EUROPEAN COMMISSION
INTERNAL AUDIT SERVICE

Directorate B – Audit of the Commission

European Commission

Internal Audit Manual

Version 3 - Date: July 2012

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Office: MADO 27/043. Telephone: direct line (32-2) 299 67 30 Fax: (32-2) 299 83 63

TABLE OF CONTENTS

Document History

Version	Date	Comment	Modified Pages
Draft	November 2009	First draft	All
Final	December 2009	Version 1	All
Final	February 2010	Version 2	9, 12-19, 38-41
Final	May 2012	Version 3	Reference to Methodological Guidance for the use of GRC regarding requirements of documentation in GRC application Additional guidance on follow-up of Multi-DGs audits (section 3.13.3)

1. INTRODUCTION

1.1. Purpose

This document provides a comprehensive overview of the IAS audit processes and methodologies.

1.2. Scope

This document – "manual" - can be used in three distinct ways.

- A read-through is suggested for first time auditors. This will clarify both the generalities and the specifics of the internal audit process as executed within the Commission.

- The more experienced auditor can use the table of contents to select a specific subject, on which he or she wants to obtain further information.

In the flowcharts presented in the next few sections of this document, processes are included in their wider context (Information sharing and document management) or broken down into more detailed activities (Audit process, Recommendation follow-up).

This document only covers the IAS processes.

2. INTERNAL AUDIT ORGANISATION AND GENERAL ISSUES

2.1. Principal references for Internal Audit

- The Guidance given on the IIA's web-site[1] under the heading of "Professional Guidance",

- Charter of the Internal Audit Service (IAS) of the European Commission – SEC(2000)1801/2, 31 October 2000, (revised, 2007)

- Conditions for the Provision of an Internal Audit Capability in Each Commission Service, SEC(2000)1803/2,

- Reglement CE – Council Regulation EC EURATOM 1605/2002 of 25/06/02, Implementing rules 2342/2002 of 23/12/02 on the Financial Regulation

- Reg (EC) 1049/2001 regarding public access to EP, Council & Commissions documents & on Commission Decisions C(2001) 3031 on its security provisions,

- Reg (EC) 45/2001 of 18/12/2000 on Data Protection

2.2. Audit Charters

The purpose, authority and responsibility of an internal audit activity are described in the Charters.

The Commission adopted the IAS's Charter in October 2000[2]. The Charter defines the Mission and the Scope of the IAS, its relations with the other parts of the Commission/DG and with other audit functions; it specifies the conditions for the definition of work programmes and the professional standards which will be applied. In broad terms, the Charter defines the scope of the IAS' work, its rights and obligations in performing its mission.

[1] http://www.theiia.org/

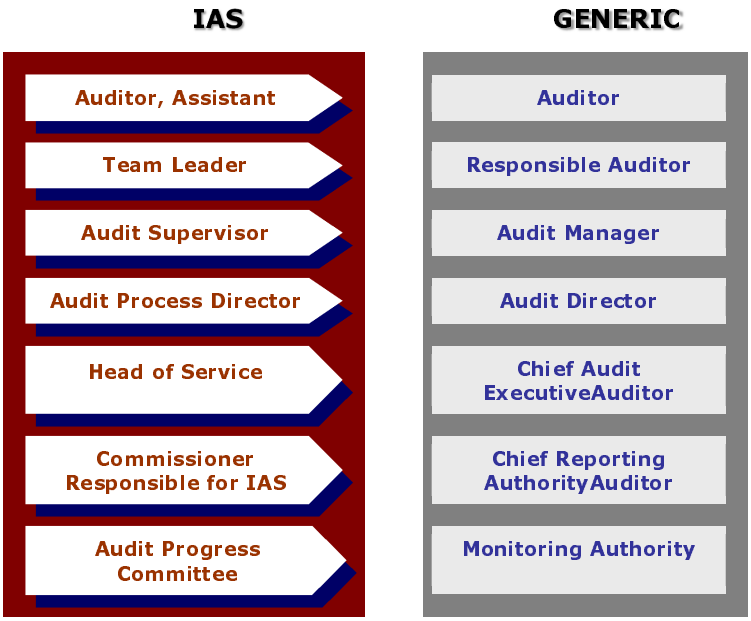
[2] Revised in 2007. See link on page 5

A review of IAS charter was performed in 2007.

2.3. Responsibility and reporting lines

As laid down in its Charter, the IAS is independent of all the Commission's operational activities.

Generic roles have been defined. The table bellow provides the correspondent functions in the IAS.



The IIA Professional Framework advises to develop the following elements concerning the responsibility and reporting:

1) Coordinate internal and external auditing work to ensure adequate audit coverage and to minimize duplicate efforts.

2) Set up a policy for selection or retention of external audit services.

3) Establish a programme for selecting and developing the human resources of the internal audit activity.

- *See IIA Professional Practice Framework: Performance Standard **2050**: Coordination,Performance Standard **2030**: Resources Management*
- *See The Audit Progress Committee (APC) of the European Commission – **C(2004)1342**,*
- *See Communication from the commission completing the reform mandate: progress report and measures to be implemented in 2004 **COM(2004) 93***
- *See Clarification of the responsibilities of the key actors in the domain of internal audit and internal control in the Commission **SEC(2003) 59***

2.4. Relations between IAS and IACs

The Commission has the two tier internal audit architecture at the level of the IAS and the IACs in the DGs, implying a need for coordination procedures.

A network ("AuditNet") of the Heads of the IACs and of the Head of the IAS exists in order to exchange best practice and discuss the questions of mutual interest in domains such as methodologies, specific training needs, recruitment, audit software and co-ordination between IACs.

Furthermore, since 2007, the IAS and IAC audit plans are coordinated in the framework of their coordinated strategic plans, covering a 3 year period, in order to avoid duplication of work and to optimise the use of audit resources. When appropriate, the IAS and the IAC may execute joint audits; the IAS may also deliver audit services at the request of Directorates General and Services. Finally, in order to ensure the horizontal flow of information between Commission auditors, the Internal Audit Capabilities systematically transmit all their finalised audit reports (i.e; after conclusion of the contradictory procedure) to the Internal Audit Service. The reports contain an executive summary which highlights all critical findings of the report. The Internal Audit Service summarises important IAC findings, recommendations and actions taken by DG management in a biannual report addressed to the APC.

The IACs make quarterly activity reports to the IAS.

2.5. Relations with the Court of Auditors

On demand, the Court of Auditors has full access to all reports from IAS[3]. The procedure regarding the submission of IAS audit reports is described in Mutual Expectations Paper issued on 11th March 2008. All audit reports are sent to ECA and other reports (documents) on request.

2.6. Role of IAS Correspondent

The Strategic paper on redefined role of IAS correspondent issued in January 2005 (and updated on 11th November 2008), defines the objectives of the IAS correspondents.

The IAS Correspondent pursues four main objectives:

1) improve the relationships with IACs and DGs,
2) ensure regular exchange of information between the IAS and IACs/DGs (Audit Supervisors are officially designated by IAS Director B as the IAS Correspondent for a "portfolio" of DGs),
3) establish a coordinated risk Assessment and planning,
4) contribute to the IAS summary report on IACs reports.

Each Audit Supervisor is responsible for a DGs portfolio and leading a stable team of Auditors. In general (with some exceptions due to planning/time constraints/expertise required), the Audit Supervisor is in charge of the audits of his/her portfolio of DGs as IAS Correspondent.

[3] Treaty article 274

Heads of Units DG's portfolios:

Unit (HoU	DGs
B1 (Cristiana GIACOBBO)	BUDG, COMM, COMP, DIGIT, BEPA, SG, SJ
B2 (Jeffrey MASON)	DGT, EMPL, INFSO, JRC, REGIO, RTD, SCIC, REA, ERCEA
B3 (Laura CANDELORO)	HR, PMO, EPSO, AGRI, MARE, MARKT, OIB, OIL, OP
B4 (Pascal HALLEZ)	CLIMA, ENER, ENTR, ENV, EACI, OLAF, SANCO, EAHC, TAXUD, MOVE, TEN-TEA, HOME, JUST
B5 (Sunil BEERSING)	DEVCO, EAC, EACEA, ECFIN, ECHO, ELARG, ESTAT, FPI, TRADE

The Head of Unit should spend the necessary time in order to fulfill his role as IAS Correspondent and designate one or more Auditors within his team to assist him in this task.

In particular, the Head of Unit is responsible for improving the relationship with the IACs and DGs management, ensuring an ongoing exchange of information, whilst the Auditor is responsible for advising and supporting his/her Head of Unit in his/her role as IAS Correspondent.

2.7. Auditors' responsibilities

The Auditor is responsible to support and advise his/her Head of Unit in his/her role as IAS Correspondent by:

- performing the day to day activities linked to the responsibilities of the Head of Unit as listed above. For practical purposes, the above responsibilities will be delegated to a specific member of the audit team for each DG in the portfolio, except, when appropriate, for contacts at management level;

- developing effective relationships with key contact persons in the DG during the course of audits carried out by the IAS;

- gathering and analysing all relevant information and knowledge: AAR, self-assessment, readiness assessment, reporting to Commissioners, CFS position papers, ECA reports/meetings, OLAF information, IAC s' plans and reports, DG Intranet...;

- identifying, for each DG, major IAS audit findings of the previous year to be communicated to the Director General of the DG concerned in the context of the AAR preparation process;

- updating key documents such as the DG risk profile, inventory of IAC reports, etc. and the DG permanent file (in ARES) and IAS Correspondent engagement files;

- contributing to better coordination (planning co-ordination, joint audits, risk assessments, consulting,…);

- providing input to the IAS summary report on IAC audits from the analysis of the IAC 's reports;
- assessing the quality of the IAC reporting and commenting about audit results;
- preparing responses to inter-service consultations and non-audit-related mail;
- preparing briefings and responding to ad hoc requests from the Head of Unit

2.8. Code of Ethics

In line with IIA standards and Code of Ethics[4], the auditor has to:

- adequately plan, control and record his/her work,
- at all times perform his/her work objectively and impartially and free from influence or any consideration which might appear to be in conflict with this requirement. S/he will always have regard to any factors that might reflect adversely upon his/her integrity and objectivity in relation to an assignment,
- carry out his/her work by having a proper regard for the technical and professional standards expected of him/her,
- conduct himself/herself with courtesy and consideration towards all with whom s/he comes into contact in the course of his/her professional work,
- not disclose information acquired in the course of his/her work except where there is a legal duty to disclose,
- not use information acquired in the course of his/her work for his/her own personal benefit or for the advantage of any third party,
- provide the contact person(s) and the respective Heads of Unit with a list of persons to be interviewed beforehand. It will be up to the IAS to arrange the appointments at a time suitable to both parties,
- ensure that meetings are not postponed due to unavailability of staff by providing a suitable representative,
- inform the auditee about the findings and observations during the course of the engagement without delay.

[4] www.theiia.org

3. AUDIT PROCESS

3.1. Introduction

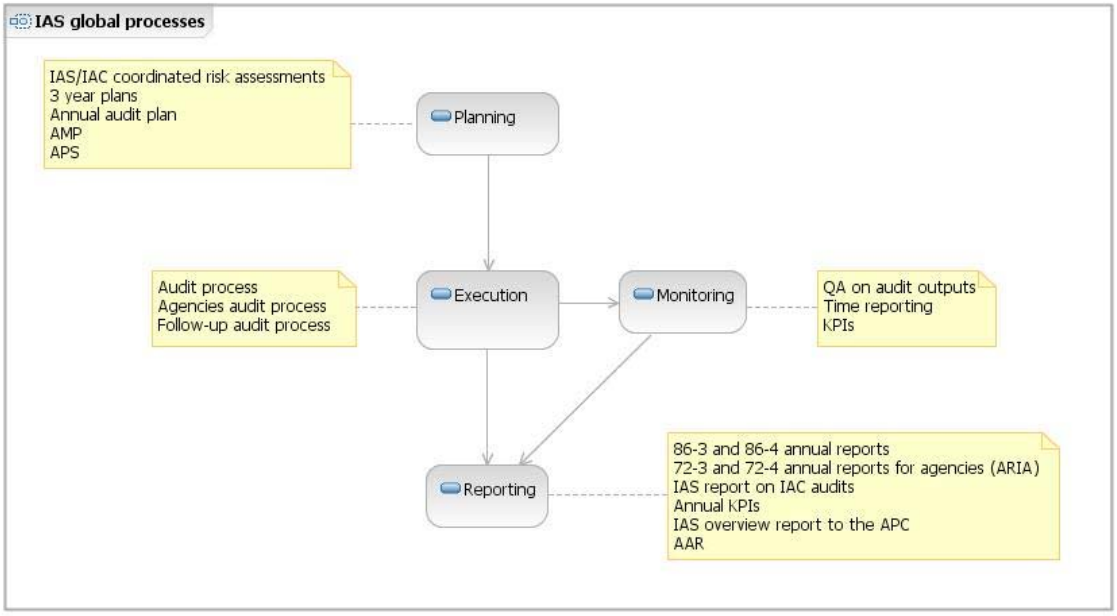
The audit processes are presented in this manual on three levels, according to the detail of the process.

The first level gives a *top level overview of the IAS's global processes*. The second level "zooms" into the *audit meta-processes*. The third level is the *activity diagram of an audit*, with the details of each meta-process.

Each level of the audit process is supported by an activity diagram. In the activity diagram, the activities are organised by vertical partitions that correspond to a role or group of actors. Certain activities produce an output (e.g. final report) that is an explicit input and prerequisite for the next activity. Actors that do not directly advance the business flow are represented as participants in an event, like a meeting or as a report recipient. The diamond symbols represent a business decision or a merge of control flows.

Detailed explanationon the process or sub-process is then provided to support the understanding of the diagram.

3.2. Global Process overview



This diagram contains the top level processes of the organisation, with their activities, inputs and outputs. Arrows between processes indicate data flows between main processes in the Planning, Executing, Monitoring and Reporting cycle.

The Planning global process consists of the following main processes: IAS/IAC coordinated risk assessment, 3 year plan preparation, AMP, APS and consequently Annual Audit Plan preparation.

The Execution part of the global processes cycle consists of core audit processes i.e. Commission audit process, audit process for agencies and follow-up audit process.

The Monitoring process consists of a set of background activities; Quality Assurance on audit outputs, Time reports and KPIs monitoring. As background activities they actually form an integral part of main execution processes; audit processes and audit follow-up process.

All the reporting activities of IAS are included in the Reporting global process. More detail on these activities is provided in the section describing Information sharing and document management process.

The execution activities (audit processes) are modelled in more detail in the following sections.

3.3. Audit strategy and planning

3.3.1. Introduction

The role of the internal auditor of the Commission is defined in Articles 85 to 87 of the Financial Regulation (FR) and article 110 of the FR implementing rules. The internal auditor is independent and enjoys full and unlimited access to all information required to perform his duties.

Article 111 of the Implementing Rules of the Financial Regulation states that "*The internal auditor shall adopt his work programme and shall submit it to the institution*". This is reflected in the mission charter of the IAS which states that its Head has the responsibility to "*Develop a three-year audit plan and an annual audit plan using appropriate risk-based methodology, including any risks concerns identified by management and submit these plans as well as periodic updates to the APC for endorsement*".

3.3.2. Overview of the audit strategy

The purpose of the audit strategy is to put in place a strategic approach which will allow the IAS to:

- Provide the Commission with assurance as to the effectiveness and efficiency of the governance, risk management and control processes,
- Provide annually an overall opinion on the state of control in the Commission focusing on financial management,
- Coordinate its work with IACs and the Court of Auditors, and
- Contribute to the achievement of a more positive DAS.

The IAS can also provide consulting services designed to add value and improve the operations of the Commission at management's request. Although the strategic audit plan does not contain specific consultancy engagements, the categorisation of individual audits (see section **Error! Reference source not found.**) provides sufficient inbuilt flexibility to cope with such demands should the need arise.

3.3.3. Basic internal audit planning principles

The audit strategy takes as starting point the Financial Regulation, the international audit standards of the Institute of Internal Auditors (IIA), SEC(2000)1803/3[5], and the IAS charter.

Article 86 of the FR states that "*The internal auditor shall advise his/her institution by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management*[6]".

The IAS charter states that in order to perform its mission properly, it must act in accordance with generally recognised principles and international standards governing internal audit. IIA standard 2010 requires that "*The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals*". IIA standard 2100 goes on to state that "*The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control activities using a systematic and disciplined approach*".

[5] Conditions for the Provision of an Internal Audit Capability in each Commission Service dated 31 October 2000.

[6] Article 86 of the Financial Regulation and implementing rules applicable to the general budget of the European Communities.

3.3.4. Audit assurance objectives

In providing assurance on the governance, risk management, and control activities as required by IIA standard 2100, the IAS evaluates the adequacy and effectiveness of controls in place in responding to risks within the organisation's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

As far as the first control objective is concerned, it has to be noted that this is the main focus of the activities of the European Court of Auditors (ECA). In establishing its plan, the IAS takes into account the work programme of the ECA to avoid any overlaps. One of its primary objectives is to provide assurance that the Commission's policies, procedures and applicable laws and regulations are complied with. Effectiveness and efficiency remains an important driver for the IAS' activity, in particular in those areas requiring specialised skills (e.g. IT). The Financial Regulation (Art. 86(1)) stipulates that the Commission's internal auditor must issue independent opinions on the quality of management and control systems and recommendations for improving the conditions of implementation of operations and promoting sound financial management.

3.3.5. A risk based planning methodology

The approach of the IAS to the Strategic Plan is threefold:

- First, to define clearly the various auditable systems, processes, units and bodies that make up the Commission's overall audit universe.
- Second, to make an assessment of the risks associated with the underlying components.
- Third, to consider the case for including issues in the planned audit coverage because, for example, they have not been covered for some time on a cyclical basis, they are fundamental in nature and/or they are inherently material by definition and failure to include them would pose a basic risk to the achievement of an overall audit opinion on financial management for the Commission as a whole.

3.3.5.1. Definition of the audit universe

The audit universe, as defined in coordination with the IACs and used for the first time as part of the 2007-2009 strategic planning process, constitutes the starting point for the preparation of the strategic audit plan. It consists of auditable entities linked to 18 standard processes sub-divided into the following two categories:

(1) Processes of a financial/budgetary nature (referred to as the financial audit universe), and

(2) Processes of a non-financial nature (referred to as the non-financial audit universe).

The following areas are scoped out of the audit plans:

- The internal control system of the Member States, since the mandate of the IAS is to assess the internal control system of the Commission. Therefore, in the area of shared management, the focus will be on assessing the adequacy of the supervisory and monitoring controls set up by the Commission's services. The same applies *mutatis mutandi* to decentralised, joint and centralised/indirect management.

- Regulatory Agencies, the EEAS and Joint Undertakings, since they are autonomous bodies and are dealt with separately by Directorate A of the IAS.

3.3.5.2. Financial audit universe

This part of the universe is defined in the Commission's annual budget and annual financial statements. It includes revenue (own resources, co-financing, recoveries, etc.), expenditure (grants, procurement, etc.), the balance sheet (loans and borrowings, inventories, debts, treasury, pre-financing, etc.) and off-balance sheet items (RAL, guarantees, forecasts of revenue, etc.).

As described in the financial statements, this part of the universe can be viewed from the perspective of:

- management method;
- policy area;
- DG or Service.

A key building block in the strategic planning process is the review of management assurances provided through the AAR and, in particular, the internal control declaration and reservations made. It is management's responsibility to lead the organisation, including the identification, assessment and management of attendant risks. As part of these responsibilities, management provides assurance to the board (the College, in the case of the Commission) and, to the extent that these assurances are published, to third parties (the budgetary authority in the case of the Commission) that such risks are appropriately addressed and are within the risk appetite of the organisation.

One of the building blocks in the provision of assurance by a Director-General as Authorising Officer by Delegation is the results from audits during the reporting year. According to Commission communication SEC(2003)59[7], an IAC's role in the context of the AAR process is defined as "*…in accordance with the nature and scope of their work during the year in question, they should express an opinion on the state of control as a contribution to the preparation of the AAR*".

Building on this management assurance, the role of the IAS is to provide "reassurance" that management's reports can be relied upon. Once it is satisfied that all significant risks have been identified, it bases its work on the strengths (i.e. management's assurance) and weaknesses (i.e. reservations in the AAR) already identified by management. The internal audit work focuses on auditing those controls that are deemed by management to be effective (i.e. strong controls identified by management). Consultancy engagements may also be conducted, in particular at management's request, in areas of qualified management assurance in order to improve the management of risks, add value, and improve the organisation's operations.

The list of auditable entities by DG forming part of the financial audit universe are in line with the Activity Based Budgeting (ABB) nomenclature.

3.3.5.3. Non-financial audit universe

As part of the three year Strategic Audit Plan and its annual updates the IAS identified a number of non-financial auditable entities. Although these entities do not belong to the financial management audit universe, they may generate significant risks for the Commission's reputation (e.g. handling of crises, IT systems supporting policies, information security, ethics, etc.), the citizens' or staff's safety (e.g. handling of pandemics, natural disasters, etc.) and also the sound financial and resource management (e.g. core business efficiency, HR policy, administrative IT systems, BCP, etc.). They also include significant policy areas with some budgetary impact such as competition policy, with resulting fines, controls over trade policy, with resulting anti-dumping measures, controls over the respect of EU law, with resulting infringement procedures. This list is updated during the risk assessment of all DGs in the audit universe and validated with the IACs. The IAS provides assurance

[7] Clarification of the responsibilities of the key actors in the domain of internal audit and internal control in the Commission dated 21 January 2003.

on these non-financial controls through the audit opinion expressed in the relevant individual audit reports and which are subsequently summarised in the Annual Report of the Internal Auditor[8].

3.3.5.4. Completeness of audit coverage

Although essentially bottom-up, the risk assessment is supplemented by "top-down" considerations aimed at identifying potential gaps in the coverage, especially due to the requirement to deliver an overall opinion on financial management. Extensive consideration is given to the need to cover all identified high-risk areas as well as major processes or systems which may have not been covered for some time and/or for which the bottom-up risk assessment did not necessarily identify any particular problems. In this regard, the IAS believes that it is important to audit each DG/department at least once during the three-year audit cycle.

3.3.6. Audit strategy for specific areas/processes

This section further elaborates on the audit strategy of the IAS for specific processes within the audit universe.

3.3.6.1. Multi-annual programmes

Multi-annual programmes account for a significant portion of the annual budgeted commitments and payments. They are by nature implemented in phases. Although inherent risks are assessed for the process as a whole, the relevant control strategies in place can only be audited as they are implemented over time. The IAS plan aims to ensure appropriate coverage of the internal control system in place for each of the key stages of the assurance building process.

3.3.6.2. Annual programmes and procurement

These processes are audited during the planning cycle based on the results of the risk assessment and, taking into account their materiality, of the need to sufficiently cover them in order to be in a position to deliver an overall opinion on financial management.

3.3.6.3. IT

The main missions of IT are to develop and operate information systems required to support EU policies and the Commission administration, to supply information technology and telecommunication infrastructure and to provide support services to its internal and external users. IT processes can pose significant risks in terms of infrastructure security, systems reliability, user satisfaction, optimal use of investments and compliance with political commitments or legal obligations which might eventually result in dysfunctions, financial losses and reputational risks. The IAS proposes to address them at DG and at corporate level from different angles to optimise its own IT audit resources.

3.3.6.4. External aid

External aid is characterised by a significant diversity of financial instruments implemented in nearly all third countries in an inherently risky environment.

The 2010-2012 planning cycle focussed on DG DEVCO's thematic budget lines and financial instruments such as budgetary support and programme estimates for the EU budget and EDF, DG ELARG's Instrument for Pre-accession Assistance and DG ECHO's delivery of humanitarian aid.

3.3.6.5. Monitoring the implementation of EU law

The control of the timely and correct application of EU legislation is one of the core activities of the Commission laid down in the Treaty in the fulfilment of its role as the "Guardian of the Treaties". The IAS audited this area in 2006 with the SG in its role as central service and a sample of operational DGs – MARKT, ENTR and ENV. More recent audits focused on other operational DGs (based on

[8] Report issued in accordance with article 86.3 of the FR.

number of directives and/or infringement cases) or on the transposition of specific directives (such as public procurement rules).

3.3.6.6. HR

HR is a fundamental area requiring audit coverage in each planning cycle with the identification of specific themes. The themes addressed so far included processes within DG HR, IT systems supporting HR processes, and HR management in Offices.

3.3.6.7. Governance

Internal audit has a key role in providing assurance that those systems, policies and procedures required for an effective governance framework are in place and operating satisfactorily. Past IAS audits on ethics focused on potential conflicts of interest and misuse of insider information and on a number of operational DGs and specific aspects during the current cycle such as risk management in the AAR process throughout the Commission.

3.3.6.8. Performance audits

In evaluating and contributing to the improvement of governance, risk management and control activities, and as part of its task to verify the proper implementation of budgetary procedures including sound financial management, the IAS carried out in 2011 its first two performance audits (in ECHO - Operational activities and EACI/ENTR – Competitiveness and Innovation Programme). Other performance audits were carried out afterwards and aspects of efficiency are examined in other audits. These audits are intended to further improve the Commission's capacity to maximise the performance of its services, which are now subject to the ECA's observations in the new chapter 10 on "Getting results from the EU budget" of its annual report.

3.3.7. Risk assessment methodology and strategic planning

The starting point of the risk assessment exercise is the performance of a desk review of specific documents of each DG (e.g. AAR, MP, IT Master Plan ("Schéma Directeur"), etc.) and other documents issued by the central services (e.g. budget, Synthesis report, EP report on discharge, Commission's cross-cutting risks, etc.) followed by interviews of key members of management.

This also includes the identification of the main risk mitigation building blocks for each DG, i.e. governance arrangements (including IT governance where appropriate), type of financial circuit in place, AAR and risk management procedures that are used as background information for the risk assessment of the auditable entities. These risk mitigating blocks may also be audited either as part of the audit of a specific process in a DG or as part of a horizontal audit at Commission level.

The risk assessment of auditable entities within the audit universe is conducted by assessing the impact/likelihood of risks to determine their significance. The Commission's standard risk typology is used to ensure that the most common risk aspects are covered. A series of indicators covering aspects such as major changes to procedures, human resources and organisational circumstances, changes to legislation, complexity of the activities, involvement/dependence on other entities or third parties, financial (materiality) impact, cumulative impact, time elapsed since last audit of the area/process, etc. are taken into account to assess the inherent risks within each entity.

Although the audit universe is a list of all the possible audits that could be performed, the focus of the coordinated plan is on auditing areas with high inherent risks[9].The cumulative impact of auditable entities not covered is however regularly assessed during the annual updates to ensure that those that become riskier over time are included in the audit plan. In that respect, the IAS is of the opinion that it is important for each DG/Service to be audited at least once during the three year audit cycle. In addition, the plan takes into account the revised IPPF of the IIA and, in particular, the two new standards on IT governance and fraud detection and prevention.

[9] Risks are assessed on a scale from 1 (low) to 5 (high). The plan focusses on entities with high inherent risks (4 and 5).

Although essentially produced on a bottom-up basis, the risk assessment is supplemented by top-down considerations (from IAS management, APC, other stakeholders, etc. and link to the achievement of the Commission's strategic objectives) aimed at identifying issues of a horizontal nature and potential gaps in the coverage that might reasonably be expected in order to form an overall assessment of the Commission's control system as a whole. Consideration is also given in preparing the plan to the identification of specific themes to be covered in order to compare existing processes against established benchmarks and to identify recommendations that would add value to those processes.

3.3.8. Coordination with IACs

Following the completion of the IAC quality review exercise in 2006, which revealed the need to enhance the overall audit planning process in the Commission, the IAS and IACs work closely together since 2007 in order to develop a common methodology covering both the definition of the audit universe and the audit risk assessment. This ultimately results in strategic and annual audit plans for the IAS and IACs which are risk-based and coordinated.

The IAS also ensures that the annual audit risk assessment is synchronised to take account of all the relevant sources of information available (AARs, internal audit reports, results of ex-post controls and on the spot audits of the beneficiaries conducted by the DGs, ECA, OLAF, discharge, briefings prepared for the Commission, etc.) and to take account of management's own risk assessment. As the timing of the audit and management risk assessments are not synchronised[10], the yearly update of the three-year plan normally takes place in Q1 of year n.

3.3.9. Annual update and presentation of results

Whilst the IAS strategic audit plan sets out the planned programme of audit work for the next three years, effective audit planning is a continuous process. The plan is reviewed and updated annually to reflect new and emerging risks as well as significant changes in the organisation's business, operations, programmes, systems and controls.

3.4. Overall opinion

The IAS charter states that it shall be accountable to the APC to "*... on the basis of the nature and scope of the work of the IAS and the internal Audit Capabilities (IACs), provide annually, starting no later than for 2009, an overall opinion on the state of control in the Commission*". The APC, at its meeting of 16 October 2009, reiterated its support to the IAS in proceeding towards an overall opinion focusing on financial management.

In developing the strategic audit plan to support the expression of an annual overall opinion on financial management, the IAS considers a number of factors, with one of them being the definition and coverage of the financial audit universe.

The methodology adopted for the definition of the financial audit universe is explained in section 3.3.5.2 above. In assessing the coverage of an auditable entity, the IAS makes a number of assumptions as follows:

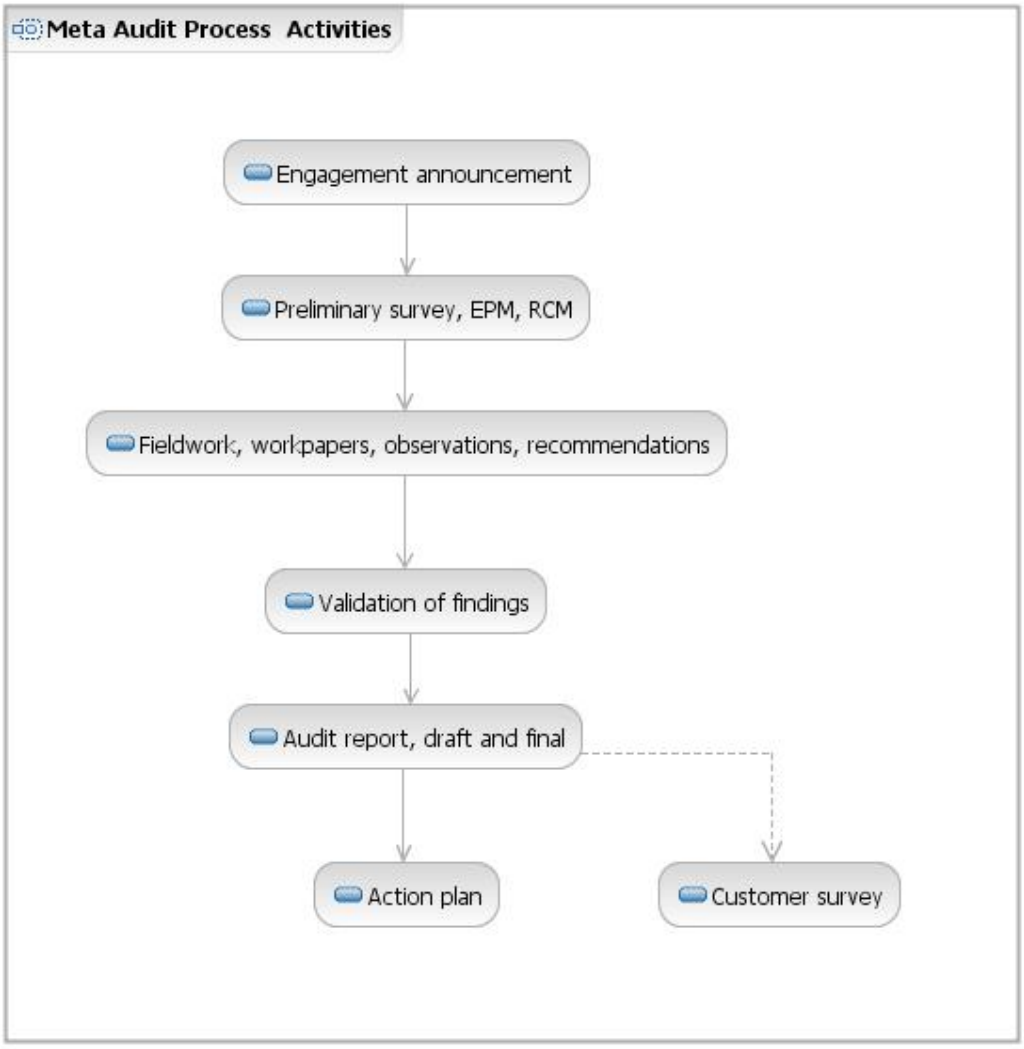
[10] The audit risk assessment normally takes place in November but management's risk assessment is normally available in December as part of the MP preparation process.

- New programmes are split into three phases: Planning (e.g. Design/Call for proposals to award decision), Implementation (e.g. contracts to final payments) and Closure (e.g. ex-post controls – including recoveries, evaluation) representing broadly 20%, 70% and 10% respectively for coverage purposes, to reflect their multiannual nature.
- Where specific procedures are in place for old programmes, only these procedures are considered as an auditable entity (and not the programming and implementation phases, which are deemed to relate to previous periods). The assurance provided in these cases is therefore limited to these specific procedures and not to the whole programming period.
- Follow-up audits are not included in the coverage calculations in order to avoid double counting (but the results of follow-ups are taken into account in assessing their contribution to the delivery of the overall opinion).
- Horizontal audits at DG level (e.g. audits on fraud prevention and detection, ethics, implementation of internal control standards, Financial Circuits across the DG) are assessed to judge the extent, if any, to which they contribute to the coverage of financial audit entities in the DG, up to a maximum of 20%.

The coverage figure expressed for commitments and payments is a product of the actual audit coverage achieved, calculated in accordance with the above assumptions, of the auditable entities within the financial audit universe expressed in terms of the appropriations. As regards the overall opinion, the coverage is expressed in terms of the 'building blocks' of the assurance given by each Director-General.

3.5. Audit process

This diagram summarises the high level activities that are common to different types of audits. It covers the essential steps executed during an audit.

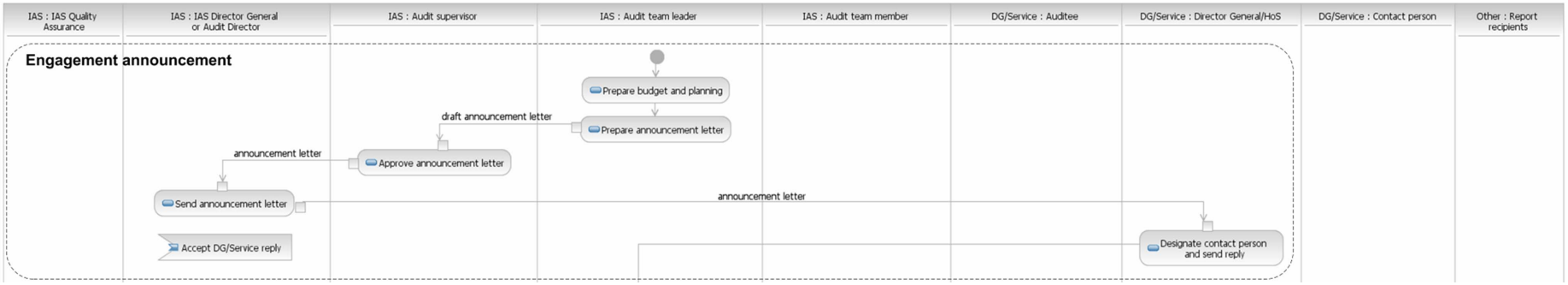


The activities of the Commission audit process (directorate B) are modelled in further detail in next chapters of this document.

Each part of the process also includes the requirements and best practices in documenting the audit in the audit management software.

3.6. Planning and Administration

3.6.1. Engagement announcement



3.6.2. Announcement letter

At least one month prior to the start of an engagement, the Director-General of the IAS will send an announcement letter to the Director(s)-General of the DG(s) or Head(s) of Service(s) concerned giving details concerning the planned scope, the start date and duration of the engagement and the names of the Head of Unit, Audit Team Leader and staff members of the team.

The DG(s) or Service(s) concerned will be invited by the IAS to designate the contact person who will act as an entry point and facilitator. The contact person should preferably not be directly involved in the areas/processes being audited but rather someone who has management's authority to discuss issues with the IAS and is available to solve practical day-to-day issues encountered by the IAS in conducting the engagement. The contact point could be, for example, the Head of the IAC, the DG Assistant or the Head of the Strategic Planning Unit of the DG or Service concerned. His/her role is to support within the DG the audit activities undertaken. The contact person should not interfere in anyway with the audit activities and should not place any restrictions on information to be provided.

The IAS will also ask the Management to send to all staff concerned a notification of the possible use of "personal data" during the audit, as described in Council Regulation No 45/2001. This notification is provided in a standard note which is attached to the announcement letter.

3.6.3. Opening meeting

An opening meeting will be held by the IAS with the contact person and/or other representatives of the Director-General to discuss logistical and practical arrangements notably in terms of office space and equipment needed at the DG's premises during the engagement and also be used as an opportunity to introduce staff and build/strengthen the auditor/auditee relationship.

Triggering event: Decision to execute planned audit with the required resources

Input:

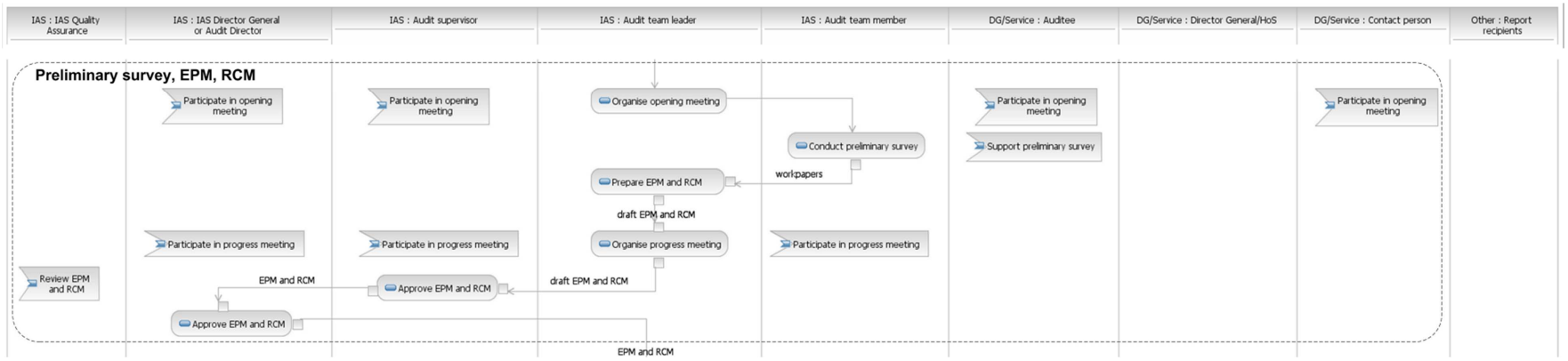
- Annual audit plan
- Definition of audit team

Output:

- Acknowledged Announcement letter
- Designated contact person

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.7. Preliminary survey



The purpose of the preliminary survey is to gain a better understanding of the business process/activity/unit included in the scope of the audit and the related risks and to perform a risk assessment to identify the risk areas that the audit fieldwork will focus on. The main source of information that the auditors use are interviews and collection and review of documentation.

The preliminary survey activity starts with an opening meeting organised by Audit team leader and attended by Head of Unit, Contact person from DG and Auditees. The meeting serves to identify relevant and reliable evidence sufficient to enable him to draw reasonable conclusions there from - the nature and extent of the tests, audit methodology adopted and choice of interviewees will vary according to the auditor's assessment of the area being audited and, where s/he wishes to place reliance on it, the system of internal control. It also helps to obtain additional background information to be collected and to allow the drawing up of a tentative list of auditee's staff to be interviewed.

At the end of the preliminary survey, the 'Engagement Planning Memorandum' document and Risk and Control Matrix (or Strengths & weaknesses analysis) is prepared, reviewed and approved by the Head of Unit and then sent for the Audit Process Director approval (in GRC). The EPM contains the outline of the engagement indicating background information, the scope and objectives, the measures to achieve them (methodology and planning) and the anticipated impact of the audit (value added) to the management. The RCM identifies per process or activity, the main risks or control objectives and the existing controls.

The standing instructions[11] for the preparation of Annual Activity Reports 2008 require DGs/Services to present the management and control system for significant areas of the budget, including both the management and control systems for grants and procurement, in annex 5 to the AAR, using an "Internal Control Template for Budget Implementation' (ICT5). The main aim of this template is to have a concise, readable and consistent presentation of key inherent control risks and the control systems in place addressing these risks. A model template is provided in appendix 5 of the standing instructions and specimen ICTs developed for particular management modes and procurement can be found on the SPP-ABM web site[12].

You should ensure that the information contained in these ICTs (as reported in the latest AAR of the DG) is properly reflected, if appropriate, in the Risk and Control Matrix (RCM) developed as part of an audit engagement. In addition, all EPMs should contain the latest ICT of the DG being audited either as an annex or attached in the "Supporting Files and Links" section of the working paper in GRC for review together with the RCM during the internal progress meeting.

The results of this scoping exercise (EPM and RCM) are discussed by the audit team with the Head of Unit, audit director and director-general during a progress meeting, before they are presented to the auditee management during the kick-off meeting in the next process.

Triggering event: Engagement announced and acknowledged

Input:

- Access to auditees and supporting information

Output:

- EPM
- RCM

[11] http://www.cc.cec/budg/rep/aar/_doc/2008/aar2008_standinginstructions_en.pdf

[12] http://www.cc.cec/home/dgserv/sg/i/spp/index.cfm?lang=en&page=aar_estab

Briefing to IAS Director-General for the Kick-off Meeting

To prepare the debriefing of IAS Director-General for the kick-off meeting, the audit lead should provide the following documents/information

(1) EPM (objectives, scope, reasons for engagement)

(2) RCM (high level overview of main risks)

(3) Audit methodology (e.g. sample size, etc.)

(4) Previous audits in the same area (IAS, IAC, ECA)

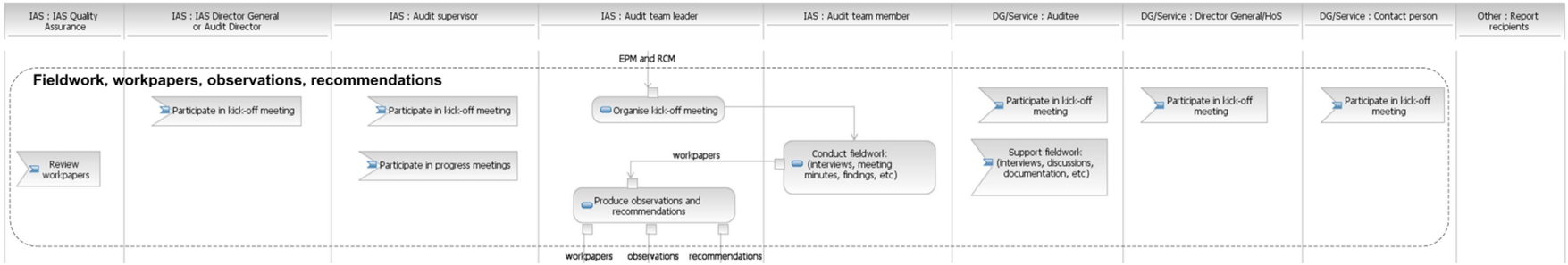
(5) Issues of interest to auditee

(6) Mutual Expectations Paper (Reporting timeframe, validation meeting, etc.)

(7) Organisation chart of DG

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.8. Fieldwork



The step preceding the actual fieldwork is a kick-off meeting. During the kick-off meeting, the results of the preliminary survey scoping exercise are presented to the auditee management. The IAS will be represented by the Head of Unit and, when appropriate, the Audit Director and/or Director-General. After the meeting, the fieldwork is being conducted.

The fieldwork is a systematic process of objectively gathering evidence about an entity's internal control system and evaluating it. The nature and extent of the fieldwork is spelled out in the Engagement Planning Memorandum (EPM). The majority of fieldwork consists of testing which, to the internal auditor, implies the measurement of representative transactions or processes and comparison of the results with established standards or criteria. The objective of the testing is to gather evidence on the validity, accuracy, effectiveness and efficiency of controls.

During the course of a fieldwork, exceptions may result from the audit tests performed. These exceptions are researched and the disposition of each exception is documented. Findings/Observations and Recommendations are created for any issues identified by either the tests of procedures or tests of transactions. For each single finfing/observation there should only be one recommendation.

In order to improve timely monitoring of audit engagements and enable early identification of issues concerning the scope, approach, progress and results of the audits and reinforce the quality assurance process throughout the whole audit cycle, it is recommended to systematically organise progress report meetings, shortly after the completion of the preliminary review.

In accordance with international audit standards, auditors' workpapers are not validated with auditees. However, regular meetings with the Resource Director(s)/Internal Control Co-ordinator(s), the contact person(s), the Head(s) of IAC and other appropriate members of the (senior) management will be arranged during the fieldwork to discuss progress of the audit. The IAS will immediately report to the DG(s)'s or Service(s)'s management any significant weaknesses in the DG(s)'s or Service(s)'s systems which come to the attention of the auditor.

Triggering event: Preliminary survey completed

Input:

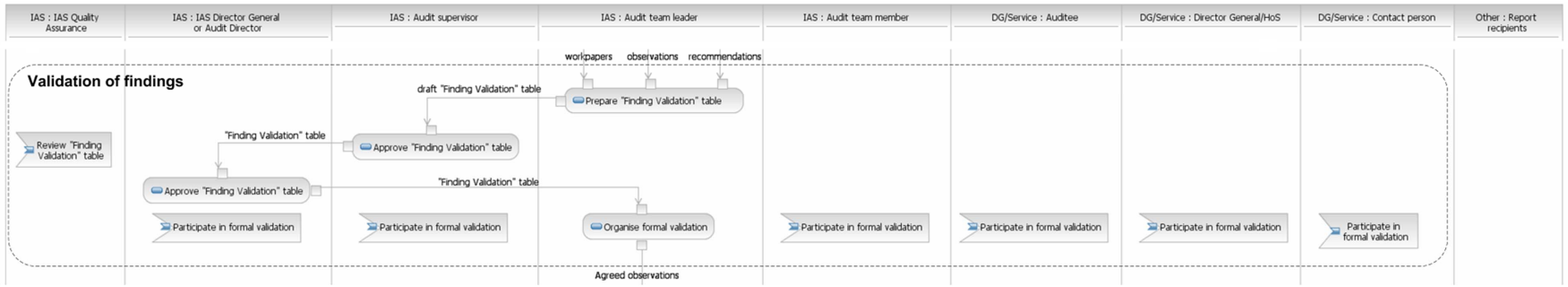
- EPM
- RCM

Output:

- Workpapers
- Observations (or Audit Issues)
- Recommendations

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.9. Validation of findings



The Validation of findings activity begins with preparation of a "Findings Validation" table consisting of findings and also indicating risks, draft recommendations and ratings. After review by the IAS Quality Assurance and approval by Head of Unit and Audit Director, the table is subject to the formal validation procedure. The aim of this procedure is to reach an agreement with the DG/Service, at the appropriate hierarchical level, on the facts/observations reported by the audit team, which will not be reopened or questioned again in the final stages of the audit.

Therefore, the auditee DG(s) and Service(s) should put in place proper procedures (including, when necessary, escalation to the appropriate management level) in order to ensure timely (i.e. before the formal validation meeting with the IAS) internal validation of the facts/observations reported by the audit team. Agreements on the individual facts/observations should be recorded in writing after the validation meeting. With this procedure subsequent discussions can focus on audit recommendations.

Triggering event: Fieldwork completed

Input:

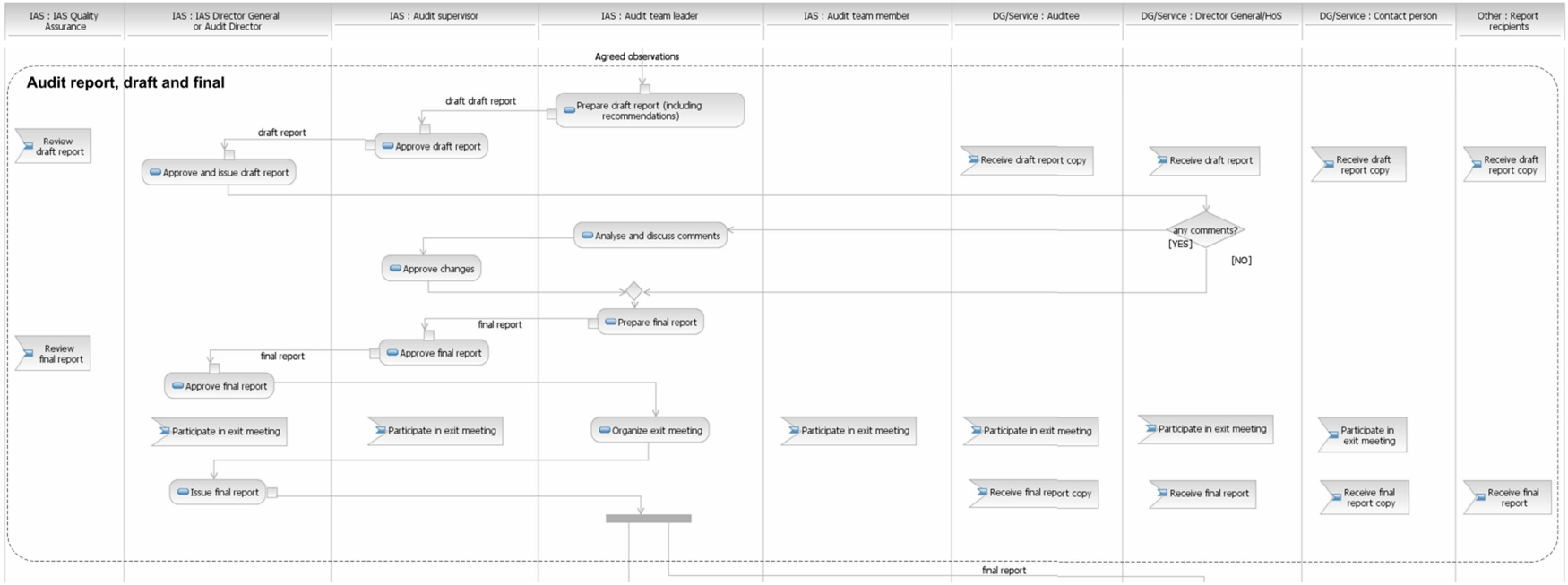
- Workpapers, observations and recommendations produced during fieldwork

Output:

- Observations agreed with auditees and their management

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.10. Reporting



The reporting process consists of a draft report and a final report followed by an exit meeting. All reports have a "Commission internal" security marking.

The draft report is sent to the auditee(s), the Director(s)-General, the head(s) of the IAC(s), the contact person(s) designated by the Director(s)-General for the audit and to the Cabinet responsible for the Internal Audit Service within one week of the formal validation meeting (as described in point 3.2.3 above). If certain issues or recommendations concern one or more DGs or Services other than those audited, a copy of the draft report is sent to these DGs or Services. The DGs and Services that have received the draft report are free to share it with their Commissioners and Cabinets.

Comments on the draft report, including an indication of the acceptance or non-acceptance of the recommendations made, should reach the IAS within a well-defined time interval after the draft report has been issued or earlier as agreed by the two parties. If no comments are received within the agreed deadline, the validation process regarding the draft report will be considered as closed.

Discussions with the auditee will be pursued on the draft report until changes are accepted or, in case of disagreement, the auditee's position will be annexed to the final report and a reference will be added to the executive summary.

Once the final report has been approved by IAS, a dialogue between the IAS and the auditee will be concluded by means of an exit meeting. The purpose of the exit meeting is for the IAS to present the audit conclusions and final report and to discuss any final issues but not to reopen a discussion on the audit report. The final report will be issued directly after the exit meeting, within a given time interval (usually one month) of the draft report being sent to the auditee.

Triggering event: End of validation of observations

Input:

- Agreed observations
- Workpapers and recommendations from fieldwork

Output:

- Completed and approved Final report, including recommendations
  To be sent to:
  - The Director(s) General of the DG(s) or Head(s) of Service concerned;
  - Contact persons designated by the Director(s) General(s) for the audit;
  - Head(s) of IAC(s);
  - Resource Director(s)/Internal Control Coordinator(s);
  - Other services responsible for implementation of the recommendations;
  - Head of the IAS Cabinet(s);
  - Head of Cabinet(s) of the DG(s) concerned;
  - APC;
  - European Court of Auditors ;
  - Accounting Officer of the Commission;
  - Central Financial Service and concerned Central Services (if applicable).

Debrief IAS DG - Exit meeting

Executive summary (opinion, C & VI obs/recs)

(1) Table summarising criticality of obs (from FVT to draft and final report)

(2) Reasons for downgrading/upgrading/dropping obs/recs from FVT to draft and final reports

(3) Subsequent events

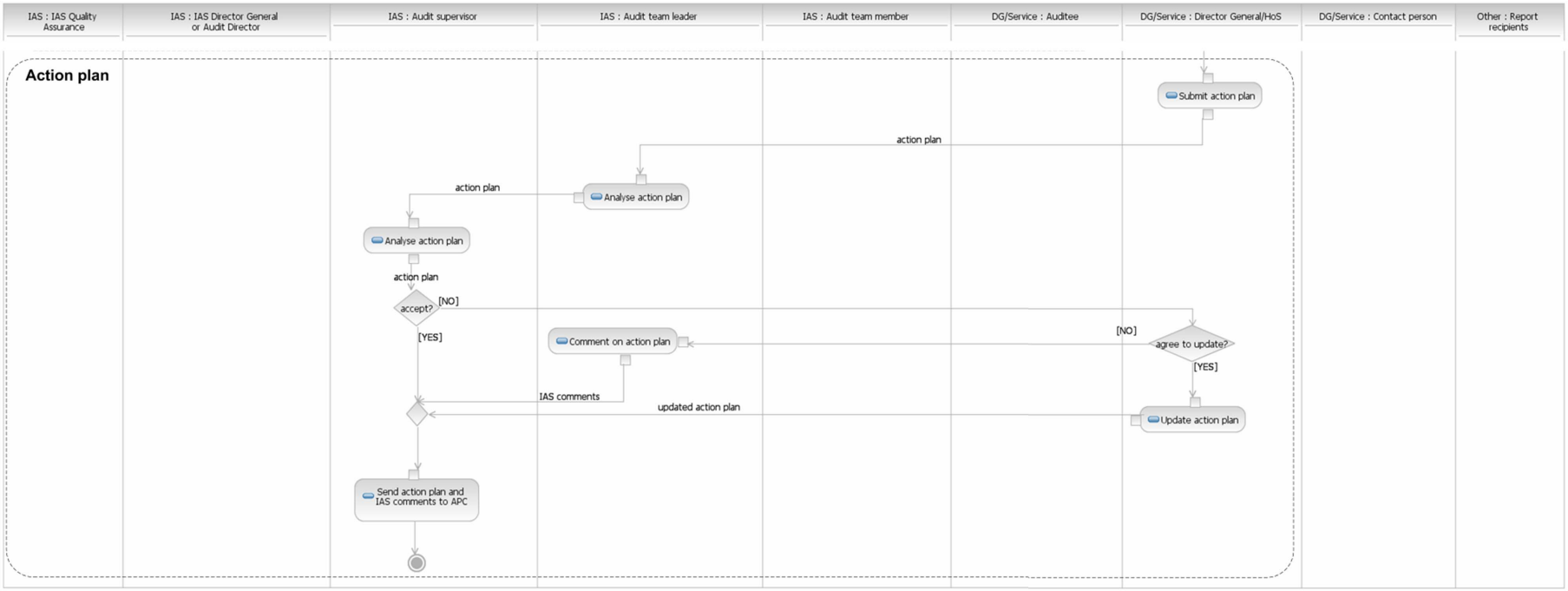
(4) Results of other audits in the same area

(5) Relationship management (conflicts, disagreements on criticality of obs/recs, FVT, etc.)

(6) Issues to be escalated to the APC (if necessary)

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.11. Action plan



This part covers mainly the steps connected to the action plan. The Director(s)-General of the DG(s) or Head(s) of Service concerned submit an action plan for those recommendations that have been accepted within 4 weeks of the final report so as to give the IAS sufficient time to analyse it before the APC meeting. If it's accepted, it will be sent to Audit Progress Committee, if not then there's still the possibility to do the necessary updates before the sending.

Triggering event: Final report issued (sent to auditee management)

Input:

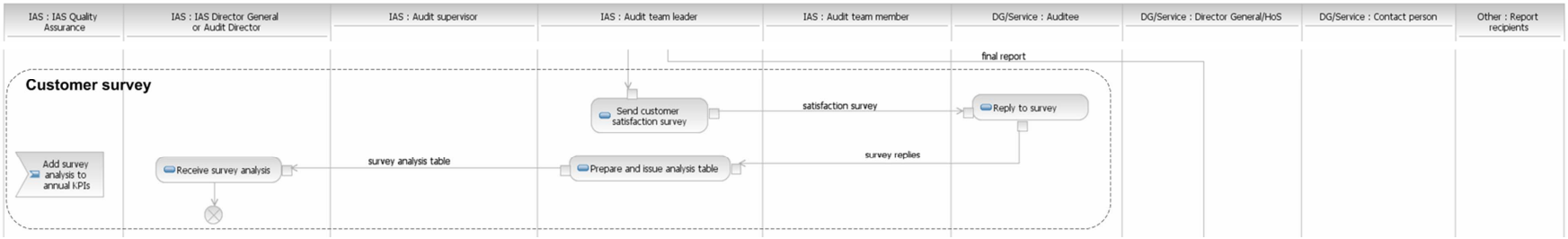
- Final report, including recommendations

Output:

- Action plan
- IAS comments on action plan

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

3.12. Auditee satisfaction survey



At the end of the audit, as part of its quality control procedures, the IAS will send an auditee satisfaction survey questionnaire.

Triggering event: Final report issued (sent to auditee management)

Input: Survey questionnaire

Output: Survey results

3.13. Follow-up

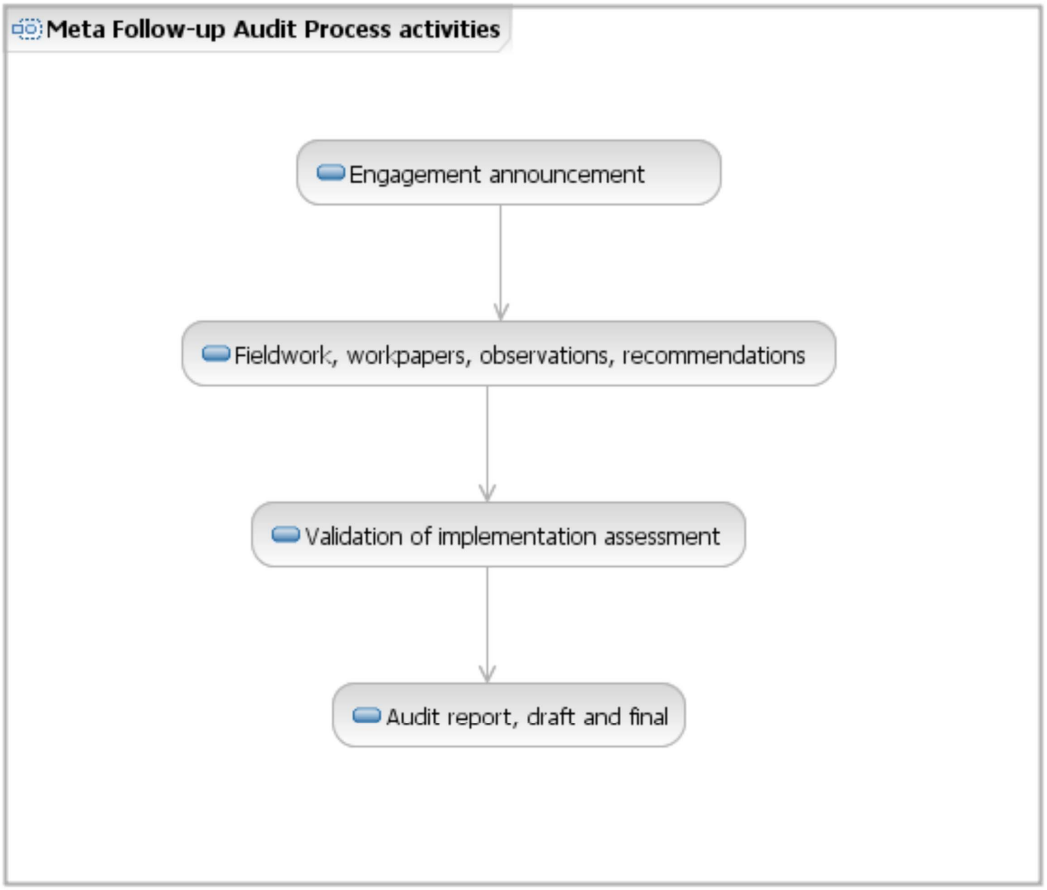
3.13.1. Planning

Planning of follow-up engagements follow two basic principles:

1. Follow up engagements are planned normally within 1 year from the date of issuance of the original audit report, taking into account the target dates for the implementation of recommendations as stated in the action plan.

2. A follow up engagement is conducted when, based on a review of the management's assessment in Issue Track, the large majority of the recommendations (in particular, Critical and Very Important ones), has been assessed by management as implemented.

The follow-up audit process is a simpler version of the audit process.



The audit program of a follow-up audit is derived from the recommendations of the original audit.

The "Validation of findings" activity of the audit process is replaced with "Validation of implementation assessment". Indeed, during a follow-up engagement, there is no audit finding (only on exceptional basis) and the work consists in reviewing the implementation of recommendations. The validation process concerns then the IAS assessment of implementation of recommendations. If not all recommendations have been implemented after two follow-up audits and the IAS assesses the level of residual risk as high, the responsible Commissioner and the APC will be informed and the audit closed.

The IAS reports annually to the College on its engagements, findings and recommendations and on actions taken by the audited DG(s)/Service(s) on those recommendations.

It is the responsibility of management to determine what action to take on audit observations, notably to decide on the implementation or non-implementation of corrective actions. This responsibility implies follow-up activities for management. Monitoring progress is therefore mainly a management responsibility.

The responsibility of the auditors is to provide an additional and independent assurance about it.

3.13.2. Risk-based approach

In order to free up resources for new audits and increase audit universe coverage, the IAS plans its follow-up audits according to the principles summarised below:

1. Apply a more risk-based approach where only high risk areas are targeted.

2. Concentrate even more tightly on the implementation of Critical and Very Important actions, taking into account risk analysis (impact of issues, reliability of management's reporting on implementation, etc.). Only Critical and Very Important issues are to be specifically reported in follow up reports. Important and Desirable issues are to be reported only by exception.

Following the above principles, the IAS applies a risk-based approach and proposes three types of follow up engagements along with indicative averages for days to be allocated for planning purposes.

Cases	Audit opinion in original audit report	Follow-up activities	Days allocated
A	Adverse opinion	• Systematic on the spot follow up. • Substantive testing for all Critical recommendations. • Other non-critical recommendations to be followed up by desk reviews (primarily using material provided by the auditee) and interviews and, when appropriate, also by selective substantive testing for Very Important recommendations • Reporting focusing on implementation of C and VI recommendations. Implementation of Important and Desirable covered in report by exception only.	30
B	Audits with qualified opinion	• Limited on the spot follow up. • All recommendations to be followed up by desk reviews (primarily using material provided by the auditee) and interviews and, when appropriate,	15

		also by selective substantive testing for Very Important recommendations only. • Reporting focusing on implementation of VI recommendations. Important and Desirable covered in report by exception only.	
C	Audits with Satisfactory opinion	• No on the spot follow up • Important and Desirable recommendations to be followed up through Issue Track review. This can be accompanied by a desk review of material provided by the auditee where this is warranted. • No report issued (closure of recommendations just documented in Issue Track).	5

In conducting the follow up engagements, the auditee's track record on management follow-up reporting in Issue Track should be taken into account. If there are concerns in this regard (e.g. former experience of biased management assessments made in Issue Track) then the intensity of the substantive testing should be higher.

3.13.3. Follow-up of multi-DG audits

Further criteria need to be taken into account to determine the planning and timing of the follow-up of multi-DG audits due to the complexity that can arise with the involvement of a number of DGs.

Multi-DG audits can involve both central services and a sample of operational DGs or just a sample of operational DGs and fall under one of the following three categories:

(i) Those where separate individual reports are issued and containing recommendations addressed to each DG,

(ii) Those where only one report is issued and containing recommendations addressed to a central service (or central services) and individual annexes with recommendations addressed to operational DGs, and

(iii) Those where a consolidated report summarising the main findings of a corporate nature is issued and which contains individual annexes with recommendations addressed to all the DGs/Services audited (central and operational services).

In each of the above cases, all DGs (central services and operational DGs) are required to submit individual action plans to implement the recommendations addressed to them.

In order to determine the timing of the follow-up, the following policy will be implemented with immediate effect:

(i) Where the implementation of recommendations by a central service (or central services) is a prerequisite for the implementation of recommendations by operational DGs: Follow-up to be conducted when:

a. at least 75% and 50% of the critical and very important recommendations addressed to the central services and individual operational DGs respectively are reported as implemented by management in Issue Track, or

b. less than 75% of the critical and very important recommendations addressed to the central services have been reported as implemented by the management in Issue Track but which includes all those enabling the operational DGs to implement recommendations addressed to them, and at least 50% of the critical and very important recommendations addressed to the operational DGs.

(ii) Where the implementation of recommendations by a central service (or central services) is not a prerequisite for the implementation of recommendations by operational DGs: Follow-up to be conducted when at least 50% of the critical and very important recommendations addressed to the individual DGs and services are reported as implemented by management in Issue Track.

(iii) Ideally, follow up engagements should be conducted only once. However, when in application of the above, not all recommendations have been implemented at the time of the first follow up engagement; a second follow-up audit should be conducted when all recommendations have been reported as implemented by management.

In order to facilitate the implementation of the present policy and the performance of the follow up audit engagement, the specificity of the multi-DG audits and the possible links between recommendations addressed separately to the central services and the operational DGs should be taken into account. When analysing the action plans submitted by the audited DGs, particular attention should be paid to the consistency between the deadlines established by the central and the operational services for recommendations requiring prior action by the former.

3.13.4. Light audit follow-up procedure for important and desirable recommendations

A simplified procedure is adopted for the follow-up of audits whereby only a limited number of important and/or desirable recommendations are outstanding after the first follow-up audit engagement.

In these cases, the follow-up audit does not need to be formally announced to the auditee with the issuance of an announcement letter. The recommendations sent for review by the auditee can be closed based on a desk review of the evidence submitted to support the implementation as reported through IssueTrack.

The follow-up audit conclusions should be communicated to the auditee in a note, indicating any recommendations closed and/or any recommendations considered open with an indication of outstanding actions to be implemented by the auditee. A template of the note to be used is attached in available on the methodology pages of the IAS Intranet.

3.13.5. Residual risks/ratings

The classification of audit observations and recommendations is set out in an annex to the standard audit report template and describes in overall terms the conditions under which the four classifications for observations are made and the nature and timing of the associated recommendations.

At the date of the follow up audit, we assess whether the agreed recommendations have been implemented as reported by the DG though IssueTrack. In doing so, we have to use our audit judgement to come to an informed view, particularly where the associated corrective actions are multi-layered, stage based and/or interdependent on other factors. This is normal practice. We aim simply to come to a reasonable view on the state of play and the remaining residual risks.

Where there are several parts to a recommendation and not all these have been implemented as intended **we should re-assess the associated residual risk and either confirm the previous residual risk/rating** or **revise the assessment**, using the standard classifications provided for in the annex to the normal reporting template.

Key factors to consider include the relative importance of the different elements making up the recommendation which have been implemented, compared to those which remain in progress, or have yet to start, for the recommendation to be implemented in full. This has to be a matter of judgement,

but it is useful to refer to standard definitions of the classifications and consider the relative importance of the different elements making up the recommendation as a whole.

The standard audit follow-up template requires any downgrading in the original rating to be included under the column **"Current Risk"** and immediately following the explanatory text:

The different options are provided for in the template and allows for the original ratings to be confirmed, or for a **Critical** rating to be downgraded to a **Very Important**, a **Very Important** to an **Important** and an **Important** to a **Desirable**.

For example, if as a result of the follow up there is no change to the IAS assessment of a finding originally rated as **Very Important**, then the following should be included under this column:

"UPDATED CLASSIFICATION: "Very Important (Confirmed)".

If, on balance, the finding is re-assessed as only **Important**, the following should be included:

"UPDATED CLASSIFICATION: Important".

An issue is not downgraded more than one level. Where an issue has been downgraded, it is reflected in the appropriate section of the body of the report. Either in Section *2.21 Critical and Very Important Recommendations* or in *Section 2.2.2 Important and Desirable Recommendations.*

Re-classification is made only where we consider that most of the constituent parts making up particular recommendation have been implemented and that the remaining part is relatively less important, ie where the risk has been substantively reduced following the actions taken by the auditee.

Any re-classification is clearly supported by the IAS assessment of the degree of implementation at the time of the audit follow up and explained under the "Current Risks" part of the body of the report and in Section 2.1.2 which summarises the IAS assessment. There should also be a brief reference in Section 1.4 of the Executive Summary dealing with Current Risks.

GRC requirements: requirements in terms of documentation of work done in the GRC application are detailed in the *Methodological guidance for the use of GRC.*

4. TYPE OF REPORTS

4.1. Audit reports

Results of the audit work conducted by the IAS are normally summarised in an "Audit Report" addressed to management and other stakeholders.

An audit report must always include the objectives and scope of the engagement, a conclusion (the audit opinion) and observations/recommendations save in exceptional circumstances where, for example, the process being audited is of an evolving nature and management is still in the process of reviewing the control system' preventing the auditor from expressing an opinion (disclaimer of opinion). Although a disclaimer of opinion is expressed, the recommendations issued will still be followed up in accordance with our usual follow-up policy.

Concerning audit opinions, the IIA has issued in April 2009 guidance on the formulation of both "macro" (overall opinion on the internal control of an organization as a whole) and "micro" (opinion at the engagement level) audit opinions. The potential impact of this guidance on the current practice at the Commission will be discussed in a separate note.

Over the course of time, results have also been communicated through "Review Reports", "Consultancy Reports" and "Management Letters".

4.2. Review Reports

A review report (sometimes also referred to as a "limited review" or a "risk assessment") is produced where it would be inappropriate or potentially misleading to produce a conventional audit report with an audit opinion. This could be for a variety of reasons, for example where the area concerned has never been audited by the IAS in the past and/or given the complexity of the process, the review is simply being used as a mechanism for the audit team to familiarise itself with the process. It could also be the result of a reaction to changing or previously unforeseen events, or a stakeholder (e.g. APC) request to have more information on a particular issue, for example an independent assessment of the progress being made in a key area. Reviews are normally based on desk reviews and interviews and result in issues for consideration rather than firm recommendations. Given that they do not generally result in opinions as such, review reports should be seen as rather exceptional by nature and do not form part of the normal audit assurance building framework. The review may be followed by an audit of the process reviewed conducted subsequently.

A review report should be clearly distinguished from an audit of the design (rather than the effective implementation) of controls in place or an audit with a reduced scope. In these cases, the results should be communicated in a normal audit report with a clear reference made in the objective and scope section of the report to the nature of the engagement.

4.3. Consultancy Reports

IPPF Standard 2010 states that "The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations".

Consulting engagements conducted by the IAS are normally based on a management request (although it can exceptionally be initiated by the IAS as well). A consultancy report should not contain an opinion.

4.4. Management letters

Management letters, which highlight weaknesses found in systems and propose issues for consideration, are usually issued to management as a by-product of an audit. These would normally consist of:

(1) recommendations related to issues affecting a process being audited but which need to be brought to the attention of a different entity than the one being audited, or issues not directly related to the process being audited which have come to our attention during the course of the audit and which are important enough for management to be informed of them,

(2) cases where sensitive matters (for example, irregularities by a staff member) are not disclosed in detail in the audit report, or

(3) the consolidation of observations relating to audits carried out on the same process in various DGs and for which there is not a readily identifiable chef de-file for the implementation of the recommendations, but are important enough to bring to the attention of one or more horizontal service.

In the cases referred to above, the recommendations should be issued as issues for consideration.

5. AUDIT REPORT EXECUTIVE SUMMARY[13]

The purpose of the Executive Summary is to provide qualitative information on the objectives, scope and results of the audit and to clearly identify risks/issues, e.g. material weaknesses.

It is the first and sometimes the only part of the report that senior management and members of the APC will read. It is therefore of the utmost importance that it is both concise and of the highest quality.

The main elements to be taken into account in drafting the Executive Summary are as follows:

- It should be no more than two pages long (on average),
- Avoid "copy and paste" of the main body of the report. The executive summary requires specific drafting taking into account it is intended primarily for Senior management and the APC,
- It should be a standalone document, i.e. it should contain enough information for a reader to get familiarised with the substance of what is discussed in the full report without having to read it,
- It should be clear, concise and accurate, and
- Sufficient time should be devoted to drafting it, in particular by the Supervisor and the team leader.

[13] Note D(2008) 761, dated 28 May 2008 on "Audit reports – Executive Summary".

6. AUDIT OPINIONS

The opinion is the auditor's *professional judgement* of the activities reviewed. It provides:

(1) a capsule comment on the assessment of the conditions found.

(2) a professional opinion on the adequacy and effectiveness of the system of control, the risk management and the governance processes within the activities audited provides useful and needed information to management.

(3) opinions on operations and the internal control system are no less important than the opinions on financial statements issued by the external auditors.

SAWYER states that: "*Internal audit opinions on specific activities audited are basically satisfactory or unsatisfactory. There may be gradations, of course: highly satisfactory, satisfactory, qualified, poor, unsatisfactory. But this can be mere hair splitting. From management's point of view, the operation either measured up to standards or it did not. Either the job was being done or it was not. Therefore, audit reports should carry overall audit opinions. Also, those opinions should besummarised to provide management and board4 with indications of the quality of both control and performance within [the Commission] as viewed by the internal auditors."*[14]

6.1. Consideration of the IAS

An "Audit Opinion" for the audit carried out and to be noted on the audit report (e.g. in the executive summary) should be formulated at the end of the audit and discussed with the auditee prior to the exit meeting. The audit opinion is always related to the *objectives and scope of the engagement*, formulated in the engagement planning memorandum and in the executive summary and the body of the report.

The "Audit Opinion" is an opinion regarding the ***adequacy of the design*** *and* ***the effectiveness of the implementation*** *of the internal control system, risk management and governance processes of the audited entity/process(es).*

The audit opinion is a critical deliverable of an audit and it supports the IAS strategy of delivering an overall assessment/opinion on the adequacy and effectiveness of the Commission's internal control system, risk management and governance processes. Moreover, it helps IAS management in its reporting obligations towards the APC and the Commission and it could help the IAC in its reporting obligation towards its Director General.

6.2. Audit opinions

The following classifications set out the different types of audit opinion and the underlying criteria which might give rise to those opinions. These criteria should be considered as guidance only and are not a substitute for the auditor's professional judgement.

0–No Opinion Required – Because of the type of the engagement no audit opinion is required (e.g. for consulting engagements/desk reviews/risk assessments).

1–Disclaimer of Opinion – An audit opinion is expected in principle but the auditors are unable to rate the engagement because of scope limitations. In this case the disclaimer should specify the scope limitations. The Institute of Internal Auditors defines scope limitation as: "a

[14] SAWYER, L.B.: *"Sawyer's Internal Auditing"* (3rd ed.), 1988, p. 635-636

restriction placed upon the internal auditing department that precludes the department from accomplishing its objectives and plan".
There are two major causes of scope limitations: restrictions imposed by the auditee (e.g. insufficient co-operation, insufficient access to data and/or staff, unacceptable delays,…) and those caused by circumstances beyond either the auditee's or auditor's control.

2–Satisfactory – This rating is given where the audit did not identify any "critical" or "very important" observations/weaknesses and the auditor considers that overall the internal control system in place provides reasonable assurance regarding the achievement of the objectives set up for the audited activity/process.

3–Satisfactory except for …….. (very important observations) – This rating is given where the audit did not identify any "critical" observations/ weaknesses and the auditor considers that overall the identified observations are not likely to cause material errors or irregularities and therefore are not likely to impair the achievement of the objectives set up for the audited activity/process.
Any very important observations should be included as qualifications to this opinion, unless these, taken as a whole, are so important that they should result in an unsatisfactory overall opinion.

4–Unsatisfactory – This rating is given where the audit identified "very important" and/or "critical" observations/weaknesses and the auditor considers that the identified observations are so important that overall the internal control system in place does not provide reasonable assurance regarding the achievement of the objectives set up for the audited activity/process.

5–Not under Control – This rating is given when a number of the identified observations are "critical" and the audit judges that the objectives set up for the audited activity/process most likely will not be achieved in practice.

6.3. Categorisation of observations

LEVELS OF SIGNIFICANCE					
OBSERVATIONS		**1 – CRITICAL**	**2 – VERY IMPORTANT**	**3 – IMPORTANT**	**4 – DESIRABLE**
	TYPOLOGY	Fundamental weakness in the audited process that is detrimental at Directorate General level	Fundamental weakness in the audited process that is detrimental to the whole process	Significant weakness in the whole audited process or fundamental weakness to a significant part of the audited process	No fundamental or significant weakness to the whole or significant part of the audited process
	RESERVATION IN THE AAR	Could lead to a reservation in the AAR			
	WAY OF REPORTING	Must be included in the Executive Summary	Must be included in the Executive Summary	*Can* be included in the Executive Summary.	Not included in the Executive Summary but in the body of the Audit Report only

6.4. Categorisation of recommendations

LEVELS OF SIGNIFICANCE					
		1 – CRITICAL	**2 – VERY IMPORTANT**	**3 – IMPORTANT**	**4 – DESIRABLE**
RECOMMENDATIONS	**TYPOLOGY**	Recommendation that mitigates the risk of a critical observation so that: • It is not detrimental at Directorate General level anymore, and that • It is not detrimental to the whole audited process anymore	Recommendation that mitigates the risk of a very important observation[15] so that it is not detrimental to the whole audited process anymore	Recommendation in response to an important observation[Error! Bookmark not defined.] [16] so that, whether: • A significant weakness to the whole audited process, or • A fundamental weakness to a significant part of the audited process is mitigated	Recommendation or correction that would add value to the audited process
	TIMING	Implementation of the Recommendation: immediate action required	Implementation of the Recommendation: prompt action required	Implementation of the Recommendation: action is required as soon as possible but it may not delay the implementation of the critical or important recommendations	Implementation desirable; non-implementation not detrimental to the audited process
	WAY OF REPORTING	• Must be included in the Executive Summary	• Must be included in the Executive Summary	• *Can* be included in the Executive Summary.	• Not included in the Executive Summary but in the body of the Audit Report only

[15] It can also contribute to mitigate the risk of a critical observation, on the condition that the critical observation is also mitigated by at least one critical recommendation.

[16] It can also contribute to mitigate the risk of a very important observation, on the condition that the very important observation is also mitigated by at least one very important recommendation.

7. REVIEW AND APPROVAL PROCESS IN GRC

The review and approval process (by the Head of Unit, QA members, Audit Director and Director-General) should be adequately evidenced in GRC. Ways to evidence these reviews are detailed in the *Methodological Guidance on the use of GRC.*

8. QUALITY ASSURANCE

8.1. Plan execution monitoring tool: KPIs

A number of KPIs is defined in the IAS Annual Management Plan. The assessment is performed twice a year (at 30.06 and 31.12).

The KPIs for Directorate B, Internal Audit Service, as defined in the management plan are:

1) Percentage (%) of the audit plan implemented (C1, C2 and consolidated)

2) Acceptance rate of critical/very important recommendations (based on the Overview report)

3) Overrun between time planned and time actually used for an audit

4) Average number of days between end fieldwork and final report

5) Average number of pages for audit reports

6) Auditee Satisfaction Surveys

7) Number of recommendations related to simplification

8) Follow-up of IAS recommendations (% of critical & very important recommendations overdue for more than 12 months and overall % of recommendations implemented)

8.2. IAS internal quality assessment – periodic reviews

The IIA Standards require the internal audit activity to undertake both ongoing and periodic internal assessments as part of an overall Quality Assurance and Improvement program (Std 1311).

As part of its response to the findings from the 2008 external review, the IAS established a separate, ongoing quality assurance function in addition to the normal day-to-day supervisory activities exercised by Management. The quality assurance function, in addition to its daily work on the reporting side and, to a certain degree on the engagement planning process, also conducts an internal assessment (internal quality review) of specific engagements.

The Standards and the associated Quality Assessment Manual allow periodic internal assessments to be based on a variety of possible inputs, including self assessment, in-depth interviews, bench marking etc.

Normally, periodic reviews would be supported by extensive self assessment work, stakeholder surveys, follow up interviews and consideration of KPIs, in addition to file reviews. The simplified internal periodic assessment focus primarily on audit engagement file reviews and an analysis of standard KPIs.

Consequently, the limited nature of the review does not result in an opinion on the overall conformity with the Standards. Instead the aim is to produce an improvement plan for each Audit Team which should in turn highlight those measures which are necessary to improve conformity with the Standards and/or IAS policies and procedures. A summary improvement plan is also made for the Service as a whole with the same objective.

9. SAMPLING METHODOLOGY FOR THE TEST OF CONTROLS

This part sets out the principles which underpin the selection of a sample of controls that need to be tested in order to evaluate its operating effectiveness, i.e. to assess if the control is operating as intended and mitigates the risk identified.

It provides guidance to the auditors for the population of controls to consider for testing, the minimum sample size to test, considering the nature of the control tested and the level of assurance expected, the different sample selection and test techniques and the basic principle for documenting the tests performed.

9.1. Definition of the sample size

The extent of the sample to test is based on judgement and the level of assurance the auditor expects to derive from the test. The sample chosen should ensure coverage of the entire population. The sample sizes should be increased where there are greater risks that the control is not operating effectively.

9.2. Analysis of the population

While the sample size does not need to be a specified percentage of the population, identification of the total population and analysis of stratums within that population is critical to ensure adequate coverage of the entire population. The stratums of a population refer to the various characteristics of that population e.g. samples are in different locations. The stratums are the layers by which the auditor can divide the population. Stratums are used as part of sample selection so that the important layers of the population can be identified and sample items chosen on this basis if necessary.

The criteria for stratifying the population can depend on any number of factors related to the control including, the objective of the control, the risks being mitigated, the significant accounts, control locations, control operators, approval levels, escalation levels.

In addition, the samples selected should be dispersed across the audit period or at least that part of the audit period for which the control being tested has been operating.

Similarly, the sample should be extracted judgementally to cover the various control periods throughout the population. As an example for a daily control, the sample should be stratified to ensure that samples are taken from each working day (Monday, Tuesday, etc.).

This analysis should provide indication of how many samples are required to be tested to ensure full population coverage across the full period. Further considerations should also be given to:

- Complexity of the control;
- Importance (or level of reliance) of the control, i.e.
- Significance of judgement in the control operation;
- Level of competence necessary to perform the control;
- Impact of changes in volume or personnel performing the control.

9.3. Minimum Sample Size

Minimum sample sizes need to be considered together with the above factors and considering the test technique that will be used, and should not be applied blindly.

For highly critical controls or where a single manual control provides the sole support for a significant account, the auditor should consider increasing the sample size above the minimum guidelines set out below.

Manual Controls

The following table represents the minimum extent of testing necessary to support a conclusion that a manual control is operating effectively:

Frequency of Performance of Control	Assumed population of control occurrences	Minimum Sample size[17]
Continuous (multiple times per day)	Over 250	25
Daily	250	20
Frequently but less than daily	53-249	15
Weekly	52	5 to 10
Monthly	12	2 to 5
Quarterly	4	2
Annually	1	1

Automated Controls

For an automated control, the minimum sample size is considered to be ONE.

However, this sample size is acceptable only if the Information Technology General Computer Controls (IT GCC) that support that automated control are reliable, i.e. IT GCC controls are designed effectively and operating effectively.

If this is not the case then additional testing of automated controls may be required.

As with Manual Controls, other factors need to be considered before deciding on the sample size.

In addition to the factors outlined for manual controls, the auditor needs to remember that the minimum sample size of ONE may need to be applied to each stratification within an automated control (e.g. if a control is that approval thresholds are set in the system, then each stratification of the threshold values need to be tested. For example: Up to 50,000; 50,000 to 250,000, Over 250,000, each need to be tested).

9.4. Sample selection

Once the auditor has determined the appropriate sample size, a sample of items from the population must be taken. Methods for selecting sample items include the following:

Nonprobabilistic Sample Selection:

In the non probabilistic sample selection method, the auditor will select items to test based on judgmental criteria. The auditor will select the items most likely to contain misstatements, with large materiality coverage, i.e. in the case of items with monetary value.

Probabilistic Sample Selection:

[17] Source: E&Y

In this method, the auditor will select a sample such that each population item has a known probability of being included in the sample. In this case, the sample can be selected using the following techniques:

- Haphazard sampling techniques, where the selection is performed without regard to size, source, or distinguishing characteristics;
- Random number techniques, where every possible combination of elements in the population has an equal chance of constituting the sample;
- Systematic sampling techniques, where the auditor calculates an interval and then selects the items for the sample based on the size of the interval. The interval is determined by dividing the population size by the number of sample items desired.

9.5. Type of Test

The types of test techniques can be classified into four categories, by increasing level of assurance:

- inquiry
- observation
- examination and
- re-performance

Combining two or more of these tests can provide greater assurance than using only one technique.

Factors to consider when determining which testing technique to use include:

- Type of control i.e. manual or automated
- Materiality of the process and risk of control breakdown
- Likelihood of a control breakdown based on the complexity of the process and whether the control is automated (generally less likely) or manual (generally more likely)
- Significance of the control and how much reliance is being placed on it for comfort. A single key control for a material process needs to be tested with more rigor than if several overlapping controls are working together to provide assurance.

9.6. Inquiry

Inquiry of a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively. Note, PCAOB Guidance states that inquiry alone is not sufficient evidence of a control's operational effectiveness. Inquiry means establishing whether a control is in place by asking oral or written questions. It is the weakest type of test and should be followed by another test.

9.7. Observation

Observation of the control provides a higher degree of assurance and may be an acceptable technique for assessing some controls, in particular some automated controls. It is more reliable than inquiry and involves observing the employee performing the control procedure. The audit evidence provided about the performance of a process or procedure is limited to the point in time at which the observation takes place.

9.8. Examination

Examination of evidence often is used to determine whether manual controls (e.g. the follow-up of exception reports) are being performed. This involves reviewing documentation and/or reports to

verify that the control activity operated as intended. It provides assurance over certain aspects of the control; however, the quality of evidence needs to be considered.

9.9. Re-performance

Re-performance of the specific application of the control provides the highest degree of assurance that the procedure or process has operated correctly. This involves the auditor re-performing the control activity independently of the person who has already undertaken this activity. It is the best type of test to ensure that the risk mitigated by the control has not actually materialised. However it does not necessarily verify that this was due to the operational effectiveness of the control.

9.10. Documentation of the testing

Documentation of the testing should provide sufficient detail to enable the exact test to be re-performed using the same sample, i.e. if the same sample item was selected again and the same test re-performed; it would produce the same result. This requires documenting detailed information about the sample chosen, providing enough information to allow identification of the exact same sample items as tested (e.g. the account number, account balance, date of report, contract reference, etc).

9.11. Evaluation of test results

Once the sample items have been tested, the auditor should conclude on the actual operating effectiveness of the control. When no exception is identified, the auditor can conclude that the control is effectively operating as intended and can confirm the management reliance on the control to mitigate the risk the control is intended to cover.

If, when using the above table of minimum sample sizes, the auditor identifies one exception in the items tested, he can conclude that the test results can not support the assertion that the control is working properly, preventing him from issuing a clean audit opinion. However, given the fact that the sample sizes reflected in the table are minimum, the exception rate found in the sample can not be extrapolated to the whole population and serve as a basis to estimate the total population error rate, which, if required, would need increased sample sizes.

We consider that an exception rate exceeding 10% of the abovementioned minimum sample sizes indicates that the control is not working properly.

10. DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Term	Description
Annual Activity Report (AAR)	*The Annual Activity Report gives account of the achievements of the key policy objectives and core activities of the DG or Service taking into account the corresponding resources used during one year's activities. In this respect, the AAR is a "mirror" of the Annual Management Plan (AMP) as it reports on the delivery of key objectives and activities identified in the AMP. The AAR is also a management report of the Director-General to the Commission. It covers all management aspects, including the implementation of Internal Control Standards.*
Management Plan (MP)	*The Annual Management Plan is a results-oriented management and programming tool, translating the APS priorities into objectives while covering all the activities and resources of a DG/Service for a year. The AMP is worked out by each service and translates the Commission's priority objectives into operational actions with resources allocated under the Preliminary Draft Budget. It includes tools enabling follow-up, information and evaluation of DGs' activities. Once the Annual Management Plan has been prepared, it has to be implemented and monitored: this entails follow-up of actions, indicators and resources associated with these actions.*
Annual Policy Strategy (APS)	*The Annual Policy Strategy defines an annual strategic framework at Commission level and identifies, early in the previous year, political priorities and key initiatives for the following year. Every year, in February, the Commission decides it's Annual Policy Strategy based on an orientation debate and the services' subsequent proposals. It involves reviewing the progress made on longer-term goals and deciding on the key initiatives and objectives for the reference year and on the resources needed to achieve them. The APS provides guidelines on policy objectives and resource requirements for the preliminary draft budget as well as for the Commission's annual work programme and the operational programming (DGs' annual management plans).*
Audit Conclusions	*PowerPoint document to be presented by the IAS Director General during the exit meeting; it is prepared by the audit team leader and then validated by the Head of Unit, the IAS Director and the IAS Director General*
Audit Management System (GRC)	*The Audit Management System is the main tool for management of audits and consultancies carried out by IAS and the Internal Audit Capabilities (IACs), management of the follow-up to audit recommendations and internal management of audit staff. It is a web based application with a single database and modules for risk assessment, planning, scheduling, workpapers, reporting, issue tracking, time and expenses, quality assurance and personnel records. The system is supplied by an external company; Paisley Consulting (acquired by Thomson Reuters).*

Term	Description
Audit work Program	*Internal document to IAS; is a document which lists the audit procedures to be followed during an audit*
Audit Progress Committee (APC)	*The Audit Progress Committee assists the College in ensuring that the work of the IAS is properly taken into account by Commission services and receives appropriate follow-up. The Committee is an advisory body, composed of five members: four Commissioners and one external member with relevant experience and knowledge of internal audit. The APC is also responsible for ensuring the independence of the IAS and for monitoring the quality of internal audit work in the Commission. It also monitors the quality of audit work in DGs.*
Engagement Planning Memorandum (EPM)	*Output of the preliminary survey and the RCM (see below); includes the objectives and scope of the audit and describes the methodology to be followed*
Finding (= Issue = Observation)	*A weakness identified in the internal control system during the audit, during the test of procedures (design) or during the test of transactions (application).*
Findings Validation Table	*Table listing the observations detected during the audit, which is validated by the auditee; produced by the audit team and approved by the Head of Unit and IAS Director*
Internal Audit Capabilities (IACs)	*The Internal Audit Capability operates within a DG and reports directly to the Director-General. It does not have any executive responsibility. Its role is to advise the Director-General on the quality of the internal control systems operating within the DG and the risks under which it operates, and to recommend improvements as necessary. The Director-General remains ultimately responsible for deciding whether or not to accept audit findings and recommendations*
Issue	*See Finding*
Key Performance Indicators (KPIs)	*Key Performance Indicators are defined to measure the quality and performance of processes and deliverables.*
Observation	*See Finding*
Risk	*Risk is the possibility that an event will occur and adversely affect the achievement of the objectives*
Risk & Control Matrix (RCM)	*Output of the preliminary survey, used as an input for the EPM; describesthe risk areas identified in the process to be audited, the existing controls as described by management and the testing approach to be followed during the audit*
Workpaper	*Workpapers document the audit and provide documentary support on the audit process and the conclusions of the auditors. They are the source of evidence on which to base conclusions and the evidence that the audit has been carried out in a professional way that can be independently verified at any stage.*