review on the sample basis their relation with the results of staff performance

8	Does personnel receive concrete, useful feedback that helps them to improve?	- Documents/ information concerning the staff's appraisal process	Review of the sample of documents/ information concerning the staff appraisal process, with the feedback provided to staff by management Analysis of the staff survey on the quality middle and senior management
9	Is the promotion process properly documented and based on the comparative merit of eligible personnel, taking into account the results of their appraisals?	- Lists of promotions - Documents concerning the dismissal cases	Analysis of staff promotions and the criteria applied, including the justification provided
10	Does the management evaluate the pressure on personnel and adjust excessive pressures (e.g. by rebalancing workloads or increasing resource levels.) to guarantee that the assigned responsibilities are fulfilled in accordance with the organisation's standards of conduct?	- HR workload statistics, staff levels - Data on the overtime charged, - Data indicating significant delays in operational activity - Minutes of the management's meetings	Review and the analysis of the ongoing evaluations of the workloads among the subsequent units of the public organisation, and the following actions aimed at rebalancing workloads or increasing resource levels Review of the risk register in line to identify the risk concerning the sufficiency of the HR Interviews with the representatives of HR unit, management and staff on the excessive pressures

Risk assessment

Principle 6: The public organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

No	Questions for the principle assessment	Main sources of evidence	Data collection and analysis methods
	GENERAL		
1.	Has the public organisation specified the objectives with sufficient clarity, distinguishing the strategic and operational objectives, enabling the identification and assessment of risks that threaten the achievement of objectives? Are entity-level objectives and associated sub-objectives specific, measurable, attainable, relevant and time-bound (SMART)?	- Strategic plans, annual activity plans, investment planning, budget plans and any other existing operations or reporting plans at the level of the public entity and its individual units	- Selection of sample of plans prepared at various levels - Review of the sample as to whether they are sufficiently clear to enable risk identification - Interviews with management and staff responsible for setting objectives at various level and preparing the plans
2.	Are entity-level objectives linked to more specific sub-objectives that apply throughout the organisation?		
	OPERATIONS OBJECTIVES		
3.	Are the operational objectives of the public organisation aligned with the national / sector strategies and policies as well as the organisation's vision and mission? Is the strategic plan of the public organisation consistent with the overall medium-term budgetary framework?	- MoF circular of instructions - Internal procedures and policies on objective setting, reporting and monitoring - Strategic plans, annual activity plans, investment planning and any other existing operations plans at the level of the public entity and its individual organisational units - Budget and procurement plans	- Review MoF circular of instructions for evidence that the macroeconomic and budgetary parameters are clearly outlined - Review of the (above) sample of plans to determine whether they are in line with the organisation's vision and mission as well as with the medium-term budgetary framework assumptions and whether they distinguish between costs for existing policies and costs for new policy initiatives (i.e. additional funding needs)

4.	Do the organisation's operational objectives reflect the desired level of operational and financial performance?	- Evidence of the operations and financial performance goals set for the public organisation, internally and externally - Evidence of the levels of risk tolerance set - Evidence on the monitoring of the achievement objectives, including the set levels of risk tolerance	- Interview with the management to determine how and by whom the performance goals are determined - Review of the sample of plans to determine whether the operations and financial performance goals are reflected within the plans
5.	Does the management consider what level of variation relative to the achievement of operations objectives is acceptable?		- Interview with the management to determine how the acceptable level of risk with regard to objective achievement is determined and monitored - Interviews with the second line of defence whether risk capacity and tolerances are considered and how is the risk tolerance level communicated within the organisation - Review any evidence of the monitoring whether the set risk tolerance levels are applied
6.	Does management use operations objectives as a basis for allocating resources needed to attain desired operations and financial performance?		- Review of the sample of plans to establish the link between the operations objectives, budget and the performance goals - Interviews with the management to attain whether the operations objectives form the basis for committing resources
	EXTERNAL FINANCIAL AND NON-FINANCIAL REPORTING OBJECTIVES		
7.	Does management establish external reporting objectives consistent with laws and regulations, or standards and frameworks of recognised external organisations?	- Legislation on mandatory financial and non-financial reporting - Information on criteria / requirements established by third parties in non-financial reporting	- Review of legislation and other information on requirements for financial and non-financial reporting - Review of internal procedures and policies

8.	Are financial reporting objectives consistent with accounting principles suitable and available for that public organisation? Are the accounting principles selected appropriate in the circumstances?	- Internal procedures on external financial and non-financial reporting - Financial reports, incl. financial statements, budget performance reports, - Audit reports on financial statements	- Structured interviews with the management, accountants and people responsible for setting the financial and non-financial reporting objectives and preparing the reports
9.	Does the management consider materiality when presenting its financial statements?	- Evidence of consideration of materiality in financial statement preparation	- Review financial statements and whether the audit reports are unqualified
10.	Does management meet the required level of precision and accuracy for user needs and based on criteria established by third parties in non-financial reporting?	- Non-financial reports to the government and other external parties	- Review criteria for non-financial reporting and the sample of non-financial reports
11.	Does external reporting reflect the underlying transactions and events within a range of acceptable limits?		
	INTERNAL REPORTING OBJECTIVES		
12.	Does internal reporting provide management with accurate and complete information regarding management's choices and information needed in managing the public organisation?	- Internal procedures and policies on internal reporting - Evidence on objective setting with regard to internal objectives - Evidence on internal reporting	- Interviews with the management at various levels to determine the system of internal reporting objectives and what internal reports exist
13.	Does management reflect the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives?		- Interviews with the staff preparing the reports - Review of the documents determining the objectives regarding internal objectives
14.	Does internal reporting reflect the underlying transactions and events within a range of acceptable limits?		- Review of a sample of internal reports

	COMPLIANCE OBJECTIVES		
15.	Are laws and regulations which establish minimum standards of conduct integrated into public organisation's compliance objectives?	- Applicable legislation - Various plans integrating compliance objectives	- Review of the legislation - Review of the applicable plans - Interviews with the management and 2nd level of defence
16.	Does management consider what levels of variation relative to the achievement of compliance objectives are acceptable?	- Evidence of the set risk tolerance levels	

Principle 7: The public organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.			
No	**Questions for the principle assessment**	**Main sources of evidence**	**Data collection and analysis methods**
1.	Has the organisation established risk assessment mechanisms, including a risk management function and risk panels?	- Legislation establishing the requirements for risk management - Appointments of personnel with responsibilities for risk management function - Internal audit reports on functioning of risk management process - Internal procedures and policies or other evidence on risk management systems and processes within the public organisation	- Review of the legislation, procedures and internal audit reports (if existing) - Interviews with the management and internal audit function - Interviews with thopse responsible for the risk management function, risk panel members
2.	Does the public organisation identify and assess risks at the entity, division, operating unit, and functional levels relevant to the achievement of objectives? Are both management and various structural units involved in the process? Are the risks properly documented?	- Risk register - Memoranda of risk panel meetings - Internal audit reports on functioning of risk management process	- Review of the risk registers, memoranda of risk panel meetings, internal audit reports - Interviews with the management, internal audit function, these responsible for risk management function and with the staff of selected organisational structures
3.	Is risk identification and analysis a regular process embedded in the public organisation's activities? Are personnel allocated to follow up on the reported risks?	- Internal procedures and policies on risk management - Evidence of risk reporting (risk signals) from various organisational structures throughout the year - Evidence on whether the reported risks have been addressed by the specifically allocated staff (e.g. updated risk registers)	- Review of the procedures, risk signals and registers - Interviews with these responsible for risk management function - Interviews with the staff of the public organisation on understanding and awareness of risk reporting
4.	Is the risk register regulary updated and used in the daily	-	-

	management? Do the identified risks mirror the organisation's objectives? Are the critical risks clearly distinguishable?		
5.	Does risk identification consider both internal and external factors and their impact on the achievement of objectives?	- Risk register and risk signal reports - Memoranda of risk panel meetings	- Review of risk registers, signal reports and memoranda of risk panel meetings - Interviews with selected risk panel members
6.	Are identified risks analysed through a process that includes estimating the potential significance of the risk?	- Risk register - Memoranda of risk panel meetings	- Review of risk registers, memoranda of risk panel meetings, evidence on the established performance measures / indicators - Interviews with the management / selected risk panel members
7.	Have the performance measures / indicators been used to determine the extent to which objectives are being achieved and potential impact of a risk on the achievement of a specific objective?	- Evidence on the established performance measures / indicators	
8.	Is the management / risk panel assessing at reasonable intervals the risks which have been identified by various organisational structures throughout the year?		
9.	Does risk assessment include considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk?	- Risk management action plans - Memoranda of risk panel meetings	- Review of risk management action plans and memoranda of risk panel meetings - Interviews with the management / selected risk panel members
10.	Has the management established accountabilities for controlling specific risks? Are actions plans developed to ensure the risks are appropriately managed?	- Risk management action plans	- Review of risk management action plans - Interviews with the management and (if possible) with those assigned to be responsible for controlling specific risks
11.	Have the reporting lines been established for various stakeholders on identified risks, their mitigation or realisation?	- Internal procedures and policies - Risk reports to various stakeholders	- Review of the internal procedures - Interviews with the management and those

			responsible for risk management function
12.	Is appropriate monitoring of the results of actions taken to mitigate risk in place? Is the management held accountable for identifying and managing the risks to the achievement of objectives?	- Evidence on risk monitoring either by the management and/or external oversight bodies	- Interviews with the management and the external oversight bodies

Principle 8: The public organisation considers the potential for fraud in assessing risks to the achievement of objectives.			
No	**Questions for the principle assessment**	**Main sources of evidence**	**Data collection and analysis methods**
1.	Is fraud risk assessment an integral part of the regular risk assessment process?	- Entity-wide policies and procedures regarding fraud - Risk register - Evidence of risk monitoring being done at a senior level - Counter fraud, bribery and corruption work plan or similar	- Review of the policies and procedures and the risk register - Interviews with management and staff of the public organisation on understanding and awareness of fraud risk and (potential) fraud reporting
2.	Does the public organisation periodically perform an assessment of its exposure to fraudulent activity and how operations could be impacted? Does this assessment include each of the public organisation's structural units?		
3.	Does the assessment of fraud risk consider: - fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur; - incentives and pressures; - opportunities for unauthorised acquisition, use, or disposal of assets, altering of the public organisation's reporting records, or committing other inappropriate acts?		
4.	Does the assessment of fraud risk consider how management and other personnel might engage in or justify inappropriate actions?	- Entity-wide policies and procedures regarding fraud	- Interviews with the management and staff of the public organisation on understanding and awareness of reasons reactions on fraud risk
5.	Is regular reporting and monitoring in place in the public organisation on its exposure to fraud?	- Evidence on risk reporting and monitoring to/by the management and/or external oversight bodies, incl. relevant meeting minutes, action points and records of their execution	- Interviews with the management and the external oversight bodies

Principle 9: The public organisation identifies and assesses changes that could significantly impact the system of internal control.			
No	**Questions for the principle assessment**	**Main sources of evidence**	**Data collection and analysis methods**
1.	Does the public organisation have mechanisms in place to identify and react to risks presented by changes to the government, regulatory, economic, and physical environment in which the public organisation operates? Does it consider the expectations of the various stakeholders?	- Entity-wide policies and procedures regarding significant changes - Risk register and signal reports - Strategies, policies and corresponding action plans describing the planned events that might require changes in the internal controls - Evidence on significant changes that have occurred	- Review of the strategies, policies, risk registers / risk signal reports - Interviews with the management and 1-2 staff members of the public organisation on understanding and awareness of emerging issues that could significantly impact the system of internal control
2.	Does the organisation consider: - the potential impacts of reorganisation, new organisational units and / or dramatically altered compositions of existing structures on the system of internal control; - changes in management and respective attitudes and philosophies on the system of internal control?	- Evidence on analysis of the significant changes with regard to the cause, effect, impact and likelihood	- Interviews with the management and 1-2 staff members to identify any changes in the external environment which might affect the organisation, whether reorganisation or changes in management have occurred - Comparison of information in the risk registers on changes that have occurred or other evidence illustrating how these changes have been addressed by the public organisation *vis a vis* the potential impact on the internal control system
3.	Are controls and an early warning system in place to identify information signalling new risks that could have a significant impact on the public organisation?		- Interviews with the management and 1-2 staff members on controls and early warning system in place; and how the changes are analysed with the view to their cause, effect, impact and likelihood
4.	Does the organisation assess the risks associated with the		

	significant changes? Has the public organisation assessed the likelihood and impact the significant changes may have on achievement of objectives and on internal control? Has the cause of the significant change and its effect on achievement of objectives been identified and evaluated?		

Control activities

Principle 10: The public organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

No	Questions for the principle assessment	Main sources of evidence	Data collection and analysis methods
1.	Has management established a system where the personnel is systematically selecting and developing appropriate control activities?	- Internal procedures and policies - Appointments of personnel with responsibilities for control activities (centralised function and/or individual responsibilities as per risk management action plans) - Evidence from various levels of public organisation on selecting and determining appropriate control activities	- Review of applicable procedures and other available evidence - Interviews with management on established system - Determining staff awareness and mandate for systematically selecting and developing appropriate control activities (e.g. selected staff interviews)
2.	Has management determined which relevant processes require control activities? Are both operational processes (those aligning with the public organisation's mission) and horizontal processes (including budgeting, investment and public procurement, payment and treasury functions, asset management, accounting, human resource management) considered?	- Process maps / flowcharts - Internal procedures and policies - Other evidence on determined processes requiring control activities	- Determining how the management has obtained understanding of the source and flow of information, has identified what could go wrong and controls that address them, including interviews with the management, people responsible for internal control / control activities
3.	The control activities: - have been documented in the form of process maps and / or internal procedures (addressing organisation's own processes for fulfilment of its mission and objectives)? - are aligned with applicable legislation and guidelines from the external oversight bodies (including budget	- Applicable legislation determining requirements on external communication, reporting etc. assuming control system in place in the public organisation to ensure submission of accurate and timely information - External guidelines subject to fulfilment by the given public organisation	- Determining how control activities are documented or if not, how managers at various levels of public organisation ensure that the control activities exist for critical processes and risks - Determining whether the control activities align with applicable legislation and external guidelines (documentation review and

	and treasury departments, budget inspection, central procurement office, etc.)? - consider the effect of the environment, complexity, nature, and scope of the organisation's operations, as well as the specific characteristics of the organisation, and control activities that have been selected and developed accordingly? - include a range and variety of controls, considering both manual and automated controls, and preventive and detective controls? - are established at various levels of the public organisation? - are regular? If *ad hoc*, have they been authorised by the responsible management		analysis, interviews with staff responsible for internal control / specific control activities / reports / communication) Determine how *ad hoc* control activities are authorised (review of 2-3internal procedures, interviews with the selected operational management)
4.	Do the control activities help ensure that risk responses that address and mitigate risks are carried out?	- Internal procedures and policies - Process maps / flowcharts - Risk management action plans - Evidence on monitoring implementation of risk management action plans - Internal audit reports	- Analysis whether the control activities (as described in the internal procedures / process maps) address and mitigate the determined risks (as documented in the risk register, risk management action plans)
5.	Before any transaction is authorised or report/communication approved, are the aspects of this transaction verified by at least one member of personnel other than the one(s) who initiated the transaction? For the same file, the same person cannot initiate and verify (four eyes principle).	- Internal procedures and policies - Process maps / flowcharts - Sample of transaction authorisation records, including regarding budget, payment, public procurement procedure or a contract, external report submission, implementation of an action plan for a given operational activity etc.	- Interviews with the operational management on the system of authorisation of transactions and reports / communications and supervision - Selecting and analysing at least two processes applicable for the public organisation, at least one operational process and at least one horizontal

6.	Is there evidence of active and regular supervision by the management?	- Evidence on management supervision in the form of meetings, review and signature of documents, or as relevant	
7.	Are incompatible duties segregated, and where such segregation is not practical, are alternative control activities selected and developed?	- Internal procedures and policies and / or other evidence on analysis of incompatible duties (recording, approval and authorisation) - Internal audit reports	- Determine how the organisation has determined and documented incompatible duties - Analyse the system of segregation of duties (analysis of documents, interviews with management and relevant staff)

Principle 11: The public organisation selects and develops general control activities over technology to support the achievement of objectives			
No	**Questions for the principle assessment**	**Main sources of evidence**	**Data collection and analysis methods**
1.	Does management understand and determine the dependency and linkage between the public organisation's processes, automated control activities, and technology general controls?	- User manuals - Process maps / flowcharts - Internal procedures and policies - Technical specifications of the technology for determining the required automated controls	- Identifying existing technology used in given public organisation and whether any controls are automated - Analysing the automated controls / technology general controls with the view to public organisation's processes and how these controls support the processes - Interviews with the operational management working with the technology
2.	Does management select and develop control activities: - over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing? - that are designed and implemented to restrict technology access rights (both physical access and electronic access) to authorised users at all levels commensurate with their job responsibilities and to protect the public organisation's assets from external threats?	- Data / IT policies - Process maps / flowcharts - Internal procedures and policies - Instructions on user rights - Technology configuration information	- Analysing the control activities over the technology infrastructure vis-a-vis ensuring completeness, accuracy and availability of technology processing - Analysing user right instructions, IT policies and procedures, disaster recovery plans etc. - Interviews with the operational management working with the technology - Walk-through interviews with selected staff working with the technology from different levels to verify whether access rights (physical and electronic) align with their job responsibilities
3.	Does management select and develop control activities over the acquisition, development and maintenance of technology	- IT investment plans - Data / IT policies, backup and recovery procedures	- Interviews with the people responsible for IT

	and its infrastructure to achieve management's objectives?	- Asset security, fire / floods / national catastrophe protection policies, disaster recovery plans - Public procurement documentation - Contracts with external suppliers	acquisition, development and maintenance - Interviews with management responsible for authorisation of IT acquisition, development and maintenance (incl. budget)
4.	Are adequate security procedures (IT and otherwise) in place to keep assets and data secure from unauthorised interference and physical damage?	- Internal procedures and policies	- Interviews with people responsible for security procedures and continuity of operations
5.	Are the procedures for operational continuity in place to ensure that significant risks to continuity (e.g. concerning loss of data, absence of individuals etc.) are identified and contingency plans put in place?		

Principle 12: The public organisation deploys control activities through policies that establish what is expected and procedures that put policies into action			
No	**Questions for the principle assessment**	**Main sources of evidence**	**Data collection and analysis methods**
1.	Has management established control activities that are built into the processes of the public organisation and employees' day-to-day activities, through policies establishing what is expected and relevant procedures specifying actions?	- Legislation or requesting establishment of internal procedures and policies - Internal procedures and policies - Other communication on establishment of regular control activities - Various operational and risk management action plans	- Determining how the control activities to be undertaken are communicated to the staff, incl. internal procedures, action plans, formal and informal communication (interviews with selected operational management and staff, review of internal procedures and relevant communication)
2.	Has management established responsibility and accountability for control activities with management (or other designated personnel) of the organisational units in which the relevant risks reside?		- Determining whether an oversight body or second level of defence monitors compliance with specific policies and procedures and vis-à-vis determined risks (considering the risk tolerance)
3.	Do responsible personnel perform control activities in a timely manner as defined by the policies and procedures? Do competent personnel with sufficient authority perform control activities with diligence and continuing focus?	- Internal procedures and policies - Evidence on execution of control activities in selected processes - HR policies	- Selection of two processes (one operational and one horizontal) - Selecting one or two control activities from both processes (based on internal procedures, action plans or other applicable document) - Analysis of timeliness of the control activity, authority of personnel who performed it - Interviews with management to determine how they assure that competent personnel is performing the control activities, how is the authority given to personnel for these control activities - Interviews with responsible staff who have carried out the control activities to

			determine competence, diligence and focus of personnel who performed the control activity
4.	Do responsible personnel investigate and act on matters identified as a result of executing control activities?	- Evidence on reported matters upon execution of control activities (e.g. mistakes, suspected irregularities, instructions for further analysis etc.) - Evidence on investigations carried out (incl. reporting to an external body responsible for the subject matter, e.g. to budget inspection unit) - Evidence on acting upon the reported matters (corrections, updated and resubmitted information / reports, etc.)	- Determining whether matters identified are documented in various processes and how - From the above selected control activities under the 2 processes, determining how the instructions are given for correction, who was responsible for performing investigation, whether responsible personnel acted upon the matter
5.	Has management periodically reviewed control activities to determine their continued relevance, and revised them when necessary?	- Evidence on management review, or review by delegated staff under management supervision - New versions of internal policies and procedures	- Understanding the process of reviewing control activities / internal procedures, incl. the incentives for review (review of internal procedures, interviews with responsible personnel)

Information and communication

Principle 13: The public organisation obtains, generates and uses relevant, quality information

No	Questions for the principle assessment	Main sources of evidence	Data collection and analysis methods
1	Has the management of the public organisation defined and identified the information requirements at the relevant level and necessary detail for the appropriate personnel? - Are these requirements defined using the results provided by the internal control system (e.g information on the mechanism of controls, risk, system deficiencies? - Where possible, is there a clear link to the public organisation's objectives?	Communication Strategy Internal and external reports related to business objectives Financial and operational reporting Internal rules and procedures related to the information e.g. Information Security Policy, Policy on the information classification, Risk register, incident register Business Continuity Plan and Business Recovery Plan	Interviews with the senior management on the data requirements, classification and its significance for achieving the public organisation's objectives Review of the data classification policy to assess if it matches the organisational risks, mechanism of controls and deficiencies identified Analysis of the means and tools used for communication Review of the risk register the spot the information security incidents Interviews with the personnel, management, DPO and information security officer on how the information management is organised
2	Does the management of the public organisation receive relevant information/data from reliable internal and external sources in a timely manner, based on the identified information requirements?	Documentation on the reconciliations, checks and verifications carried out by the public organisation personnel, Documentary evidence for	Interviews with the personnel and management responsible for receiving the information/ reports Examination of sample of reporting documents to assess their timelines, extent and significance of modifications needed
3	Does the management of the public organisation evaluate if the information provided by both internal and external sources is:		

	- reliable, - of good quality in particular if it is: appropriate, current, complete, accurate, accessible, and provided on a timely basis	modifications to the original data Findings and audit reports on the reporting process	
Principle 14: The public organisation ensures proper internal communication			
1	Have the current arrangements used for internal communication been analysed?	Communication Plan Minutes of the management meetings, team briefings Intranet homepage Internal posters, brochures and journals Documentation of the internal thematic campaigns Help desk, incidents' register	Interviews with management and personnel on the current arrangements for enhancing internal communication, in particular whether it: - provides targeted and timely communications to personnel - ensuring they hear about news from managers and not the grapevine or the media - provides important messages face-to-face via line managers or via senior management at all-staff meetings - takes opportunities to create dialogue and engagement with personnel and managers. Analysis of the personnel and management comments on various activities (intranet) Analysis of the result of the personnel survey on communication
2	Are arrangements in place to ensure that management and personnel of the public organisation is informed of other units' decisions/ projects/ initiatives that may affect their responsibilities and tasks?		
3	Are there any recent examples where flaws in internal communication have caused problems or impacted on the public organisation's performance? - Have the underlying causes been analysed? - Have measures been taken to prevent similar communication issues in the future?	Risk resister, incidents' register, complaints' register Audit findings and report Documentation on the follow-up action	Interviews with management and personnel on how the communication efficiency impacts the organisational performance Analysis of the records / findings of the deficiencies resulting from weak communication (usually the inter service crosscutting responsibilities) and assessment of the corrective action taken

4	Does the oversight body receive the quality information that flows up the reporting lines from management and personnel?	Agendas and minutes of the oversight body meetings	Analysis of the agendas and minutes of the oversight body meetings Interviews with the oversight body members, management and personnel
5	Can the personnel use alternative reporting lines to go around upward reporting lines when these lines are compromised (e.g. whistle-blower and ethics hotlines, for communicating confidential information)?	Reports, complaints on confidential issues Incident register	Comprehensive review of existing reporting lines guaranteeing unimpaired reporting on confidential issues (including possible violations of law by management), to confirm that they are effective and result in timely reports.
6	Are the management and staff of the public organisation sufficiently aware of the information systems security policy? - Is information system security a regular topic at management meetings? - Are objectives for information security established and monitored? - Do the results of the regular supervision of IT systems, audit findings or information from other sources suggest that there may be security-related issues for IT? - Are these issues escalated to and discussed at the appropriate management level?	Information security policy Training records Agendas and minutes of the management meetings Internal communications and documentation of the information's sessions on the information security Internal and external audit reports, incidents' register	Interviews with senior and middle management on the information security and data protection. Review of the training records to conclude on the information security awareness practices Analysis of the agendas and minutes of the management meetings concerning the information security issues, to conclude if the security objectives are defined and monitored by management Analysis of the audit reports concerning the information security deficiencies and their impact on the public organisation objectives, Interviews with the auditors on risks exposure, vulnerability of the information security related issues
7	Is feedback from IT users regarding system performance collected and analysed to detect the potential effectiveness and efficiency deficiencies? - Are statistics on IT system performance indicators regularly analysed?	Documentation of help desk service IT user satisfaction survey Technical documentation of the IT systems	Analysis of reports / statistics on the number of changes, updates, service failures, resolved IT problems Interviews with the management and personnel (IT users) to find out how they rate services and support provided by IT and their

	- Are IT system performance issues reported to the appropriate management level?	(requests for update or change of the IT systems, applications etc.)	impact on the achievement of the pubic organisation objectives Analysis of the agendas and minutes of the management meetings concerning the IT performance management
Principle 15: The public organisation ensures proper external communication			
1	Have the current procedures and methods used for external communication been analysed to identify their strengths and weaknesses, including cost-benefit aspects?	External communication plan. Documentation from the press conferences, seminars, workshops, personal visits, i.e. visits to key individuals or key public organisations, Documentation on media communication: press releases, articles in newspapers, professional press and on web sites, TV/ radio, Documentation on communications to the main stakeholders of public organisation	Interviews with management and personnel on the current arrangements enhancing the external communication in particular if it: - develops and maintains positive, collaborative relationships with the main stakeholders of public organisation, - maximises awareness and support of public organisation goals, objectives and programs, - establishes supportive connections between the subsequent budget users, - establishes "one clear voice" to stakeholders through key messages and talking points. Analyses of the different methods and means used for the external communication to assess the coherence and efficiency of information provided
2	Does the public organisation's management receive and assess the information from external sources concerning significant matters relating to risks, changes, or issues that affect the public organisation's internal control system?	Complaints register, risk register Correspondence from stakeholders, citizens and business partners	Analysis of the information from external sources concerning significant matters relating to risks, changes, or issues that affect the public organisation's internal control system in order to conclude on: - the number of complaints/risks concerning the business

			activity (also compared to the past periods), - the percentage of complaints upheld by public organisation, - corrective action taken.
3	Does the public organisation's management seek and analyse feedback from target audiences (e.g. main stakeholders, citizens, business partners) regarding communication impact? - is the information obtained reliable and pertinent? - is relevant feedback escalated to the appropriate level and used to adapt ongoing communication strategies?	Documentation of the public consultation, satisfaction survey conducted by public organisation	Interviews with representatives of main public organisation stakeholders, citizens and business partners on the public organisation service delivery satisfaction Assessment of the public consultation process to conclude if it factually brings the public involvement in large-scale projects or laws and policies prepared by public organisation.

Monitoring activities			
	Principle 16: The public organisation selects, develops and performs ongoing and/or separate evaluations		
1	Are evaluation activities appropriately organised and resourced to meet their purposes?	Management Plans and Implementation reports Performance indicators- BPIs (business performance indicators), KPIs (key performance indicators) Monitoring procedures Audit Committee and Internal Audit Charter	Interview with the management to conclude whether the monitoring activities are organised guarantying the comprehensive monitoring of main objectives of the public organisation Discussion with the management and personnel on the established indicators (output versus outcome) Analysis of the management plans and their implementation reports Assessment of gaps identified (deficiencies in the internal control system) and the corrective action taken
2	Does the public organisation's management plan the evaluation activities in a transparent and consistent way so that relevant evaluation results are available in due time for operational and strategic decision-making and reporting needs?		
3	Do evaluation activities provide reliable, robust and complete results? - Are the evaluation reports used by management in practice, i.e. do they have a real impact on the public organisation's decision-making or the policy and legislative proposals prepared? If not, why? - Is it ensured that on-going and specific monitoring is developed and performed to ascertain that the components of internal control are present and functioning at all levels?	Monitoring reports Internal and external audit results	Interviews with management on the timelines and the quality of reporting on the internal control system Impact assessment of the recommendations resulting from the monitoring activities in the decision making process
4	Are evaluation results communicated in such a way that they ensure maximum use of the results and that they meet		

	the needs of decision-makers and stakeholders?		
5	Do the public organisation's managers and personnel who participate in self-assessments of the organisation's internal control systems have a sufficient understanding of internal control and risk management? - If not, what is done to avoid misinterpretations or misunderstandings that could affect the results and conclusions they reach?	Training records Documentation of the internal awareness sessions, management trainings and seminars on the internal control and risk management	Interviews with: head of public organisation, senior management and internal auditor on the main goals and objectives of the internal control system and risk management to recognise their understanding of the subject
6	Is the self-assessment well organised, pragmatic and value adding (or is it regarded as a "bureaucratic burden")? Is it sufficiently sponsored by senior management of the public organisation („tone of the top")?	Monitoring procedures Monitoring reports (including the self-assessment reports) Internal and external audit reports	Interviews with management and internal auditor on the monitoring practices to recognise if they include the following methods: - periodic evaluation and testing of controls by internal audit, - continuous monitoring programs built into information systems, - analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure, - supervisory reviews of controls, such as reconciliation reviews as a normal part of processing, - self-assessments by management regarding the tone they set in the public organisation and the effectiveness of their oversight functions, - oversight body (Audit committee) inquiries of internal and external auditors, and
7	Is the self-assessment focused on the public organisation's main activities, objectives and risks of the public organisation?		
8	Are the self-assessment results and conclusions sufficiently supported, by a reliable and accurate evidence, for example via references to other relevant sources?		

			- quality assurance reviews of the internal audit Review of the results (on the sample basis) of the above mentioned activities Assessment of the audit trail and the source evidence of the monitoring activities
9	Does the public organisation's management identify changes in the internal control system that either have occurred or are needed because of changes in the organisation and its environment?	Monitoring (self-assessment reports) Risk register	Interviews with management on the main risk and challenges for the public organisation Analysis whether the recommendations of the monitoring reports match/reply the risks and challenges described
10	Is the internal audit function carrying out regular specific assessments to provide higher management with independent review of the subordinate systems?	Internal audit charter and procedures Internal audit strategic and annual plan Internal audit risk assessment Internal audit report and annual report including the annual opinion External audit report on the assessment of internal audit service Agendas and minutes of oversight body (audit committee)	Analysis of the internal audit arrangements, Analysis of the strategic and annual audit plans and their actual implementation, to determine if they reflect and take into account public organisation's related risk. Examine a sample of audit report to assess how they reflect the internal control issues. Interviews with head of public organisation, senior management, audit committee representatives on the effectiveness and quality of internal audit work.
	Principle 17: The public organisation evaluates and communicates deficiencies		
1	Does the personnel report internal control issues through established reporting lines to the	Reports, complaints on	Analysis of the sample of the reports on the deficiencies, incidents and risks, reported by

	appropriate internal and external parties on a timely basis to enable the public organisation to promptly evaluate those issues?	confidential issues Incident register Register of exceptions and non-compliance events	internal and external parties, to conclude whether they are encouraged, and if judged significant or systemic, escalated at the appropriate management level.
2	Does the public organisation's management take adequate and timely actions to analyse and correct deficiencies reported by the personnel, internal audit function, financial and non-financial internal and external monitoring activities?	Agendas and minutes of management meetings Action plans Quality improvement programmes	Interviews with management on the corrective capacity of the public organisation Analysis of the examples of the corrective action taken by management to reinforce the effectiveness of internal control system, in particular in case of: - exceptions and non-compliance events detected (e.g. breach of existing regulatory and/or contractual provisions, control weaknesses, errors, fraud, illegal acts, ineffectiveness, and inefficiency), - exceptional circumstances that may impose decisions which represent a deviation from established processes and procedures (e.g. conflicts of interest,).
3	Does the public organisation's management monitors the status of corrective actions taken so that they are completed on a timely basis and bring the expected result (e.g. the recommendations of the internal audit or results of monitoring activities)?	The recommendations ' register Documentation on the status of the follow up actions Annual report of internal auditor	Review (on sample basis) whether the implemented corrective actions are highlighted and provide evidence of the effective functioning of the related internal control principles Analysis of the status of the follow up actions concerning the external and internal audit reports. Interview with management and internal auditor on the process of the implementation of internal and external audit recommendations

			(effectiveness, efficiency and overall impact)

Annex 2. Legislation, internal rules and procedures for IC quality assessments for central harmonisation units

IC systems and systems for assessing the quality of IC should be structured and implemented by the administrations according to their respective overall legal and governmental arrangements, taking into account each of the constitutional stakeholders, government, parliament and the supreme audit institution, as well as the arrangements that exist between these stakeholders.

Accordingly, there should be a set of legislation and internal procedures that establish the scope, objectives, rights and responsibilities relevant for conducting IC quality assessments.

In general, the following should be regulated through **primary legislation** (for example, in the budget system law or in a special law for PIC):

1. Assigning the responsibility for putting in place the IC system and for the quality of the IC system to the heads of the public organisations;
2. Assigning the responsibility for co-ordination, harmonisation and monitoring of IC to the ministry of finance, and respectively the CHU, according to the PIFC rules;
3. Committing the public organisations to:
    - Continuously assess the quality of the IC system within their organisation (and their subordinate organisations, where applicable);
    - Report on the results of their internal quality assessment to the CHU;
    - Grant the ministry of finance (and accordingly, the CHU) access to any information, premises and resources necessary for carrying out the IC quality reviews;
    - Follow up on CHU recommendations upon the IC quality reviews and communicate to the CHU any actions taken in timely manner.

Furthermore, **bylaws** should regulate in further detail:

1. The reporting responsibilities (format, timing, preconditions) between the public organisations and the ministry of finance (e.g. annual reports on IC);
2. The reporting responsibilities between the ministry of finance and the government (the consolidated annual report on the IC);
3. The requirements with regard to the appointment of the personnel responsible for various aspects of the IC (e.g. the FMC manager, the risk manager);
4. The tasking and authorisation of the ministry of finance (and accordingly, the CHU) to carry out the IC quality reviews in the public organisations.

The central rulebook on IC (as issued by the CHU) should include the methodology for assessing the quality of the IC in public organisations.

The individual internal procedures of the CHU and public organisations should describe how the IC legislation and central rulebook are implemented in their organisations (who does what, when and how). In particular, the CHU internal procedures should establish the approach and methodology for conducting the IC quality assessment, including:

1. Obtaining information on the public organisation and the quality of its IC;
2. Preparation of an annual plan for IC quality assessments, including risk-based selection of the public organisations for review during the budgetary year;
3. Performing the IC quality reviews including desk-based review and analysis of the information, and on-the-spot checks, including collection of evidence on the functioning of the IC system in practice;
4. Providing feedback to the public organisation on the results of the IC quality review;
5. Consolidating the results of the IC quality assessments and reporting to the government.

The CHU should be responsible for ensuring the existence of an appropriate legislative base and harmonised guidance.

Annex 3. Internal control and internal control quality assessment: basic information

Principles of internal control

Position Paper No. 1 "Principles of Public Internal Control"[20] published by the PIC Network[21], describes the overall principles of effective IC, as follows:

1. Good public governance in the public interest is the context, the purpose and the driver of IC:
    a. IC is part of the broader internal governance arrangements;
    b. it supports effective, efficient, prudent and financially responsible administration in the public interest;
    c. it occurs on an ongoing basis throughout all stages of the policy, service delivery and budget cycles.
2. IC is focused on performance:
    a. IC is oriented to objectives, outcomes and outputs – all to be achieved in a legal, appropriate, ethical and financially responsible way;
    b. IC, through measurement, analysis and reporting of actual outcomes and outputs in relation to the objectives is at the heart of the performance management system;
    c. Performance information is used for accountability and learning regarding the delivery of value for money for the citizens.
3. IC is based on COSO and INTOSAI:
    a. A process effected by people providing reasonable assurance that objectives are achieved;
    b. Five integrated and interrelated components – all present and functioning: control environment, risk assessment, control activities, information and communication, and monitoring;
    c. Seventeen integrated COSO 2013 framework principles associated with those five components
4. The accountability triangle is a cornerstone of IC:

[20] EC (2015), *Public Internal Control Systems in the European Union: Principles of Public Internal Control,* Position Paper No. 1. "Public Internal Control, An EU approach." Ref. 2015-1. http://ec.europa.eu/budget/pic/lib/docs/2015/CD02PrinciplesofPIC-PositionPaper.pdf

[21] The PIC Network was set up by the European Commission as a response to the Member States' wish to continue discussions at a PIC conference in February 2012. The PIC Network is made up of European Commission and IC specialists from all 28 EU Member States. The network meets via regular conferences. It issues PIC Compendiums and various papers on key IC topics, published at http://ec.europa.eu/budget/pic/index_en.cfm

a. Correspondence and consistency between authority (empowerment), responsibility and accountability throughout all levels within the public entity: no responsibility without authority on the one hand (authority as a precondition to responsibility), no responsibility without accountability on the other (accountability as a necessary consequence of responsibility);

b. Overall and final authority, responsibility and accountability with those charged with governance: the highest political and/or administrative levels in public sector entities – e.g. ministers, senior management, governing bodies – are authorised, responsible and ultimately accountable for all aspects of the public entity's functioning, its results and impact;

c. Balance between responsibilities and means: no responsibility should be assigned or accepted without the necessary resources to deliver.

5. IC is organised according to three lines of defence: To support their final authority, responsibility and accountability for IC, those charged with governance establish subordinate lines of defence: management control by operational management (first line), specific risk management, control and inspection functions (second line), and independent assurance by internal auditing (third line):

    a. operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis;

    b. functions in the second line help to ensure that the first line is properly designed, fully in place, and operating as intended. Each of these functions have some degree of independence from the first line, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems;

    c. internal audit reports to the most senior level in the public sector entity and provides ministers, the governing bodies and top management with comprehensive assurance based on the highest level of independence and objectivity within the entity.

6. IC requires a functionally independent internal audit function:

    a. internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defence achieve objectives;

    b. outspoken support by (senior) management;

    c. may be centralised or decentralised;

    d. operated with the highest level of professionalism in compliance with IIA and other relevant standards;

    e. direct reporting line to the minister, governing body and senior management;

    f. supported by Audit Committee (or comparable body).

7. IC is harmonised at an appropriate level: IC includes a function for the coordination and harmonisation of internal control and audit in the public sector at large. This harmonisation function ensures that:

a. the basic conditions for the effective implementation of IC in terms of legal framework, working methods, guidelines and training are met;

b. stakeholders' expectations are obtained, understood, coordinated and taken into consideration;

c. the coherence, credibility and added value of IC are visible and communicated to relevant players.

8. IC adopts a continuous improvement perspective:

a. IC is a dynamic concept. It is continuously improved through mindful consideration and appropriate implementation of recommendations and guidance from both internal and external parties e.g. organisational input, internal auditors, external auditors, external advisors, and professional organisations and networks, as well as good practices from entities in both the national and international environment. Active interaction between internal and external actors and an open mind-set are crucial to build an adequate learning environment.

Furthermore, SIGMA has defined the minimum requirements for IC in public organisations[22]: Accordingly, the public organisations should put in place IC procedures which shall:

- Clarify responsibilities within the public organisations;
- Ensure that risks are regularly assessed and risk-mitigation measures are implemented;
- Ensure that policy proposals initiated by the public organisations include an estimate on budgetary costs;
- Make calculated choices between alternative ways to achieve objectives;
- Keep financial commitments within budget limits;
- Ensure that the use of financial resources (e.g. through procurement operations or human resource costs) is in accordance with the existing budget;
- Enable detection and reporting of irregularities (both for national and IPA funds);
- Allow an audit trail of key financial decisions, including those relevant to IPA-funded programmes.

[22] Principle 7: Each public organisation implements IC in line with the overall IC policy, p.4. OECD (2017), *The Principles of Public Administration*, OECD Publishing, Paris: http://www.sigmaweb.org/publications/Principles-of-Public-Administration_Edition-2017_ENG.pdf

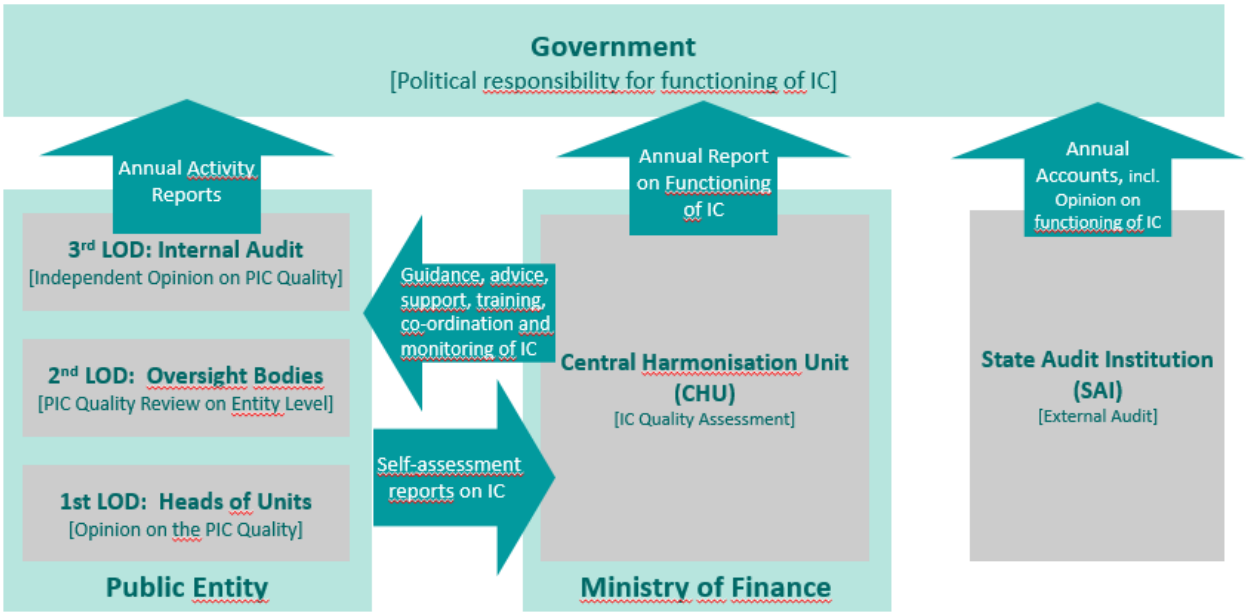
Internal control and internal control quality assessment - roles and responsibilities

In setting up IC systems in public organisations, the heads of public organisations should ensure compliance with the above principles described above. The IC quality assessment should evaluate whether the principles have been respected.

The IC framework distinguishes the respective levels of accountability: the public organisation level, the ministry of finance and the government. The accountability structure in the public sector should establish an "integrated internal control system" where each governance level builds its opinion on the IC quality on previous levels in a pyramidal manner. It is the key component of the accountability chain and constitutes the foundation on which the government takes overall political responsibility for the national budget.

The main actors involved in the IC quality assessment are the CHU, the management and the personnel of the public organisation, and internal and external auditors. Even though monitoring of the quality of IC system is the primary responsibility of the CHU, management of the public organisations should assess on a continuous basis the effectiveness of the IC systems. Figure 1 presents the respective roles and responsibilities for the IC quality assessment in terms of accountability.

Figure 1. Accountability framework for the IC quality assessment.



In order to conduct the IC quality assessment, a system that clearly distinguishes the responsibilities of various public sector organisations must be established. In particular, the respective players should take on the following roles and responsibilities:

Minister of Finance / CHU

The Minister of Finance is in charge of co-ordination of development, establishment, implementation and maintenance of the IC. On their behalf, the CHU is responsible, among other things, for:

- Establishing the legal and procedural framework for IC and IC quality assessments;
- Providing guidance to the public organisations on the establishment and assessment of the IC system;
- Monitoring the functional state of the IC system in the administration based on the annual IC reports from the public organisations;
- Monitoring the quality of the IC system by conducting the sample-based IC quality reviews in the public organisations[23];
- Preparing annual reports on the functioning of the IC based on its annual monitoring and analysis in order to provide a valid and factual picture of progress and the status of IC to the government;
- Co-operating with the heads of public organisations and other persons responsible for IC.

Head of public organisation

The head of the public organisation has the ultimate responsibility for IC. In particular for:

- achieving the objectives of the public organisation by managing public funds in a legal, economical, efficient and effective manner;
- establishing an organisational structure and working procedures to ensure functioning, monitoring and development of sound financial management and control;
- establishing processes for on-going monitoring and review of the IC system;
- based on the various internal and external reports on the IC system, forming their own view on the effectiveness of IC based on the evidence it obtains, exercising the due standard of care;
- reporting to the MoF on the implementation of IC, including preparing the IC (self-assessment) report;
- granting the CHU access to any information, premises and assets required to out the IC quality review.

[23] Based on *The Principles of Public Administration*, the CHU in the EU candidate countries and potential candidates should organise at least one annual review of progress across the public organisations with regard to aligning financial management and internal controls to the established legal and operational requirements. OECD (2017), *The Principles of Public Administration*, OECD Publishing, Paris: http://www.sigmaweb.org/publications/Principles-of-Public-Administration_Edition-2017_ENG.pdf

Operational level in the public organisation

The operational, mid-level managers have an overall responsibility for the effective and efficient implementation of IC and its regular on-going assessment on daily basis (self-assessment of IC quality).

Internal audit:

Internal audit provides the head of the public organisation an independent, objective assurance and consulting service, looking at the effectiveness and efficiency of the risk management, control and governance processes with special reference to IC (carrying out risk based internal audits and providing feedback on the IC quality).

External auditor (SAI, EU audits, ECA):

External auditors shall perform an independent external audit, addressing any serious management and control weaknesses identified by the IC (the external audit results may feed into the IC quality assessment).

Annex 4. Country examples

This Annex presents country examples taken from a variety of sources and organised principle-by-principle with the intention of illustrating how COSO principles enhance the execution of IC in public organisations. It is structured around COSO components and principles.

The purpose of this Annex is to provide examples of practical implementation of COSO principles by European countries. Although some of the proposed cases may not be suitable or adequate for the specific conditions in a given public organisation, they may be seen as examples of good practices in place.

Control environment

Principle 1: The public organisation demonstrates a commitment to integrity and ethical values[24]

Ireland – Civil Service Code of Conduct

The Civil Service Code was introduced to underpin the change process, an integrated approach to the values, standards and behaviour of civil servants. The Code sets out a clear framework within which civil servants must work. It sets out in a single document the principles which should govern the behaviour of civil servants and the values which the Civil Service espouses.
It builds on the principles set out in "The Ombudsman's Guide to Standards of Best Practice for Public Servants". It is not intended to be an exhaustive list of guidelines for all possible eventualities. Individual Departments and Offices will wish to provide additional guidance as appropriate for their own personnel relevant to their own particular circumstances.
Moreover, in Ireland, after years of campaigning and working with a number of whistle-blowers from all sectors, the Protected Disclosures Act was finally passed in parliament in 2013 and it entered into force in July 2014. It offers comprehensive protection for whistle-blowers. It replaces a patchwork of protections that had previously been scattered in different Irish legislation. In addition to using a broad definition of a worker protected under the act, the protection offered to whistle-blowers extends to personnel who might not have made a disclosure themselves, but who might have suffered as a consequence of someone else making a disclosure.
The manner in which the burden of proof has been regulated is also of interest: it is up to the employer to prove that the disclosure was not a protected disclosure. The law lays down clear requirements and procedures for making and receiving a disclosure, and it envisions periodic reviews to ensure it remains relevant.

Spain - Code of Good Governance

The Code of good governance for members of the Government and high-ranking officials of the Central State Administration (Código de Buen Gobierno de los miembros del Gobierno y de los altos cargos de la

[24] Source: based on Transparency International (2015): *Speak up: Empowering citizens against corruption,* https://issuu.com/transparencyinternational/docs/2015_speakup_en?e=2496456/12424694

Administración General del Estado) establishes an explicit commitment on the part of state officials (ministers, secretaries of State, higher-ranking officials, and those working in top positions in the public sector, etc.) to act in accordance with the demands of their positions and in terms of a series of ethical principles laid down in the text.
A law relating to conflict of interest situations amongst high-ranking state officials lists a series of obligations for personnel affected by this norm with the aim of avoiding such situations. Regarding civil servants, the Basic Statute of the Public Employee contains a code of conduct for all public employees. This code is based on the general obligation of all employees working in public administrations to fulfil their duties diligently and to be guided by the general interests of the state. The Code lays down 12 ethical principles and elaborate behavioural norms.

Italy - Anti-corruption Law and Anti-corruption Plans

The anti-corruption law in Italy includes mandatory anti-corruption plans to be developed every year by each public organisation, through the overview of an anti-corruption official. These plans must highlight the activities in which the risk of corruption is higher; foresee those prevention mechanisms in the areas of training and audit that allow the central public administration to successfully prevent the risks of corruption; ensure that a systematic mechanism of reporingt to the hierarchy is put in place, notably for those activities where the risk of corruption is higher; provide adequate monitoring tools to ensure the respect of the terms of reference and the successful conclusion of public bids and procurement procedures; identify specific mechanisms that allow for the inquiry about the relations between the public administration and all those private subjects that have concluded contracts and ensure they are interested in authorisation mechanisms or are entitled to economic benefits.

Poland - Government Anti-Corruption Program

In 2012, the Ministry of Interior and Administration, in co-operation with other central offices, prepared the document 'Government Anti-Corruption Program for 2012-2016' ('Government Program'). This programme is a continuation of activities envisaged by previous government anti-corruption programmes (carried out since 2002). Its main objective is to decrease the level of corruption in Poland achieved by the implementation of two specific objectives: strengthening prevention and education in the area of corruption and increasing the effective elimination of corruption crimes.
Moreover, the document sets out detailed objectives, goals and numbers of activities as well as the institutions involved in their accomplishment.

Greece – Handling the Corruption Complaints

All institutions in the country are tasked with receiving and handling corruption complaints from citizens and publishing annual reports on their complaints data. In addition, the national Ombudsman is seen as fairly independent and well resourced. In 2012, it reported receiving 11,702 complaints – representing a 10% increase from the previous year. Of those, nearly 60% were found to be justified and the Ombudsman reports having successfully resolved 82% of these complaints[25].
When combined with clear and widespread communication, such confidence-building measures can truly influence peoples' willingness to use the systems in place.

[25] The Greek Ombudsman Independent Authority (2013), *Annual Report 2012*, https://www.synigoros.gr/resources/annualreport2012--3.pdf

Principle 2: The public organisation exercises oversight[26] responsibility[27]

Slovakia and the United Kingdom - Audit Committee

In **Slovakia and the United Kingdom** the audit committee responsibility is the most complex and includes the oversight of the following elements: values and ethics, risk management, internal control framework including fraud and irregularities, internal audit function, external audit function and financial and non-financial reporting.

In the UK, under the Corporate Governance Code in Central Government, boards are tasked with setting the organisation's risk appetite and ensuring that the framework of governance, risk management and control is in place to manage risk within this limit. As the role is a challenging one and needs strong, independent members with an appropriate range of skills and experience, the "Audit and risk assurance committee handbook" was prepared to support government departments, executive agencies, non-departmental public bodies and other arm's length bodies.

Following this development in 2017, the NAO published "the Audit Committee checklist" as a part of the range of guidance and tools to assist public sector audit committees.

In **Poland**, the Act of 27 August 2009 on public finance implemented in 2010 developed a new concept of management control and accountability at the higher (secondary) level of management, the minister in charge of the government administration branch, and introduced one audit committee for each line ministry. Audit committees are meant to strengthen the internal audit function in its task of assessing management control throughout the entire branch. The audit committee may inform and give advice to the minister about risks connected with implementation of their objectives throughout the entire branch.

The aim of the audit committee
The aim of the audit committee is to provide consulting services with a view to ensuring adequate, efficient and effective management control and providing efficient internal audit services to the minister in charge of the branch. It should be emphasised that the scope of the audit committee guidance covers the functioning of the management control and internal audit in all units supervised by the relevant minister. One joint audit committee may be established for the branches managed by one minister. For example: the Minister of Finance established one joint committee for three branches: Budget, Public Finance and Financial Institutions.

The members of the audit committee
The audit committee shall comprise a minimum of three members, including: 1) a person in the rank of the secretary or undersecretary of state designated by the minister as the chairman of the committee; 2) at least two independent members people not employed in the ministry or in organisations of the branch. In the

[26] The oversight is used in the following context:
- Within the public sector, it is the first-level budget user (e.g. the ministry of agriculture) which oversees their subordinate structures or organisations (e.g. the land agency);
- Within public organisations, the oversight body may be a board of directors (e.g. for the state-owned enterprises), an audit or risk committee or other body, which is independent from the management of a public organisation.

[27] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html

opinion of the Ministry of Finance, the optimal size of the audit committee is five to nine persons including the chairman. This size of audit committee gives all members a chance to actively participate in the deliberations and effectively perform the tasks of the committee. In practice by the end of 2012, the audit committees ranged from three to seven members. The Ministry of Finance recommends that independent members shall make up at least half of the audit committee. It is also recommended to maintain a constant size of the audit committee. Independent audit committee members should jointly have knowledge, skills and experience to perform their tasks competently and effectively. In the provisions of the Regulation of 29 December 2009 on Audit Committee, the Minister of Finance specified the qualifications of the independent members, the rules of procedure the audit committee should respect and the method of remunerating independent members. The organisation and operation of the audit committee is specified by the rules of procedure stipulated in the internal regulation granted by the minister on request of the chairman of the committee.

Audit committee tasks and annual report
Audit committee tasks shall include the following, in particular:
indicating material risks indicating material weaknesses in the management control of the branch and proposing measures to improve them setting priorities for annual and strategic internal audit plans reviewing material results of internal audit activity and monitoring the implementation of reviewing statements on the execution of the internal audit plan and on the assessment of management control monitoring the effectiveness of the internal audit, including reviewing results of internal and external assessments of the internal audit activity authorising the dissolution of employment contracts and any change in salary and employment conditions of the chief internal audit executives in organisations within the branch.
By the end of February each year, the audit committee shall submit a report on the implementation of tasks in the preceding year to the minister in charge of the branch and the Minister of Finance. The report on the implementation of tasks shall be published in the Public Information Bulletin on the website of the relevant ministry. The first reports were submitted to the Minister of Finance in 2011

Principle 3: The public organisation establishes structures, reporting lines, authorities and responsibilities[28]

The Netherlands – Organisational Roles and Responsibilities

The minister is the highest-level manager. Within a ministry, three levels of control are distinguished:

- the senior management/strategic level — minister, state secretary, secretary-general (SG) and directors-general (DGs), who are responsible for the strategic planning;
- the middle management/tactical level — the heads of the directorates (directors), who are responsible for the development of the policy programmes and the operational support management;

[28] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html

- the executive management/operational level (activity and transactions) — the heads of the departments, units and internal agencies, who are responsible for policy implementation and operational support management activities.

The minister or the state secretary takes the strategic decisions, after consulting the senior management (level one). Decisions that are not taken by the minister or state secretary have been mandated to the SG and sub-mandated to the DGs; they have been authorised to act on behalf of the minister. A further sub-mandate has been mandated to level two (directors) and sometimes to level three (heads of departments, etc.) depending on the nature of the activities. The minister, however, remains fully accountable to parliament for all decisions taken either by them or on their behalf.

Principle 4: The public organisation demonstrates commitment to competence[29]

Estonia – Recruitment and Selection Process

The Public Service Act brought fundamental changes to the recruitment and selection process. Internal or open competitions are now required for posts at all levels of public entity. In addition to the competition requirements, calls for all open competitions must be published on the central public service website and the website of the public body to facilitate searches by potential applicants for civil service positions.

Assessment is mandatory for almost all personnel and takes the form of an annual meeting with, and feedback from, the immediate superior. A fair range of criteria is used, including activities undertaken, outputs, improvement of competencies and interpersonal skills.

Assessment is of high importance to contract renewal. In addition, Estonia uses performance-related pay (PRP) for most public employees. Its application is managed by ministries and it typically takes the form of permanent pay increments.
Educational qualifications and performance appraisals are relevant determinants of promotion for all levels of personnel, although performance is not relevant for technical support personnel. Education levels may prove an informal restriction to promotion between hierarchical grade, in addition to other requirements specific to the post.

Germany – Recruitment and Selection Process

The recruitment system in the German public service is a career-based system. Entry into the public service is gained through a competitive examination for a specific post, with selection managed at the level of organisations. No posts are open to external recruitment and external applicants first have to apply for entry into the public service.
However, there have been some measures to increase the use of external recruitment for professionals.
Disabled persons have preferential right for a job interview and receive preference in the selection process. Women are also entitled to preference in the selection process and are subject to hiring targets of: 12.2% of

[29] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html and OECD (2012) Human Resource Management Country Profiles for Estonia and Germany, http://www.oecd.org/gov/pem/hrpractices.htm

top management; 14.1% of middle management; 26% of professionals; 23.3% of secretarial positions; and 20.5% of technical support.
Years of experience, performance appraisals and qualifications are factors in promotion decisions for all grades of public servants. To change between job categories, employees must take an examination and minimum education requirements apply. Openings are placed on a transparent listing which is accessible government wide. The HR department compiles a shortlist of candidates, there is systematic use of panels, some use of assessment centres and the decision of the panel/centre is binding.

.

Principle 5: The public organisation enforces accountability[30]

Denmark – Accountability Framework

The Danish state has not set out a Public Internal Control (PIC) framework in a separate document or in a set of rules. However, based on the existing regulations (e.g. the Public Accounting Order) and prescriptive guidelines ('Responsibility for Management - Guidance on Management, from Group to Institution'), there is a clear framework for the responsibilities allocated to state institutions in order to ensure appropriate internal controls and management of the institution. Accountability is placed, to some extent, on the local institution, in particular through requirements for objectives and performance management, appropriation management and procedures for the approval of accounts. For this reason, internal control and accountability are closely linked. The incentives for managers can be performance-based salary contracts and other measures, and the institution's management must ensure the optimum utilisation of resources in accordance with the institution's objectives.

The Danish public sector is divided into ministerial portfolios, whereby each portfolio has a department with subordinate agencies and institutions, which together constitute a portfolio group. The minister bears the ultimate political responsibility for his/her portfolio. Powers of allocation and inspection have been delegated to the administrative level.

Management responsibility in state institutions
The institution's management must assure optimum resource utilisation in relation to the institution's objectives. Financial management covers the management of the institution's financial resources, activities, resources and results. The basic requirements for the institution include budget contributions, appropriation management and budget control, as well as accounting and annual reports.
The department creates a framework for objectives and the performance management process, including the management tools that should be used. It may contain a timetable, and possibly procedures for negotiating on the determination of objectives and reporting, monitoring and evaluation of performance and fulfilment of objectives.
For institutions, there are four basic requirements which must be met in order to satisfy the department's overall objectives and performance management:

1. The institution must set objectives for its core tasks.
2. The institution must establish HR policy quality objectives. These may be included in the institution's performance or directors' contracts or made public in some other way.

[30] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html

3. In its annual report, the institution must report on all external objectives, i.e. objectives set out in the Finance Act or otherwise agreed between the relevant department and the institution.
4. The institution and the department must review the institution's objectives and results at least once a year.

As a minimum, institutions must report on objectives in their annual reports. In this regard, the department is required to review and evaluate the institution's progress, even if this is sometimes done before the annual report is prepared. The head of department may enter into a performance-based salary contract with an agency or institution director which includes a variable pay clause in addition to the fixed salary. This practice is aimed at clarifying the objectives and direction for the institution's development and to give the director a financial incentive to ensure the control and management of the institution with a focus on results and impact.

France – Accountability Framework

The accountability framework is based on the principal assumption of managerial accountability.
Senior managers assume responsibility for establishing an adequate IC system by setting up and supporting an organisational control unit called the '*Revision interne'*, hereafter internal audit.
Managerial accountability is carried out by the head of the authority. The IA unit reports directly to the management, which cannot transfer its competence to other offices in the authority.
An authorised budget officer is to be appointed for every department that manages revenue and expenditure, as the manager of the department does not perform this task themself. The authorised officer is to report directly to the head of the department. The authorised budget officer must draw up the financial planning documents and the documents for drafting and executing the budget. They are to be involved in all financially significant measures. They can delegate tasks involved in executing the budget and are also responsible for reporting.
The management can establish which specialist departments are to be entrusted by the authorised budget officer with managing budgetary funds. As a rule, the amount of expenditure an authority can devote to each purpose is already laid out in the budget. The management normally delegates the decision on which specialised departments can make payments, and the volume of these payments, to the authorised budget officer.[31]

[31] More about accountability in: OECD (2014), *Accountability and Democratic Governance: Orientations and Principles for Development*, DAC Guidelines and Reference Series, OECD Publishing, Paris, https://doi.org/10.1787/9789264183636-en.

Risk assessment

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of objectives across the public organisation are considered in relation to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the public organisation. Management should specify objectives with sufficient clarity to be able to identify and analyse risks to those objectives. Management should also consider the suitability of the objectives for the public organisation. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own mission and responsibilities that may render IC ineffective.

Principle 6: The public organisation specifies suitable objectives[32]

France - Objective-oriented Management of Public Management

France has implemented a new approach to public management: an objective-oriented management. It is one of the key principles of the Organic Law governing Budget Laws. The general budget is structured on three levels: mission, programme and action.
One of the major issues of the public management reform was to make the State pass from a means-based culture to a results-based culture, so that each euro spent could be more useful and more effective. Thus, performance, i.e. the ability to attain the results expected, lies at the centre of the new budgetary framework. Consequently, Parliamentary debates both to vote on the adoption of the budget (initial budget law), and to examine budget implementation (budget review law), no longer refer only to the appropriations and their justification, but also to the strategies and objectives of public policies. A chain of responsibilities was thereby established in the administration, in which public authorising officers play a major part.
The State's major policies are transposed into missions. The Parliament votes on the budget per mission.
A mission is established at the Government's initiative and can be ministerial or interministerial. The mission contains programmes.
The programmes or the allocations define the implementation framework of public policies: the programme is the unit for parliamentary authorisation. It constitutes a global and restrictive package of appropriations. It issues from a single ministry and includes a coherent group of actions. It is assigned to a manager, appointed by the relevant minister. Each programme is associated with specific objectives and expected results. An indicative component of the programme, the action provides details on the intended destination of the appropriations.

In order to identify the use of public funds, each programme displays a double presentation of its appropriations: by destination (actions) and by type of expenditure (personnel, operating, investment, intervention, etc.).

[32] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapter on France. www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html
Example concerning Austrian budget reform: 1) The Austrian Federal Budget Reform. Federal Ministry of Finance, https://english.bmf.gv.at/budget-economic-policy/The-Austrian-Federal-Budget-Reform.html
2). Steger, G. (2010), *Austria's Budget Reform: How to Create Consensus for a Decisive Change of Fiscal Rules,* OECD Journal on Budgeting, Volume 2010/1, OECD Publishing, Paris https://www.oecd.org/austria/48168584.pdf

Each programme has a corresponding strategy, objectives and quantified performance indicators. These elements are included in the annual performance plans annexed to the draft budget law.
Under the authority of the respective minister, the project manager undertakes to meet these requirements. He/she reports the results obtained to the Parliament when the budget review law is being examined, in the annual performance report.
The State operators ("public agencies"), which implement certain sections of public policies, are included in the annual performance plans in order to identify and assess their contribution.
The introduction in the same document of financial elements and performance assessment encourages the continuous improvement of public expenditure effectiveness. The relevance, reliability and truthfulness of the indicators are evaluated by the Court of Auditors

Austria – Performance-based Budgeting and Medium-term Expenditure Framework

In December 2007 and December 2009, Austria's Federal Parliament decided on a far-reaching, comprehensive budget reform package. The introduction of a legally binding medium-term expenditure framework (MTEF), of accrual budgeting and accounting as well as performance budgeting marks a decisive change, not only in steering the budget, but even more so in the Austrian administrative and political culture.

The MTEF contains legally binding expenditure ceilings four years in advance on a rolling basis. The ceilings apply to groups of chapters (so-called "rubrics"). Each of the five rubrics has its own expenditure ceiling, which add to one ceiling for the federal budget. The five rubrics represent the following budget clusters:

1. Law and security (ministries for justice; interior; defence; foreign affairs; the administration of the MoF; Chancellery).
2. Employment, social services, health and family (self-explanatory).
3. Education, research, art and culture (self-explanatory).
4. Economic affairs, infrastructure and environment (ministries for economy; agriculture, forestry, water and environment; infrastructure; part of the MoF).
5. Financial management and interest (part of the MoF).

The Austrian system distinguishes between two different expenditure ceilings. One is a nominal fixed ceiling, expressed in euros, which applies to most (75%) of the expenditure. The other is a variable ceiling that oscillates along defined parameters. Variable ceilings are only provided for in the case of certain elements that either depend on the performance of the economy or on tax revenue levels. The amounts of those variable ceilings are determined by clearly defined parameters. In this way, the budget helps to stabilise the economy. The ceilings are set, and can be amended, by the Austrian Parliament. Thus, the political process helps to maintain the necessary spending discipline but is simultaneously able at all times to react to changes in priorities. Accordingly, the Austrian Parliament always retains the final say with respect to the budget.

The MTEF with its legally binding multi-year approach helps the MoF and the line ministries to improve budget planning. While the MoF is interested in enforcing restrictive expenditure ceilings and sticking to them even in difficult times, the line ministries do have their part of the deal: if they save money within the expenditure ceilings, they are allowed to build reserves (and use them in later years – even for different purposes).

A crucial element of the Austrian reform is performance budgeting. Each ministry has to define a strictly limited number of intended policy outcomes, outputs, and performance indicators which require the approval of parliament. Gender equality is one of the dimensions of this framework, and the only one that is completely cross-cutting and mandatory for all ministries. For each of the 32 budget chapters, a maximum of five outcome/impact objectives (and related performance indicators) have to be defined by the ministries, out of which one objective must be related to improving gender equality.

Principle 7: The public organisation identifies and analyses risk[33]

Estonia – Regulating the Risk Management in Legislation and Guidelines

Section 10(3) of the Government of the Republic Regulation "Types of strategic development plans, the procedure for their preparation, amendment, implementation and evaluation and the reporting procedure" stipulates that as regards the analysis of the organisation's current situation, a summary of the risk analysis and an analysis of the activity environment must be submitted. This ascertains the readiness of the state authority to achieve the objectives set in the development plan, and provides a description of the main risks in relation to the implementation of the development plan and activities to manage these risks. Other legislative acts do not refer to risk assessment. In the third part of the activity report, the head of the state accounting entity indicates whether a risk assessment was carried out in the ministry or its area of government during the reporting period. The guidelines for risk assessments drawn up by the Ministry of Finance were replaced in 2011 by up-to-date risk management guidelines.

Ireland – Risk Management Governance within the Government Departments and Offices

The accounting officer of a department has ultimate responsibility for risk management. Each Department is required to have a pro-active management-led risk management policy as part of their governance framework.
The accounting officer and heads of offices should define the management boards' role in regard to risk and ensure that there are adequate systems in place for identification and management of risk. The role of the managers and relevant officials with responsibility for policy and financial risk should be clearly defined in each department's framework of assignments under the Public Service Management Act 1997 and in the Statement of Internal Financial Control.

[33] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapters on Estonia and the UK www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html

Example from Ireland: Department of Public Expenditure and Reform (2016) *Risk Management Guidance for Government Departments and Offices*, Section 1.1 Governance https://govacc.per.gov.ie/wp-content/uploads/2016/02/Risk-Management-Guidance-February-2016.pdf
Example from the NHS: Sheffield Teaching Hospitals NHS Foundation Trust (2013), *Risk Management Policy*. Summary based on Appendix C https://www.sth.nhs.uk/clientfiles/File/Enclosure%20K%20-%20RiskManagementPolicyStrategy.pdf

The management board should ensure that the risk management policy is an integral part of the business planning, decision making and management process, with appropriate structures, management and reporting. The risk management policy should:
- add value to business activity and contribute to the economic, effective and efficient delivery of business objectives, at both strategic and operational level;
- reflect organisational culture and values; and
- take account of the environment, both internal and external, in which the department operates.

England – Risk Assessment and Registration at the National Health Service (NHS)

Identification and registration of risks
Risks can be identified in a number of ways and from a range of sources.
Once a risk is identified it must be documented using a Risk Assessment Form, assessed and an action plan developed to reduce the risk to an acceptable level.
Risk assessments can and should be made at any level in the organisation. However, before a risk can be formally recorded on DATIX Risk Management system (a web-based incident reporting and risk management software for healthcare and social care organisations), it must be reviewed and approved by the relevant risk forum to ensure that the minimum level of information required is captured and facilitate appropriate challenge. Specifically, the risk forum is required to assess and approve:

- The initial / current risk score with existing controls but prior the treatment plan.
- The achievability of the treatment plan, considering such aspects as affordability, timescales, service delivery etc.
- The scoring of the target risk score.
- The frequency of review.

Guidance and support is available from the Patient and Healthcare Governance department.

Escalating the risks
Risks rated as Moderate or above (i.e. risk score 4 or more (out of max. 25)) shall be reported to the Risk Validation Group (RVG) who will validate the score and risk grade and provide a monthly report to Safety and Risk Management Board and Trust Executive Group (TEG). This provides further opportunity to scrutinise and challenge the risk assessment and action plan. It also allows for consideration of where the management of the risk best lies.

Risk aggregation
Ensuring appropriate aggregation of common risks is a key challenge of any risk management process. Many departments and directorates face similar risks e.g. in-year cost pressures, recruitment problems etc which may be assessed as low rating and locally managed. Taken individually these risks will not significantly impact on the organisation but collectively have the potential to threaten achievement of the strategic objectives.
On an ongoing basis, relevant risk forums must consider the potential for risk aggregation when reviewing new risks. The potential may result from several common risks being identified across a number of areas or as a result of a risk having been identified in one area that has implications across a wide number of services. In such circumstances, a new risk assessment of the aggregated risk should be undertaken and documented on the Risk Assessment Form (ensuring that all the subordinate risks are fully described) and registered on DATIX. It is possible that the aggregated impact score will be different from the individual risks and also that the action plan will require revision. The aggregated risk will supersede the subordinate risks, which

should be removed from DATIX. The Risk Validation Group will consider the implications for risk aggregation and will report these issues as they arise to Safety and Risk Management Board and TEG.

Reviewing a risk registered in DATIX
Risks registered on DATIX must specify when the current risk score, action plan and target risk score will be reviewed. It is expected that as action plans are progressed the current risk score will move towards the target risk score and may be closed (if the risk has been eliminated) or tolerated (if the risk remains but all planned mitigating action has been taken). This may be achieved within one review period but it may take longer, in which case a new review date must be set. All risks must be reviewed at least once a year. A new Risk Assessment Form shall be completed for all subsequent reviews and must be uploaded on to DATIX.

Principle 8: The public organisation assesses fraud risk[34]

UK – Embedding Fraud Risk Assessment into the Risk Management Framework

The National Audit Office (NAO) works with a range of government and non-government bodies to tackle fraud and reduce the cost of fraud to the UK economy. Stakeholders include the National Fraud Authority (NFA), the Cabinet Office Fraud Error and Debt unit, the CIPFA Better Governance Forum, the Audit Commission and the Counter Fraud Champions. The NFA is an executive agency within central government that brings together the efforts of a large number of counter-fraud bodies across the private, public and voluntary sectors that are involved in gathering intelligence and taking action against fraudsters. In central government a network of Counter Fraud Champions has been established, representing all main departments, with a view to tackling fraud and error. The Counter Fraud Champions will lead the fight against fraud and error in their own central government department and in the agencies and other public bodies for which the department has responsibility. Their priorities will include instilling an anti-fraud culture in their organisation, measuring fraud in their departments and publishing the figures for the first time, making sure new policies and programmes are fraud proofed by undertaking fraud risk assessments.

England - NHS Counter Fraud Authority and Standards on Fraud Risk Assessment

The NHS Counter Fraud Authority (NHSCFA) is a new special health authority charged with identifying, investigating and preventing fraud and other economic crime within the NHS and the wider health group. As a special health authority focused entirely on counter fraud work, the NHSCFA is independent from other NHS bodies and directly accountable to the Department of Health and Social Care (DHSC).

[34] Source: European Commission (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapter on UK.
www.ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html
NHS example: NHS Counter Fraud Authority website: https://cfa.nhs.uk/about-nhscfa/who-we-are
Summary based on: NHS Counter Fraud Authority (2018), *Standards for NHS Providers 2018-19*
https://cfa.nhs.uk/resources/downloads/standards/NHS_Fraud_Standards_for_Providers_2018.pdf?v=1.0

Under the NHS Standard Contract, all organisations providing NHS services (providers) must put in place and maintain appropriate counter fraud arrangements. The NHSCFA has published a set of standards for the providers, consisting of four key sections that follow the NHSCFA's strategy:

- Key Principle 1: Strategic Governance. This section sets out the standards in relation to the organisation's strategic governance arrangements.
- Key Principle 2: Inform and Involve. This section sets out the requirements in relation to raising awareness of crime risks against the NHS and working with NHS staff, stakeholders and the public to highlight the risks and consequences of fraud and bribery affecting the NHS.
- Key Principle 3: Prevent and Deter. This section sets out the requirements in relation to discouraging individuals who may be tempted to commit fraud against the NHS and ensuring that opportunities for fraud to occur are minimised.
- Key Principle 4: Hold to Account. This section sets out the requirements in relation to detecting and investigating economic crime, obtaining sanctions and seeking redress.

The NHSCFA has established a quality assurance programme which comprises of two main processes:

- The quality assurance process, which includes an annual self review against the standards, which is conducted by organisations and submitted to the NHSCFA.
- The assessment process, which is conducted by the NHSCFA's Quality and Compliance team in partnership with the organisation.

The NHSCFA requires organisations to provide an annual statement of assurance against the counter fraud standards. This statement of assurance is provided through completion of the annual report and the Self Review Tool (SRT).

Selection of NHS standards for providers related to risk assessment practices

Standard 1.3 requires the provider to employ or contract in an accredited, nominated person (or persons) to undertake the full range of counter fraud, bribery and corruption work, including proactive work to prevent and deter fraud, bribery and corruption and reactive work to hold those who commit fraud, bribery or corruption to account.

Standard 1.4 requires the provider to carry out risk assessments to identify fraud, bribery and corruption risks, and have in place counter fraud, bribery and corruption provision that is proportionate to the level of risk identified. Measures to mitigate identified risks shall be included in an organisational work plan, progress shall be monitored at a senior level within the organisation and results shall be fed back to the audit committee (or equivalent body).

Standard 1.5 requires the provider to report annually on how it has met the standards set by NHSCFA in relation to counter fraud, bribery and corruption work, and detail corrective action where standards have not been met.

Standard 1.6 requires the provider to ensure that those carrying out counter fraud, bribery and corruption work have all the necessary tools and resources to enable them to carry out their role efficiently, effectively and promptly. This includes (but is not limited to) access to IT systems and access to secure storage.

Principle 9: The public organisation identifies and analyses significant changes

Estonia – e-Government Risks[35]

The Estonian Cyber Security Strategy is the basic document for planning Estonia's cyber security and is a part of Estonia's broader security strategy. It highlights important recent developments, assesses threats to Estonia's cyber security and presents measures to manage threats.

The main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population. Therefore, the key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. Additional supporting activities will include shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions.

[35] Source: Summary based on Ministry of Economic Affairs and Communication (2014), *Estonian Cyber Security Strategy 2014-2017*, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Control activities

Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the IC system, which includes the public organisation's information system.

Principle 10: The public organisation selects and develops control activities[36]

Estonia – Control Requirements in Accounting Processes

The responsibility of accounting unit personnel is determined by their job description. Document control requirements are laid down in the accounting principles and procedures, which also establish who is responsible for ensuring that:

a) the document shows the business transaction correctly;

b) the amounts, prices and other conditions shown in the document are in line with contracts previously concluded;

c) a transaction is lawful and necessary;

d) a transaction is in compliance with the budget;

e) the terms and conditions of a transaction are in line with the terms and conditions of similar transactions;

f) the contracts were concluded in accordance with the principle of economy.

g) When checking documents and preparing transfer documents, the personnel of an accounting unit must ensure that the following information is checked and entered correctly in the accounting system:

   a. the transaction was carried out in accordance with the principles for monitoring budget implementation;

   b. the accounts, transaction partner, field of activity, source, cash flow and budget classification codes are accurate;

   c. the term of payment;

   d. the accrual period;

   e. information of the recipient, including when value added tax is shown on the purchase document, performing checks to confirm whether the supplier is registered as a person liable to value added tax and whether the invoice is prepared in compliance with the Value Added Tax Act;

   f. whether the particular goods, service or other benefit has been paid for beforehand;

   g. whether the purchase transaction was checked according to the requirements set for document checks and was approved by the person(s) authorised to do so.

[36] Source: EC(2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapter on Estonia http://ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html

The requirements for document checks must ensure that the authorised person (signatory) and the employee of the accounting unit are separate. The head of the authority will appoint the authorised person(s) within the scope of his/her competence. Every source document must be signed by both the authorised person and the employee of the accounting unit.
If possible, two persons (four-eye principle) must be involved in the money transfer process. Where electronic transfers are made, the rights are assigned so that one person cannot perform a transfer alone. In order to fulfil this requirement, the person entering a transfer must be different to the person accepting the transfer. Another person besides the cashier approves the cash payment order.
These measures ensure that the responsibilities are separate when transactions are made, approving rights are assigned, four-eye principle is applied, and that the information systems include automatic checks of access to resources and data access, data are reconciled and supervision is exercised.

Principle 11: The public organisation selects and develops general control activities over technology[37]

Estonia – Automated Control Measures in Information Systems

The control measures in information systems are automated and mainly ongoing.
For example, the following checks are run in the system on a payment order entered into the e-Treasury:

a) that the payment order has been filled in correctly;

b) that the authority has free state budget funds, or for state foundations, the balance of e-Treasury revenue accounts is checked;

c) that the minimum payment amount to the recipient via a domestic bank transfer is EUR 0.05 and to a foreign country EUR 1.90.

The control measures within the IT systems are constantly being updated to keep abreast of the rapid development in the IT systems.

UK - Business Continuity Management in the NHS

5.1. Business Continuity is the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
5.2. The Business Continuity Management System (BCMS) requirements apply to all directorates, and all Trust departments are expected to adhere to the BCMS and associated processes and procedures.
5.3. To achieve the intended outcome(s) of the BCMS, the Trust has identified internal and external issues that have been taken into account when developing the BCMS.

[37] Source: EC (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapter on Estonia http://ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html
NHS example: NHS (2014), Summary from the Business Continuity Policy of South Western Ambulance Service. Version 7.1, effective date of issue 16.10.2014.
https://www.swast.nhs.uk/welcome/about-us/welcome-to-south-western-ambulance-service-nhs-foundation-trust-swasft

5.16. The Business Continuity objectives have been agreed for 2014-2017 as:
5.16.1. To develop, maintain and continuously improve a Business Continuity Management System which satisfies the requirements of ISO 22301. The Trust is committed to conforming to ISO22301 in its entirety across the whole organisation. At this time, accreditation is not being considered.
5.16.2. Use the BCMS to identify, protect and maintain prioritised activities, in order to deliver and recover service to an acceptable level
5.16.3. Each identified critical and essential departmental business continuity planning shall complete a cycle of the BCMS annually within their respective department.
5.16.4. The Trust-wide Business Continuity planning shall complete a cycle of the BCMS annually with associated documentation including all relevant areas of the Trust.
5.16.5. Trust-wide awareness and consideration of Business Continuity will factor in daily activity for all Trust staff. This will be promoted through awareness campaigns, workshops, training and exercising. The awareness and use of the "SWASFT 5" slogan and associated material will be recognised and understood by all Trust staff
5.16.6. To guide the Trust into a position where it can easily demonstrate through audit and peer reviews alignment to Business Continuity standard ISO 22301:2012
5.16.7. To develop and integrate technology to assist with the BCMS
5.26. Every Trust department will complete a cycle of the BCMS within their department by completing:
5.26.1. Business Impact Analysis (BIA) (Analysis)
5.26.2. Publishing of a Business Continuity Plan (Design)
5.26.3. Awareness training (Implementation)
5.26.4. Exercising (Validation)
7.1. For every BIA there will be an associated BCP detailing the arrangements to reduce any risks identified and arrangements in place to manage any impact from a disruptive incident, owned by each Trust Directorate.

Principle 12: The public organisation deploys control activities through policies and procedures[38]

Estonia – Scope of Public Organisation's Accounting Principles and Procedures

A large part of control activities is laid down by law and internal rules regulating the work in various sectors. For example, according to the general rules for state accounting, an entity's accounting principles and procedures have to establish requirements for preparing and checking source documents, entering data into an accounting information system, assessing accounting journals and ledgers, and preserving documents. The general rules also include requirements for the deadlines for submitting documents and reports.

Hungary – Scope of Internal Procedural Rules

[38] Source: EC(2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Chapters on Estonia and Hungary
http://ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html
NHS example: NHS (2014), Summary from the Business Continuity Policy of South Western Ambulance Service. Version 7.1, effective date of issue 16.10.2014.
https://www.swast.nhs.uk/welcome/about-us/welcome-to-south-western-ambulance-service-nhs-foundation-trust-swasft

The head of the public budgetary organisation shall establish control activities dealing with the acknowledged risks and contribute to the achievement of the organisation's objectives. The internal procedural rules shall regulate at least the following: procedures of authorisation and approval; access to information; physical controls (access to equipment); procedures of reporting.

UK – Procedures as a Response to the Business Continuity Risks the NHS

7.2. The Trust will document procedures for managing and responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe.
7.7. Procedures will be established through the Business Continuity planning to manage a disruptive incident and continue activities based on recovery objectives identified in the business impact analysis. Documented procedures (including necessary arrangements) shall:
7.7.1 Establish an appropriate internal and external communications protocol
7.7.2 Be specific regarding the immediate steps that are to be taken during a disruption
7.7.3 Be flexible to respond to unanticipated threats and changing internal and external conditions
7.7.4 Focus on the impact of events
7.7.5 Be developed based on stated assumptions and an analysis of interdependencies
7.7.6 Be effective in minimising consequences through implementation of appropriate mitigation strategies
7.8. Specific procedures that shall establish, be documented and implemented across the organisation shall include a response structure that shall:
7.8.1. Identify impact thresholds that justify initiation of a formal response
7.8.2. Assess the nature and extent of a disruptive incident and its potential impact
7.8.3. Activate an appropriate business continuity response
7.8.4. Detail activation, operation, coordination and communication of the response
7.8.5. Detail the resources required
7.8.6. Methods of the detection of a Business Continuity incident 7.8.7. Provide regular monitoring of an incident
7.8.8. Provide internal communication
7.8.9. Record vital information about the incident, actions taken and decision made
7.9. Recovery from a disruptive incident shall follow a documented procedure to restore and return Trust activities from a temporary state to support normal Trust business following an incident (Business Continuity incident, major or critical incidents).

Information and communication

Management of the public organisation uses quality information to support the IC system. Effective information and communication are vital for a public organisation to achieve its objectives. The management needs access to relevant and reliable communication related to internal as well as external events.

Principle 13: The public organisation obtains, generates and uses relevant, quality information

Estonia - Interoperability of Information Systems[39]

Since 1990, Estonia has used a personal identification code (isikukood) to uniquely identify each citizen and resident in government information systems. This has the advantage of facilitating data exchanges between different administrations and is an important building block for the implementation of the "once only" principle.

In 1997, the "once only" principle became a legal obligation, meaning the public administration could not ask an individual to provide information she or he had already provided to any part of the administration. Political commitment to make the principle a reality, coupled with the understanding that speedy and comprehensive availability of information for decision makers is critical in a country with limited human and natural resources, led to the development of a national interoperability infrastructure for real-time exchanges between organisations. The data exchange layer X-Road was launched in 2001 and has since become the standard platform for streamlining services between government agencies in Estonia. It is also used to create seamless workflows that involve non-government actors, e.g. to exchange information on income and assets from private companies to taxation and social security authorities.
The Digital Signatures Act in 2000 recognises digital signatures as being fully equivalent to hand-written signatures, both in commercial transactions as well as transactions with the public sector. The Estonian national identification card and later the equivalent mobile-ID (jointly hereinafter: national digital ID) became the building block of a national personal key infrastructure (PKI), turning it into a legitimate means for authentication and authorisation in digital transactions, i.e. electronic signing. The dual use for commercial and public sector transactions, as well as the obligation for the public sector to recognise the national digital ID, created an environment that stimulated the development of compatible public services as well as their take-up by the general population. All digital public services can be accessed using the national digital ID, including electronic voting, electronic prescriptions, electronic health records, registration of businesses, declaration of residence, social benefits claims.
Estonia established as a principle that an individual should have control over how their personal data is used and should be able to see which civil servant accessed their data. This was put into practice by creating a mechanism that logs any access to personal data and lets personnel use the public service portal www.eesti.ee (or the national healthcare portal for healthcare records) to monitor which department consulted their data. A data protection claims procedure can be launched at the suspicion of a privacy breach. This is a very important vector for openness and transparency as it gives citizens not only the right to have their privacy protected, but also the actual tools to empower them to monitor if that right is being respected.

[39] Source: OECD (2015), *OECD Public Governance Reviews, Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders*, OECD Publishing, Paris, https://doi.org/10.1787/9789264229334

Principle 14: The public organisation ensures proper internal communication[40]

UK – Government Security Classifications

UK – Government Security Classifications describe how the Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners. stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.
Everyone who works with government has a duty to respect the confidentiality and integrity of any HMG information and data that they access, and is personally accountable for safeguarding assets in line with this policy.
HMG information assets may be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.
Government Departments and Agencies should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. NDPBs and Arms Length Bodies) and wider supply chain.

Principle 15: The public organisation ensures proper external communication[41]

Estonia - Participatory Budgeting in Tartu

In 2013, the City of Tartu, the second-largest city after Tallinn, became the first municipality in Estonia to launch participatory budgeting. Participatory budgeting grants citizens a better understanding and say of how the budget is spent, in this case on the local level.
The participatory budget process granted citizens of Tartu the opportunity to decide on how a portion of the city budget (amounting to EUR 140 000 of the investment budget, or 1%) should be spent. The initiative was part of the broader programme to raise awareness of local governance and foster broader engagement. The aims of the programme included:

- better explaining the logic of budget to citizens and reducing criticism
- increasing the understanding of how decisions are made in the city, and increasing trust in those decisions
- increasing co-operation inside the community and between the communities

[40] Source: The UK Government Security Classifications, April 2014, https://www.gov.uk/government/publications/government-security-classifications
[41] Source: OECD (2015), *OECD Public Governance Reviews, Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders* , OECD Publishing, Paris, https://doi.org/10.1787/9789264229334 and information from https://e-estonia.com

- building discussion among all stakeholders in relation to the problems the city faces and the possible solutions
- increasing citizens' readiness to take part in activities of the city.

In March 2013 a working group of participatory budgeting was created in the Tartu city government. From March to June, a working group of the political and administrative leaders had meetings to decide how to implement participatory budgeting in Tartu. The City Council adopted the scenario for implementing participatory budgeting and assigned 1% of the investment budget to it.
In August, the process was presented to the public and an online platform was launched. From the period 21 August-10 September 2013 the public could submit their suggestions for the portion of the investment budget via the website. Suggestions had to meet three basic criteria: i) be an investment in the public sphere of the city that would benefit as many people as possible; ii) cost less than EUR 140 000; iii) be feasible within a year. The people of Tartu submitted 158 ideas (one on paper, all others electronically).
In September and October, the proposals were analysed by field experts, similar ideas grouped together, and for each idea an assessment was made about its feasibility and its estimated cost. Based on the above criteria, the experts passed 74 ideas to the public vote. In November, the proposed ideas were published on Tartu's municipal website and on 19 November a public presentation event took place. The event provided the opportunity for proposed ideas to be presented.
Public voting took place during 2-8 December on the 74 proposals. All citizens of Tartu, 16 or older, had the opportunity to vote, either electronically (using ID-card or mobile-ID) or on paper ballot. Altogether, 3.3% of Tartu's citizens participated in the public ballot. Ninety percent of the votes were given electronically and 10% on paper ballot. The average age of the voters was 38 years, 42% were men and 58% women.
The proposal to invest in presentation equipment in the Cultural Quarter won the ballot and was granted the investment sum via the adoption of the budget by the City Council in December 2013.
Lessons from the first participatory budgeting process revealed that the scenario should be changed to enable public discussions in the initial phase and engage more non-profit organisations in the planning phase, as well as the need to change the voting system to give smaller ideas more chance.
Since 2014, the participatory budgeting process in Tartu is synchronised with the budgetary process of the city, both starting in the spring. In 2014, along with Tartu continuing with participatory budgeting, the Estonian town of Kuressaare will also launch participatory budgeting, assigning EUR 30 000 to be decided by the citizens.

Estonia – e-government solutions

When Estonia started building its information society about two decades ago, there was no digital data being collected about the citizens. The general population did not have the internet or even devices with which to use it. It took great courage to invest in IT solutions and take the information technology route. Below are some of the e-solutions that have led to Estonia becoming one of the world's most developed digital societies.

Modern e-solutions have made setting up and running a business in Estonia quick and easy. Estonian e-solutions for business, such as electronic tax claims, have pared bureaucracy down to a bare minimum and facilitated an environment where business is extremely convenient. Today, one can pay the taxes in Estonia only in one click - all it is needed is 3-5 minutes for the tax filing process and it's done. That is why each year, around 95 per cent of all tax declarations in Estonia are filed electronically.

Nearly every one of Estonia's 1.3 million citizens has an ID card, which is much more than simply a legal photo ID. Technically, it is a mandatory national card with a chip that carries embedded files, and using 2048-bit public key encryption, it can function as definitive proof of ID in an electronic environment. Functionally, the ID card provides digital access to all of Estonia's secure e-services, releasing a person from

tedious red tape and making daily tasks faster and more comfortable whether we are talking about banking or business operations, signing documents or obtaining a digital medical prescription.

Moreover, Estonia was the first nation in history to offer internet voting in a nationwide election in 2005. Completely unrelated to the costly electronic voting systems with their problematic machinery used in some countries, the Estonian open-source voting solution is simple and secure. The groundbreaking i-Voting system allows citizens to vote at their convenience, no matter how far they are from a polling station, since the ballot can be cast from any internet-connected computer anywhere in the world. i-Voting has become a reality only thanks to the fact that the majority of the residents have a unique secure digital identification provided by the state. i-Voting takes just 3 minutes and brings votes from all over the world.
The introduction of IT has helped to strengthen public order in Estonia and assist in the case of accidents. The use of IT tools in the security services (e-Police, rescue board, emergency centre) has halved the number of deaths by accident in Estonia over the last 20 years. Employees of the security services are now able to remotely determine 35% of the locations of accident victims to within a 5-metre radius, and 93% of emergency calls are answered within 10 seconds. Estonian police are no longer allowed to stop cars for technical checks, as all the relevant data is available using their onboard computer. This has made the police 50 times more efficient.

Monitoring activities

Monitoring of the IC system is essential in helping IC remain aligned with changing objectives, environment, laws, resources, and risks. IC monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews.
Corrective actions are a necessary complement to control activities in order to achieve objectives.

Principle 16: The public organisation selects, develops and performs ongoing and/or separate evaluations[42]

Malta – Statement on internal control

As part of the reporting system, a statement on IC is in the process of being adopted across the public administration in Malta in order to ensure further accountability and responsibility. This shall include a declaration that the internal control system supporting the achievement of the ministry/department/ entity's policies, aims and objectives has been put in place, and that public funds and all organisations' assets are being safeguarded.
Moreover, it will also comprise an affirmation that a risk management system designed to identify and prioritise the risks to the achievement of the ministry/department/entity's policies, aims and objectives has been implemented. Top management positions will be expected to sign this statement on internal control at the end of each year for the organisation they manage as part of the annual report.
Moreover, government departments, ministries and entities are currently required to submit an annual report detailing the activities carried out, as well as an action plan outlining what activities are to be undertaken.

Sweden –Monitoring the efficiency of the higher education institutions.

The Swedish Higher Education Authority (UKÄ) is responsible for monitoring the efficiency of the operations of the higher education institutions. The Government's objective is that education and research at higher education institutions (HEIs) should maintain high international standards and be run efficiently.
The monitoring of efficiency at Swedish HEIs includes, for instance:

- Looking at the way the higher education institutions use their resources and in particular developing ways of monitoring inactive students.Looking at the way the higher education institutions use their resources and in particular developing ways of monitoring inactive students.
- Developing methods of measuring developments in efficiency and productivity in as many of the sector's tasks as possible.Developing methods of measuring developments in efficiency and productivity in as many of the sector's tasks as possible.

It follows up and analyses the operations of higher education institutions, primarily to provide the Swedish parliament (Riksdag) and Government with material on which to base decisions about higher education. It monitors developments in the higher education sector, mainly in Europe and the USA but also in the rest of the world.
Its responsibilities include:

[42] Source: Department of Public Expenditure and Reform (2014) http://govacc.per.gov.ie/wp-content/uploads/2014/06/Statement-on-Internal-Financial-Control-for-website.pdf%20%20 , Compendium 2014 and http://english.uka.se/

- to ensure that the statistics are objective
- to ensure that the statistics are documented
- to ensure that the statistics are quality-assured

HEIs and the Swedish Higher Education Authority (UKÄ) have a shared responsibility for quality assurance in higher education and research. Most quality assurance efforts are to be conducted by the HEIs. This requires HEIs to have systematic quality assurance processes that UKÄ is responsible for assessing. UKÄ is also responsible for ensuring that all the courses and programmes are encompassed by these processes. This is done partly by UKÄ evaluating a selection of programmes and partly by the HEIs having responsibility for quality assuring their own courses and programmes and that UKÄ monitors that this has been carried out.

Assessment material

The basis for the review consists of a self-evaluation by the HEI, a student report, interviews, site visits, audit trails and other information. All assessment material for the review is to be weighed together.

1. The HEI's self-evaluation. The HEIs are asked to describe, analyse and evaluate how they systematically ensure and follow up that they fulfil the assessment criteria for the different aspects and perspectives. Examples should be given to support the presentation.
2. Student report. The local student union has the option of submitting a written statement, known as a student report, in which the union gives its opinion of the quality assurance work at the HEI.
3. Interviews and site visits. Interviews will be conducted both before and during the site visit. The purpose of the initial interview is to gain an overall picture of the quality assurance processes, to improve planning for the site visit, and to identify the areas that the panel wants to gain a detailed picture of during the site visit. Initial interviews and site visits involve representatives from the HEI and student representatives, and possibly employer and labour market representatives with which the HEI cooperates.
4. Audit trails. To examine how quality assurance processes work in practice, the assessors examine one or more areas of focus. In this context, areas of focus are quality assurance processes, related to the aspects, perspectives and assessment criteria in the selected and assessed environment during the site visit. To see how quality assurance processes work in practice, the process is followed from the overall organisation at the HEI to the local level, that is, an environment which could consist of one or more courses and programmes (main field, subject area, programme) or other types of environments, like a library.
5. Other assessment material. Prior to reviews, UKÄ produces data for the HEI relevant to the aspects to be examined. This data could be previous inspections, appraisals of degree-awarding power applications, programme evaluations and national statistics showing student completion and establishment levels, and illustrating the HEI from a national perspective.

Assessments and reports

The assessment panel's judgment on whether the HEI meets the assessment criteria for the reviewed aspect areas and perspectives results in a report that serves as the basis for UKÄ's decision. Before UKÄ's final decision, the panel's preliminary judgement will be sent to the HEI for review.

One year to address the problems

If the quality assurance processes do not meet the criteria, the HEI has one year to present the measures it has taken to address the problems. UKÄ will appoint an assessment panel to review the measures. If the HEI's quality assurance processes still do not meet the assessment criteria in the follow-up review, this means

that an additional follow-up review should be conducted after a period agreed upon by UKÄ and the HEI jointly. This also means that an increased number of the HEI's programmes can be evaluated by the HEI.

Principle 17: The public organisation evaluates and communicates deficiencies[43]

UK - Risk Register of Civil Emergencies

The National Risk Register of Civil Emergencies 2017 **e**dition provides an updated government assessment of the likelihood and potential impact of a range of different civil emergency risks (including naturally and accidentally occurring hazards and malicious threats) that may directly affect the UK over the next five years.

In addition to providing information on how the UK government and local responders manage these emergencies, the National Risk Register also signposts advice and guidance on what members of the public can do to prepare for these events.

In addition to using the National Risk Register, the public can also find information about risks to their local area through their Community Risk Register. The NRR provides links and information about how to find your local Community Risk Register.

UK -Complaints procedure

The Home Office defines a complaint as an expression of dissatisfaction with the services provided by the Home Office. This is not the same as general correspondence from members of Parliament, the public expressing disagreement with a policy, or requests under the Freedom of Information Act. If a person is dissatisfied with the service you receive from Home Office, one should contact it.

The complaint can be made by emailing: public.enquiries@homeoffice.gsi.gov.uk, or in writing. One can also telephone the government switchboard on 020 7035 4848. The switchboard handles calls for many departments and tries to put you through to the appropriate member of staff. The person contacting the HO should give full details and include information (if she/ he has it) about the part of the department she/ he felt provided a dissatisfactory service. She/ he should also provide the following details:

- the area of the Home Office to which your complaint refers and a contact name,
- information on whether it is an original complaint or a follow-up to a reply the person was not satisfied with,
- a clear description of the complaint and what she/ he would like the HO to do to sort things out;
- postal address, phone number and e-mail address.

[43] Compendium 2014 and Cabinet Office (2017), *National Risk Register of Civil Emergencies* https://www.gov.uk/government/publications/national-risk-register-of-civil-emergencies-2017-edition

The aim is to respond within 20 working days if the complaint is in writing. If it is not possible to give a full reply within this time (for example, if the complaint requires more detailed investigation), the HO explains what is being done and when a full response can be expected.

The HO acknowledges where things could have been done better, an explains what will be done to avoid the same thing happening again. Equally, if the HO does not uphold the complaint, it explains why.

The SIGMA Programme

SIGMA (Support for Improvement in Governance and Management) is a joint initiative of the OECD and the European Union (EU), principally financed by the EU. SIGMA has been working with partner countries on strengthening public governance systems and public administration capacities since 1992.

In partnership with the European Commission (EC) Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR), we currently work with:

- Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia, and Turkey as EU candidate countries and potential candidates; and
- Algeria, Armenia, Azerbaijan, Belarus, Egypt, Georgia, Jordan, Lebanon, Moldova, Morocco, Palestinian Authority[1], Tunisia and Ukraine as EU Neighbourhood countries.

SIGMA provides assistance in six key areas:

1. Strategic framework of public administration reform
2. Policy development and co-ordination
3. Public service and human resource management
4. Accountability
5. Service delivery
6. Public financial management, public procurement and external audit.

SIGMA reviews and gives feedback on:

- Governance systems and institutions
- Legal frameworks
- Reform strategies and action plans
- Progress in reform implementation.

SIGMA provides:

- Advice on the design and prioritisation of reforms
- Methodologies and tools to support implementation
- Recommendations for improving laws and administrative arrangements
- Opportunities to share good practice from a wide range of countries, including regional events
- Policy papers and multi-country comparative studies.

For further information on SIGMA, consult our website: www.sigmaweb.org

* This designation is without prejudice to positions on status, and is in line with United Nations Security Council Resolution 1244/99 and the Advisory Opinion of the International Court of Justice on Kosovo's declaration of independence.

[1] Footnote by the European External Action Service and the European Commission: this designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the European Union Member States on this issue.