BENAZIR INCOME SUPPORT PROGRAMME
GOVERNMENT OF PAKISTAN

INTERNAL AUDIT MANUAL

PART - ONE

The document has been produced with the assistance of Asian Development Bank

This document – Internal Control Manual – is produced by the Internal Audit Wing of Benazir Income Support Programme, with the assistance of the Asian Development Bank. The document does not constitute a formal communication and does not necessarily represent the official position of the Asian Development Bank. With the aim of improvement of the financial management and control system, this Manual will be the subject of continuous review and will be updated by the Internal Audit Wing of the Benazir Income Support Programme.

PART ONE: INTERNAL AUDIT STANDARDS, POLICIES AND PLANNING

TABLE OF CONTENTS

FOREWORD

The quality of Internal Audit performance in BISP depends on the application of the rules and methods presented in this Manual, as well as your full involvement as a professional. Professionalism depends significantly on the objectivity of your views and judgment, the quality of the thought processes in applying Audit Standards and the impact and practicality of your recommendations.

The manual is based on the internationally accepted standards developed and adopted by the Institute of Internal Auditors. To help you in your day-to-day work the relevant standard is shown, where appropriate, at the start of each main section of the manual.

Internal Audit does not play an inspectorial role. It needs the co-operation of staff and officers in order to obtain sufficient genuine information to carry out its duties. The best way to foster an atmosphere of mutual trust and co-operation is for Internal Audit to adopt a participative approach, be transparent in its work and objectives and to maintain professional relationships at all times.

It is essential therefore that the requirements of this Manual are complied with to ensure a consistently high standard of internal audit to be delivered. However, auditing is an art rather than a science and the manual is not intended to mechanise the audit process. Professional judgment remains an essential feature in applying many areas of our approach.

PURPOSE AND STRUCTURE OF THE MANUAL

Purpose

This Manual is intended for the use of staff employed in Internal Audit Wing in BISP.

Its purpose is to act as a common reference point for Internal Auditors, to assist in a common understanding of the principles of modern auditing techniques and terminology, and to assist them in carrying out their work.

The procedures and methodologies contained in the Manual comply with the International Standards for the Professional Practice of Internal Audit as set out by the international Institute of Internal Auditors (IIA), (October 2012). They have been adapted to make them relevant to the situation in the Benazir Income Support Programme, Pakistan.

To ensure that both the methodology and the procedures remain consistent with best practice and reflect changes in both the legal and audit environment, the Auditor General of Pakistan is responsible for reviewing, and where necessary amending, the contents of the methodology and procedures. This review will be done annually or more frequently if needed.

It is internal audit wing's responsibility to ensure that all amendments to the methodology and procedures are understood and incorporated into the Manual.

Structure

The Manual comprises two parts:

- Part 1 – Internal Audit Standards, Policies and Planning which contains guidance on the key policy matters that affect the management and the work of IA wing.
- Part 2 – Performing an Audit which explains the steps that have to be followed when carrying out an audit. It also provides guidance on report writing.

Auditors are expected to apply the guidance and, where appropriate, the approaches and techniques set out in the Manual.

1. INTRODUCTION TO INTERNAL AUDIT IN THE PUBLIC SECTOR IN PAKISTAN

The purpose of internal audit

The Institute of Internal Auditors defines Internal Audit as follows:

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.

Audit in the public sector adds value not just by analyzing and reporting what has happened, but also by being forward looking, by identifying areas where improvement can be made and by encouraging good practice. In this way it helps to promote improved standards of governance, better management and decision-making, and a more effective use of the taxpayer's resources.

Legal framework for Internal Audit

The principal & framework for Internal Audit (IA) is defined by IIA which states that IA:

Provides expert opinion and advice on the adequacy of the financial management and control system and check if internal controls, procedures and systems, are set up to ensure that work is carried out in accordance with management policies, organization's assets are safeguarded and transactions are accurately recorded in the department's books in an orderly state and are free from error or fraud. It does this by:

- Segregation of Duties
- Proper Authorization
- Adequate Documentation
- Physical Safeguards
- Independent checks
- Vacations and rotation of duties
- Clear definition of responsibilities
- Supervision and Review

In addition, the following decrees and regulations govern the work of IA:

- Decree on Establishing Internal Audit in BISP (Section 15 (2) BISP Act 2010)
- Decree on titles of Internal Auditors (System of Financial Control and Budgeting, 7-ix)
- Decree on observance of Internal Control (System of Financial Control and Budgeting, 7-viii)
- Decree on exercising Internal Checks (Para 13 of General Finance Rules, GOP)

Operational framework for the work of Internal Audit

IA operates in accordance with the Code of Ethics and the International Standards for the Professional Practice of Internal Auditing laid down by the Institute of Internal Auditors[1]. Together these set the framework for how internal auditors should behave and the way they should carry out their work. Further details can be obtained on the IIA website www.theiia.org

Code of Ethics The purpose of this Code of Ethics is to promote an ethical culture in the profession of internal audit. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control, and governance. It applies to all staff performing the duties of internal audit as set out in CGA ordinance/ GFR. Any failures to comply with these ethical requirements could lead to disciplinary action being taken.

This Code of Ethics extends beyond the definition of internal auditing to include two essential components:

- Four key Principles that are relevant to the profession and practice of internal auditing;
- Rules of Conduct that describe behavior norms expected of internal auditors in respect of each of those Principles. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

Principle 1 - Integrity

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

Rules of Conduct Internal auditors:

- Shall perform their work with honesty, diligence and responsibility.
- Shall observe the law and make disclosures expected by the law and the profession.
- Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organisation.
- Shall respect and contribute to the legitimate and ethical objectives of the organisation

Principle 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 judgments.

[1] The Code of Ethics and the Standards for the Professional Practice of Internal Auditing given in this Manual are based on those issued by the IIA in 2012.

Rules of Conduct Internal auditors:

- Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organisation.
- Shall not accept anything that may impair or be presumed to impair their professional judgment.

- Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

Principle 3 ï 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.

Rules of Conduct Internal auditors:

- shall be prudent in the use and protection of information acquired in the course of their duties.
- shall 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 organisation.

Principle 4 - Competency

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

Rules of Conduct Internal auditors:

- shall engage only in those services for which they have the necessary knowledge, skills and experience.
- shall perform internal auditing services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.
- shall continually improve their proficiency and the effectiveness and quality of their services.

Internal Audit Standards

The purpose of the Standards is to:

- set out basic principles that represent the practice of internal auditing as it should be;
- provide a framework for performing and promoting a broad range of internal audit activities which benefit and add value to the organisation;
- establish the basis for the evaluation of internal audit performance, and
- foster improved organisational processes and operations.

The Standards consist of Attribute Standards (the 1000 Series) and Performance Standards (the 2000 Series), and Implementation Standards. Details of each of the following standards can be seen in Appendix B to this Part of the Manual.

a. **The Attribute Standards** address the characteristics of organisations and individuals performing internal audit activities. They are:

- Standard 1000 ï Purpose, Authority and Responsibility;
- Standard 1100 ï Independence and Objectivity;

- Standard 1200 ï Proficiency and Due Professional Care; and
- Standard 1300 ï Quality Assurance and Improvement Program.

b. **The Performance Standards** describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be measured. The Attribute and Performance Standards apply to internal audit services in general.

- Standard 2000 ï Managing the Internal Audit Activity;
- Standard 2100 ï Nature of Work;
- Standard 2200 ï Assignment Planning;
- Standard 2300 ï Performing the Assignment;
- Standard 2400 ï Communicating Results;
- Standard 2500 ï Monitoring Progress; and
- Standard 2600 ï Managementõs Acceptance of Risks.

It is compulsory for all members of Internal Audit (IA) to work in accordance with these Standards.

2. INTERNAL AUDIT CHARTER

1000 Purpose, Authority and Responsibility The purpose, authority and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the *Definition of Internal Auditing*, the *Code of Ethics* and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Purpose

The purpose of the charter is to set out clearly the role of Internal Audit and to clarify the environment necessary for Internal Audit to function effectively and add value in an organisation. It also sets out the working relationships between Internal Audit and the organisation. The Audit Charter should:

a. give an outline of the role of Internal Audit
b. make reference to the scope of work of Internal Audit
c. set out the authorities and access of Head of Internal Audit (HIA) and staff of audit department
d. set out the responsibilities of the Head of Internal Audit of the organisation
e. detail the reporting arrangements, and
f. explain how the independence of IA is secured.

The IA Charter should be reviewed on a regular basis and whenever major structural or other changes take place in the organisation.

As an interim measure, where IA Units have already agreed an IA Charter no immediate action needs to be taken to review that charter. However the Head of Internal Audit should review the content and operation of that Charter 12 months from the issue of the Audit Manual, taking into account the guidance provided in the manual and experience gained over that period.

IA Charter is set out below

ROLE

The role of an internal audit is to:

- Provide independent appraisal of all the activities of BISP aiming to add value, improve operational efficiency, risk management and internal control systems.
- Review, appraise and report upon policies, procedures and operations in place in order to help the organization to:
    - Maintain financial and operational control;
    - Ensure the accuracy of financial reporting;
    - Secure their assets;
    - Limit the potential for fraud and corruption;
    - Ensure security and confidence in MIS; and
    - Comply with, AGP and the organisation's own and applicable local regulations
- Maintain an Internal Audit Manual to support compliance with Internal audit standards.

OBJECTIVES AND SCOPE OF WORK

The prime objective of audit wing is to examine and evaluate whether the BISP's framework of risk management, control, and governance processes, is adequate and functioning properly.

In addition, the objectives of audit wing include advising and recommending senior management for improvements in internal control and risk management systems.

In order to fulfill its objectives, audit wing's scope of work includes:

- The examination and evaluation of the adequacy and effectiveness of the internal control systems at various operations and activities of BISP.
- Review of the application and effectiveness of risk management procedures and risk assessment methodologies at various operations and activities of BISP.
- The review of the management information systems, including the electronic payment system. The review of the accuracy and reliability of BISP accounting records and financial reports.
- Evaluation of adherence to legal and AGP's requirements and approved policies and procedures.
- Evaluation of effectiveness of existing policies and procedures and giving recommendations for improvements.
- Identifying opportunities for cost savings and making recommendations for improving cost efficiencies.
- Examining that resources are acquired economically, used efficiently and

safeguarded adequately.

- Carrying out surprise audits based on risk assessments.
- Precisely, every activity and every entity of BISP fall within the scope of the internal audit for independent appraisal. The Director General and staff of audit department are, however, not allowed to:

    - Perform any operational duties for BISP outside audit department function.
    - Initiate or approve accounting transactions external to audit department.
    - Direct the activities of any BISP employee not employed by the audit department, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

AUTHORITY & ACCESS

The Director General and staff of audit department are authorized to:

- Have unrestricted access to all BISP departments, offices, affiliates, activities, records, information, properties and personnel, relevant to the performance of audit function.
- Determine scope of work and apply the techniques required to accomplish audit objectives.
- Obtain the necessary assistance of personnel in various departments/ offices of BISP where they perform audits.
- Have unrestricted access to Management Information System (MIS) and allied systems of BISP..
- Appoint required resources for the Internal Audit function as approved by the Board. Obtain assistance of specialists/ professionals where considered necessary from within or outside BISP.
- Perform surprise / snap / full scope audits beyond approved annual audit plan based on updates in risk assessment

RESPONSIBILITY

The Director General audit department has responsibility to:

- Perform risk assessments and formulate an annual audit plan in consultation with Audit Committee and management.
- Implement the annual audit plan, including as appropriate any special tasks or projects requested by the audit committee.
- Maintain requisite professional audit staff strength with sufficient knowledge, skills, experience, and professional qualifications to meet the requirements of this Charter.
- Issue periodic reports on a timely basis to the audit committee and summarizing results of audit activities.
- Deploy resources freely as and when required.
- Keep the audit committee informed of emerging trends and developments in

internal auditing practices and give recommendations for necessary revisions in Internal Audit Charter and Internal Audit Manual. Provide a list of significant measurement goals and results to the audit committee.

- Assist in the investigation of significant suspected fraudulent activities and notify the audit committee of the results.
- Ensure that the department complies with sound internal auditing principles and best practices; seek guidance from the standards issued by the Institute of Internal Auditors, and Information Systems Audit & Control Association, (USA).
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on the organization.

The Director General and staff of audit department have responsibility to:

- Follow the guidelines and methodology given in the Internal Audit Manual.
- Exercise due professional care in carrying out audit assignments.
- Maintain objectivity and integrity.

The internal audit process, however, does not relieve departmental heads/ directors of their responsibility for the maintenance and improvement of controls in their respective areas.

ACCOUNTABILITY AND REPORTING

The Director General audit department, in the discharge of his duties, shall be accountable to the audit committee to:

- Submit an assessment on the adequacy and effectiveness of the BISPôs processes for controlling its activities and managing its risks in all the core areas of BISP operations on six monthly basis and in non core areas on annual basis.
- Report significant issues related to the processes for controlling the activities of BISP and its regional offices, together with recommendations for improvements to those processes.
- Provide information on the status and results of the annual audit plan.

INDEPENDENCE

To maintain the independence of internal audit wing following needs to be assured:

- The internal audit activity will remain free from interference by any element in the organization.
- Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditors' judgment.
- Audit department shall exercise its assignment on its own initiative in all departments, offices and functions of BISP.
- Director General Audit department shall be authorised to communicate directly, and on his own initiative, to the members of audit committee and the board.
- The internal audit function should be subject to an independent review as and when required and at least once in five years. This review can be carried out by independent professionals e.g. practicing chartered accountants.

CONTINUITY AND IMPARTIALITY

- Internal audit within BISP shall be a permanent function.
- Audit department shall be objective and impartial in performing its assignment.
- Objectivity and impartiality entails that the internal audit wing itself seeks to avoid any conflict of interest. To this end, staff assignments within audit department shall be rotated periodically. Internally recruited/transferred auditors shall not audit activities or functions they performed in the past two years and they will not be allowed to audit the work earlier performed by them and every staff is bound to sign declaration of independence before the start of any audit assignment.

Approved by

_____

3. ROLE OF HEAD OF INTERNAL AUDIT

The Head of Internal Audit has a key role to play in the development of internal audit in his/her organisation. In particular it is important to overcome the misconceptions about what internal audit is here to do, and make it clear that it is not ôinspectionóby another name, but that it can play a positive and constructive part in the organisation.

The precise responsibilities of the Head of Internal Audit are set out in audit charter.

Which states that:

- Perform risk assessment and formulate an annual audit plan in consultation with Audit Committee and management.
- Implement the annual audit plan, including as appropriate any special tasks or projects requested by the audit committee.
- Maintain requisite professional audit staff strength with sufficient knowledge, skills, experience, and professional qualifications to meet the requirements of this Charter.
- Issue periodic reports on a timely basis to the audit committee and summarizing results of audit activities.
- Deploy resources freely as and when required
- Keep the audit committee informed of emerging trends and developments in internal auditing practices and give recommendations for necessary revisions in Internal Audit Charter and Internal Audit Manual. Provide a list of significant measurement goals and results to the audit committee.
- Ensure that the department complies with sound internal auditing principles and best practices; seek guidance from the standards issued by the Institute of Internal Auditors, and Information Systems Audit & Control Association, (USA).
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on the organization.

In addition the Head of Internal Audit unit should:

- Ensure the right conditions exist for audits to be carried out in an effective way and in accordance with the internal audit plan;
- develop strategic and annual work plans for internal audit unit,
- follow up recommendations, i.e. whether recommendations are implemented properly, efficiently and on time.

4. AUDIT PLANNING

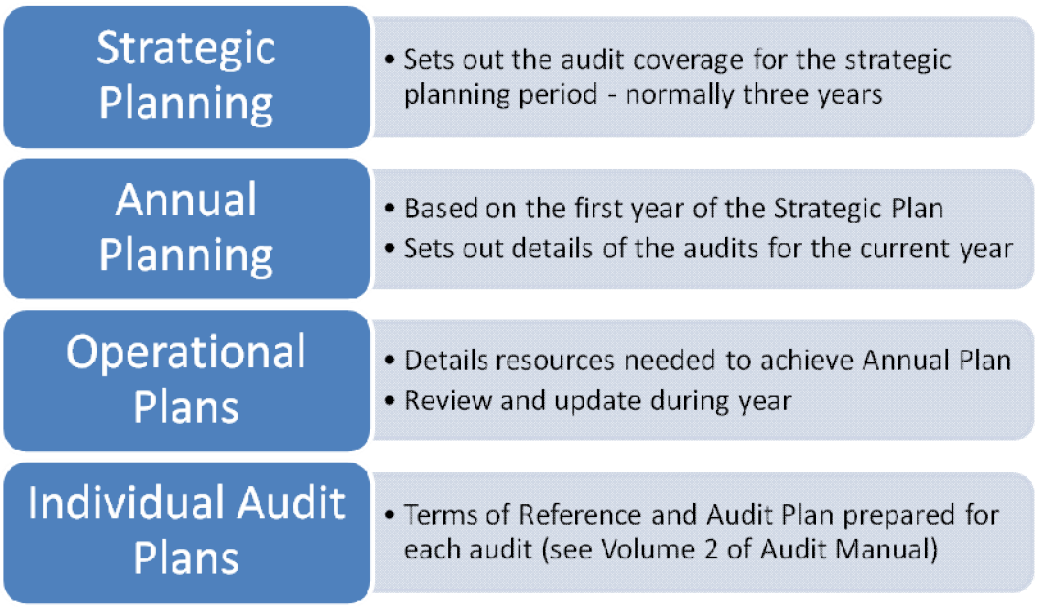
2010 Planning

The head of internal audit must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goal

Audit planning is needed to enable Internal Audit (IA): to achieve its objectives; to establish its priorities and to ensure the efficient and effective use of audit resources. It also provides:

a. a basis for the assessment of future resource requirements;
b. authority to act once the plan is approved by senior management;
c. yardstick against which actual performance can be measured;
d. means of getting management ôbuy-inóto the work of IA , and
e. a permanent record of the factors considered and the judgments made when setting the plan.

Planning is a key part of the audit process and comprises four stages.



4.1 Strategic Planning

A good Strategic Plan will:

a. Help to identify the ôaudit universeóï i.e. all possible areas that should be subject to audit
b. Provide an objective risk-based approach to defining IAós work

c. Help IA to provide an assurance on systems of internal control, and
d. Allow IA to optimize the use of its resources and improve its effectiveness as a service to management.

The IIA Standards require Audit Units to carry our risk-based planning and to review and update those plans annually.

The following are the stages involved in the preparation of a Strategic Plan:

a. STEP 1 - Establish the audit environment
b. STEP 2 - Identify all the auditable systems/areas
c. STEP 3 - Carry out a risk assessment for each system/area
d. STEP 4 - Decide on your audit strategy, and
e. STEP 5 - Prepare an audit needs assessment.

In the early years of setting up IA it may be necessary to take a more pragmatic and less time-consuming approach to strategic planning, for example by grouping the auditable systems identified and/or by reducing the number of risk factors.

Step 1 - Establishing the Audit Environment

The starting point for strategic planning is to have a good understanding of the context in which the organisation is operating. This involves considering such things as:

- Managementõs attitude to control;
- Information about the general level of control in the organisation;
- The risk appetite of the organisation ï is it very averse to risk or prepared to accept high levels of risk, and
- The willingness of management to accept and embrace change etc.

Based on this it is often worth trying to establish what your broad audit strategy might be. For example: what might be an appropriate period for the plan (e.g. 3 years or 5 years?) and what do you want to achieve over the period of the plan ï possible objectives include raising awareness of risk management in the organisation; assisting the development of accountability in the organisation and encouraging the use of objectives by managers.

Step 2 - Identify auditable systems

The next step is to identify what you are going to audit. Your objective should be to identify and define systems which cover all the objectives and activities of the organisation. Keep in mind that some systems will fully address a particular management objective(s) and others may only partially address an objective(s). It is useful to try to keep the number of systems or groups of systems to a manageable number.

You will need to find out about the organisation and the way it is structured. Areas of work by system or sub-system can be identified through consultation with different levels of management. Use should also be made of previous work done by IA and any other knowledge and experience gained by IA staff. Other possible sources of information include:

- Management information, policy papers and laws which may provide details of aims, objectives and targets;
- contracts and service level agreements;

- organisational charts and systematisation schedules;
- the organisationôs office directory;
- annual reports and performance targets;
- Board minutes of meetings, BISP future action plans, and
- Management accounts and budgets.

As well as identifying areas of work by system and sub-system you should:

- establish interfaces between systems;
- establish inter-departmental systems, and
- get directorôs opinion on which areas or particular factors are considered high risk.

By way of guidance the following are two common ways of classifying systems:

a. *By function* – dividing systems into functional types which differ according to the part they play in the internal control system. Examples of these are:
   - Monitoring - information systems are likely to cover all parts of an organisation. They provide tools to a hierarchy of management. Potentially, work done on these systems can reduce the effort required to audit the systems at lower levels. If the organisation is relying on such systems as primary tools they should be priority systems in the audit plan
   - Operational - systems for carrying out the business of the organisation, including policy matters. The audit priority afforded to these systems will depend on their level and nature.
   - Service - administrative systems such as personnel, purchasing, finance, office services cover many parts of an organisation. For the well known types of systems it may be convenient to adapt existing audit methodologies to the systems, thus saving development time. Although each system is unique at the detailed level, each system will often be based on a common pattern

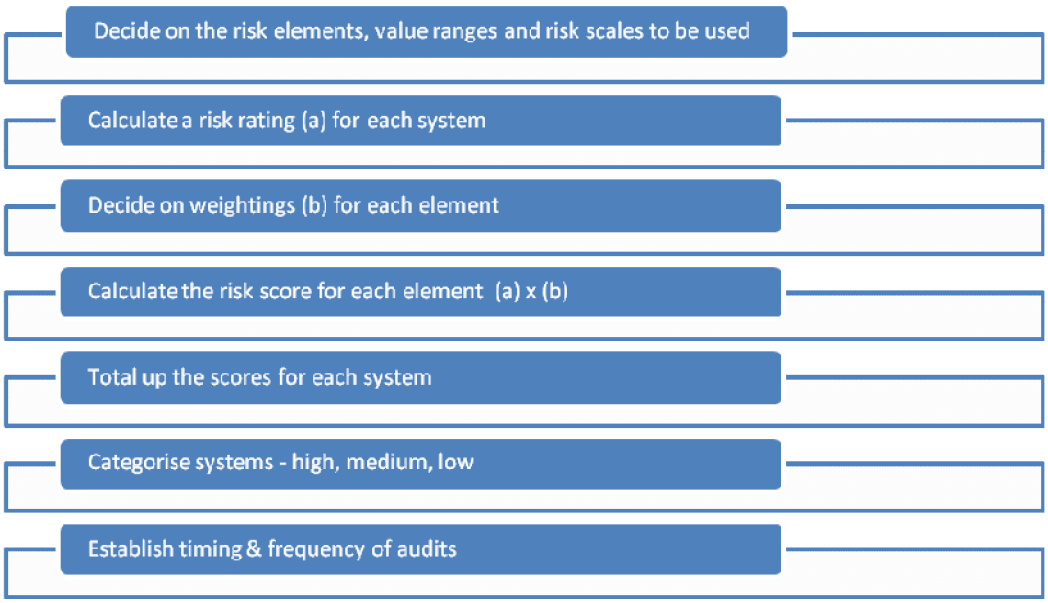
b. *Hierarchical*
   - Senior management will tend to view the organisation as sub-divided into a fairly small number of areas, approximately matching the organisation chart. These systems will have associated risks and may be linked to budget holder responsibilities and also to the organisationôs critical success factors. If systems are analysed in this way, the links between systems will be particularly important. Systems are rarely confined to one part of the organisation and there are usually links and interrelationships between different parts of the organisation.

Regardless of the classification method used, the Head of Internal Audit needs to examine interfaces between systems within each institution to identify the extent to which the audit of one system can provide findings relevant to another system. Where one system acts as a control over another it may be possible to plan the audits in a more efficient way to take account of these links.

Whatever method is used to categorise systems, audit plans should still be based on a systems based audit approach. The objective is to plan a programme of audits which will provide evidence to support an assurance regarding the adequacy of the systems of management control. Value for Money and Performance Audits can be scheduled separately within the strategic plan, where appropriate.

Step 3 - Risk assessment of the areas identified

Once all systems have been identified, an assessment of risk needs to be done. This provides a rationale for the direction of audit resources over the long term. The purpose of this is to focus audits on those activities, which carry greater risk for the organisation as a whole.
The process of risk assessment involves the following main steps:



Risks can often be determined through interviews with management and staff; use of questionnaires and group discussions between auditors. The amount of research undertaken should be influenced by the cost and degree of difficulty in collecting data for the assessment of systems.
The following are common risk categories that can be used to help identify risks:

a. Reputational risk - arising from adverse publicity and exposure;
b. Operational risk - affecting the relationship between service and general public e.g. disruption to service;
c. Strategic risk - affecting the organisation in the long term;
d. Legal risk - arising from legislation;
e. Social risk - arising from changes in demographic, residential or socio-economic trends;
f. Contractual risk - relating to the failure to deliver goods/services at the agreed cost & specification;
g. Financial risk - risks that have a purely financial base;
h. Managerial risk - relating to the day to day responsibility and accountability of staff;
i. Property risk - relating to theft, deterioration etc. ;
j. Regularity risk - relating to legal action, external inspection etc. ;
k. Technological risk - relating to the capacity to manage and harness technological change;
l. Professional risk - relating to particular professions e.g. protection, duty of care;
m. Specific risk - such as health & safety;

n. Natural risk - flood, fire, earthquake etc.; and
o. Governance risk - relating to the governmentós objectives and the roles and responsibilities of ministers.

Risk assessment is based essentially on subjective judgment but various techniques can be used to make the analysis more systematic and, to some extent, more objective. Use of them will strongly support the auditorós judgment on the priority and frequency of audits. They can also help to identify areas of high exposure which might not otherwise have been identified. Each stage of the risk assessment exercise should be fully documented.

One commonly used approach to the assessment of priorities and frequencies involves the calculation of risk indices. It combines determining a risk rating for each of a number of pre-determined characteristics or elements of a system and assigning weights to each of them, thereby incorporating a judgment of their relative importance - on a scale of 1(low) to 5(high) risk. This enables the calculation of a risk index for each system. Some typical risk elements include:

- Value of transactions,
- Volume of transactions,
- Value of income,
- Value of expenditure,
- Asset value and liquidity,
- Systems characteristics,
- Organisational factors - number of staff, supervisor to staff ratio, staff turnover etc,
- Complexity of the system,
- Distance from the center,
- Stability of the system - tendency to or likelihood of change,
- Special elements unique to the system,
- Sensitivity of the system - e.g. political sensitivity, general public, pressure groups,
- Scope and effect of the system,
- Effect of system on future events and decision making,
- Effect of system on other systems,
- Management and control,
- Staff morale - speed of staff turnover,
- Quality of internal control within the system,
- Amount of control over the system exerted by other systems,
- Date and findings of the last audit, and
- Opinion expressed by other review bodies (e.g. external audit, inspection).

It is necessary to decide which risk elements you are going to apply, since the same ones will be used to determine the risk rating for each system. An example of some typical risk elements and their values is given in the table below:

Risk element	**Value range**	**Risk rating**
Staff Numbers	≤ 100 ≤ 500 ≤ 1000 ≤ 10000 > 10000	1 2 3 4 5
Direct expenditure (Excluding procurement)	≤ 10,000 PKR ≤ 50,000 PKR ≤ 80,000 PKR ≤ 200,000 PKR > 200,000 PKR	1 2 3 4 5
Value of transaction/procurement	≤ 10,000 PKR ≤ 50,000 PKR ≤ 80,000 PKR ≤ 200,000 PKR > 200,000 PKR	1 2 3 4 5
Sensitivity of activities	Scale of Low to High	Scale of 1-5 1 5
Geographical spread	Fully centralized Partially centralized Considerable centralized	1 3 5

These risk ratings for each element cannot be used as they stand. They need to be weighted to reflect your assessment of the relative significance of the different elements. In allocating weights, you need to judge between the relative significance of different elements. For example, the degree of stability of the system may be more important than the volume of transactions because systems which change may have new and unproven internal controls. Organisational elements such as the effect of one system on another or on a range of sub-systems might be weighted higher than elements which apply only to the system in question. Similarly, systems which have far-reaching effects on future decisions e.g. forecasting or research and development might be weighted higher than systems whose effect is more immediate.

The elements and weighting factors should be combined into a formula which can be used to calculate the risk index. In choosing weighting factors, the auditor must avoid introducing unfair bias into the formula. That formula should be checked to ensure that small variations in the elements and weighting factors do not lead to significant changes to the order of priority or frequency, particularly where subjective judgment is required.

The weighting system should be kept as simple as possible, and often a scale of one to five is used. An example of how this might be applied in practice is shown below.

Calculation of risk indices

Risk Factor	System 1			System 2			System 3			System 4		
	Rating	Weighting	Total	Rating	Weighting	Total	Rating	Weighting	Total	Rating	Weighting	Total
Total Spend	2	5	10	5	5	25	5	5	25	3	5	15
Volume of transactions	5	2	10	5	2	10	5	2	10	1	2	2
Staff numbers	3	3	9	3	3	9	3	3	9	2	3	6
Direct expenditure (excluding procurement)	2	4	8	5	4	20	2	4	8	3	4	12
Procurement	3	5	15	5	5	25	2	5	10	5	5	25
Sensitivity' of activities	3	3	9	2	3	6	2	3	6	4	3	12
Geographical spread	3	4	12	5	4	20	5	4	20	3	4	12
Managerial 'Approach'	5	3	15	5	3	15	5	3	15	5	3	15
Risk Index	**88**			**130**			**103**			**99**		

Step 4 - Audit strategy

Once the systems have been defined and the risk indices calculated the Head of Internal Audit should discuss and agree the results with management.

Once this has been done the audit strategy needs to be defined. The broad audit strategy defined earlier in the process should provide a good starting point for this. It is not realistic, or necessary to cover all aspects of the internal control system in detail every year. The objective of the strategy should be to provide sufficient coverage of the main areas to allow an overall opinion to be given on the adequacy of the systems of control.

Based on the risk indices you will need to categorise the audit systems into high, medium and low risk. For example, you could decide:

a. Audits with a risk index of 85 are high risk;
b. Audits with a risk index of 40 ï 84 are medium risk, and
c. Audits with a risk index of 39 or less are low risk.

The audit strategy should involve auditing higher risk systems more frequently ï usually every year ï in order to confirm that these vitally important systems are under effective control. On the first audit of a high-risk system, controls will be reviewed down to a detailed level in order to establish which controls are the key ones and how effective they are. Subsequent audits of high risk systems will be limited to confirming that the system objectives, control objectives, risks and controls remain the same and carrying out compliance tests on the key controls.

Medium risk systems may be audited less frequently. If the audit cycle is three years then these systems could be subject to some audit work two out of the three years of the cycle. This may be justified partly because not auditing them in any one year leaves a relatively small exposure.

Low risk systems could be audited only once every three years ï and in some cases that audit could be restricted to two or three of the key systems.

The first time a strategic plan is prepared it will probably be necessary to assign standard times to each category of audit, eg:

I. High Risk Score ï 40 days per annum (i.e. 120 days per system over the cycle)
II. Medium Risk Score ï 25 days (i.e. 75 days per cycle)
III. Low Risk Score ï 25 days per audit cycle.

In later updates of the strategic plan these figures can be refined and specific times allocated to audits as more experience is gained.

This will enable you to calculate the number of auditor days needed for each year of the strategic plan. The medium and low risk audits should be distributed evenly over the period of the strategic plan.

Step 5 - Assessment of audit need

The next stage is to determine the resource (staff) requirements - the audit needs assessment. Estimates of staff time by auditor grade for each audit assignment should be made. Initially, the audit needs of an organisation should be determined without regard to constraints such as the time and resources which may be available.

Ideally, these estimates should be based on anticipated performance and competence of audit staff. Untrained or inexperienced staff will take longer to perform tasks. The total staff time inputs should include basic direct time and any time inputs by the Head of Internal Audit. Basic direct time includes all stages of an audit such as collecting background data, preparing the audit plan, fact finding, documenting, testing, preparing reports, discussing audit findings, immediate follow up and monitoring of systems changes. It should be analysed to reflect the need for specialist skills (such as computer auditors, accountants etc) and to show where the audit requires the expertise of a more experienced auditor.

In practice a simple way to do this in the early days of setting up IA is to calculate the number of audit days available using your existing audit staff. In deciding the number of days available for each auditor you should subtract the following from the total of 260 available working days per auditor per year:

- Annual leave
- Public holidays
- Training (remembering that higher levels of training will be needed in the early years, or if there are a large number of relatively new staff)
- Sickness
- Admin (typically 15 days per annum)

This will give you the net days available for each auditor, and this should be totaled. To this total should be added the number of direct days per audit which the HIA is expected to contribute (say between 3 and 5) to give a grand total of days available. This grand total should be compared with the number of days needed, enabling the HIA to determine whether he/she has enough staff, and if not how many additional staff are needed to achieve a level of coverage that will enable a reasonable level of audit assurance to be provided.

If additional resources are required (which will often be the case) the HIA will have to discuss this with the Head of the Organisation to decide whether the necessary extra audit staff can be made available. If it is only possible to provide a limited number of additional staff (or no additional staff) the Head of Internal Audit will need to discuss and agree the level of assurance that can be provided, and where the resources of IA should be focused. Throughout the planning process you need to keep in mind that it will never be possible to provide total assurance

Following these discussions a revised strategic plan should be prepared showing:

- resources - the resources expected to be available each year. This will take account of specific skill requirements and a preference for smoothing out peaks and troughs
- the audits to be carried out ï annual tasks identified in the needs assessment will be the first charge against each yearÕs available resources.
- contingency - there should be a contingency element in each year of the plan consistent with the overall contingency in the needs assessment
- priority - as a general rule systems with the highest priority should be scheduled as early as possible in the timetable within the available annual resources

- frequency - has already been considered in the needs assessment and determines how often a system should be audited
- centralised systems - the approach should reflect the extent to which systems are centrally prescribed or fall within delegated authority limits. This applies particularly in the case of a network of offices operating a common system. Audit visits may be necessary only to test the broad control arrangements in place
- logistics - there may be good reasons why certain audits should be done (or should not be done) within a short time of each other. There may also be certain audits which require specialist staff and the allocation of these to any year should be consistent with the specialist staff available in it. This factor becomes more critical in annual plans

Other factors to consider once the IA unit is properly staffed

The need to plan for the audit of systems under development. It may be necessary to build a contingency into the plan for this. Where there are major known developments planning can be more precise and should take account of predicted timescales. There will normally be key stages at which different types of audit activity will be required. Knowledge of the project development methodology used will allow estimates to be made of the stage at which the greatest amount of audit time will be required and blocks of work built into the audit plan.

Similarly, it is necessary to allow time for other work such as specific follow-ups, performance audit, advice to management and fraud investigation. Finally, a ócontingencyô (typically 10 ï 15%) may be included to allow for unplanned events ï e.g. an unforeseen restructuring of the organisation or an expansion of the organisationós responsibilities, which may require audit input.

The strategic plan should be reviewed and updated annually, with the second year of the current strategic plan becoming the first year of the new plan and also the basis of annual plan for the forthcoming year. A full re-assessment should take place every four to five years ï or sooner if major changes occur within the organisation.

Presenting the Annual Plan to the Audit Committee

The plan should:

a) Identify clearly the main objectives of the entity and the main policy instruments through which these objectives are to meet.
b) Identify the major risks to the achievement of high-level objective.
c) Explain (briefly) how the areas to be audited have been determined and how individual systems grouped for audit purposes.
d) Explain how risks have been assessed and systems etc ranked for audit.
e) Identify the frequency of coverage for high medium and low risk systems/audit missions, and explain that the aim is normally not to cover all aspects of the internal control system in detail every year, but to obtain sufficient coverage of the main areas to allow a general opinion to be formed
f) Identify the resources required and those available to implement the strategy, drawing attention to the impact of resource shortfalls.
g) Provide the annual work plan for the first year of the strategy.
h) Explain the arrangements for accommodating additional (ad hoc) audit missions and how these can be accommodated within the annual work plan.
i) Comment generally on the quality and effectiveness of the audit resources available and the staff training needs.

4.2 The Annual Plan

The annual plan, which is developed from the strategic plan, is prepared on an annual basis, and must be approved by the Audit Committee. It is based on the first year of the strategic plan and should provide additional detail, for example defining the tasks to be performed and identifying critical areas, setting target dates and allocating resources for the forthcoming year.
It must take account of any new developments. For example:

- have there been any changes in the organisationós activities which have not been reflected in the strategic plan?
- is the original assessment of risk and priority still appropriate?
- are the staff available now and are they more or less experienced than anticipated?
- has there been any slippage in previous annual plans which must now be rescheduled, either into this annual plan or the strategic plan?

The following stages are involved in drawing up the annual plan:

- Establishing the staff and other resources available over the planning period. This involves identifying known absences, expected changes in staff and other commitments;
- based on the re-appraisal above, select the appropriate audits from the strategic plan, consistent with the balance of available resource;
- identify the man days, in direct time, needed for each audit; and schedule the audits by months/quarters - ensuring that there are no inconsistencies. It is important to consider whether any audits must or must not be done at specific times.

The Head of Internal Audit should consider the strengths and weaknesses of the staff available and allow for the need to develop and train his or her staff. Team Leaders may be responsible for specific blocks of audits - either by function, location or programme. In such circumstances, the preparation of parts of the annual plan may be delegated to them but the Head of Internal Audit remains responsible for the overall coordination and consistency of the plan.

Operational Plans
The operational plan sets out the precise allocation of resources to specific audits and is an important management tool for the Head of Internal Audit. Progress against the plan (and against the overall annual plan) should be reviewed at least monthly to identify any shortfalls and to decide on the corrective action to be taken.

Assignment Plans
Detailed guidance on preparing assignment plans for individual audits is given in Volume Two of this Manual.

5. STAFFING POLICIES

2030 RESOURCE MANAGEMENT

The head of internal audit must ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan.

Having good staff is key to the success of internal audit. That is why particular emphasis is given to recruiting high calibre people and to training and developing them. The HIA should discuss and agree internal audit recruitment and training needs with the head of the organisation. This section sets out the main policies relating to staff management.

Selection

The HIA is responsible for ensuring that the staff appointed to Internal Audit have the necessary background and personal attributes to work effectively in IA and that they have, or will be able to acquire, the knowledge and skills needed to carry out the work of IA. In order to do this the HIA will need to be actively involved in the selection of audit staff. The way in which this will be achieved should be discussed and agreed with Audit Committee. This procedure should be referred to in the IA Charter.

The minimum requirement is a first degree. This will often be in Law, Economics, Management, Accounting, Finance or some other relevant discipline. However, applicants with degrees in other subjects should also be considered, because it is important to have a wide range of knowledge and a variety of different approaches and attitudes amongst IA staff.

When recruiting staff the HIA also needs to try to ensure that the unit as a whole has the experience necessary to audit the wide range of activities in which most organisations are involved. These include: management; administration; organisational issues; security; IT and information systems. In practice it will be very difficult to achieve this, but it is an objective which the HIA should always have in mind.

Equally important as educational achievement and experience are personal attributes and skills. These include:

- The analytical skills to understand and appraise systems and controls quickly and to make sound judgments;
- The determination to follow investigations through to their logical conclusions, but also to use judgment to decide when unproductive lines of enquiry should be dropped;
- An imaginative approach to work;
- Being capable of gaining the respect and co-operation of auditees and colleagues;
- Being able to communicate orally and in writing in a tactful and convincing manner and to argue their conclusions to senior levels if necessary;
- Being able to stand their groundóand argue the case effectively;
- Negotiating skills;

- The ability to solve problems and come up with practical solutions;
- Tact and diplomacy, and
- Personal integrity.

In the early stages of development of Internal Audit in BISP, if any, candidates for posts in Internal Audit will not have prior audit experience. In such cases it will be essential to establish whether or not candidates have the personal and interpersonal skills needed for them to become effective internal auditors.

In some cases it may be appropriate to employ specialist staff such as surveyors, engineers, lawyers or statisticians for a specific audit, or on a short-term basis to provide particular expertise for particular audits. The HIA is responsible for ensuring that such specialists receive the audit training they need to do their job effectively.

The HIA is responsible for preparing and keeping up to date Job Descriptions for each audit post including his/her own.

6. EXTERNAL RELATIONSHIPS

2050 COORDINATION

The head of internal audit must share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts.

Relationships with management, staff, external auditors, and other review agencies must be centered on the need for mutual confidence, understanding of the role of Internal Audit and cooperation. Management and staff at all levels must have complete confidence in the integrity, independence, and capability of Internal Audit. This should be reflected and maintained in good working relationships between auditors and auditees.

Relationships with management

General liaison

The HIA is responsible for consulting with management of the organisation in preparing and updating the Audit Needs Assessment, the Audit Strategy and the Annual Audit Plan. The HIA should maintain regular contact with senior management in the organisation, by means of regular meetings and six monthly reports on Internal Audit activities. As a general rule all audit staff are encouraged to make contact with line management at the appropriate level during the course of planning and conducting an audit assignment. Unless the HIA decides otherwise, Auditors should normally feel free to contact staff up to Head of Department or equivalent level in the course of their work. Above that level, the HIA should be consulted beforehand. The HIA should maintain contact with Heads Department in respect of:

- Discussion and review of assignments which it is proposed to include in the Annual Audit Plan, before the program is finalized by the HIA;
- Keeping abreast of organisational and systems developments in the organisation, and
- Gaining a fuller understanding of the operational problems facing Heads of Department in order to help identify areas of potential audit interest.
- Making the arrangements to set up individual audit assignments. This will involve:
  - Notifying management of any pre-audit planning work which is to be undertaken;
  - Discussing audit terms of reference with the auditee and confirming them in writing;
  - Providing, where necessary, periodic oral progress reports to the client, and
  - Holding an exit meeting with the client to discuss audit findings, conclusions, and potential recommendations

Requests by management for advice and guidance

Internal Audit staff will be approached for advice on a wide range of matters, often on an informal basis. Whilst it is important that Internal Audit should be seen to be responsive and helpful to such requests, it should not be done in a way that may jeopardize the independence and objectivity of Internal Audit.

Staff must exercise professional judgment and caution to avoid giving the impression

that Internal Audit is participating in the client's decision process.
When dealing with ad hoc requests for advice and guidance:

- Internal Audit staff must promptly inform their HIA of any request by management;
- Written guidance should only be given by the HIA;
- If oral advice is given on the spot by an auditor it is important to make it clear that it is purely informal advice, and should not be taken to reflect Internal Audit's official view on the matter.

Relationship with the Auditor General of Pakistan

The principal role of the of Auditor General of Pakistan (AGP) is to express an opinion on whether the BISP's financial statements present a fair view of its financial position, and whether they conform to generally accepted government accounting principles and International Accounting Standards (where appropriate). As such, their objectives differ substantially from those of Internal Audit, although certain areas of common interest exist. Internal Audit does not act on behalf of the AGP, although the AGP may decide to rely on some of the work done by internal audit.

The HIA will hold meetings with the Directorate General of Federal Audit. The objective of these meetings is to develop cooperation with the external auditors, thereby ensuring that the organisation is provided with a comprehensive audit service and minimize duplication of effort. These contacts will involve:

- Discussion of work programs;
- Exchanging copies of reports;
- Allowing access to audit files; and
- Holding regular liaison meetings.

1. Copies of all Internal Audit reports may be sent to AGP when the final version is agreed, approved and issued by the audit committee.

Access to files

Internal Audit will make its audit files available to external audit on request.

7. QUALITY ASSURANCE POLICIES

1300 Quality Assurance and Improvement Programme The head of internal audit must develop and maintain a quality assurance and improvement programme that covers all aspects of the internal audit activity.

1310 Requirements of the Quality Assurance and Improvement Programme The quality assurance and improvement programme must include both internal and external assessments.

The IIA Standards stress the importance of quality and continuous improvement in internal audit. It is the HIAós responsibility to develop and maintain a quality assurance (QA) programme that covers all aspects of the internal audit activity and continuously monitors its effectiveness. This involves defining the appropriate standards and level of quality for audit outputs and then establishing comprehensive procedures which will ensure that this level of quality is achieved and maintained.

QA takes place at two levels:

- Level One involves internal assessments to ensure that individual audits are carried out to an acceptable level of quality; and
- Level Two involves broader external reviews of the full range of audit tasks to establish that laid down policies and procedures are adhered to and that they actually do ensure that work is carried out to an acceptable level of quality.

Internal assessments

Each audit needs to be supervised and reviewed in order to ensure that the quality of audit work is maintained and that the coverage and timing of the audit is in line with the audit plan. The HIA is responsible for ensuring that individual audits are adequately resourced and properly supervised throughout and should review each audit on an ongoing basis. The specific arrangements for supervising and reviewing individual audits are set out in Part Two of the Audit Manual.

External QA reviews

In addition to assessing the quality of individual audits it is important to obtain independent assurance that the internal audit policies and procedures for carrying out audits are being adhered to and that they are achieving their objectives. It is also important to obtain assurance about the processes for the way the internal audit function is being managed.

Whilst the IIA recommend that an external quality review should be carried out at least once every five years, this is unlikely to be practical in Pakistan in the medium term. In the meantime it is suggested that such reviews could be done by:

- Ministry of Finance
- The AGP, or
- The HIA of another Government institution.

It is important that these reviews are carried out in a way which is consistent with

the guidance set out in the IIA Quality Assurance Manual.

In the longer term, when internal audit in Pakistan is more established, it may be possible for a review to be conducted by a reviewer or a review team from outside of the public sector.

8. FRAUD POLICY

Introduction

Fraud can be defined as theft with deception. It includes bribery, extortion, forgery, theft, conspiracy, false representation, misappropriation, and concealment of material facts. It may involve either direct gain (e.g. money or property) or indirect gains such as power, influence, promotion, or bonuses.

There are three basic types of fraud:

- *Corruption,* which involves offering, giving, soliciting or accepting an inducement or reward that may influence the action of any person. It can take the form of outside;
- Pressures or of collusion between staff and third parties;
- *Employee fraud*, which is committed by an employee against the organisation to the direct benefit of the employee or, due to the position they hold, committed against a third party; and
- *External fraud,* which is committed by an outsider (either with or without internal help) via the deliberate misinterpretation of information for gain, or by recognising and exploiting weaknesses in systems.

There are two main groups of factors that can allow fraud to occur - operational and personal. Examples of these factors are:

- *Operational factors*
    - A weak control environment;
    - Staff being asked to carry out duties which exceed their capabilities; and
    - Staff shortages at management level

- *Personal factors*
    - Personal financial difficulties;
    - Personal character traits; and
    - Pressure being exerted on an employee by a third party.

For fraud to occur there must be:

- The means ï e.g. knowledge of the job/systems in operation;
- The motive ï e.g. the employee has large personal debts or other financial problems; and
- The opportunity - in the form of operational or control weaknesses.

Responsibilities for safeguarding against fraud and corruption

Management

The responsibilities of management in relation to fraud are set out in Article 1.5 of the BISP FM, which makes it clear that any case of suspected fraud should be notified, by putting a complaint in a complaint box which can only to be opened by Director Administration. Anonymous complaints against any official will be handed over to the respective head of the department for investigation.
When the possibility of a fraud or internal control failure is suspected, management has a maximum of ten working days to investigate the issue. As soon as the fraud/internal control issue is confirmed, then the matter should be reported immediately to the MD/Secretary.

Internal Audit

The responsibilities of IA in relation to fraud are to notify, in writing, to the head of the organization/audit committee/risk and governance committee. However, IA is **not** responsible for identifying fraud and corruption, but to help management to ensure that the procedures and systems of internal control they have are efficient to minimise the risk of fraud and corruption taking place without detection.

Internal Audit should consider the risk of fraud and corruption when preparing strategic plans and planning individual audits. Likely high-risk systems include:
The handling of cash;

- Assets and stores;
- Awarding contracts;
- Receipt of funds from outside the organisation;
- Payments of all kinds by the organisation;
- Travel claims; and
- Wages and salaries.

When doing an audit the systems should be tested to ensure that the risk of fraud, both internal and external, is minimized and auditors should be alert to any control weaknesses which could allow fraud to occur. If significant control weaknesses are discovered auditors should test to identify whether the weakness has been exploited.

Where sufficient indicators of fraud emerge to justify an investigation the auditor must put the evidence in a safe place and inform the HIA immediately. The HIA will decide how the matter should be handled. Under no circumstances should any aspect of the case be discussed with client management or staff without the prior approval of the HIA.

Investigating fraud

The prime responsibility for conducting fraud and corruption investigations rests with management. Where fraud is suspected in connection with the use of Foreign Funds there are set procedures that must be followed for reporting and handling those cases.

9. OVERVIEWS OF THE MAIN TYPES OF AUDIT

The BISP FM (Article 7.1) sets out the main types of audit that may be carried out in BISP are

a) Internal Audit
b) External Audit

Types of audit that may be carried out by internal audit.

These are as follows:

- Systems audit;
- Compliance audit;
- Performance audit;
- Financial audit;
- Information technology audit.

This section provides a brief explanation of each of the audit that may be carried out by internal audit.

Systems Audit

Systems Audit is the structured analysis and evaluation of the extent to which systems of internal control ensure that objectives of each organisation will be achieved. It is used extensively in internal audit and the approach to systems audit work is set out in detail in Part 2 of this Audit Manual.

Systems audit involves:

- Analysing the organisationós systems in an assessment of audit need. This enables internal auditors to see systems in the proper perspective of:
  - Their relative risk and materiality to the organisation;
  - Which parts of the organisation they impact upon; and
  - The relationships between different systems.

- Assessing how internal controls are operating within a system, so that a view can be formed on whether reliance can be placed on the system to help management achieve its objectives;
- Providing management of each organisation with assurances that systems are doing what they were designed to do;
- Making constructive and practical recommendations to strengthen systems and manage identified risks; and
- Using the findings of the audits of individual systems to feed into an overall assurance on the adequacy of controls.

The audit of a system will normally involve the following stages:

- Ascertaining and recording the system by:
  - Identifying the objectives of the system;
  - Identifying all activities involved, covering inputs, processes and outputs;
  - Establishing control objectives;
  - Identifying risks; and
  - Identifying controls.

- Evaluating controls against risks;
- Testing the operation of the controls to establish whether they can be relied upon;
- Arriving at conclusions ï by assessing what has been discovered during evaluation and testing to form an opinion on the reliability and adequacy of internal control.

Compliance Audit

An alternative approach to Systems Based Audit is Compliance Audit. It is frequently adopted by external audit and is available to the internal auditor where he/she feels it is appropriate.

The main objective of Compliance Audit is to confirm the accuracy and correctness of the records and assets of the organisation and to ensure compliance with all relevant statutes and regulations. It usually involves large sample sizes in order to comply with the auditorsó standard on appropriateness of evidence and may incur a large commitment of auditor time. A compliance audit will normally involve the following stages:

- Identifying all accounting records;
- Selecting audit objectives;
- Designing tests to substantiate records; and

- Arriving at conclusions and an opinion.

Some examples of where compliance audit can be used are where:

- There are limitations on the internal control procedures which have been designed into the system;
- The auditor assesses a very high control risk and therefore reliance cannot be placed on just carrying out limited tests of the controls in the system; and
- It is considered to be more cost effective, for example in the case of small systems where it may not be appropriate to spend lots of time documenting systems.

Performance Audit

Performance audit ï also referred to as Value for Money Audits (VFM), Management Audit or Operational Audit ï is the assessment of whether public resources are used in a way which achieves the organisationós objectives in an economical, efficient and effective manner.

It is an objective and systematic examination of evidence in order to provide an independent assessment of the performance of a government organisation, program, activity, or other function. It is intended to provide information to improve public accountability and facilitate decision-making by those responsible for overseeing or initiating corrective action.

Performance audits can be very complex and should not be done by inexperienced audit staff. It is unlikely that any will be done in the first two years of setting up an IA unit.

The benefits of performance audits include:

- Improving specification of the goals of policies and the ways of achieving particular policies;
- Improvement of the impact of programs and policies;
- Increasing outputs;
- Minimisation of costs and growth of revenues or benefits;
- Improvement of management performance, the level of internal control and the level of accountability;
- Provision of an independent overview of the area/results/impact;
- Development of assessment criteria for use in planning and managing future programs and activities;
- Drawing the attention of management to a problematic area; and
- The ability to identify best practice in one part of an organisation and adopt it in other relevant areas.

Therefore, performance audit frequently puts emphasis upon auditing control and information systems that support the production of data relating to the objectives, impacts and resources of a specific policy.

Performance audits ï are concerned with the soundness of management policies and practices with respect to the Economy, Efficiency, and Effectiveness of the operations.

Economy is obtaining supplies and services of an appropriate quality at the best possible price.

Efficiency is using those supplies and services in the most effective way to achieve the required result or output.

Effectiveness is an assessment of the extent to which the actual outputs of each system or program meet the desired objectives and achieve the intended impact.

Performance audit differs in emphasis from systems audit. Systems audit involves an assessment of the systems of control established by management, but tend to focus more upon the adequacy of those controls. Unlike performance audits they do not normally attempt to evaluate the results and outputs of the system under review. Some typical controls with which performance audits are concerned are:

- Planning (including setting objectives);
- Management information;
- Performance measures and indicators;
- Policy performance; and
- Evaluation and suitable control over costs.

In certain circumstances, specific performance audits may be conducted at the request of management, or if a systems audit indicates that a more detailed performance review is required to evaluate the outputs of a specific system. Such audits could involve investigating signs of possible waste; the effect of important projects or the efficient conduct of standard managerial operations. Performance audits typically involve:

- Establishing clearly the area for review;
- Using all available sources, both internal and external;
- Establishing the true scale and scope of the function or activity to be reviewed;
- Comparing levels of spending and activity over time and against available comparable organisations within the public sector, and where relevant outside it (benchmarking); and
- Being prepared to question what is being done and why? And being willing to identify and consider alternative approaches; and

Recommending alternative approaches and establishing the costs and benefits associated with them. The term Performance Audit also includes **Program Audits** which focus on determining:

- The extent to which the desired results or benefits established by the organisation are being achieved;
- The effectiveness of the organisationós programs, activities, or functions; and
- Whether the organisation has complied with significant laws and regulations applicable to the program.

Program audits may, for example

- Assess whether the objectives of a new, or ongoing program are proper, suitable, or relevant;
- Determine the extent to which a program achieves a desired level of program results;
- Assess the effectiveness of the program and/or of individual program components;
- Identify factors inhibiting satisfactory performance;
- Determine whether management has considered alternatives for carrying out the program that might yield desired results more effectively or at a lower cost;
- Determine whether the program complements, duplicates, overlaps, or conflicts with other related programs;
- Identify ways of making programs work better;
- Assess compliance with laws and regulations applicable to the program;
- Assess the adequacy of the management control system for measuring, reporting, and monitoring a programós effectiveness; and
- Determine whether management has reported measures of program effectiveness that are valid and reliable.

An example of a program audit would be a review of the system for administering and distributing aid to local communities i.e. BISP.

Financial Audit

In internal audit financial audit is normally limited to evaluating the financial systems of an organisation. The internal auditorsó primary interest is not the accounting reports and figures as such, but rather the controls which ensure the quality and accuracy of accounting information and of financial reporting.

Financial audits include:

- *The audit of financial and accounting statements and reports* which are intended to provide reasonable assurance about whether the financial statements of an organisation present fairly the financial position, results of operations, and cash flows and that they have been prepared in accordance with generally accepted accounting principles; and
- *Financial related* audits which include determining whether: (i) financial information is presented in accordance with established or stated criteria, (ii) the organisation has adhered to specific financial compliance requirements, or (iii) the internal control structure relating to financial reporting and/or safeguarding assets is suitably designed and has been implemented in an appropriate and effective way.

Financial related audits may, for example, include audits of the following items:

- Segments of financial statements; financial information (for example,

statement of revenue and expenses, statement of cash receipts and disbursements, statement of fixed assets); budget requests; and variances between estimated and actual financial performance;
- Internal controls over compliance with laws and regulations, such as those governing bidding for, accounting for, and reporting on grants;
- Internal controls over financial reporting and/or safeguarding assets, including controls using computer-based systems;
- Compliance with laws and regulations; and
- Allegations of fraud

Information Technology Audit

Information Technology (IT) Audit is the application of auditing skills to the technological aspects of business processes. It embraces the independent review and testing of practices and procedures related to:

- The secure provision of business processing;
- The processes for planning and organising IT, and developing and acquiring new systems and facilities; and
- The economy, efficiency, and effectiveness of the use and exploitation of Information Technology facilities.

All auditors are expected to be familiar with the basic concepts of internal control as applied to Information and Communication Technology (ICT) business systems and processes within the organisation. The audit of controls in such systems will normally form part of the standard systems audit. However, the increasing complexity and diversity in the application of technology means that more specialised IT skills will be needed for the review of specific activities.

IT Auditors provide advice and support to other auditors in respect of:

- *IT strategies, planning, organisation and policies.* This involves:
  - Helping to provide an overview of IT systems and identify areas of greatest risk;
  - Testing the effectiveness of the segregation of duties and authority within the IT domain; and
  - Examining the procedures relating to ICT developments (projects, quality assurance etc).

- *Systems development controls*
  Internal Audit should be able to advise on controls at the earliest possible stage in the systems development process. In this way controls can be installed more easily and at lower cost.

Ideally IT auditors should have the opportunity to input ï through their comments on documents submitted to them or by discussing the proposed process ï at each stage of the development process, including:
  - Determining the need for the system development;
  - Establishing the objectives for the new system;
  - Consideration of alternative approaches to the development;
  - Organising and controlling the development process;
  - The systems implementation phase; and
  - Post-implementation evaluation.

- *Applications (or business systems) controls*

In order to examine, test and evaluate computerised controls in live systems, and the technical documentation supporting computerised elements of systems, it is necessary to carry out application control audits. These audits involve:

- Operations Testing ï which means examining whether the application provides expected outputs in relation to standard inputs. Standard test files may be used to test the operation of all parts of the system after each change in the system is implemented. Regular automated testing can speed up the implementation of new versions.
- Security Tests ï involve examining the actual access rights and how these are built into the working of the application (data reading and writing, user administration, administrator rights to new installations etc). Security testing also deals with the existing application outputs while examining whether sensitive data are not passed on to less secure systems.

The audit planning process should take account of the need for an integrated approach which addresses both computer and user controls, and the potential for using computer assisted audit techniques to enable testing of large quantities of data.

- *ICT Environmental controls*
- This involves assessing the extent to which controls over resource management, technical support, business continuity/disaster recovery and security are adequate and effective

- *Infrastructure controls*
- This focuses on the security, integrity and availability of the infrastructure, including the network, servers and internet access. Auditors may focus, for example, on the configuration changes in individual ICT items, and on whether the changes have a significant impact on the security or operation of the entire system.

- *Locally-developed systems controls*
- Systems developed by individual departments and sections may pose risks to the organisation, e.g. they may give rise to poor security or involve improper use of software. These systems are often not subject to independent testing and as such they are more susceptible to operation errors.

- *Contracted services controls*
  Contracted services must be monitored and assessed for performance. Valid contracts must include a provision stipulating the quality of service required. Procurement relating to particularly complex systems and services can be a high-risk area, since often there is a great dependency on a single supplier.

10. MECHANISM FOR SETTLEMENT OF INTERNAL AUDIT PARAS

The Audit Committee meeting held on March 04,2019 has approved the mechanism of Settlement of Internal Audit Paras. Audit Committee approved the following three compositions of Departmental Accounts Committee (DAC) for settlement of Internal Audit Paras:

- **(In-House DAC Meeting-I)**
- If replies from the concerned wing/Field DG office received within 3 weeks of issuance of IA report , Composition of the DAC is as follows :

DG (concerned)	Chairman
DG (IA)	Member
Director (Internal Audit)	Secretary

- **(In-House DAC Meeting-II)**
- If replies from the concerned wing/Field DG office not received within 3 weeks of issuance of IA report, reference will be sent by DG IA to the Principal Accounting Officer (PAO)/Secretary .Composition of the DAC in this case would be as :

PAO/DG (Concerned)	Chairman
DG (IA)	Member
Director (Internal Audit)	Secretary

- **Pre-Audit Committee Meeting**

The unsettled/pending paras discussed during In House DAC meetings will be submitted to the Pre-Audit Committee meeting as per composition appended below:

PAO	Chairman
DG (Concerned)	Member
DG (IA)	Member
Director (IA)	Secretary

- The minutes of the meetings will be recorded by the Director (IA)/IA Wing for onward submission to the DG(IA) for approval/finalization in each case.
- DG(IA) will inform Audit Committee of the settled paras in In House DAC.
- DG(IA) will present unsettled audit observations to the Audit Committee for decision.
- DG(Concerned) will defend/elaborate management action in Audit Committee meeting

Appendix A

Glossary of Terms

This glossary gives a brief description of significant terms used by internal auditors.

Assurance
The Head of Internal Auditós professional opinion on the adequacy, effectiveness, and reliability of the departmentós internal control system.

Audit cycle
The length of time over which all systems in the agreed audit needs assessment will be audited.

Audit evidence
The information obtained by internal auditors to arrive at and to support their findings and recommendations.

Audit needs assessment
An assessment of the systems covering the whole range of the organisationós activities, their relative importance; the frequency with which each should be audited and the resources required to do so.

Audit work plan
A detailed plan that sets out the direction and control of an individual audit assignment.

Benchmarking
Is a process whereby one organisation is able to compare its performance with that of one or more other organisations, in order to establish comparative measures of performance.

Compliance testing
Testing designed to establish whether the controls established by management are operating as intended and are effective.

Control environment
Sets the tone of an organization. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

Control objectives
The objectives of control, derived from the management objectives of the system, used by the auditor as criteria against which to appraise the adequacy of internal controls.

Controls
Individual actions, procedures or operations taken or put in place by management in order to ensure that activities and procedures achieve their objectives.

Current audit file
A file of audit documents put together during the course of a specific audit.

Detective control
A control designed to detect error, irregularity, inefficiency, or other failure to meet managementós objectives.

Directive control
A control designed to detect and correct inefficiencies, errors, or irregularities. They normally operate after an event has occurred or an output has been produced.

Due professional care
The standard of competence and diligence internal auditors should exercise in carrying out their duties.

Economy
Is obtaining supplies and services of an appropriate quality at the best possible price.

Efficiency
Is the use of supplies and services in the most effective way in order to achieve the required result or output.

Effectiveness
Is an assessment of the extent to which the actual outputs of the organisation/activity meet the desired objectives and achieve the intended impact.

Exposure
The product of risk and materiality, where these can be quantified.

External auditor
An auditor whose main function is to give an opinion on financial statements in related to a specified time period.

Flowcharting
A diagrammatic method of recording and describing a system which can show the flow of documents, information or processes and the related controls within that system.

Framework of control
A description of the range of controls present within an organisation, usually including classification of controls and other control measures.

Frequency of audits
The number of times an audit should be undertaken within the audit period.

Interim review
A limited audit examination of a system previously subject to a full systems audit.

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

Internal control
A process carried out by management and other personnel designed to ensure that objectives are achieved. Further guidance on Internal Control is given in Appendix B.

Internal control questionnaire
A list of questions, related to control objectives, used by internal auditors to assist in the evaluation of internal control.

Internal control system
The whole network of systems established in an organisation to ensure that its objectives are achieved and in the most economic and efficient manner.

Judgment sampling
Selection, based on the auditor's experience, knowledge and understanding of the system, of a sample of items for audit testing that are representative or that will yield relevant audit evidence.

Materiality
The significance of undesirable events, which are identified, or which may occur. Applied to systems it reflects the significance of a failure to achieve management objectives.

Objectives
Statements of what is planned to be achieved.

Output measure
A directly quantifiable means of assessing what is produced or achieved.

Performance indicator
This is an indirect measure of the extent to which effectiveness, efficiency and economy, quality and service levels have been achieved in an activity or function. Normally used where direct measures are not available.

Performance measure
This is a directly quantifiable means of assessing the extent to which effectiveness, efficiency and economy, quality and service levels have been achieved.

Performance audit approach
The assessment of whether public resources are used for fulfilment of the objectives of the organisation in an economical, efficient and effective manner. It encompasses the audit of the economy, efficiency and effectiveness of a system, service or activity (also known as value for money auditing), and program audit.

Permanent audit file
A file of audit documents, relating to the audit of a particular system or group of related systems, that provide ongoing and live information that is likely to be of continuing relevance to future audits.

Preventive control
A control designed to prevent error, irregularity or inefficiency.

Priority of audits
The extent to which an audit assignment needs to be undertaken earlier rather than later in the audit programme.

Quality assurance
A combination of internal and external reviews to provide reasonable evidence that audit work conforms to the standards and best practices defined in Internal Audit Methodology.

Re-performance test
An audit test which functions by re-processing a transaction or re-performing a procedure to compare the auditor's result with that already achieved.

Risk elements
The factors to be quantified in determining risk and materiality in audit planning.

Risk index
A method of combining risk elements in determining the relative risks and materiality associated with systems in audit planning.

Statistical sampling
Methods of sampling whole populations so that conclusions may be drawn about all the items which make up those, to particular levels of confidence (certainty).

Compliance testing
Testing of transactions and other data to enable a conclusion to be reached on the completeness, accuracy and validity of data tested and on the effect of weaknesses in internal control.

System
A series of related activities designed to operate together to achieve a planned objective.

Systems based audit approach
The structured analysis and evaluation of the internal controls of a system, process or area of activity in relation to appropriate control objectives.

Verification
Checking the accuracy, completeness and validity of information and records by comparing the stated position with actual conditions or with independent records to establish consistency.

Vouching
Checking a transaction with supporting documentation.

Walk through testing
A preliminary examination of a system to confirm the auditorís understanding of the way it functions; sometimes called cradle to grave testing.

Appendix B

WHAT IS INTERNAL CONTROL?

Definitions

The most widely accepted definition of "internal control" is that developed by COSO (Committee of Sponsoring Organisations of the Tread way Commission). This states that:

> "Internal control is broadly defined as a process effected by management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following overlapping categories:
>
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations".

The COSO control framework identifies five interrelated control categories that together provide effective internal control:

- **Control Environment** - The core of any organisation is its people. Their individual attributes of integrity, ethics and competence and the environment in which they operate determine the success of the operation.

- **Risk Assessment** - Organisations must be aware of, and deal with, the risks that they face. They must set objectives that integrate key activities. They must also establish mechanisms to identify, analyze and manage the related risks.

- **Control Activities** - Control policies and procedures must be established and executed to help ensure that actions necessary to achieve the university objectives are effectively carried out.

- **Information and Communication** - Surrounding the control activities are information and communication systems. These enable the organisation's people to capture and exchange the information needed to conduct, manage and control its operations.

- **Monitoring** - The entire process must be monitored and modified as necessary. Thus, the system can react dynamically to changing conditions.

Within the GOP, AGP has provided a definition of internal control in the public sector – usually referred to as Project to Improve Financial Reporting and Auditing (PIFRA) – as follows:

> "The overall financial control system performed internally by a Government or by its delegated organisations, aiming to ensure that the financial management and control of its national budget spending centres (including foreign funds) complies with the

relevant legislation, budget descriptions, and the principles of sound financial management, transparency, efficiency, effectiveness and economy.

Internal auditors and internal control

When auditors are considering the adequacy of the systems of internal control there are a number of things they have to keep in mind.

First, it is important to remember that an effective system of internal control should have the following characteristics:

- Establishment of standards;
- Measurement of actual performance;
- Analysis and comparison of actual results to standards;
- Implementation of a program of corrective actions; and
- Review and revision of the standards.

Second, controls should be economical in time and money and should measure performance in relation to the planned result. Controls should also be timely and easily understood by the people using them. Good controls will reflect the goals of the audited organisation, indicate when the goals are not being achieved and measure the critical items - those that have the most impact on achieving goals.

Third, the risk of failure and the potential effect of not achieving objectives must be considered, along with the cost of establishing the control. Excessive control is costly and counterproductive. Too little control presents undue risk and there should be a conscious effort made to strike an appropriate balance.

Finally, internal audit is concerned not only with internal control in the critical financial systems, but also the entire range of managerial and operational systems in the organisation being audited.