Audit Manual

Internal Audit Division
Office of Internal Oversight Services

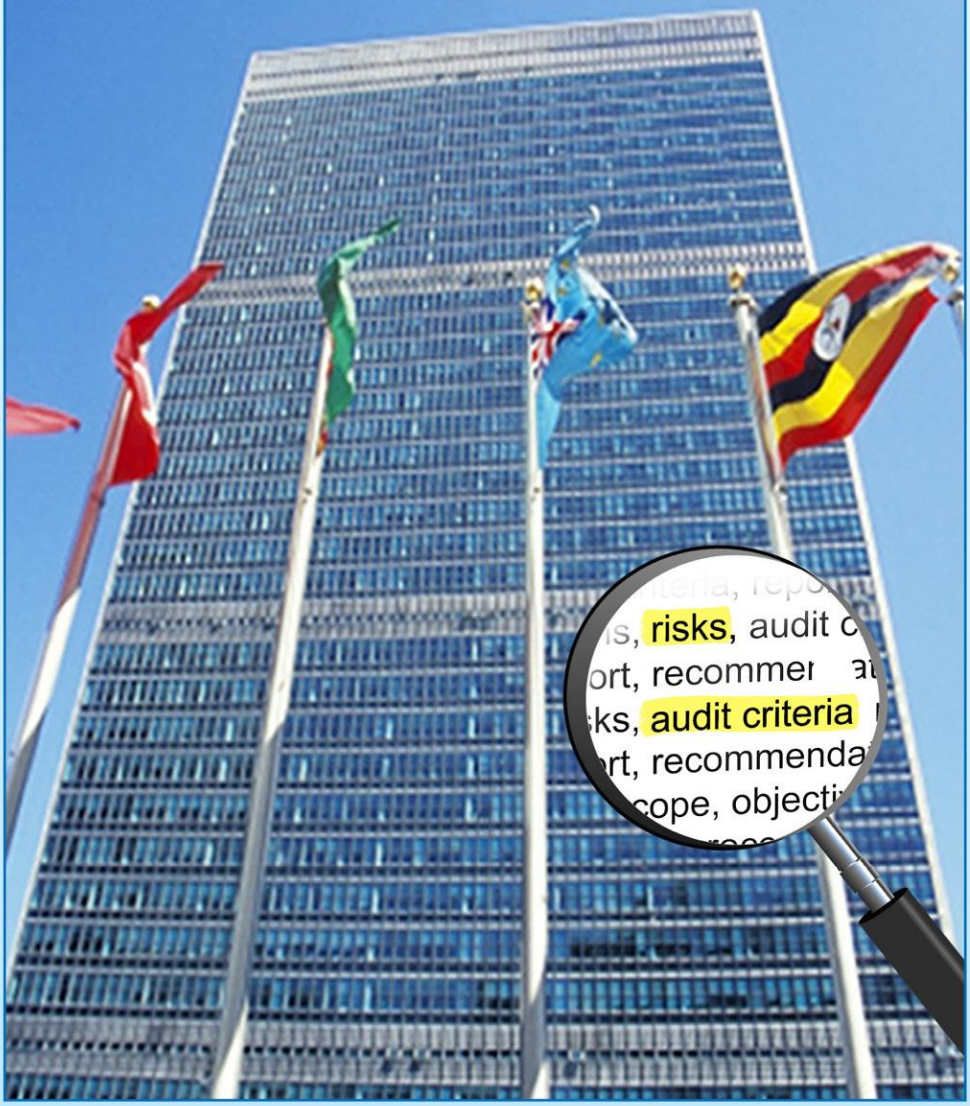


Table of Contents

1 Introduction 14

1.1 Scope and purpose of the Manual **14**

2 Purpose, authority and responsibility of IAD 15

2.1 Introduction **15**

2.2 Purpose **16**

2.3 Authority and responsibility **17**

2.4 Position within the organization **18**

2.5 Organizational structure of IAD and responsibilities of staff **19**

3 Application of Professional Standards 19

3.1 Introduction **19**

3.2 The IIA Standards and definition of internal auditing **19**

3.3 Ethical standards **19**

3.4 Independence and objectivity **20**

3.5 Use of consultants **20**

3.6 Continuing professional development **21**

3.7 Quality assurance **21**

4 Relationships with stakeholders 21

4.1 Introduction **22**

4.2 Key stakeholders **22**

4.2.1 Clients **23**

4.2.2 Audit committees **23**

4.2.3 Fifth Committee **25**

4.2.4 The United Nations Board of Auditors **25**

4.2.5 The Joint Inspection Unit **26**

5 Risk assessment and work planning 26

5.1 Introduction **27**

5.2 The work plan development **27**

5.3 Validating and updating the audit universe **28**

5.4 Identifying strategic and business objectives and related risks **28**

5.5 Assessing and ranking risks related to auditable activities **28**

5.6 Identification of audit assignments and resource gap analysis **28**

5.7 Developing the three-year rolling work plan **28**

5.8 Consultations with BOA and JIU **29**

5.9 Finalising the work plan **29**

5.10 Communication with client **30**

5.11 Submission of work plans to audit committees **31**

5.12 Changes to the work plan **32**

5.13 Advisory assignments **32**

6 Engagement planning 33

6.1 Introduction **33**

6.2 The engagement planning process **34**

6.3 Issuing audit notification memorandum **34**

6.4 Understanding the client **34**

6.4.1 Documenting the system **35**

6.4.2 Conducting activity-level risk assessment **35**

6.4.3 Developing audit criteria **36**

6.5 Developing audit objectives 36
6.6 Defining audit scope and methodology 38
6.7 Developing preliminary audit plan and programme 39
6.8 Conducting the entry conference 41
6.9 Issuing the terms of reference 41
6.10 Finalising the audit plan and programme 42
7 Performing the engagement 42
7.1 Introduction **43**
7.2 Audit testing **43**
7.2.1 Testing key controls and the absence of key controls **43**
7.2.2 Audit sampling **44**
7.2.3 Analytical procedures **45**
7.2.4 Root cause analysis **45**
7.3 Recording information during the audit **46**
7.4 Evaluating the results of audit testing **47**
7.5 Supervising the audit **32**
7.6 Staff appraisals **33**
7.7 Communicating with IAD management during fieldwork **33**
7.8 Fraud and misconduct **34**
8 Communicating results 34
8.1 Introduction **34**
8.2 Communications during the engagement **35**
8.3 Exit conference **35**
8.4 Engagement reporting **36**

8.5 Detailed audit results **36**

8.6 The draft audit report **38**

8.7 The final audit report **39**

8.8 Use of personally identifiable information in audit reports **41**

8.9 Reporting to the General Assembly, audit committees and senior management **41**

8.10 Publication of audit reports **42**

8.11 Ownership and retention of working papers **42**

9 Recommendation monitoring and follow-up 43

9.1 Introduction **43**

9.2 Recording recommendations **43**

9.3 Following up on and closing recommendations **44**

ANNEX I **45**

Practice Guides 45
Standard Operating Procedures 46
Forms and Templates 47

Preface to the May 2023 edition

I am pleased to present the 2023 edition of the Audit Manual of the Internal Audit Division (IAD).

The Manual provides guidance to IAD staff on the principles of the IAD audit process. It explains general concepts and refers to specific procedures to be followed.

This edition of the Manual is more principles-based, and it incorporated: revisions and enhancements to the IAD policies and procedures; and additional requirements by Member States.

To complement the Manual, IAD has also developed a number of Practice Guides, Standard Operating Procedures and Templates to provide further guidance to staff and to facilitate the audit process. A list of current documents, including those under development, can be found in Annex I and are stored in the audit management system of IAD.

The Manual and supporting guidance are living documents; and therefore, they will be updated to ensure that it represents the latest standards and practices, and the policies and procedures that govern the conduct of internal auditing at the United Nations. The Professional Practices Section will communicate any changes.

The Manual is the result of a dedicated team effort, and I sincerely thank all those IAD staff who contributed to its successful completion.

Director, Internal Audit Division
OIOS

New York, May 2023

1 Introduction

1.1 Scope and purpose of the Manual

The Internal Audit Manual (the Manual) is for the use of staff of the Internal Audit Division (IAD) and provides the policies, principles, standards and code of ethics governing the professional practice of internal auditing at the United Nations. The Manual describes the audit management process of IAD, from planning the audit to conducting the fieldwork, reporting results and following up on recommendations.

The purpose of the Manual is to:

- Provide guidance on all aspects of the audit process;
- Explain the context of the work of IAD to audit staff; and
- Promote the highest level of professional competence in IAD.

The Manual includes references to standard operating procedures (SOPs) and practice guides. These documents provide detailed instructions and useful information on processes, procedures, tools and techniques, which IAD staff are either: (a) required to comply with; or (b) adopt as recommended good practices. These documents are available on the IAD content management system.

The Manual is not designed to be all-inclusive or unduly restrictive. Its provisions are intended to supplement the experience, competencies, skills and judgement of internal auditors in planning, conducting and reporting on audits.

The available resources are invaluable and should be utilized consistently. However, IAD staff should be sensitive to their work environment, use good judgement throughout the audit process and ensure that stakeholders and clients are aware of and are in agreement with the intentions, objectives and practices of their respective audits.

2 Purpose, authority and responsibility of IAD

2.1 Introduction

This chapter provides an overview of the mandate, authority and responsibility of IAD, and provides an overview of the organizational structure of IAD and responsibilities of audit staff.

2.2 Purpose

The Office of Internal Oversight Services (OIOS or the "Office") was established in 1994, under General Assembly resolution 48/218 B of 29 July 1994, to enhance the oversight functions within the United Nations (or the "Organization"). IAD is one of three divisions of OIOS (the others being the Investigations Division and the Inspection and Evaluation Division). With respect to internal audit, the General Assembly resolution outlines the mandate of OIOS within the United Nations:

> "*The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization*."

2.3 Authority and responsibility

OIOS is assigned responsibility for internal auditing in the United Nations. The Secretary-General's Bulletin on the Establishment of the Office of Internal Oversight Services of 7 September 1994 (ST/SGB/273) describes the organizational structure and functions of OIOS, including:

> *OIOS responsibilities "shall extend to the resources and staff of the Organization, including separately administered organs."*
>
> *OIOS has "the authority to initiate, carry out and report on any action it considers necessary to fulfil its responsibilities" in regard to the audit function.*
>
> *OIOS shall "discharge its responsibilities without any hindrance and need for prior clearance," and shall have the right to direct and prompt access to all staff, records, documents and premises of the Organization and to obtain all necessary information and explanations.*
>
> *OIOS shall conduct "ad hoc audits of programme and organizational units" whenever there are reasons to believe that programme oversight is not sufficiently effective and that there is "potential for the non-attainment of objectives," waste of resources, or otherwise, as the Under-Secretary-*

General/OIOS "deems appropriate," with a view to recommending to management corrective measures.

OIOS shall "undertake management audits, reviews and surveys to improve the Organization's structure and responsiveness to the requirements of programmes and legislative mandates; and monitor the effectiveness of the Organization's systems of internal control".

Additionally, the Fifth Committee regularly reviews the functions and reporting procedures of OIOS, as called for in paragraph 13 of resolution 48/218 B. The Fifth Committee's periodic (every five years) reviews of the OIOS mandate resulted in subsequent provisions and requirements on OIOS. These are contained in General Assembly resolution 54/244 of 23 December 1999, General Assembly resolution 59/272 of 23 December 2004, General Assembly resolution 64/263 of 29 March 2010, General Assembly resolution 67/258 of 3 June 2013, General Assembly resolution 69/253 of 29 January 2015, General Assembly resolution 74/257 of 9 January 2020; and United Nations Financial Regulation 5.15.

The mandate as well as the relevant resolutions and administrative issuances are on the OIOS website.

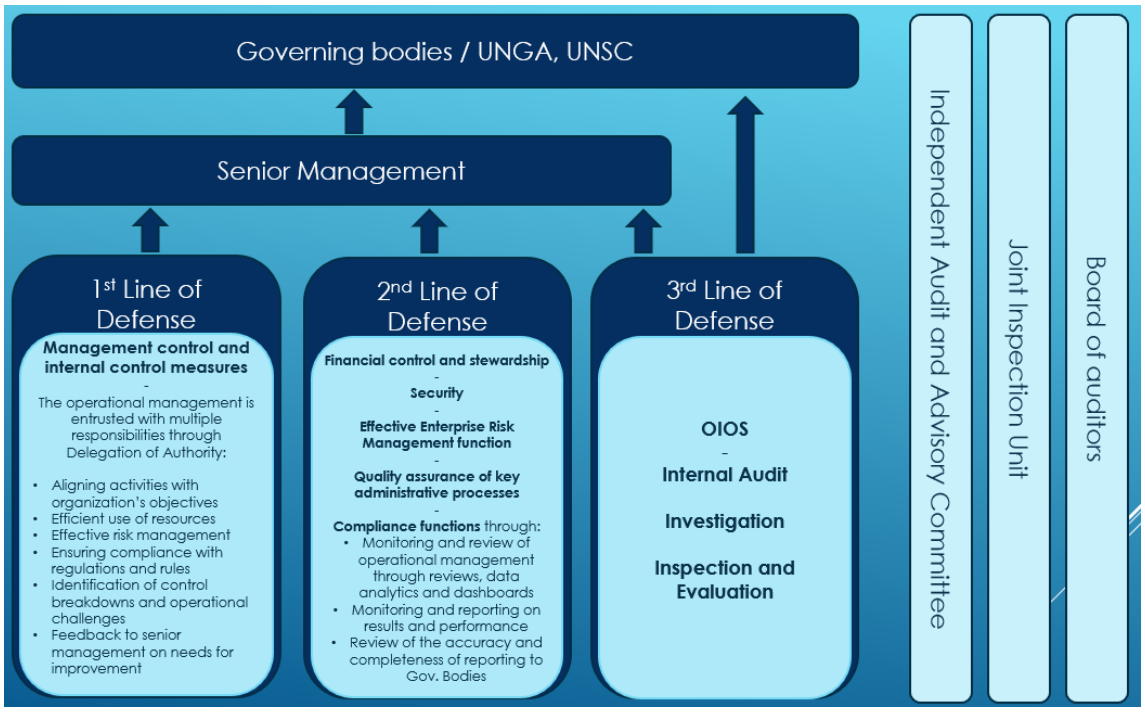
2.4 Position within the organization

The General Assembly established OIOS as operationally independent, under the authority of the Secretary-General, in the conduct of its duties. This operational independence ensures that OIOS has:

- The authority to initiate, carry out and report on any action which it considers necessary;
- The ability to submit reports directly to the General Assembly;
- The authority to select staff for appointment and promotion up to the D-1 level;
- The ability to obtain access to United Nations staff directly and confidentially, and to be protected against repercussions; and
- Been provided adequate resources to carry out its duties.

The Organization has adopted the three lines of defence model defined by the IIA. As shown in Figure I below, OIOS, constitutes the organization's third line of defence, responsible for independent oversight activities. The United Nations Board of Auditors (BoA), the Joint Inspection Unit (JIU) and the Independent Audit Advisory Committee (IAAC) also play important roles in the organization's control structure by providing independent, external assurances to the General Assembly.

Figure I: United Nations three lines of defence model

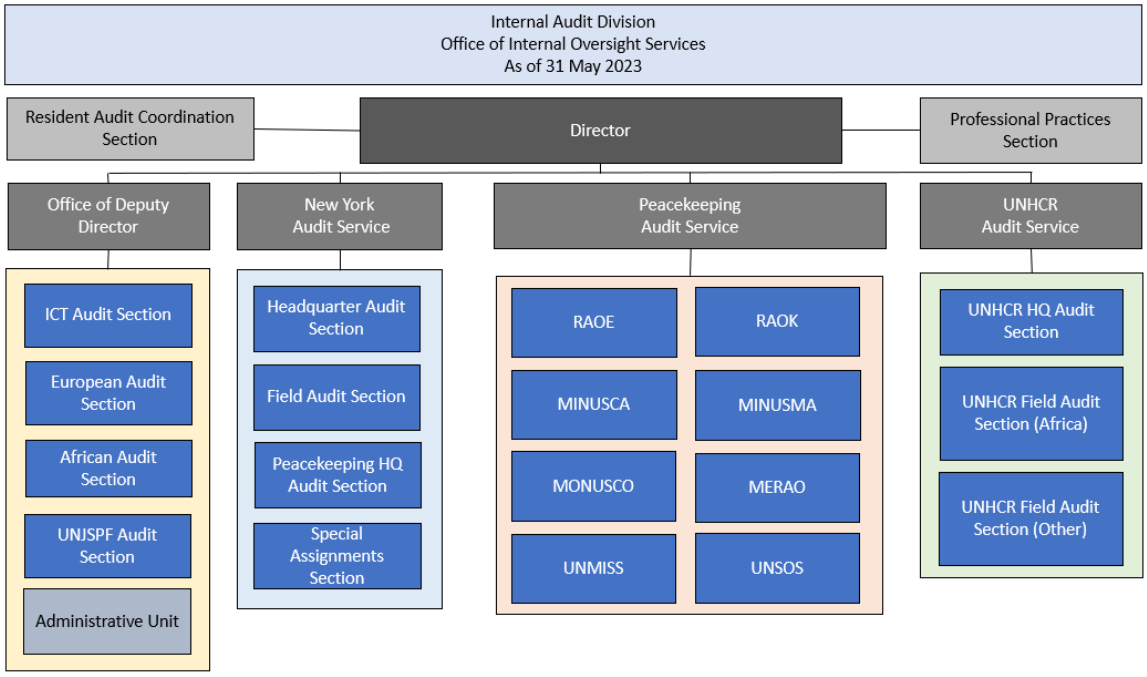


Source: Report of the Secretary-General on the seventh progress report on the accountability system in the United Nations Secretariat: strengthening the accountability system of the Secretariat under the new management paradigm A/72/773

2.5 Organizational structure of IAD and responsibilities of staff

The organizational structure of IAD is shown below.

Chart I: Internal Audit Division Organization Structure



Director has overall responsibility for all IAD activities, including: planning, directing and implementing the annual risk-based work plan; coordinating with other OIOS Divisions and oversight bodies; overseeing budget and recruitment; and implementing the quality assurance programme and has the direct oversight of the crosscutting functions of the Professional Practices and the Resident Audit Coordination Sections.

Deputy Director supports the IAD Director in planning, directing and coordinating the work of IAD, and implementation of the annual work plan. In addition to supervising the audit sections under his/her responsibility, the Deputy Director has also direct oversight of the Administrative Unit.

Service Chiefs report to the Director of IAD and oversee audit operations under their supervision. Service Chiefs are responsible for ensuring the quality of all work performed by their sections, for delivery of the annual work plan

and managing client relationships. Service Chiefs provide guidance and supervision to Section Chiefs and audit staff.

Section Chiefs and **Chief Resident Auditors (CRAs)** report to the Service Chiefs and are responsible for the development and delivery of the work plans for their section or office, for the quality of work completed by their staff and general supervision and development of staff under their supervision.

Professional Practices Section (PPS) coordinates and monitors the IAD Quality Assurance and Improvement Programme. PPS develops audit methodology and provides technical guidance for its implementation. PPS further coordinates the risk assessment and work-planning processes, and supports IAD management in monitoring performance of the internal audit activity. PPS also provides guidance for and coordinates professional development of staff.

Resident Audit Coordination Section (RACS) is responsible for coordinating the work-planning process for the audit of peacekeeping activities, coordinating thematic audits undertaken in more than one peacekeeping mission, and backstopping/support to section chiefs in implementing their work plans. RACS also reviews audit reports from resident audit offices and coordinates training and development for peacekeeping audit staff.

Auditors-in-Charge (AIC) report to the Section Chiefs and are responsible for managing audit assignments. AICs supervise team members and provide guidance and coaching for the development of staff. AICs are responsible for timely completion of working papers in the audit management system. AICs also monitor the status of audit recommendations.

Assisting Auditors are responsible conducting audit assignments under the supervision of the AIC. They are also responsible for timely completion of working papers in the audit management system.

3 Application of Professional Standards

3.1 Introduction

This chapter provides an overview of the professional standards and United Nations requirements that are most applicable to the work of IAD and describes the responsibilities and professional standards that auditors have to maintain both in their work and in their continuing professional development.

3.2 The IIA Standards and definition of internal auditing

In 2002, IAD adopted the International Standards for the Professional Practice of Internal Auditing that is developed and maintained by the Institute of Internal Auditors (IIA), as mandatory guidance for the practice of internal auditing in the United Nations. IAD auditors are expected to be familiar with the IIA Standards and definitions to ensure that their work is in accordance with the Standards.

IIA Standards are available on the Standards and Guidance page of the IIA website. The IIA Standards are referred to in this Manual and in the SOPs and practice guidance where applicable.

IAD has adopted the IIA definition of internal auditing:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

IAD provides both assurance and advisory services. Assurance services involve an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements. Advisory services involve advisory and related client service activities, the nature and scope of which are usually agreed with the client, that are intended to add value and improve an organization’s governance, risk management and control processes without the internal auditor assuming management responsibility. Examples may include counsel, advice, facilitation, and training. In this Manual, assurance and advisory services are referred to as “audit/advisory engagements” or “audit/advisory assignments”.

3.3 Ethical standards

IAD staff members must ensure their behaviour and activities are in accordance with the highest level of ethical values, integrity and professionalism. The United Nations has adopted a strong ethical framework that reinforces core values and supports a culture of ethical decision-making, accountability of staff at all levels and a commitment to proper conduct.

The relevant legal norms drawn from the Charter of the United Nations and the Convention on the Privileges and Immunities of the United Nations identify core values and set standards for all United Nations employees. The Annex to the Secretary-General's bulletin on status, basic rights and duties of United Nations staff members (ST/SGB/2016/9) contains the Standards of Conduct for the International Civil Service, promulgated by the International Civil Service Commission. All United Nations personnel are required to comply with the Standards of Conduct for the International Civil Service.

Article 101(3) of the Charter of the United Nations states that:

> *The paramount consideration in the employment of staff and in the determination of the conditions of service should be the necessity of securing the highest standards of efficiency, competence and integrity.*

Standards of Conduct for the International Civil Service state that:

> *... international civil servants must remain independent of any authority outside their organization; their conduct must reflect that independence. In keeping with their oath of office, they should not seek nor should they accept instructions from any Government, person or entity external to the organization... The independence of the international civil service does not conflict with, or obscure, the fact that it is the Member States that collectively make up – in some cases with other constituents – the organization.*

Regulation 1.2(b) of the Staff Regulations (ST/SGB/2023/1) states that:

> *Staff members shall uphold the highest standards of efficiency, competence and integrity. The concept of integrity includes, but is not limited to, probity, impartiality, fairness, honesty and truthfulness in all matters affecting their work and status.*

Secretary-General's Bulletin on Post-Employment Restrictions (ST/SGB/2006/15) places post-employment restrictions on "staff members participating in the procurement process," including those involved in "auditing the procurement process."

As professional auditors, IAD staff members shall respect and contribute to the legitimate and ethical objectives of the organization and abide by the Code of Ethics of the IAA (Global Internal Auditing Code of Ethics | The IIA). The IIA Code of Ethics requires all professional auditors to apply and uphold the following principles:

1. Integrity

   The integrity of internal auditors establishes trust and thus provides the basis of reliance of their judgement.

2. Objectivity

   Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgement.

3. Confidentiality

   Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

4. Competency

   Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

As required by the IIA Code of Ethics, internal auditors should be prudent in the use and protection of information acquired in the course of their duties, and will not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization. To maintain the confidentiality of information and reports, including detailed audit results, draft reports and withheld final reports, OIOS developed the following measures:

- In the Statement of Independence and Confidentiality signed annually and before the start of each assignment, the staff member declares that he/she: (i) shall be prudent in the use and protection of information acquired in the course of their duties, (ii) will not use information for any personal gain or in any manner that would be contrary to relevant United Nations regulations and rules or detrimental to the legitimate and ethical objectives of the organization; and (iii) will appropriately maintain and protect the confidentiality of any information or data to which they may have access, including audit files and reports.

- As mentioned in the Guidelines for maintaining operational independence, OIOS staff members should not make public statements about the results of ongoing assignments to avoid undue influence from the client and other stakeholders, which may impair operational independence.

If an audit assignment is expected to contain sensitive and confidential information and documents, it should be dealt with as detailed in the SOP on Data Privacy and Data Protection in IAD.

3.4 Independence and objectivity

The internal audit activity must be independent, and every internal auditor must be independent and objective. IAD staff must always maintain independence, objectivity and a perspective based on facts when conducting audits. The fact that an internal auditor is an employee of the Organization does not in itself have an impact on objectivity. Auditors should have an impartial, unbiased attitude, characterized by integrity and an objective approach to work, and they should avoid conflicts of interest. They should not allow external factors to compromise their professional judgement. They should display appropriate professional objectivity when providing their opinions, assessments and recommendations. When assigning staff members to audits, IAD requires that the staff members be free of any restrictions that will affect their independence and objectivity in performing audits.

An internal auditor's objectivity is presumed to be impaired when she or he is assigned to audit an activity for which she or he previously had operational authority or responsibility. Persons transferred to or temporarily engaged by IAD should not be assigned to audit or advise on activities for which they previously had responsibility for at least one year from the date they were reassigned.

IAD staff should review and ensure that they comply with the IIA Standard on objectivity. If it is likely that an auditor will not meet the on objectivity standard, either at the commencement or during the course of an audit engagement, this should be reported to either the Section or Service Chief, who will reassign the staff member.

In the Statement of Independence and Confidentiality, staff members declare that (i) he/she holds no views or opinions that could bias the engagements in the annual work plan assigned to him/her; (ii) he/she has no official, professional, personal, or financial relationships that might cause him/her to limit the extent of his/her inquiry, to limit disclosure, or to weaken or slant audit observations in any way; (iii) there is no external interference or influence that would cause him/her to improperly or imprudently limit or

modify the scope of the audit engagements; (iv) there is no external interference that would affect the selection or application of audit procedures or the selection of locations to be examined; and (v) he/she will promptly notify the management of IAD of any known conflict of interest, which would inhibit his/her independence in carrying out an audit engagement.

Additionally, all staff members at the D-1 level and above are subject to the United Nations Financial Disclosure Programme, stipulated in ST/SGB/2006/06, to identify, resolve and mitigate conflict of interest risks arising from staff members' personal financial assets, liabilities, investments, and outside activities.

3.5 Use of consultants

IAD occasionally uses consultants (a person or firm with expert knowledge, skills and experience in a particular discipline) to provide assistance on assignments when IAD does not have the requisite competency. This assistance can vary depending on needs but may include assistance in developing specific audit procedures or in conducting part of the audit.

The Service Chief, together with the Section Chief, is responsible for selecting and hiring consultants, and for ensuring that adequate funding exists for such services. The Service Chief should keep the Director informed of any external sourcing of expertise.

3.6 Continuing professional development

IAD staff are responsible for continuing their education to maintain the required level of proficiency, knowledge and skills. IAD staff are responsible for staying informed about improvements and current developments in the internal auditing standards, procedures and techniques. IAD staff are required to complete a minimum of 40 hours (five days) of continuing professional education for each annual performance cycle. On average, IAD staff have the opportunity to attend in-house training for about five days per year.

IAD also encourages audit staff to obtain professional certification and facilitates this achievement by providing time off and reimbursing fees and costs incurred to attain certain professional audit related certification, e.g., Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA) and Certified Fraud Examiner (CFE).

The IAD Learning and Development Strategy provides further information on the professional development of staff.

3.7 Quality assurance

Quality assurance and improvement plays a fundamental part in ensuring the effectiveness of internal auditing and in assuring stakeholders as to the quality of IAD audits.

IAD has implemented a Quality Assurance and Improvement Programme (QAIP) that covers all aspects of the audit and advisory services provided by the Division. The QAIP is designed to periodically assess and take action to ensure that IAD operates in an efficient and effective manner, and is consistently complying with the IIA Standards, the IIA definition of internal auditing, the Core Principles for the Professional Practice of Internal Auditing and the IIA Code of Ethics through the conduct of periodic and ongoing internal assessments.

PPS coordinates all quality assurance activities outlined in the QAIP. All audit staff in IAD play an important role and have responsibility for implementing the quality assurance activities.

In addition, as required by the IIA Standards, IAD will undergo external quality assessments every five years. These external assessments will be conducted by qualified persons who are independent of IAD and who do not have either a real or an apparent conflict of interest. The results of the external assessments shall be submitted to the IAD Director who will be responsible for implementing the recommendations. OIOS will communicate the results of the QAIP to senior management and governing bodies annually.

The quality assurance and improvement programme can be found on the IAD SharePoint.

4 Relationships with stakeholders

4.1 Introduction

A wide range of stakeholders play an important part in IAD achieving its mandate. IAD staff who are involved in interactions with the stakeholders, whatever the purpose of the interactions, must treat the stakeholders with respect and give due consideration to their point of view. This chapter identifies and describes the relationship of IAD with key stakeholders.

The Section Chiefs and CRAs are responsible for keeping Service Chiefs and the Director advised of significant interactions with senior managers of the United Nations (e.g., heads of entities) and members of the various oversight committees. All relevant interactions should be documented to maintain an institutional memory and, when related to a specific audit, to provide an audit trail of decisions made by IAD staff.

4.2 Key stakeholders

IAD is committed to establishing a professional working relationship with all its stakeholders. Therefore, IAD maintains close and regular contact and open lines of communication with stakeholders to create long-lasting relationships.

4.2.1 Clients

OIOS provides internal auditing, investigation, inspection and evaluation services to all United Nations entities under the Secretary-General's authority and to those entities with which OIOS has signed a memorandum of understanding.

4.2.2 Audit committees

IAD interacts with three audit committees:

IAAC serves in an expert advisory capacity and assists the General Assembly in discharging its oversight responsibilities.

Independent Audit and Oversight Committee of the High Commissioner of the United Nations High Commissioner for Refugees (UNHCR) serves in an expert advisory capacity to assist the High Commissioner and the Executive Committee in exercising their oversight responsibilities within UNHCR.

Audit Committee of the United Nations Joint Staff Pension Fund (UNJSPF) assists the United Nations Joint Staff Pension Board in fulfilling its oversight responsibility relating to UNJSPF.

The roles and responsibilities of the above committees can be found on the IAD content management system.

4.2.3 Fifth Committee

The Fifth Committee is the main committee of the General Assembly entrusted with responsibilities for administration and budgetary matters. The Fifth Committee is assisted by the Advisory Committee on Administrative and Budget Questions (ACABQ).

General Assembly reports, (either mandated by the General Assembly or initiated by OIOS) are formally introduced for discussion by the Under-Secretary-General/OIOS at the relevant session of the Fifth Committee.

More information about the work of the Fifth Committee can be found on their website (UN General Assembly - Fifth Committee - Administrative and Budgetary Questions)

4.2.4 The United Nations Board of Auditors

General Assembly resolution 74 (I) of 7 December 1946 established the United Nations BOA to audit the accounts of the United Nations—the 24 United Nations organizations as well as its funds and programmes—and to report its findings and recommendations to the General Assembly through ACABQ.

More information about the work of BOA can be found on their website (United Nations Board of Auditors).

4.2.5 The Joint Inspection Unit

JIU is an independent external oversight body of the United Nations system, mandated to conduct system-wide evaluations, inspections and investigations.

More information about the work of JIU can be found on their website (Joint Inspection Unit of the United Nations System | (unjiu.org)).

5 Risk assessment and work planning

5.1 Introduction

IAD uses a risk-based approach in developing its three-year rolling audit work plan, which is updated on an annual basis.

The purpose of risk-based work planning is to ensure that IAD assignments are directed at areas where achievement of the United Nations objectives is at higher risk. In identifying risk, IAD has adopted the risk universe and

definitions contained in the United Nations enterprise risk management (ERM) framework as well as the risk management frameworks of UNHCR and UNJSPF. It also consults with management and other relevant stakeholders in developing the work plan and takes their ERM risk registers into consideration.

OIOS assurance strategy aims to cover all high-risk areas over a period of three years, and medium-risk areas over a five-year horizon.

This chapter provides a broad guide on the risk-based work planning steps undertaken each year. IAD issues, to supplement the process, specific guidance and tools before the commencement of the annual risk-based work planning process.

5.2 The work plan development

The main steps in the annual risk assessment and work planning process are shown below.

Figure I Risk assessment and work planning process

5.3 Validating and updating the audit universe

Each year, IAD validates and updates its audit universe, which represents the potential range of all auditable activities and is based on entities for which IAD has the internal oversight responsibility. These are entities within the United Nations but may also be Secretariat departments or even smaller organizational units. Also, clients generally include a range of programmes,

functions, structures and initiatives which collectively contribute to the achievement of the organization's strategic objectives.

Examples of auditable activities include:

- A process or function, e.g., recruitment, procurement, fuel or travel management
- The operations of an organizational unit, programme or subprogramme, e.g., department/office, country office, mission, division or section;
- An information management system such as Umoja or Inspira; and
- A major contract such as travel or fuel;

The Section Chief/CRA is responsible for validating and updating the audit universe through systematic gathering of information. The Service Chief should oversee the process and ensure that new entities and initiatives are included in the audit universe. Information normally available for each client includes, but not limited to mandate and organizational objectives and priorities; details of major initiatives and policy developments; etc.

The Section Chief/CRA is required to maintain, in an organized and accessible manner, all information relevant to the IAD audit universe and those documents used to validate and update the audit universe.

5.4 Identifying strategic and business objectives and related risks

The IAD annual audit work plan is based on the identification and analysis of strategic and business objectives of the audit universe, and risks that threaten the achievement of those objectives. The Section Chief/CRA is responsible for carrying out new risk assessments or updating the existing ones for all assigned clients. Identification of new and emerging risks comes from Service Chiefs/Section Chiefs/Auditors discussions with management, and review of relevant documents. When updating the risk assessment, the Section Chief/CRA is responsible for ensuring any significant changes since the previous year have been taken into account.

Information required to perform/update risk assessments can come from a variety of sources, including:

- Clients' risk registers, where available;
- Security Council and General Assembly resolutions;
- Secretary-General's thematic priorities and strategies (e.g., gender parity, data strategy, disability inclusion);
- Secretary-General's bulletins on organization of departments/offices;
- Clients' strategic plans and frameworks;
- Senior managers' compacts

- Policies, directives and internal management reports;
- Organization charts, budget documents and staffing tables;
- Manuals and operating procedures;
- Historical financial data;
- Client's website, websites containing official documents of the United Nations, press and media releases, other United Nations organizations and government institutions.

Interviews and meetings with management and key staff in client entities can provide useful insight and help auditors to gather relevant information about the entity's mandate, strategic objectives, challenges, processes and information systems involved.

Previous audit, inspection and evaluation reports by OIOS, Joint Inspection Unit and Board of Auditors must be also considered during the risk assessment. Some clients have their own evaluation and/or inspection functions, whose reports should also be obtained and considered in the risk assessment.

The Section Chief/CRA must also consider the potential for the occurrence of fraud and how the client manages fraud risk. The Section Chief/CRA should identify specific fraud schemes and risks and assess their likelihood and significance. Fraud risk assessment addresses the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and illegal acts (including corruption).

All collected information should be stored in an organized and accessible manner by Section Chiefs/CRAs. Interview notes/minutes of the meetings held with clients must be recorded in the audit management system

5.5 Assessing and ranking risks related to auditable activities

The Section Chief/CRA is responsible for identifying a list of auditable activities for their assigned clients, including activities or topics that are highly susceptible to fraud. Once all auditable activities have been identified, the risks associated with these activities are analysed in terms of their likelihood and impact. This process enables IAD to develop a risk score for each identified auditable activity. Auditable activities are then classified by these risk scores into the categories of high, medium or low, taking into account our understanding of existing internal controls and the effectiveness of governance processes.

The results of the risk assessment must be documented in the audit management system. The Annual Risk Assessment and Work Planning

Methodology issued by PPS provides detailed guidance for performing and documenting the risk assessment.

5.6 Identification of audit assignments and resource gap analysis

IAD Director and management team (Service Chiefs and Section Chiefs/CRAs), in coordination with PPS, is responsible for identifying thematic priority areas[1] to be included in the annual work plan based on: (1) areas outlined in the OIOS strategic programme budget and the results-based budgeting framework for the support account for peacekeeping operations; (2) recommendations of legislative and oversight bodies; (3) key organizational priorities of the Secretary-General; (4) outcomes from the Senior Management Group discussions; and (5) emerging cross-cutting risks in the Organization.

For each auditable activity with high and medium risk, the Section Chief/CRA should identify and propose an audit(s) for inclusion in the three-year rolling work plan, taking into account the last time an audit was conducted in that specific area and considering that IAD strategy is to cover higher risk areas over a period of three years, and medium risk areas over five years. Section Chief/CRA should also include an audit(s) from the thematic priority areas, as applicable to their audit universe.

As part of the work planning exercise, IAD examines the staffing resources required to conduct the assignments included within the above assurance strategy and compares them with available posts to identify any gaps that may impact the assurance coverage.

To identify resource gaps, the Section Chief/Service Chief compares available audit staff per type of funding[1] against IAD planned number of assignments for the next three years. The Section Chief/Service Chief also takes into consideration the skills and experience of auditors to determine whether specialist skills are required, and whether they can be sourced in-house or need to be contracted externally. Where the analysis indicates there are insufficient resources available, the Service Chief is responsible for preparing a request for additional resources to the Director. If the Director agrees with the request, the Director proposes these changes to the Under-Secretary-General/Assistant Secretary-General for their approval and appropriate action. This action could involve interactions with client management or submission of a proposal to the relevant body as part of the budget process.

[1] *Thematic areas are cross-cutting high-risk areas to be covered in several standalone assignments in different entities with the aim of identifying systemic issues and good practices across entities.*

5.7 Developing the three-year rolling work plan

The Section Chief/CRA, based on available resources prepares a preliminary list of assignments to be included in their three-year rolling work plan. The Section Chief/CRA submits the proposed assignments to their respective Service Chief.

PPS is responsible for consolidating the work plan and conducting a quality review to ensure that it has been developed in accordance with the guidelines issued. After the quality review, PPS submits the proposed annual work plan to the Director for review and preliminary approval.

The three-year rolling work plan is documented in IAD Work Planning Tool.

5.8 Consultations with BOA and JIU

IAD shares the preliminary work plan with BOA and JIU to ensure there is no duplication of oversight efforts and to enable synergies in forthcoming activities. IAD, BOA and JIU also have periodic meetings and discussions throughout the year to provide update on work plan implementation and sharing of key results.

5.9 Finalising the work plan

The Under-Secretary-General (USG), taking into consideration results of consultations with other oversight bodies, audit committees and client management, reviews and approves the annual work plan.

PPS allocates assignment numbers once the work plan has been approved and schedules the assignments in the IAD audit management system. During the year, the Section Chiefs/CRAs are responsible for scheduling audits and communicating the timing of audits to clients.

5.10 Communication to client

Once the annual workplan is approved by the USG, PPS will prepare letters to all clients (head of entities) informing them of the assignments scheduled for the year. Clients are also advised to inform IAD of issues that may warrant audit attention.

5.11 Submission of work plans to audit committees

IAD submits its work plans to the IAAC and the audit committees of UNJSPF and UNHCR for review and discussion. IAD work plans are normally supported by the IAD budget submissions to the governing bodies as well as details of

any identified resource gaps to gain audit committees' support for additional resources.

5.12 Changes to the work plan

Throughout the year, the Section Chiefs/CRAs may revise the annual work plan because of emerging risks due to changes in operations or the environment. Amendments may also be required to the initially planned timing of the audit due to emerging priorities.

IAD clients may also identify new risks and request an audit or an advisory service that was not included in the work plan. The Section Chiefs/CRAs should consider all requests, and if it is determined that the requested assignment is important compared to the planned audits, it should be discussed with the Service Chief as to whether it should be included.

All changes to the originally approved work plan need to be tracked. For all proposed changes, the Section Chief/CRA should prepare an Amendment to Work Plan Form to be approved by the Service Chief and authorized by the Director.

5.13 Advisory assignments

Advisory and related service activities, the nature and scope of which are normally agreed with the client, are intended to provide value adding suggestions and solutions to improve the efficiency, economy and effectiveness of programmes, projects, operations or activities. Advisory services do not provide an independent assurance on the governance, risk management and control processes to stakeholders.

The Director, together with the Service and Section Chief/CRA should consider requests for advisory services in light of the identifiable risks of the activity involved, existing work plans and available resources, as well as any potential impairment to operational independence.

In conducting advisory assignments, IAD should apply the IIA Attribute and Performance Standards as they relate to consulting engagements. The nature and scope of the advisory engagement are subject to agreement with the client. The focus in advisory engagements will be on the final product and providing the observations and suggested action to client management.

An advisory engagement process includes the planning, fieldwork and reporting phases. However, when IAD provides ad-hoc advice, which may only take a few hours/two to three days, the structured three phases of the audit process may be waived by the Service Chief.

As in audit engagements, the work performed in an advisory engagement (not including ad-hoc advice) should be recorded in the IAD audit management system.

The assigned team leader should develop an appropriate communication strategy for discussion and approval by the Service and Section Chief/CRA, in consultation with the Director.

Since advisory reports are for the sole use of management, the reports are not made public on the OIOS website. Suggestions for improvement made in the report are not recorded in the OIOS recommendations database and are not monitored for implementation. However, IAD follows up on these during the annual risk assessments and as part of related future audit assignments. A summary of advisory activities may be reported in the OIOS Annual Report. For detailed guidance on advisory engagements, please refer to the SOP on Advisory Engagements.

6 Engagement planning

6.1 Introduction

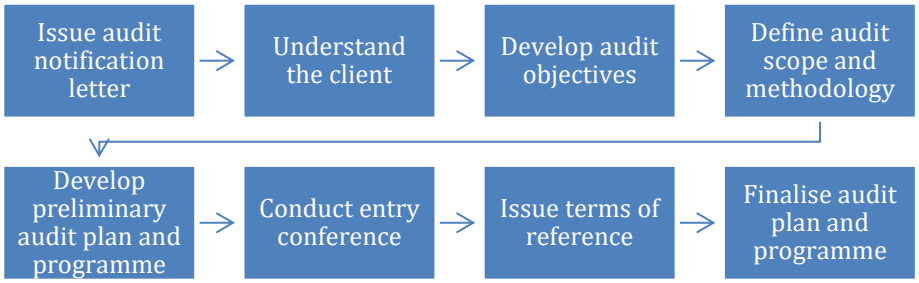
Engagement planning is conducted to: develop an in-depth understanding of the business objectives of the subject to be audited; carry out an activity-level risk assessment to identify the significant risks to achievement of the subject's business objectives; and develop audit tests of controls required to provide reasonable assurance that risks are effectively managed.

The engagement planning phase also involves selecting and providing resources for the audit, notifying the client, collecting preliminary information and conducting preliminary testing as part of the assignment risk assessment, defining the audit objectives, scope, criteria and methodology, conducting the entry conference and preparing and approving an audit plan and programme.

6.2 The engagement planning process

An overview of the engagement planning process is shown below.

Figure II Engagement planning process



6.3 Issuing audit notification memorandum

Each audit engagement is formally opened by the issuance of an audit notification memorandum drafted by the AIC, reviewed by the Section Chief/CRA and signed by the Service Chief.

For detailed guidance, auditors should refer to the SOP on Audit Notification and the relevant template.

6.4 Understanding the client

The AIC is responsible for gathering and analysing information to obtain a good understanding of the audit subject's business objectives, the environment and entity-level controls to ensure that the audit methodology is relevant and efficient. Gathered information should be sufficient to understand the purpose and context of the engagement, as well as the governance, risk management, and controls relevant to the area or process under review. The Section Chief/CRA and in some instances the Service Chief, should outline to the audit team why the audit was included in the plan and what the audit should achieve.

Useful sources of information include:

- Security Council, General Assembly resolutions and documents of other governing bodies;
- Client strategic plans and frameworks;
- Policies, directives and internal management reports;
- Organization charts, budget documents and staffing tables;
- Manuals and operating procedures; and
- Data from Umoja or other ERP systems.

To obtain a thorough understanding of the client's operations and to conduct an objective appraisal of activities and assessment of risks, auditors must also analyse and assimilate the information collected.

6.4.1 Documenting the system

There are many types of information that can be gathered about the audit subject from a variety of sources. To demonstrate that the internal auditor understands the client and the audit subject, adequate documentation should be maintained. This will also facilitate a supervisory review of the working papers.

The most common ways of documenting our understanding of the client's operations are flowcharts (high-level or detailed) and meeting and narrative notes. In deciding on the extent of documentation, the auditor should assess how much documentation is necessary to be able to identify the key controls. At the end of the analysis stage, the auditor should have documented all of the key controls, indicating which ones will be relied upon and which ones (that should be in place) are absent.

Regardless of the methodology used, documenting the process flows helps provide an understanding that is critical to the next steps in engagement planning. The audit team should invest enough time in understanding and documenting the process to enable a solid assessment of process design adequacy.

6.4.2 Conducting activity-level risk assessment

The AIC (and rest of audit team where applicable) after obtaining a good understanding of the audit subject is responsible for conducting an activity-level risk assessment to identify risks that may adversely impact the achievement of the objectives of the audit area. The audit team, under the supervision of the Section Chief, should also brainstorm about fraud scenarios to identify potential fraud risks and assess the identified fraud risks to determine which risks require further evaluation during the engagement. (For more information see Section 7.8 Fraud and Misconduct of this Manual.)

The AIC also needs to gain a good understanding and make a high-level assessment of the adequacy and effectiveness of key controls put in place to manage the identified risks. This may include walk-through exercises and limited test checks. The activity-level risk assessment involves, for example, considering business process risks, understanding the control environment, assessing capacity of client staff and management, and assessing adequacy of guidelines, directives, systems and procedures.

Controls can include both manual and automated controls. Both types of controls need to be assessed to determine whether business risks are effectively managed. In particular, the AIC needs to assess whether there is an appropriate combination of controls, including those related to information

technology, to mitigate business risks within established organizational tolerances.

Table 1 provides an example of an activity-level risk assessment for an audit of procurement activities:

Table 1 Activity-level risk assessment to identify major risks to effective procurement activities (abstract)

Objective of the activity/process	To procure adequate goods and services to allow the entity undertake the tasks necessary to meet the business objectives.		
Risk	Procurement activity may not result in the acquisition of goods and services that are sufficient for the achievement of business objectives.		
Activity-level risk 1	The type, quantity and timing of goods and services necessary to meet the business objectives may not be identified in advance to meet those objectives.		
Key control 1	All sections/units must prepare annual acquisition plans in advance of the need for goods and services. These plans must be aligned with their operational plans.		
Key control 2	Prior to the launch of the solicitation exercise, the requisitioning sections/units must determine minimum requirements (quantity, quality, timing etc.) necessary to meet the performance standards when developing specifications of goods and services to be acquired. These specifications must be documented clearly and unambiguously.		
Key control 3	Proposals from vendors can only be considered if they pass the technical evaluation based on the clearly documented minimum criteria (quantity, quality, timing etc.).		
Assessment for risk 1	Likelihood *Remote*	Impact *High*	Overall risk *Medium risk*
Activity-level risk 2	The entity may not be acquiring the required goods and services at the lowest possible cost.		
Key control 1	Responsible procurement officers must take action to ensure that they have identified all vendors who meet the specified requirement at a competitive price.		

Key control 2	All identified potential vendors must be invited to submit offers to meet the requirement.		
Key control 3	All solicitation announcements should provide sufficient information to allow vendors to make an informed response. Information should include specification, contract requirements, deadlines etc.		
Key control 4	Financial evaluation should take into account all costs associated with offers which meet the requirement specification.		
Assessment for risk 2	Likelihood *Possible*	Impact *High*	Overall risk *Higher risk*

6.4.3 Developing audit criteria

The IIA Standards provide that "Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board."

Audit criteria are reliable, objective, useful and complete standards of performance against which the achievement of control objectives can be assessed. Effective audit criteria are relevant, unambiguous and acceptable.

The AIC should set out in the audit plan the criteria to be used, which should normally be agreed upon with the client management. For detailed guidance on audit criteria, auditors should refer to the Practice Guide on Control Analysis.

6.5 Developing audit objectives

The purpose of the internal audit activity is to evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach.

The audit objectives should articulate specifically what the engagement is trying to accomplish. The audit objectives could include one, or more of the following:

- Achievement of the entity's strategic objectives;
- Reliability and integrity of financial and operational information;

- Effectiveness and efficiency of operations and programmes;
- Safeguarding of assets; and
- Compliance with mandates, regulations, policies, procedures and contracts.

The AIC is responsible for developing the audit objectives to address the risks associated with the activity under review. When developing engagement objectives, the AIC and Section Chief must consider the probability of significant errors, fraud, noncompliance, and other exposures.

6.6 Defining audit scope and methodology

The audit scope is determined after the audit objectives have been established and sets the boundaries of the audit. Audit scope should include the time period, geographical locations and major processes that will be covered by the audit. The scope needs to clearly define what is included in the audit, and what is not included if there are areas that would reasonably be expected to be within the audit scope but are excluded.

Methodology is a general statement describing the types of activities that will be undertaken in conducting the audit. Generally, these will involve interviews, analytical reviews and tests of controls but in some cases specific activities will be indicated such as surveys, consultation with subject-matter experts, or benchmarking.

6.7 Developing preliminary audit plan and programme

The AIC, assisted by the audit team, must develop and document a plan for each engagement. The audit plan summarizes the background information collected on the client's business, including key financial and operational data, and analyses the risks that threaten the client's business objectives in the activity to be audited. The audit plan outlines the objectives, scope, criteria and methodology to be adopted. It also indicates the timing and resource allocations.

The Section Chief/CRA and AIC must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints and available resources. Timing and resources should include estimates of the audit team's effort as well as target dates for the end of planning, fieldwork, reporting and the closure phases of the audit.

The AIC should develop an audit programme outlining the detailed procedures for collecting, analysing, interpreting and documenting information during the fieldwork. The auditor must design tests to assess whether existing controls are sufficient to mitigate the identified risks. Collectively, the procedures

should enable the auditor to reach a conclusion on each audit objective. The audit programme should be prepared directly in the IAD audit management system and should:

- Outline the audit criteria and the steps that will be undertaken to draw conclusions on each criterion;
- Identify technical requirements, objectives, risks, processes and transactions that are to be examined;
- State the nature and extent of testing required; and
- Document the procedures to be used for collecting, analysing and interpreting information during the audit.

6.8 Conducting the entry conference

A formal entry conference with the client should take place normally no more than one month after the Notification Memorandum has been issued.

The AIC, in conjunction with the Section Chief/CRA, arranges and attends entry meetings with the management responsible for the activity under review. The Service Chief should attend the entry conference, where feasible. The audit team should summarize the discussions and any conclusions reached from the meetings and document them in the IAD audit management system.

An agenda and an entry conference briefing paper, including a PowerPoint presentation if applicable, should be sent to the client ahead of the scheduled date of the conference. The main content of the briefing paper/PowerPoint presentation includes background to the selection of the audit area; risk assessment and status of previous audit recommendations; preliminary audit objectives and scope; audit methodology and criteria; planned timing, milestones and deliverables of the different audit phases.

6.9 Issuing the terms of reference

Shortly after the entry conference (no longer than 3 weeks), the AIC should prepare terms of reference (TOR) for the audit. The purpose of this document is to provide client management with an accurate picture of what the audit will cover. The TOR is based on the audit plan and the information from the entry conference. It represents a commitment by IAD to provide the specified audit to the client management. The sources from which the audit criteria will be drawn should also be indicated in the annex to the TOR.

The TOR will be reviewed by the Section Chief/CRA and approved and signed by the Service Chief for transmittal to the client. The TOR should not be amended without the Section Chief/AIC communicating the changes to the client management beforehand.

In drafting the TOR, the auditor should refer to the SOP on Audit Terms of Reference and the TOR template.

6.10 Finalising the audit plan and programme

After the entry conference, and issuance of the TOR, the AIC should be ready to finalize the audit plan and programme, incorporating the comments and concerns expressed by the client and the agreed criteria. The final plan and programme should be reviewed by the Section Chief and approved by the Service Chief.

7 Performing the engagement

7.1 Introduction

Audit fieldwork involves executing the audit plan and audit programme in accordance with the IIA Standards and this Manual. Activities central to the fieldwork phase include: collecting and analysing information, documenting the system, audit testing, developing conclusions and recommendations, discussing issues with the client, and documenting evidence. The fieldwork phase ends with the holding of the exit conference.

7.2 Audit testing

Auditors must base conclusions and engagement results on appropriate analyses and evaluations. Where the system or activity under review has few transactions or processes, or where the processing of data is fully automated, it may be possible to test the operation of controls for the entire population (using suitable data analysis tool such as IDEA).

Auditors must gather sufficient, reliable, and relevant audit evidence to reach conclusions regarding the achievement of audit objectives. The methods of gathering audit evidence include: observations, interviews, re-performance, analytical procedures, vouching, inspection, walk-throughs, surveys and questionnaires.

7.2.1 Testing key controls and the absence of key controls

Aside from testing the controls that do exist, the auditor should assess whether the absence of controls has affected the achievement of objectives. Auditors sometimes omit this second type of test, reporting just the risk of something going wrong because controls are absent, rather than going the extra step and identifying what has gone wrong in the absence of the controls. The auditor must prepare two test plans: one to test the consistent operation of the identified key controls and their effectiveness, and another to determine the

impact of (any) absent key controls. The Practice Guide on Audit Testing, Sampling and Audit Test Documentation provides more guidance on this subject.

7.2.2 Audit sampling

Where testing the whole population is not feasible, the auditor must review a sample of the population. IIA Practice Advisory 2320-3 defines audit sampling as "the application of audit procedures to less than 100 per cent of items within a class of transactions or account balance such that all sampling units have a chance of selection". Population is defined as the entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions.

Audit sampling can use either a statistical or a non-statistical approach. Statistical sampling involves determining the sample size objectively, selecting the samples from the population randomly and evaluating the sample results mathematically to draw conclusion about the population. Statistical sampling approach must be used if the auditor wishes to extrapolate sample results to draw conclusion about the entire population. On the other hand, non-statistical sampling approach relies solely on the auditor's professional judgment, and the auditor uses his or her own experience and knowledge to determine the sample size and the method for selecting the samples from the population. Non-statistical sampling (e.g. judgmental samples) may not be objective and the results of such sampling normally pertain only to the sampled items, and cannot be mathematically extrapolated over the population.

Effective audit sampling procedures increase the coverage, focus, and efficiency of audits and statistical sampling allow the auditor to provide assurance on processes that impact the Organization's achievement of its goals and objectives. The Practice Guide on Audit testing, sampling and audit test documentation provides more detailed guidance on audit sampling and evaluating the results of a sample.

7.2.3 Analytical procedures

Internal auditors may use analytical procedures to obtain audit evidence. Analytical procedures involve studying and comparing relationships among both financial and non-financial information. The application of analytical procedures is based on the premise that, in the absence of known conditions to the contrary, relationships among information may reasonably be expected to exist and continue. Examples of contrary conditions include unusual or non-recurring transactions or events; accounting, organizational, operational, environmental and technological changes; inefficiencies; ineffectiveness; errors; fraud; or illegal acts.

Analytical procedures often provide the auditor with an efficient and effective means of obtaining evidence. The assessment results from comparing information with expectations identified or developed by the auditor.

When analytical audit procedures identify unexpected results or relationships, the auditor evaluates such results or relationships. This evaluation includes determining whether the difference from expectations could be a result of fraud, error, or a change in conditions. The auditor should ask client management about the reasons for the difference and obtain corroborating evidence. Unexplained results or relationships from applying analytical procedures may be indicative of a significant problem (e.g., a potential error, fraud, or illegal act). If the results indicate the possibility of a fraud or misconduct, this should be brought to the immediate attention of the Section Chief/CRA, as explained in Section 7.8 Fraud and Misconduct of this Manual.

7.2.4 Root cause analysis

Root cause analysis is defined as the identification of why an issue occurred (versus only identifying or reporting on the issue itself). In this context, an issue is defined as a problem, error, instance of non-compliance, or missed opportunity. Examples of audit issues include: ineffective operations, misuse of resources, inadequate safeguarding of assets and exceeding the delegated authority.

Root cause analysis benefits the organization by identifying the underlying cause(s) of an issue. This approach provides a long-term perspective for the improvement of business processes. Without the performance of an effective root cause analysis and the appropriate remediation activities, an issue may have a higher probability to reoccur. It is important to recognize that there are often multiple related or unrelated causes of an issue.

There are a range of techniques that can be used for root cause analysis. In certain circumstances, root cause analysis may be as simple as asking "five whys." For example:

> The Procurement Division received a limited number of responses to a solicitation exercise.
>
> - *Why?* Limited number of vendors was invited to participate in the solicitation.
> - *Why?* Only few new vendors were added to the vendor roster in the recent period.
> - *Why?* Vendor registration process was lengthy and cumbersome.

- *Why?* Management did not establish targets and timelines for the vendor registration process and did not monitor the process against these timelines.

By the fifth "why," the auditor should have identified or be close to identifying the true root cause. More complex issues, however, may require a greater investment of resources and more rigorous analysis. The resources spent on root cause analysis should be commensurate with the impact of the issue or potential future issues and risks. Auditors may not have all the skill sets necessary to conduct the specific root cause analysis under consideration. When the anticipated time commitment or necessary skill levels exceed what is available within the internal audit activity, the AIC should develop recommendations that address the underlying issue and, as appropriate, include a recommendation for management to conduct a root cause analysis.

7.3 Recording information during the audit

IAD uses an electronic audit management system to record all elements of the engagement, including the results of planning and other meetings with client management or staff, risk assessment procedures, the audit work plan and audit programme, test results and all relevant information to support the conclusions and engagement results, and recommendations.

Auditors should develop working papers as the audit progresses. The contents of the file should clearly support the bases of the observations and recommendations to be reported to the client and provide evidence that the audit was performed in accordance with the IIA Standards and this Manual. The working papers should also explain why any deviation was made from the audit programme. The audit working papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The working papers should include a description of the source of the population, the sampling method used and sampling parameters, items selected, and details of audit tests performed and conclusions reached.

Only sufficient, reliable, relevant and useful information shall be collected and stored, to support the engagement results and conclusions. It is the responsibility of the auditors and their supervisors to ensure that the attached working papers meet the above criteria. Any document filed in the IAD audit management system carries the implicit understanding that it has been read fully by at least one member of the audit team. Auditors should be careful not to include anything in the working paper file for an assignment that they have not read and considered in full. If a document that is included in the working paper file has not been read, and it contains information that would have

affected the direction or result of the audit had the audit team been aware of it, the credibility of IAD may be affected significantly.

Where documents are readily available electronically on the Organization's intranet, for example manuals and administrative instructions, only a link to the document need be included in the audit working papers. If only a small part of a document is relevant, then only that part should be extracted and saved in the working papers.

For further guidance on recording information during the audit, please refer to the Teammate Protocol.

7.4 Evaluating the results of audit testing

The auditor evaluates the results of audit testing to determine whether:

- The objectives of key controls have or have not been met;
- The criteria have or have not been satisfied; and
- The risks are adequately managed.

Control analysis must be done with the overall objective in mind to produce a report incorporating the following elements in relation to each audit criteria:

- Criteria: The "what should be". The standard used to assess compliance, efficiency, effectiveness, etc.;
- Condition: The "what is". What the audit activities identified in relation to the criteria; and
- Conclusion: The auditor's assessment that the criterion has been met, or that there is a gap between the criterion and the condition.

For those criteria that the auditor concludes as not met, the following elements are also required:

- Cause: The "why?". The reason why there is a gap between the criterion and the condition;
- Consequence: The "so what?". The actual or potential negative impact of the criterion not being met; and
- Corrective action: The "recommendation". The action OIOS is suggesting to alleviate the condition so that the criterion and condition are in alignment.

7.5 Supervising the audit

Each phase of the audit is supervised by, as appropriate and necessary, the AIC, the Section Chief/CRA, the Service Chief and the Director, who are required to provide guidance, based on the competency and experience of the auditors.

Supervisors should review the working paper as soon as possible after it is completed. The review of working papers entails ensuring that:

- The approved engagement programme is carried out unless changes are both justified and authorized;
- Engagement working papers adequately support the engagement observations, conclusions and recommendations;
- Engagement communications are accurate, objective, clear, concise, constructive and timely; and
- Engagement objectives are met.

All available working papers must be completed and reviewed by, as appropriate, the AIC and the Section Chief/CRA prior to submitting the detailed audit results to the Director for review.

All issues/comments raised in the review of working papers must be resolved before engagement results are communicated to the client.

Managing the audit includes managing the schedule and the resources used to complete the audit. The Section Chief/CRA and the AIC are responsible for ensuring that the deadlines set out in the audit plan are met as much as possible and that the budget for the total number of days for the audit is not exceeded. Supervisors are also responsible for ensuring that auditors complete their time sheets in the audit management system in a timely manner.

7.6 Staff appraisals

Senior members of the audit team train and develop staff, and evaluate their performance. Staff appraisals should be conducted at the end of each assignment for all members of the audit team who spent five days or more on the audit. Their purpose is to assess the performance of the audit team member while this is still fresh in the minds of the appraiser. Such appraisals should be used to provide input into the annual performance document, and enable the first reporting officer to base his/her evaluation of the staff on performance throughout the year rather than on the best or worst assignment. The appraisal also gives more immediate feedback to the team member.

Staff appraisals may be completed using the established Audit Staff Appraisal Report (ASAR) form.

7.7 Communicating with IAD management during fieldwork

The Section Chief/CRA should routinely brief the Service Chief of the progress made in performing the engagement and of any problems related to it. Where deadlines are not likely to be met or the budget is to be exceeded, the AIC

should advise IAD management in advance and explain why the targets will not be met. The Service Chief provides the guidance necessary to resolve any issues being faced by the audit team.

The Service Chief is also responsible for bringing to the attention of the Director significant delays and challenges being faced by audit teams to take action, where necessary.

7.8 Fraud and misconduct

The auditor should determine the probability and impact of typical fraud schemes and scenarios as well as the adequacy of preventive and detective controls when performing the activity-level risk assessment. The audit team should also design and perform audit procedures to test the effectiveness of relevant controls. When the circumstances warrant, the audit team should design and conduct effective procedures to detect red flags of potential fraud. The performance of such procedures and the conclusions reached should be documented in the working papers.

If at any time during the audit, it becomes apparent to any member of the audit team that fraud or misconduct may have actually occurred, it should be brought to the immediate attention of the AIC and Section Chief/CRA. They will review the matter and should inform the Service Chief of the issue, if necessary. The Service Chief will determine whether the issue needs to be further escalated to the Director for a decision on whether to refer it to the Investigations Division. The Service Chief or Director may also decide to bring the issue formally to the attention of the client in the form of an interim written communication and/or expand the scope of the audit.

PPS maintains IAD's central repository of referrals to the Investigation Division, and therefore, needs to be copied on all formal correspondence.

8 Communicating results

8.1 Introduction

IAD is responsible for communicating its audit results, conclusions and recommendations. Communicating results is an integral part of the audit assignment, with results communicated verbally and in writing during the audit, and more formally through written communications that are prepared by the audit team and reviewed by IAD management prior to issuance to the client. For a more in-depth discussion of report writing, please refer to the Practice Guide on Drafting Audit Reports.

8.2 Communications during the engagement

Throughout the audit, the audit team is expected to be in regular contact with the operational managers and staff of the activity being audited to: (a) collect necessary information; (b) conduct audit tests and discuss any related issues as the audit progresses; and (c) share audit results and proposed recommendations. Issues arising and discussed in these meetings should be documented in the audit working papers. Audit teams should keep the concerned audit focal point informed about the progress of the audit and seek appropriate assistance as needed.

8.3 Exit conference

As soon as possible after completion of the fieldwork, the AIC will organize an exit conference to advise the client of the engagement observations and overall audit results. It serves several important purposes:

- Informs the client of the audit results and whether the criteria have been met;
- Reaches agreement on findings and recommendations;
- Communicates planned or corrective actions taken to address deficiencies disclosed by the audit; and
- Advises the client of the reporting process.

To facilitate discussion at the exit conference and as a matter of courtesy, the audit team should give client management a full brief of the issues and conclusions. This brief may be in the form of the (Detailed Audit Results) discussed in section 8.5. Where the issues are complex, it may be worthwhile to prepare a presentation to be used to guide the exit conference discussion.

Similar meetings may be held at the physical locations where the fieldwork has been conducted, to apprise local management of the results of the audit work in that location. This should be followed by a formal exit conference with the client management with overall responsibility for the activity within the scope of the audit[2]. For audits that are sensitive, complex or high profile, or if the client is located in New York (or Geneva for UNHCR), the Service Chief and Director, may attend the exit conference if deemed necessary. The Section Chief/CRA should attend the exit conference at her or his location.

The AIC or a designated team member should take note of the points discussed and comments made during the exit conference and incorporate them in the audit working papers. A formal exit conference concludes the audit fieldwork.

[2] *This is the meeting which will be regarded as the "Exit conference" for milestone reporting purposes.*

8.4 Engagement reporting

To formally communicate audit engagement results to programme managers/heads of departments, offices or missions, IAD issues the following:

- Detailed Audit Results (DAR);
- Draft Report; and
- Final Report.

For advisory, engagements, IAD issues a Draft Advisory Report and a Final Advisory Report.

IAD uses standard templates for each type of audit and advisory communication. Client is given the opportunity to comment before the report is finalized. These steps are discussed in more detail below.

8.5 Detailed audit results

IAD uses DAR to communicate engagement observations to programme managers at the operational level. The AIC is responsible for preparing DAR, which is a detailed document that combines both positive results and deficiencies in controls, including the cause and impact of reported deficiencies.

The transmittal memorandum should contain a caption summarizing the overall conclusion on the assignment. The caption is a short, succinct sentence which encapsulates and conveys to readers the broad message emerging from the report. This message should address the audit objective. The memorandum should request the client to respond to the DAR within 15 calendar days from issuance date, providing comments on the factual accuracy of the report and their acceptance of the recommendations.

The body of DAR includes the following elements:

- Summary description of the background;
- The objective, scope and methodology of the audit, and the rationale for conducting it;
- The overall conclusion section, (which in one paragraph, should include an overall summary of the audit results, including positive assessments, if any and significant);
- Detailed discussion of the audit results; and
- Recommendations for addressing issues identified (also itemized in an annex to DAR)

For each audit result discussed in DAR, the auditor must have actively considered elements of the audit logic process:

- Criteria: The standards, measures, or expectations used in making an evaluation and/or verification (the correct state);
- Condition: The factual evidence that the internal auditor found in the course of the examination (the current state);
- Cause: The reason for the difference between the expected and actual conditions;
- Consequence: The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the differences); and
- Corrective action: The recommended action the auditor is suggesting to address the root cause of the condition. It should stand-alone, be specific, clear and concise, action-oriented, and doable.

There are three types of recommended actions:

- **Critical recommendations** address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization;
- **Important recommendations** address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization; and
- **Opportunities for improvement** do not meet the criteria for either critical or important recommendations but rather present suggestions for enhancements in governance, risk management or internal control processes. These suggestions address deficiencies that are unlikely to prevent the achievement of control or business objectives, but which would initiate improvements in governance, risk management or internal control processes that could result in improved efficiency or effectiveness. Implementation of these opportunities for improvement is at the discretion of client management.

Critical and important recommendations are included in the same annex; while opportunities for improvement for discretional implementation by management are included in a separate annex.

The Service Chief reviews and issues DAR to the client for comment. If DAR contains critical recommendations or pervasive deficiencies, it needs to be reviewed by the Director, or in the absence of the Director, by the Deputy Director. The USG should also be informed of such critical recommendations or pervasive deficiencies.

The Practice Guide on Drafting Audit Reports provide more detailed guidance on preparing DAR.

8.6 The draft audit report

Auditors are expected to produce finished-quality writing for review. The draft report, in addition to the elements of DAR, includes an executive summary. The executive summary is a brief synopsis of the audit report, and it should concisely capture the audit results, conclusions and recommendations. Any positive observations should also be presented to give a balanced view of the audit results. The executive summary replaces the overall conclusion section included in DAR and should not exceed one page.

The draft audit report is addressed to the client's head of entity. The transmittal memorandum should request a response within 15 calendar days, including action plans to address recommendations, along with target dates and the title of the official responsible for implementation, and rationale for accepting the risk associated with unaccepted recommendations. The transmittal memorandum should advise the head of entity that their full response to the draft report will be appended to the final report. It should also indicate that unaccepted critical recommendations will be escalated as necessary up to the level of the Secretary-General for reconsideration.

In the body of the draft report, the response from the client should be treated as follows:

- If a recommendation is accepted and being/will be implemented, state that the recommendation remains open pending the required action is taken;
- If recommendation is accepted but OIOS does not agree with the proposed action plan to address the situation satisfactorily, provide OIOS rebuttal statement and reiterate the recommendation and requests that the client develop a satisfactory action plan to implement the recommendation; and
- If the client does not agree with the audit results or recommendation(s) in DAR, the AIC should reconsider whether the result or recommendation is still valid or whether it needs to be amended:

  -If IAD considers that the result or recommendation is still valid (i.e., disagrees with the client), IAD should clearly state its position and rebut the client's arguments; and

-If the client provides adequate evidence and justification, IAD should amend or remove the corresponding result and recommendation.

Client comments to individual recommendations should be summarized as succinctly as possible without omitting any important or relevant details and shown in italics.

The draft report does not include opportunities for improvement; however, the issues could still be reported in the narrative of the relevant sections, as appropriate.

Both the Director and the Service Chief review the draft audit reports. When the Director (or the Deputy Director in the absence of the Director) is satisfied with the quality and contents of the report, s/he will transmit the draft report to the USG for review and approval for issuance. The template "USG Review Form – Draft Report" should be used.

The Practice Guide on Drafting Audit Reports, provide more detailed guidance on preparing draft audit reports.

8.7 The final audit report

The final audit report should incorporate the comments that were provided by the client to the draft report. General Assembly resolution 64/263 requires that the verbatim, unaltered management response be included in the final report as an appendix.

The content of the final report is similar to that of the draft report. Comments received from the client on the draft report should also be treated similarly in the final report.

In case the client does not provide a target date for implementing an accepted recommendation, the Section Chief/AIC should establish a target date using the following criteria:

- **Critical recommendations:** the target date should be the last day of the quarter following the final report date (e.g., final report date is 2 February 2023, the target date would be 30 June 2023).
- **Important recommendations:** the target date should be the last day of the 12-month cycle following the final report date (e.g. final report date is 12 January 2023, the target date would be 28 February 2023).
- **Recommendations indicated as implemented by the client but no supporting evidence provided:** since the client indicates that the recommendation is already implemented, it should not take too long to

provide the evidence of implementation, and therefore, the last day of the quarter following the final report date will be the target date.

If a critical recommendation is not accepted, the Service Chief, in consultation with the IAD Director, should inform the Office of the USG OUSG about the recommendation, including (a) the background of the recommendation and its associated risks; (b) client rationale for the non-acceptance; (c) OIOS rebuttal and rationale for maintaining the recommendation; and (d) any recommendation on action to be taken by EOSG. Upon the approval of the USG, the Service Chief should inform the head of the concerned entity about the intention of OIOS to:

- Escalate the unaccepted critical recommendation to the Secretary-General through the Chef de Cabinet (CdC); and
- Finalize the relevant IAD report.

OUSG will escalate the unaccepted critical recommendation to the Secretary-Genaral through CdC. The SOP on Audit Recommendations provides more detailed guidance on unaccepted recommendations.

Both the Director and the Service Chief review the final audit report. Before a final report is submitted to the Director for approval, all working papers in the audit management system should be reviewed and signed off. When the Director (or the Deputy Director in the absence of the Director) is satisfied with the quality and contents of the report, s/he will transmit the final report to the USG for review and approval for issuance. The template "USG Review Form – Final Report" should be used.

The Practice Guide on Drafting Audit Report provide more detailed guidance on preparing final audit reports.

8.8 The draft advisory report

The draft advisory report includes an executive summary which should concisely capture the advisory results, conclusions and suggestions for improvement. The executive summary should not exceed one page and should include positive observations to give a balanced view of the advisory results.

The draft advisory report is addressed to the client's head of entity. The transmittal memorandum to the head of entity should request a response within 15 calendar days. The transmittal memorandum should advise the head of entity that the final advisory report will be for the sole use of management and will not be made public on the OIOS website. It should also indicate that suggestions for improvement made in the report will not be included in the OIOS recommendations database for follow up. However, OIOS may consider

any good practices and areas for improvement identified in the report as part of its future engagements.

Both the Director and the Service Chief review the draft advisory reports. When the Director (or the Deputy Director in the absence of the Director) is satisfied with the quality and contents of the report, s/he will transmit the draft advisory report to the USG for review and approval for issuance. The template "USG Review Form – Draft Report" should be used.

8.9 The final advisory report

The content of the final advisory report is similar to that of the draft advisory report and should incorporate the comments that were provided by the client to the draft advisory report.

Both the Director and the Service Chief review the final advisory report. Before a final report is submitted to the Director for approval, all working papers in the audit management system should be reviewed and signed off. When the Director (or the Deputy Director in the absence of the Director) is satisfied with the quality and contents of the report, s/he will transmit the final report to the USG for review and approval for issuance. The template "USG Review Form – Final Report" should be used.

8.10 Use of personally identifiable information in audit reports

To address concerns relating to the protection of personally identifiable information, draft and final audit reports should not contain names of third parties, including individuals and corporate or other entities (suppliers, vendors, staff members, implementing partners, etc.). This practice is important as OIOS reports are publicly available, and the identity of parties mentioned should be kept confidential to avoid any potential reputation damage. There is also an element of natural justice as the third party had not been provide an opportunity to respond to the comments made.

8.11 Reporting to the General Assembly, audit committees and senior management

Audit results are communicated to the General Assembly on an annual basis in the OIOS annual reports. The report on the non-peacekeeping activities of OIOS covers the 12-month period from 1 July to 30 June of each year. This report is submitted to the General Assembly during its main session. Oversight results pertaining to peacekeeping operations and special political missions cover the 12-month period from 1 January to 31 December of each year and

are submitted to the General Assembly during the resumed session. The annual reports are also submitted to the IAAC.

OIOS shares audit results with the audit committees.

OIOS also reports to the senior management on the implementation of recommendations issued to programme managers – quarterly for overdue critical recommendations and biannually for all outstanding recommendations.

The SOP on Audit Recommendations provides more guidance on updating and reporting the implementation status of recommendations.

8.12 Publication of audit reports

General Assembly resolution 69/253 requires OIOS to publish all final audit reports on the OIOS public website, except for reports containing confidential or sensitive information, which the USG/OIOS may decide to withhold or redact. Where elements of a report are considered sensitive, the responsible IAD Administrative Assistant shall redact final reports in accordance with approvals provided by the USG based on the suggestions from the concerned Service Chief.

The OUSG shall post on the OIOS website the titles of final audit reports on the day when the reports are issued to clients to provide senior management and the representatives of Member States the privilege of requesting access prior to public release. The full reports are available on the website 30 days after issuance.

Any queries received by OIOS staff, for example from the media or the general public, relating to audit reports posted on the OIOS website, should be referred to the OUSG.

Staff should review the OIOS Policy Directives on Information Handling and Access (Directive No. 2021/03), and Classification, Protection and Disclosure of OIOS Work Product (Directive No. 2021/04) and SOP on Public Disclosure of Audit Reports to gain a fuller understanding of the requirements for report publication.

8.13 Ownership and retention of working papers

According to paragraph 3 of ST/SGB/2007/5 on Record-keeping and the Management of United Nations Archives:

> *"All records, including electronic records and e-mail records, created or received by a staff member in connection with or as a result of the official work of the United Nations, are the property of the United Nations."*

Consequently, all working papers produced by IAD are owned by the Organization. Nonetheless, access to IAD working papers shall be restricted to authorized IAD staff members at all times. Requests for access to assignment working papers by management and officials of the Organization including other OIOS Divisions, the BOA or JIU shall be granted only after the approval of the IAD Director. Any requests from parties outside the Organization may be granted after the approval of the IAD Director, USG/OIOS and/or the Office of Legal Affairs.

IAD management and staff must respect the confidentiality of information acquired during the audit and not disclose information without appropriate authority, unless there is a legal or professional obligation to do so.

All IAD working papers, including electronic records in the IAD audit management system shall be retained in accordance with the OIOS-IAD Records Retention Schedule.

Staff should review the OIOS Policy Directives on Information Handling and Access (Directive No. 2021/03), and Classification, Protection and Disclosure of OIOS Work Product (Directive No. 2021/04) and SOP on Data Privacy and Data Protection in IAD to gain a fuller understanding of the requirements for report publication.

9 Recommendation monitoring and follow-up

9.1 Introduction

Recommendation monitoring consists of recording recommendations in the recommendations monitoring database, following up with the client's management on the status of their implementation and resolving long-outstanding audit recommendations.

9.2 Recording recommendations

OIOS maintains all recommendations issued in the automated audit management system. In addition to holding the text of the recommendation and other administrative information, the database includes details of the impact, rating, risk, cause, related United Nations cross-cutting principle, and financial implication of the recommendation. This information enables OIOS to analyse recommendations according to any of these factors and monitor the status of their implementation.

Where more than one office is involved in the implementation, the recommendation should specify the lead office.

After the audit report has been finalized, the AIC must record all critical and important recommendations in the audit management system within two business days of issuing the final audit report. PPS conducts quality checks for each assignment to ensure all the recommendations are recorded and released to the issue tracking in a complete and accurate manner.

For further guidance on recording recommendations, please refer to the SOP on Audit Recommendations.

9.3 Following up on and closing recommendations

Implementation of overdue critical recommendations is monitored on a quarterly basis. Implementation of all outstanding recommendations is monitored biannually. The database may also be updated at any time for any known and validated information regarding the status of the recommendation.

The AIC is responsible for reviewing client's progress updates and making the final determination as to the status of the recommendation (i.e. whether the recommendation is still in progress, or should be closed as implemented etc.). The AIC will document the final status of the recommendation in the audit management system. If the AIC has left the Section, then the Section Chief assumes this responsibility.

To determine whether a recommendation should be closed, auditors must review the evidence provided by the client, assess its credibility, and establish whether the action taken is valid and sustainable.

Long overdue recommendations (defined as overdue for more than 1 year past the target date), shall be reviewed for potential closure, unless reasonable action plans for full implementation are provided. The original target dates for implementation (as provided when finalizing the report) shall remain unchanged. Those recommendations that are "closed without implementation" will be reported in OIOS Quarterly Activities Report and Annual Reports.

For further guidance on following up on and closing recommendations, please refer to the SOP on Audit Recommendations.

ANNEX I

Practice Guides

No.	Name
1.	Project and Working Papers Management Protocol for TeamMate+ Users
2.	Time Tracking in TeamMate+
3.	Audit Testing, Sampling and Audit Test Documentation
4.	Control Analysis
5.	Performance Auditing
6.	Drafting Audit Reports
7.	IAD Annual Risk Assessment and Work Planning Methodology
8.	Fraud Risk Assessment and Audit Procedures
9.	Delegation of Authority
10.	A Toolkit for Auditing Strategic Management and Governance
11.	Using Interviews Effectively in Audits
12.	Using Surveys Effectively in Audits
13.	Guidelines for Maintaining Operational Independence during the Conduct of OIOS Duties
14.	Assessing Organizational Culture
15.	Guide to Auditing Gender Equality

Standard Operating Procedures

No.	Name
1.	Use of acronyms in audit reports
2.	Public disclosure of audit reports
3.	Audit recommendations
4.	Audit notifications
5.	Terms of reference
6.	Key performance indicators
7.	Advisory engagements
8.	Data privacy and data protection in IAD
9.	Referral of fraud red flags to Investigations Division
10.	IAD Remote Auditing Approach

Forms and Templates

No.	Name
1.	Statement of independence and confidentiality
2.	Amendment to work plan form (AWPF)
3.	Audit notification memorandum
4.	Terms of reference (TOR)
5.	Entry conference agenda
6.	Entry conference notes
7.	Audit plan
8.	Audit programme
9.	Exit conference notes
10.	Audit report clearance check sheet
11.	USG review forms (Draft report/Final report)
12.	USG final report disclosure review form
13.	Detailed audit results
14.	Draft audit report
15.	Final audit report
16.	Audit closing memorandum
17.	Audit staff appraisal report (ASAR)
18.	QAIP: Checklist for TM+ fields and working papers
19.	Referral of potential fraud cases to Investigations Division