Audit and Assurance Arrangements
publicjobs

Prepared by: Catherine Dobbins, April 2016
Reviewed by: Catherine Dobbins - Annual Review Conducted May 2024
Approved by: Management Board: 15th May 2024
publicjobs Board Meeting: 24th June 2024
Audit Committee Meeting: 20th June 2024

Content

Audit and Assurance Arrangements

We, at publicjobs have a number of audit and other arrangements in place which, together, provide assurance that the organisation is managing its resources properly and that it is actively assessing and managing risk. This is an accompanying document to the Corporate Governance Framework.

Role of Audit Committee and reporting arrangements to the Chief Executive

The organisation has an Audit Committee which operates in accordance with published Civil Service guidance. The Committee has an independent role in the provision of assurance to and from the Chief Executive. This includes consideration of the adequacy and effectiveness of the internal control systems (through the findings from the programme of audits), overseeing the work of the Internal Audit Unit, and providing advice and guidance in relation to the development of the Unit. The Audit Committee has a purely oversight role in terms of the risk management framework (including systems and processes) and has no role in relation to the identification and management of individual risks. The Committee may provide challenge in relation to the systems and processes in order to provide a level of assurance and advice to the Accounting Officer in line with their responsibilities under the Audit Committee Charter.

The Audit Committee operates under a written charter. The Chairperson of the Audit Committee, and all Committee Members, are external to the organisation, and the Committee has appropriate expertise.

The Audit Committee prepares an annual report to the Accounting Officer, reviewing its operations, and invites the Office of the Comptroller and Auditor General, as the external auditor, to meet with it at least once a year.

The Internal Audit function

The majority of the Internal Audit function's reviews are outsourced to a professional services firm. The function operates to a three-year audit plan approved by the Chief Executive and under the oversight of the Audit Committee.

All draft audit reports are submitted to appropriate members of the Management Board for the preparation of management responses. Once finalised, the completion of any actions arising is tracked and monitored via regular reports by management to the Audit Committee.

The Head of Corporate Services is also a member of the Civil Service "Heads of Internal Audit Forum" which provides a forum for the discussion of policy and operational issues relating to internal audit within civil service bodies as well as disseminating good practice and new developments within the internal audit profession.

Risk Management

The organisation has a risk management system in place. This includes a Risk Management Framework and Risk Management Policy appropriate to the size and scale of the organisation and is in accordance with the relevant Civil Service Risk Management Guidance. An integrated and holistic approach to risk management is one of the key elements to achieving effective corporate governance. The organisation takes its risk management responsibilities seriously and has processes in place to respond appropriately to significant business, strategic, operational, financial, compliance and other risks that threaten the successful achievement of the strategic and operational objectives of the organisation.

A Risk Management Committee oversees the implementation and monitoring of this process. This committee operates under the terms specified in the Risk Management Strategy and Policy outlined later in this document. The Committee (through the Chair) reports to the Audit Committee at each meeting, and updates on current risks facing the organisation are given to the Board at each meeting. The Committee (through the Chair) report to the Management Board and the Accounting Officer following each meeting of the Risk Management Committee. The Committee is a designated sub-group of the Management Board, and also contains functional expertise and representation.

Internal Audit Charter

Introduction

This Charter sets out the purpose, authority and responsibilities of the Internal Audit function in publicjobs.

Internal Audit Function

In accordance with the recommendations of the Accountability of Secretaries General and Accounting Officers, publicjobs is committed to maintaining and supporting a quality internal audit function.

The Internal Audit function will conduct its activities in accordance with the Internal Audit Standards issued by the Department of Public Expenditure, NDP Delivery and Reform and will have regard to best practice as enunciated by the Institute of Internal Auditors.

publicjobs will as necessary retain the services of an independent and suitably qualified Audit Provider.

The Internal Audit function ensures that an appropriate contract is put in place for outsourced internal audits and ensures that the contract terms are met and that the audits are conducted to a high standard.

Role and Responsibilities

The primary role of Internal Audit within the Office is to give assurance to the Accounting Officer and the Audit Committee as to the adequacy and effectiveness of the office's internal control system and the risk management environment.

Responsibility for internal control, including the prevention and detection of fraud and risk management, rests fully with line managers who, notwithstanding audit activity, ensure that appropriate and adequate arrangements exist within their area of responsibility.

Responsibility for implementation of audit recommendations also rests fully with the line management concerned.

Scope

The Internal Audit function will review and appraise the following:

(a) The adequacy, reliability and integrity of the information being provided for decision making and for accountability, and the extent to which this information is used;

(b) The degree of compliance with legislation (domestic and international) and other requirements laid down centrally (i.e. Department of Public Expenditure, NDP Delivery and Reform) and management plans, procedures and policies;

(c) The acquisition and disposal of assets and the safeguarding of assets and interests from losses, including those arising from fraud, malpractice and irregularity;

(d) Arrangements for the economic and efficient use of resources within the area under review.

In discharging this responsibility Internal Audit will also identify and report on any deficiency or weakness in systems and controls and make appropriate recommendations for improvement.

The Internal Audit Function will ensure that all information and records are treated in the strictest confidence throughout the Audit process. The Internal Auditor is responsible for ensuring the confidentiality and safekeeping of all records and information accessed in the course of its work.

Authority

The Internal Audit function derives its authority from the Accounting Officer.

In order to perform its functions, internal audit staff are authorised by the Accounting Officer to have full, free and unrestricted access to all the Office's records, assets and personnel at

all reasonable times, and are entitled to request and receive all the information and explanations they require for the proper performance of their duties.

Independence

To ensure the independence and objectivity of the Internal Audit function, the function will not assume operating responsibilities for, and will remain independent of, the activities it audits. This is to provide it with an environment in which it can make unbiased judgements and provide impartial advice to management. In publicjobs this independence is achieved by using an outsourced internal audit provider who carries out audits on the basis of a Strategic Audit Plan approved by the Audit Committee (the membership of which is entirely external to the organisation). If any audits are to be conducted by the internal quality audit function, these will only be conducted on areas not within the remit of the Head of Corporate Services (who also has responsibility for Internal Audit).

Internal Audit Universe

The internal audit unit has the right to review all the management and control systems, both financial and operational. The internal audit unit has unrestricted access to all functional areas, records (both manual and electronic), property and personnel in the performance of its audits.

Audit Methodology

The internal audit function will produce a three-year audit work plan for all areas under its remit. The plan will be approved, and executed, by the Audit Committee.

In the course of each audit the Internal Audit function/outsourced Internal Auditor will:

- work constructively with management and staff
- give adequate notice to the Head of Sections prior to the commencement of an audit
- determine and confirm system to be audited with line management

- discuss progress with the relevant line manager and liaise with the Head of Corporate Services throughout the audit process
- issue a draft report to the relevant line manager to confirm its factual accuracy and to agree where possible the conclusions and recommendations for improvements
- agree a timescale for managements' response
- issue the report, incorporating managements' response to the relevant line manager, relevant Head of Section and Head of Corporate Services
- issue the report to Accounting Officer
- present the final report to Audit Committee
- circulate the final report to Management Board.

The final reports will also issue to the Comptroller and Auditor General as requested.

Follow-up reports will be carried out within a timescale to be determined by the Audit Committee. Summary follow-up reviews will issue to the Audit Committee informing them of any instances where audit recommendations have not been implemented as agreed.

Where Internal Audit and management fail to reach agreement on issues/recommendations considered to be of material importance by Internal Audit, the final audit report will reflect the position of both. The Audit Committee's attention will be drawn specifically to these issues/recommendations, so that appropriate action can be taken.

Audit Committee Charter and Terms of Reference

PURPOSE

The Audit Committee is part of the control environment, tasked with providing independent advice to the Accounting Officer regarding the suitability and robustness of the organisation's internal control

systems and procedures, including the operation and development of the internal audit function and the relationship with external audit.

The Audit Committee is not responsible for any executive function and it is not vested with any executive power.

AUTHORITY

- The Audit Committee is appointed to provide independent advice to the Accounting Officer and is responsible to him/her for its performance in this regard.
- The Audit Committee shall have the authority to investigate any matters within its terms of reference (the Audit Committee's role in relation to risk is described in the review paper of May 2024, agreed at the meeting in June 2024); the resources, and outside professional advice, it needs to do so and full access to information.
- The Audit Committee Charter is agreed between the Accounting Officer and the Audit Committee.
- The Audit Committee shall be fully briefed and kept up-to-date on any significant matter relating to their role and duties.

MEMBERSHIP

- The Accounting Officer will appoint members and the Chairperson, unless otherwise provided by law.
- The Chairperson of the Committee will come from outside the organisation and has right of access to the Accounting Officer.
- All members of the Committee will be external to the organisation.
- At least one member of the Committee will be a nominee of the Board.
- The Committee will collectively possess an appropriate range of skills to perform its function to the required standard. At least one member will have relevant financial experience and other members will have experience relevant to the Audit Committee, including: risk management; internal audit; governance; an understanding of the public sector

environment, in particular accountability structures and current public sector reform initiatives.

- Members should have, or should acquire as soon as possible after appointment, an understanding of:
    - Organisational culture, objectives and challenges
    - Organisational structure, including key relationships
    - Relevant legislation or other rules governing the organisation.
- The role requirements will be clearly communicated to potential members at the outset including time commitments and an indication of frequency of meetings.
- Members may serve a three-year term, with the option to extend by a further three-year term.
- A statement of members' interests will be prepared on an annual basis.
- Where a conflict of interest arises in the course of the work of the Audit Committee, the member will bring this to the attention of the Chairperson and, where necessary, leave the room for the duration of the discussion and not take part in any decisions relating to the discussion. A note to this effect will be included in the minutes of the meeting. Declarations of conflicts of interest is a standing item on all Committee meeting agendas.

INDUCTION AND ONGOING TRAINING

All new members will complete an Induction Process. This will include briefings on key areas including:

- Organisational objectives, culture and challenges
- Organisational structure, including key relationships
- Relevant legislation and governance arrangements
- Risk Management Framework
- Performance Reporting

All new members will receive an Induction Pack, containing key governance material, including the Governance Framework, related Legislation, the Audit and Assurance Arrangements, the Corporate Strategy, the Customer Action Plan, and the Corporate Risk Register.

Where the Committee deems training is required, the organisation will support members in attending training related to their functions as members of the Committee. The organisation is a member of the

IPA Governance Forum, and as part of this will offer ongoing learning and development opportunities to Committee Members.

MEETINGS

- To facilitate regular engagement with the organisation, the Audit Committee will meet at least quarterly, with the authority to convene additional meetings as circumstances require.
- All Committee members are expected to attend each meeting. Each member must meet the minimum attendance of 75% at Audit Committee meetings. A quorum shall consist of three Committee members, and in the absence of the Chairperson, a deputy Chairperson will be chosen from members and will chair the meeting.
- If a vote is required on any issue, a simple majority of all members present, including the Chairperson, will carry the motion, with the Chairperson having the casting vote in the event of a tie.
- Each member should take personal responsibility to declare any potential conflicts of interest arising in relation to any items on the agenda for the meeting.
- The Audit Committee should invite members of management, internal auditors or others to attend meetings and provide information, as necessary.
- The Chairperson of the Audit Committee will meet with the Accounting Officer twice annually.
- The Chairperson will meet with the Chair of the Risk Management Committee twice annually.
- The Committee should ensure that it communicates effectively with the Board (through the Board nominee on the Audit Committee), the Head of Internal Audit, the external auditor and other stakeholders.
- Any internal audit or audit items that relate to the Board's areas of responsibilities should be communicated to the Board as soon as they are identified (through the Board nominee on the Audit Committee).
- The agenda and supporting papers shall be circulated to all members at least one week prior to the meeting.
- The agenda of the Audit Committee will be approved by the Chairperson and each Member of the Committee shall be entitled to put forward matters for inclusion on the agenda.

- Draft minutes will be prepared and once approved by the Audit Committee, will be circulated to the Accounting Officer and Management Team with the aim of circulating them within ten working days after the date of the meeting.
- The Head of Corporate Services (with responsibility for Internal Audit, Risk Management and Finance) shall normally attend meetings. In addition, such persons as are from time to time invited by the Chairperson to attend may attend.
- The Internal Auditor will attend the relevant portion of meetings required to present any audit report prepared by them.
- Appropriate records of the work of the Audit Committee will be maintained.
- The Committee will make minutes of Audit Committee meetings available to the Board in the Board papers for the following Board meeting.
- The Internal Audit support unit (which is part of the Corporate Services division) will provide administrative support to the Audit Committee.

ACCESS

- The Chairperson of the Audit Committee shall have a right of access to the CEO on any matter pertaining to the internal audit function as the Committee considers appropriate or necessary, including its overall effectiveness, resources, training, use of technology etc.
- The Audit Committee shall have a right of access to such information or documents, which, in the Committee's opinion are relevant to matters falling within its terms of reference.

FUNCTIONS

The Audit Committee will carry out the following functions:

Internal Control

- Advise on the organisation's internal control systems, including information technology security and control.
- Obtain and review internal audit reports, significant findings and recommendations together with management responses.

- Monitor management's implementation of audit recommendations from internal audit, external audit and other sources.

Governance and Risk Management

Advise on the systems of control underlying the risk management framework and processes, through:

-receiving feedback from the Chair of the Risk Management Committee, the internal auditor, external auditor and the organisation's management on the effectiveness of the risk management process;

-taking such feedback into account for input into the priorities of the Internal Audit Unit work programme, including identifying the need for value for money audits.

-Reviewing and endorsing the Risk Management Framework annually.

The Audit Committee has a purely oversight role in terms of the risk management framework (including systems and processes) and has no role in relation to the identification and management of individual risks. The Committee may provide challenge in relation to the systems and processes in order to provide a level of assurance and advice to the Accounting Officer in line with their responsibilities under this Charter.

Internal Audit

- Review assessments of the internal audit function, including compliance with the Internal Audit Standards; evaluation of conformance with the IIA Standards 1300 (the results of which will be communicated to the Accounting Officer and Audit Committee) will be conducted every three to five years.
- Review with the Head of Corporate Services (with responsibility for Internal Audit and Finance) and as necessary discuss with management, the Internal Audit Unit's charter, audit plans, activities, staffing, and organisational status.
- Receive progress reports on the audit plan assignments.
- Raise any concerns with Accounting Officer regarding the independence of the Internal Audit unit.

- On a regular basis, meet separately with the Head of Corporate Services (with responsibility for Internal Audit, Risk Management and Finance) to discuss any matters that the Audit Committee or Internal Audit Unit believes should be discussed privately.

External Audit

- On at least an annual basis, meet with the nominee of the Comptroller and Auditor General.
- Review the Internal Audit working relationship and liaison with the nominee of the Comptroller and Auditor General to ensure co-operation, avoidance of duplication and potential gaps in audit coverage.
- Review the external audit management letter and the organisational response.

Financial Management

Advise on the systems of control underlying the financial management processes, including:

- reviewing the results of the external audit; and
- reviewing the framework associated with financial management and budgeting.

Reporting Functions

- Regularly report to the Accounting Officer about Audit Committee activities, issues, and related recommendations by:
  - circulating to the Accounting Officer and the Management Board the agreed minutes of Audit Committee meetings as a matter of normal practice;
  - submitting an annual report to the Accounting Officer, within three months following year end, of the activities of the Audit Committee;
  - providing the Minutes of the Audit Committee to the Board and attendance by the Chairperson at two meetings of the Board annually); and
  - availing of the Chairperson's right of access to the Accounting Officer.
- Providing an open avenue of communication between internal audit, the Office of the Comptroller and Auditor General, and the Accounting Officer.

Other Functions

- Through a programme of financial and other related audits, promote good accounting practices, ensuring better and more informed decision making and improved focus on value for money throughout the organisation.
- Perform other activities related to the charter as requested by the Accounting Officer.
- Review and assess the adequacy of the written charter on an annual basis and request Accounting Officer approval for proposed changes.
- Respond to any special reporting requests, on matters relevant to the Committee, made by the Chief Executive Officer.
- The Audit Committee may, following consultation with the CEO, obtain outside legal or other independent professional advice and secure the attendance at Committee meetings of outsiders with relevant experience and expertise if it considers this to be essential.
- Confirm annually that all functions outlined in the written charter have been carried out.
- The Audit Committee evaluates its own performance on a regular basis.

ANNUAL REPORT

An annual report reviewing the Audit Committee's operations should be prepared for the Accounting Officer and submitted within three months following year end. This report will include an assessment on the work of the Internal Audit Unit, the supports provided to the Audit Committee and a self-assessment of the Audit Committee's own effectiveness. The annual report will also include confirmation that a review of this written charter has been completed on an annual basis and that all functions outlined in the written charter have been carried out. The Audit Committee will follow up on any recommendations from the Accounting Officer arising from this report, or in the course of other interactions.

PROTECTED DISCLOSURES

The role of the Audit Committee in relation to protected disclosures is agreed with the Accounting Officer, in line with organisational policy and any relevant guidelines. Board Members may report their concerns to the CEO, with escalation channels to the Chairperson of the Board or the Chair of the Audit Committee. No investigation of the suspected fraud should take place until the Head of Corporate Services and/or CEO has been informed. If the case involves /both of these individuals, the Chairperson

of the Audit Committee should be informed. Full details of the relevant investigation process are set out in the Fraud Policy and the Protected Disclosures Policy.

Quality Assurance and Improvement Programme

Introduction

Internal Audit's Quality Assurance Improvement Programme (QAIP) is designed to provide reasonable assurance to the various stakeholders (the Audit Committee, Senior Management, the Board, the Comptroller and Auditor, etc.) that Internal Audit:

- Conforms to the definition of internal auditing, IIA standards 1300 and any central policy guidance;
- Has an adequate internal audit charter, goals, objectives, policies and procedures;
- Contributes to the organisation's governance, risk management and control processes;
- Has complete coverage of the audit universe;
- Complies with applicable laws, regulations and other standards that the internal audit activity may be subject to;
- Has identified the risks affecting the operation of the internal audit activity itself;
- Has an effective continuous improvement activity in place and adopts best practice; and
- Adds value to improve the organisations operations and contributes the attainment of the organisation's objectives.

The Head of Corporate Services is ultimately responsible for the QAIP, which covers all types of Internal Audit activities, including outsourced internal audits. The QAIP includes both internal and external assessments. Internal assessments are both ongoing and periodical and external assessments will be undertaken at least once every three to five years.

The QAIP is reviewed on an annual basis.

Internal Assessments

Internal Assessments are made up of both ongoing reviews and periodic reviews.

Ongoing reviews

Ongoing reviews provide assurance that the processes in place are working effectively to ensure that quality is delivered on an audit by audit basis. This includes continuous monitoring of:

- Engagement planning and supervision (preapproval of the audit scope, innovative best practices, budgeted hours, and assigned staff with key performance indicators set for each audit);
- Standard working practices (including working paper procedures, sign off, report review, checklists to ensure that the audit process has been followed);
- Feedback from stakeholders on quality at audit level; and
- Analysing performance metrics to measure audit plan completion and stakeholder value.

Periodic reviews

Periodic assessments are designed to assess conformance with Internal Audit's Charter, the IIA Standards, the quality of the audit work, policies and procedures supporting the internal audit activity, the added value to the organisation and the achievement of performance standards.

Periodic assessments will be conducted through an annual review of:

- Working paper reviews for conformance to IIA Standards, and internal audit policies and procedures;
- Internal audit performance measures including implementation of the Strategic Audit Plan;
- Assessment of quality at internal audit activity level;
- Implementation of recommendations made during that year (based on an assessment of the implementation of all recommendations);
- Annual review of all relevant Charters, Policies and Procedures.

The periodic self-assessment should identify the quality of ongoing performance and opportunities for improvement. The self-assessment will be completed on an annual basis in conjunction with the development of the Annual Report for the Audit Committee.

External Assessment

The External Assessment will consist of a broad scope of coverage that includes the following:

- Conformance with the IIA Standards, definition of Internal Auditing, and internal audit's Charter, plans, policies, procedures, practices, and any applicable legislative and regulatory requirements;
- Expectations of Internal Audit as expressed by the Board and Senior Management;

- Integration of the Internal Audit activity into the governance process;
- The mix of staff knowledge, experiences, and disciplines, including use of tools and techniques, and process improvements;
- A determination as to whether Internal Audit adds value and improves operations.

An external assessment will be conducted every three to five years by a qualified, independent assessor from outside the organisation. The assessment will be in the form of a full external assessment. The format of the external assessment will be agreed with the Audit Committee, Head of Corporate Services and the CEO.

Awareness Raising

Annual awareness raising will be conducted into the area of corporate compliance for all managers and staff (including internal audit, risk management and CPSA compliance); this will take place as part of Risky Business Month.

Risk Management Strategy and Policy

Introduction

In order to look ahead and meet the demands from stakeholders, the organisation needs to constantly adapt and consider the way in which it operates. Change inevitably involves taking risks. Understanding all of our risks will enable us to take informed and better decisions and ultimately create increased added value for stakeholders.

This Risk Management Strategy and Framework presents the organisation's approach to risk management. This document has been approved by the CEO. The purpose of this document is to:

- Summarise the approach to risk management.
- Outline the responsibilities for risk management within the organisation for the following:
  - Board
  - Management Board
  - Chief Executive Officer
  - Heads of Function
  - Functions
  - Risk Management Committee
  - Audit Committee
  - Risk Officer
  - Risk and Action Owner
  - Staff
  - Internal Audit

This document has been designed to assist the organisation to identify, mitigate and report on the key risks that will prevent the organisation from achieving its objectives as outlined in the business plan. Responsibility for the Identification, mitigation and reporting of risks will initially reside with the Risk Management Committee and the Management Board.

Objectives

Risk Management is the process by which risks are identified, assessed, managed and controlled.

The purpose of a Risk Management Policy is to provide a framework for management to identify, assess, rate and develop strategies to deal with risks in order to provide reasonable assurance that the strategic objectives will be achieved.

The Risk Management objectives include:

- Raise awareness of the need for risk management;
- Integrate risk management within the culture of the organisation;
- Manage risk in accordance with best practice;
- Ensure that all key risks are identified and assessed;
- Ensure that an adequate system of internal control is in place to manage all risks; and
- Ensure that the Senior Management Team and staff are aware of risks and their responsibilities.

Appendix I sets out summary of definitions.

Background

It is the intention of the organisation to comply with best practice governance and accountability obligations as appropriate. The organisation has always incorporated risk assessment as part of the strategic and operational decision making process. It has a strong control environment, which has been strengthened by new controls that have been put in place, as required. Risks to the achievement of the organisation's strategic goals should be managed proactively with a view to optimising the probability of successful achievement of the goals. A Risk Management Committee will be maintained, as a sub-group of the Management Board and with a membership representative of the various functions in the organisation, to provide support to the ongoing implementation of the risk management framework. The effectiveness of the framework and the key risks identified for the organisation will be reviewed by the Management Board on a quarterly basis.

Risk Management and Mission Statement

The Risk Management Policy is to adopt best practice in the identification, assessment and control of risks to ensure that they are eliminated or reduced to a level acceptable to the Management Board in the achievement of its objectives.

Risk Profile

Risk is defined as anything that prevents an organisation from achieving its objectives. The organisation utilises a number of planning, reporting and risk management processes to ensure it operates towards the best standard applicable. It is essential that all key risks be identified and controlled/deemed acceptable and that all risk events be reported and fully investigated.

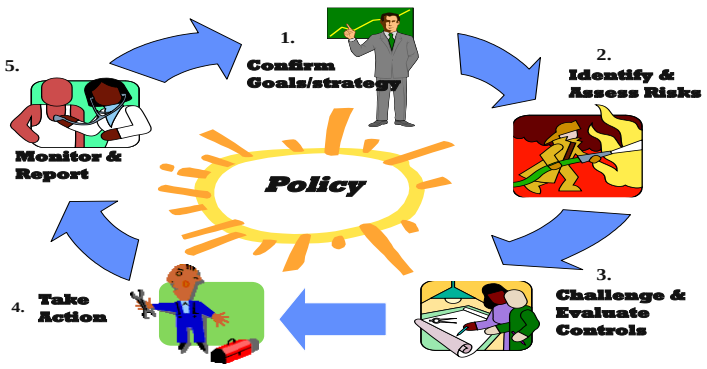
Persons Affected

The persons affected by this policy are outlined in this the document.

Scope of the Policy

The scope of this policy is to establish a framework to identify potential events that may expose us to risk, to control and manage this risk within the Management Board's risk appetite, and to provide reasonable assurance regarding the achievement of the organisational objectives.

The process can be described as follows:



Risk management is an umbrella discipline that cuts across all areas of the organisation's activities. This reflects the fact that risks permeate across all activities and functions. However, to facilitate the capturing and reporting of risks in a consistent manner the following categories of risks have been identified:

- Strategic
- Reputational
- Financial

- Operational

This policy sets out the following;

- Roles and Responsibilities
- Risk Identification and Assessment Process
- Risk Monitoring and Reporting Process.

Roles and Responsibilities

The various roles and responsibilities are summarised hereunder:

Area	*Responsibilities*
Board	• Formally approve the Risk Management Policy and Framework and review this annually as part of the review of the Audit and Assurance Arrangements. • Review any updates in the risk management documentation, as required. • Review the corporate risk register on a quarterly basis. • Review the risk management annual plan on an annual basis. • Engage with reviews of key risk areas.

Area	*Responsibilities*
Management Board	• Overall responsibility for the system of risk management and internal control. • Responsible for reviewing the risk management framework on a regular basis including i) progress against plan and ii) effectiveness of the risk management framework within the organisation. • Responsible for reviewing the corporate risk register every quarter, including prior to Board approval. • Responsible for reviewing the Risk Management Policy and Framework, prior to Board approval. • Supporting the Risk Management Committee and actively feeding into risk reviews and "deep dives" and participating in comprehensive deep-dives into key risk areas. • Responsible for the identification, mitigation and reporting of risks. • Responsible for the review of the risks identified at function level. • Be satisfied that adequate mechanisms are in place to mitigate identified risks. • Promote the on-going enhancement of the risk management process.
Chief Executive	• Responsible for ensuring the existence of an appropriate risk management system. • Responsible for ensuring that risk management is embedded in the management processes. • Responsible for ensuring that key strategic risks are being addressed and managed appropriately. • Responsible for ensuring that procedures for managing risk are fully understood and implemented by all staff as part of the business planning process. • Ensures that appropriate staff receive training, as and when is required in key risk areas. • Responsible for approving the risk management policy.

Area	*Responsibilities*
Audit Committee	Advise on the systems of control underlying the risk management framework and processes, through: -receiving feedback from the Chair of the Risk Management Committee, the internal auditor, external auditor and the organisation's management on the effectiveness of the risk management process; -taking such feedback into account for input into the priorities of the Internal Audit Unit work programme, including identifying the need for value for money audits. • -Reviewing and endorsing the Risk Management Framework (as outlined in the Audit and Assurance Arrangements) on an annual basis; • -Reviewing the Corporate Risk Register with an internal audit lens twice each year.

Area	*Responsibilities*
Risk Management Committee	• Review the risk management framework and propose amendments where necessary. • Prepare an annual plan of activity in relation to risk management and present to the Management Board. • Report to the Management Board after each Risk Management Committee meeting on i) progress against the plan and ii) effectiveness of the risk management framework within the organisation. • Offer support to the management of each function charged with implementing risk management across the organisation. This should include: – Facilitating risk identification / assessment workshops – Development of risk awareness training material – Development of a culture of responsibility – Review and feedback on process and outputs in each division • Monitor the effectiveness of the risk management framework (both Corporate and Functional). • Actively participate in deep dives into key risk areas. • Report to the Management Board after each meeting on items identified for escalation to the senior management team on the activity of the committee, any risk incidents occurring since the last report and any assurances which can be given regarding the effectiveness of the risk management framework. • Liaise with and report to the Audit Committee as requested from time to time by the Audit Committee or the senior management team. • Support the Management Board by proposing risk policies, by overseeing the detailed operations of the risk framework, by monitoring and reporting on the effectiveness of the risk management framework and by reviewing the corporate risk register.

Area	*Responsibilities*
Function	• Carry out a risk identification exercise on an annual basis to coincide with the development of the function's business plan. The main risks identified through this exercise will be recorded in the corporate risk register. It is not expected that these risk should exceed ten in number for any one function. • Review the functional risk register on a biannual basis in conjunction with the business plan review. • Be aware of significant risks that come within their area of responsibility, the possible impacts those risks could have on other areas of the office and the consequences other unit's risks could have on them • Report systematically and promptly to the Management Board about risk management, in particular about perceived new risks or failures of existing controls
Head of Function	• Conduct interim reviews of the list of identified risks at functional level so that these risks are managed. • Document the controls that are in place to mitigate against the risk materialising.
Risk Officer (Chair of the Risk Management Committee)	• Report directly to the Management Board after each Risk Management Committee meeting. • Support the Audit Committee, Senior Management Team and staff in fulfilling their responsibilities by providing a comprehensive framework to identify, develop, manage, monitor and report on risks within the organisation. • Responsible for developing and implementing Policies and the Framework on Risk Management. • Provide on-going guidance to Risk and Action Owner regarding the identification and management of risks, including ensuring that all relevant risks are assessed and that risks are scored in a consistent manner. • Ensuring that sufficient risk management training is provided to management and staff. • Meet with the Chair of the Audit Committee twice each year to discuss risk management processes. • Report to the Board on Risk at each meeting. • Provide a quarterly update to the Audit Committee on the implementation of the risk management framework.

Area	*Responsibilities*
Risk and Action Owner	• Own and manage risks delegated in the corporate (or functional) risk register (and business plans) on a day-to-day basis. • Comply with controls as stated in the corporate (or functional) risk register (and business plan) and report any control gaps/weaknesses). • Identify and report risk incidents. • Ensure risks are identified and reported in a timely and efficient manner. • Participate in the identification, measurement, prioritisation and management of risks and controls. • Be responsible for monitoring controls and implementing actions identified. • Report systemically and promptly to the Risk Officer any perceived new risks or failures of existing control measures.
Staff	• Being aware of the nature of risks in their day-to-day work. • Provide input into the identification and management of risks as required. • Understand their accountability for individual risks. • Take responsibility for carrying out control activities, reporting on control gaps/weakness along with any perceived changes in the risk environment, as appropriate. • Monitor the effectiveness of management procedures created to mitigate identified risks. • Proactively raise risks or concerns within their function and be responsive to the changing nature of risks faced by the organisation. • Ensure all risks and associated controls are identified and reported in a timely and effective manner.
Internal Audit	• Provide assurance to the Management Board and the Audit Committee on the effectiveness of the Risk Management process. • Help ensure key risks are being managed appropriately and that the system of internal control is operating effectively.

Risk identification and Assessment Process

Risk Identification

Risks will be identified, assessed and controlled through the following steps:

- Risk identification involves summarising the organisation's exposure to uncertainty through consideration of its service delivery, reputation, financial, legal, HR and infrastructure environment as well as its strategic and operational objectives. In summary, risks will be categorised as:
  - Strategic: Risk that policies, procedures, systems or activities would fail, thus, restricting progress towards achieving organisational objectives.
  - Reputational: Risk that the organisation would engage in activities or be perceived to engage in activities that would threaten its good name brand and public image.
  - Financial: Risk of failing to safeguard the organisations assets, financial misreporting or failure to achieve value for money.
  - Operational: Risk that policies, procedures, systems or activities would fail, thus, restricting progress towards achieving organisational objectives.
- A thorough risk identification exercise will be carried out in each function annually, to coincide with the development of the function's business plan. This will include:
  - Review of ongoing risks to the functioning of the division;
  - New risks which arise from the changes proposed in the business plan; and
  - Potential risks arising as a result of the changing environment
  - Identification of risks which could arise from not pursuing opportunities.
- The agreed Risk Appetite Statement (Appendix 5) must be taken into consideration when considering risk.
- The main risks identified through this exercise will be recorded on the corporate (or functional) risk register, using the eRisk system. It is not expected that these risks will exceed ten in number for any one function.
- Interim reviews of the list of identified risks will be managed by the head of function, where there is a change to the strategic or operational agenda or where there are changes to the external environment which could introduce additional risks. An interim review should also be conducted in conjunction with the mid-year business plan review.

Risk Assessment

Risks identified at a) above should be assessed to determine:

(i) The likelihood of the risk materialising.

(ii) The consequence on the strategic goals of the organisation if the risk were to materialise.

Output from the above assessment will be captured on the corporate (or functional) risk register on the eRisk system. Risks will be assessed on a scale of 1 – 5 in terms of impact (post existing mitigations):

IMPACT: scale of 1 - 5

1. Insignificant
2. Minor significance
3. Moderate
4. Major
5. Catastrophic

Appendix II provided further information on the above.

Risks will be assessed on a scale of 1 – 5 in terms of likelihood (post existing mitigations):

LIKELIHOOD: scale of 1 - 5

1. Rare
2. Unlikely
3. Likely
4. Very likely
5. Almost certain

Appendix III provides further information on the above.

On a regular basis, at the functional meeting, those management controls which have the effect of preventing a risk from materialising or reducing the negative impact of a risk to within acceptable levels should be considered to determine:

(i) What controls are already in place to prevent the risk materialising or to mitigate the impact if it does materialise

(ii) The adequacy of these controls to manage the risk to within acceptable levels

(iii) Additional controls / actions required to reduce the risk rating to within acceptable levels

(iv) The owner for the risk and the owner of the actions agreed under (iii) above

(v) The due date for the actions agreed under (iii) above.

The head of function is expected to document the controls that are in place to mitigate against the risks materialising. The control descriptions are included in the corporate (or functional) risk register.

Each head of function together with their staff is responsible for implementing and enforcing controls that effectively manage and mitigate risks identified, to a level that is within the tolerance limits approved by the Management Board. In considering the effectiveness of controls consideration will be given to the appropriate balance between the cost of implementing, the likelihood and potential impact of the risk event if it occurred and residual risk. Risks identified are then scored/assessed based on the impact and likelihood criteria as outlined above.

Net risk assesses the impact and likelihood of a risk post the application of the key controls. It is the responsibility of the organisation to ensure that a system is in place to review and consider controls identified to ensure that they are operating effectively on an on-going basis. The higher the total score of each risk, the more immediate action it requires. All risks should be planned for but resources must be channelled to those risks most likely to occur and which have the most serious consequences.

The total score of the risk is then considered on a range of:

- High 15 - 25
- Medium 9 - 14
- Low 1 – 8

All strategic risks, having been identified and assessed, will be documented on the corporate risk register.

Action Plans for Risks

Where controls are deemed to be less than adequate in the light of the risk appetite, an action plan will be put in place to increase the level of control effectiveness. The Risk and Action Owner will be identified and a time scale agreed within which the action plan will be implemented. This information is also documented in the corporate risk register.

Where mitigating actions / controls exist but are not being followed and monitored, then it is the policy that it is deemed that adequate controls do not exist, as in order for mitigating practices / controls to be effective they also must be communicated, actioned and monitored. This information is also documented in the corporate risk register.

As a result of the risk and control assessment process, actions with clear accountabilities will be set for all risks where gaps in the control environment are identified. These action plans as determined by the Management Board or Functional Head are developed to introduce new controls or improve existing controls as required.

To ensure accountability these actions will be linked to the risk and therefore to the underlying business objective. If this part of the process does not occur, then the benefits of the risk identification process will not be realised. The Management Board is tasked with delivering under the business objective will also be responsible for delivering under these actions.

All corporate risk controls to be implemented will be recorded in the Corporate Risk Register and reviewed until implemented. A formal audit trail must exist that relates the risk identification and assessment process to the actions arising. This is achieved through effective use of the eRisk system and ongoing management of the Corporate Risk Register.

The action plans will set out the following:

- Planned control actions to address risk

- Responsibility for undertaking the planned activities
- Timeline for action.

The Management Board monitors the implementation of the mitigating control action plans for corporate risks and the Risk Management Group monitor the implementation of mitigations on functional risk registers and report after each risk management meeting (through the Chair of the Risk Management Committee) if there are any difficulties arising in relation to the progress of same to the Management Board. Any such delays should be flagged to the Risk Management Committee by the relevant functional owner. All outstanding risk mitigations are also included on the Action Tracker which is monitored by the Compliance and Quality function on a quarterly basis.

Risk Monitoring and Reporting Process

The output of the above, which is captured on the corporate risk register and on functional risk registers is the key reporting and monitoring tool for risk management in the organisation. The functional risk register owner is responsible for ensuring that the risk management policy is implemented and that the output, in the form of an updated risk register, is recorded on the eRisk system.

The risk management committee will produce an annual plan of activity and will report to the Management Board after each Risk Management meeting on (i) progress against plan and (ii) effectiveness of the risk management framework in the organisation.

Prior to the introduction of new initiatives / projects, a comprehensive risk analysis exercise will be undertaken and noted. The appropriate risk register(s) will be updated and controls added to the risk register where appropriate.

Incident Management Policy

All incidents (and "near misses") rated at "3" in terms of impact will be reviewed by the relevant senior manager and the overall estimated rating compared to the risk statement to determine its seriousness. Any incident which is rated at the same level or higher than the risk appetite will be

escalated to either the Risk Management Committee (using the Incident Report form – Appendix 4) or the Quality Administration Team (using the CAPA process) whichever is deemed most appropriate by the relevant senior manager. The appropriate risk register(s) will be updated following this review.

Risks rated below the risk appetite will be managed at a local level with controls put in place to mitigate the risk and both the risk and controls recorded in the functional risk register. Consideration will be given to other similar risks / potential incidents which may occur. These risks/near misses should also be reported to the Quality Administration Team (using the CAPA process) if deemed necessary by the relevant senior manager.

All relevant incidents / "near misses" will also be explored with the Leadership meetings where issues impacting on quality are shared and shared learning points identified. These learning points will then passed on from the Leadership Group to their teams. A mitigation plan for reducing the impact of these incidents / risks will be agreed and actioned (through the Leadership Group or other agreed fora).

All major business continuity related events will be reviewed in terms of key learning identified in order to reduce the impact over these risks where the organisation does not have control.

Training

Training will be provided to the Risk Management Committee every two years to ensure that they are kept up-to-date on developments in risk management in the public service and other relevant corporate governance related issues.

Staff will be made aware of a number of key areas on an annual basis; this will include:

- Risk Management Objectives
- Functional Responsibilities
- Line Manager Responsibilities
- Staff Responsibilities
- Incident Management Policy – Risks and Near Misses.

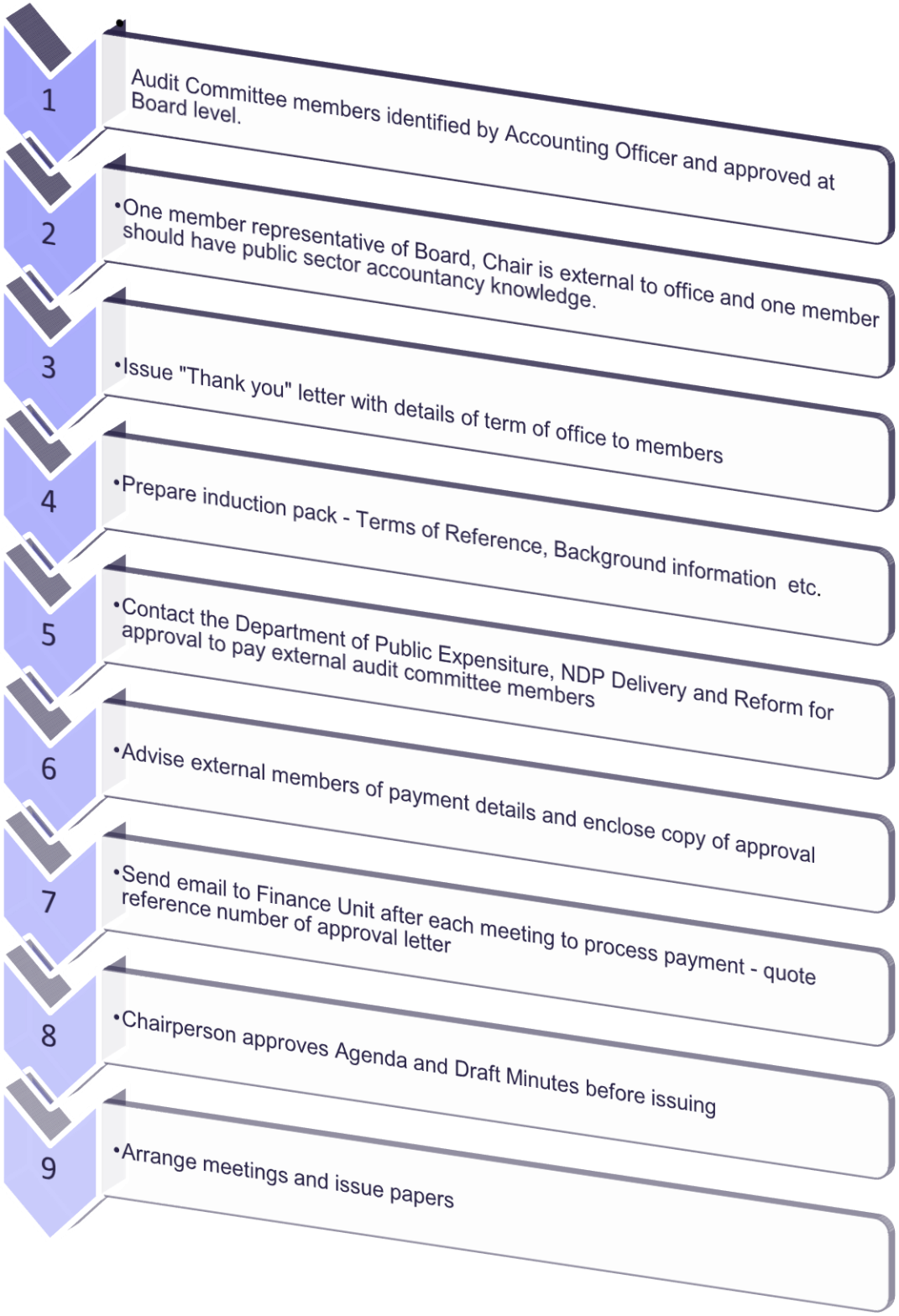
Staff will also be encouraged at Business Awareness Sessions to share and discuss learning incidents and issues impacting on quality in order to ensure ongoing innovation and quality improvements.

Role of and Procedures for the Internal Audit Function

- Revise Charter and Terms of Reference for both the Internal Audit Function and Audit Committee on an annual basis as part of the review of the Audit and Assurance Arrangements
- Develop Strategic Audit Plan every three years
- Ensure agreed audit programme is implemented
- Provide administrative support to the Audit Committee and act as Secretary
- Conduct agreed internal quality audits and report to management on findings
- Liaise with outsourced Internal Auditors as necessary
- Maintain records of work carried out and expenditure of outsourced Internal Auditors
- Report to the Accounting Officer/Board on progress
- Prepare an Annual Report for the Audit Committee in QI of each year
- Invite C&AG to attend Audit Committee Meeting each year
- Issue follow-up questionnaires on all audit reports following circulation
- Maintain progress report on implementation
- Report to Audit Committee on implementation of recommendations
- Review implementation of all recommendations on an annual basis and issue report to Committee
- Issue Audit Reports to senior managers
- Ensure awareness of improved methods of auditing/developments in this area
- Embed the concept of audit throughout the office
- Carry out procurement exercise to retain the services of professional Internal Auditors
- Review membership of Committee every three years

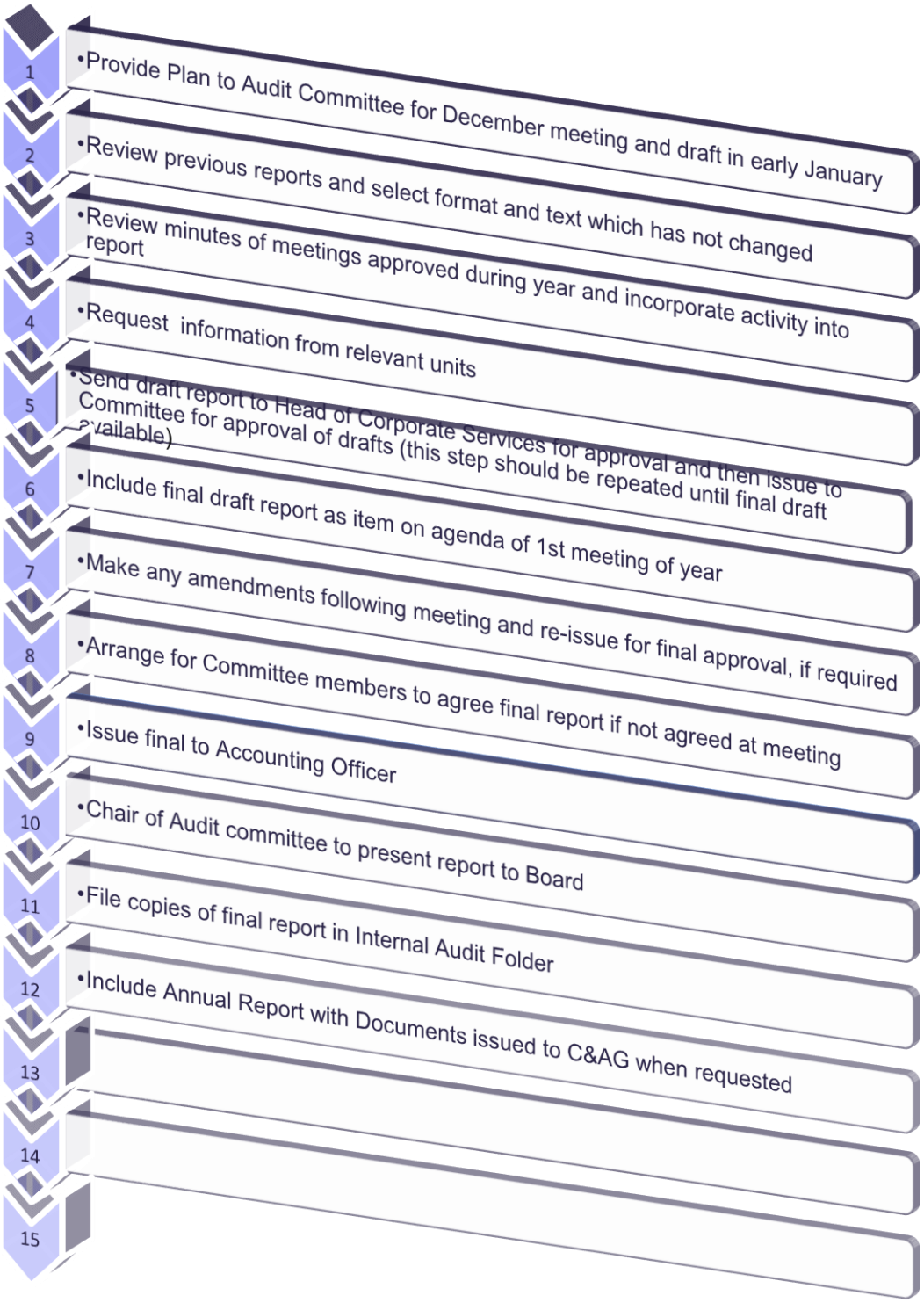
FLOWCHARTS FOR INTERNAL AUDIT SYSTEMS

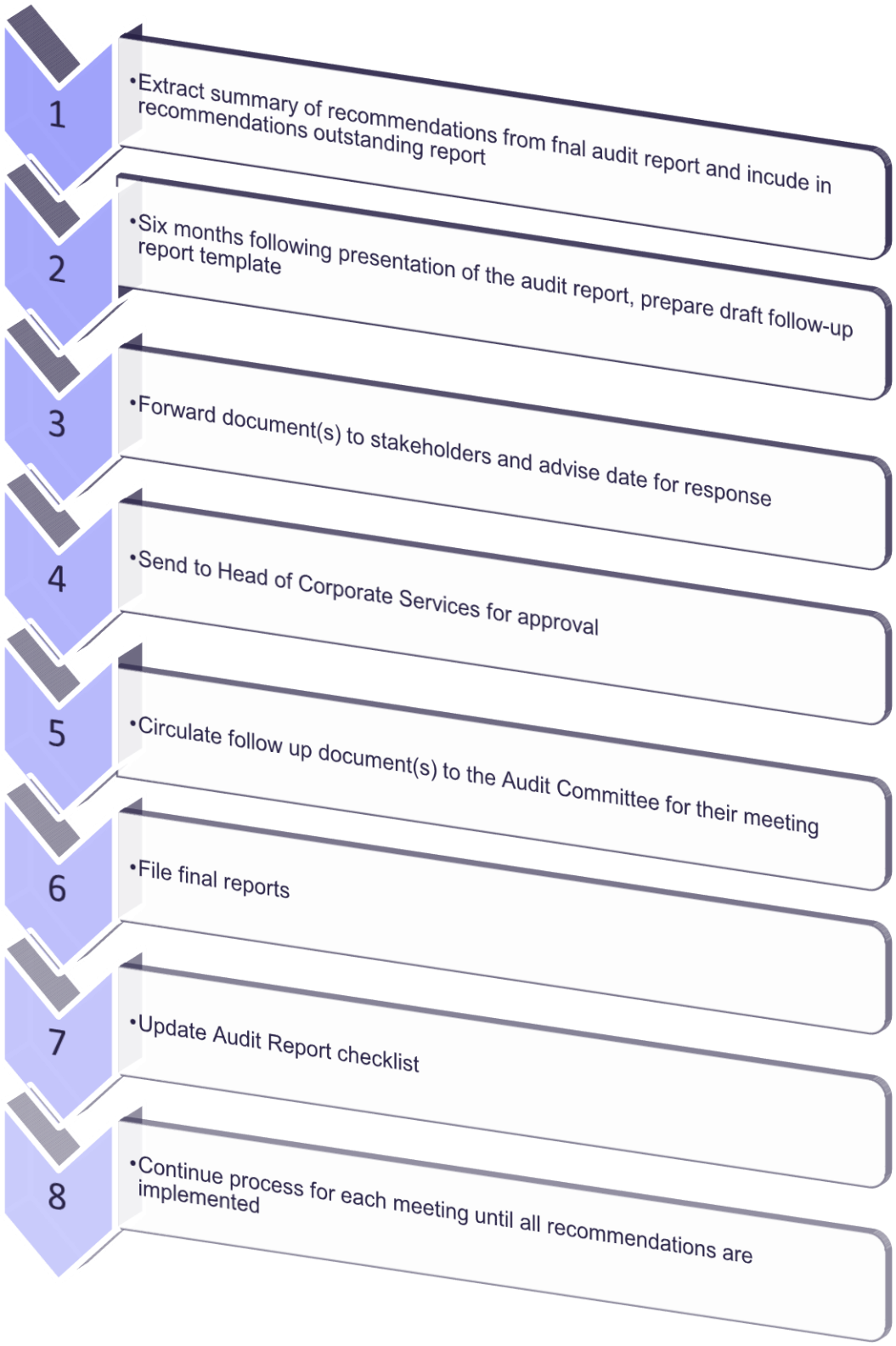
Audit Committee



Internal Audit Reviews

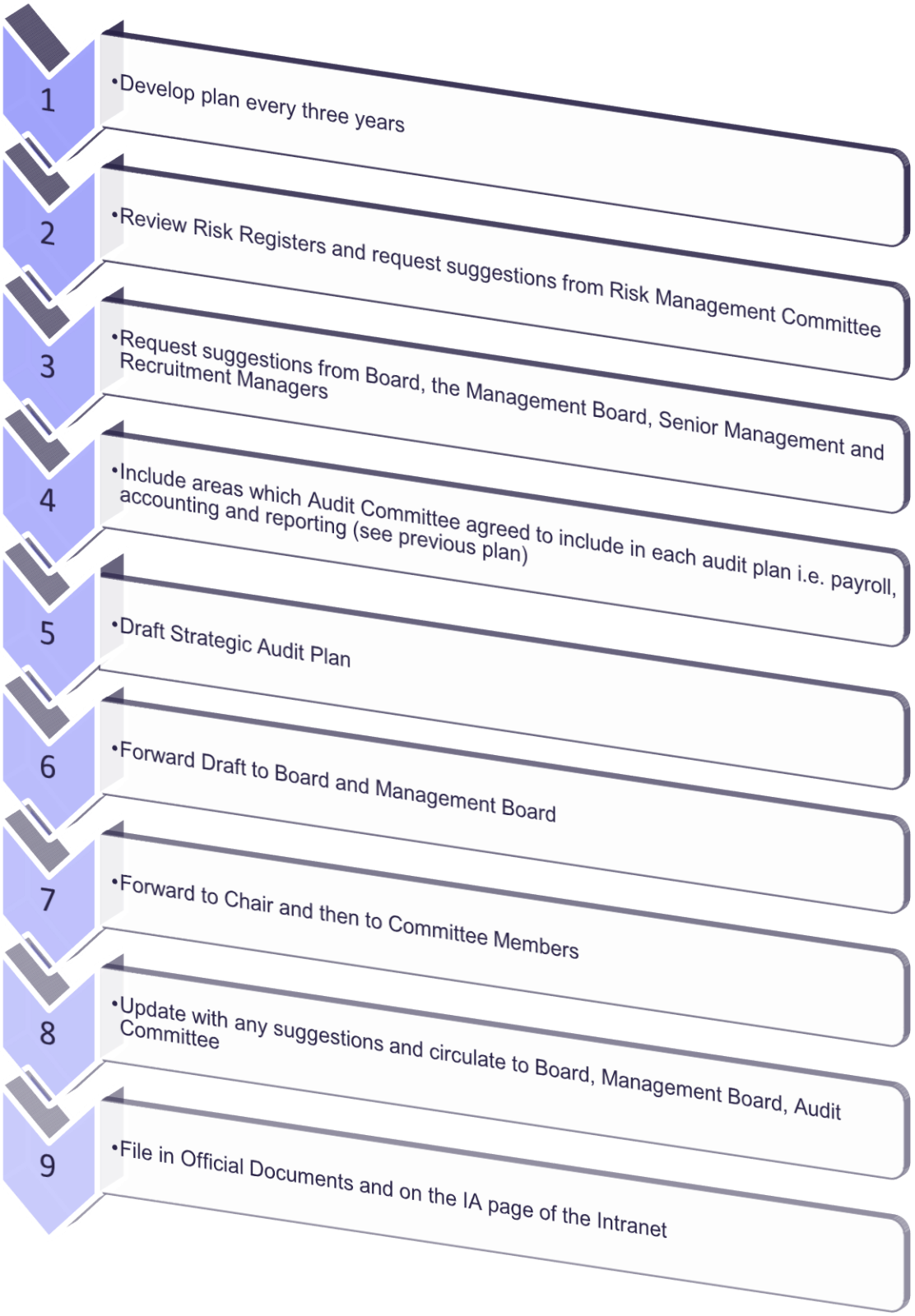
Audit Committee Annual Report





Follow up Procedure

Preparing Audit Plan



Audit Checklists

Checklist for Individual Audit

Area	Issues Identified	Review / How Issues Addressed	Date Completed
Approve audit scope and agree KPIs (timescales, budget, hours to be worked, staff to be assigned, expectations for final report)	KPIs agreed:	Performance Against KPIs:	
Issues identified during the audit (if any)			
Draft Report Received			
Management Comments Agreed			
Draft Report to CEO			
Agreed Reponses to Internal Auditor			
Draft Report to Audit Committee			
Approved Report to Management Board			
Approved Report to Board			
Quality of Report assessed by Audit Committee			
Quality of Report assessed by Management Board			
Quality of Report assessed by Board			
Number of recommendations made			
Number of recommendations implemented	Meeting Date: Meeting Date: Meeting Date:		
Number of recommendations not implemented	Meeting Date: Meeting Date: Meeting Date:		
Issues to be raised with Auditors			

Issues to be raised with Quality Function			

Annual Checklist for Audit Function

Area	Update/Issues	How Issues Addressed	Date Completed
Review of all reports for conformance to agreed scope and standards			
Number of overall recommendations			
Number of overall recommendations implemented			
Number of overall recommendations not implemented			
Independent assessment and re-review of all recommendations implemented			
Independent assessment and re-review of all recommendations not implemented			
Review of all individual checklists for issues identified and overall conformance			
Follow up on progress with all issues identified in checklists and issues referred to Quality Team			
Feedback sought from Audit Committee on quality of audit reports and audit function in previous twelve months			
Feedback sought from Management Board on quality of audit reports and audit function in previous twelve months			
Feedback sought from Board on quality of audit reports and audit function in previous twelve months			

Review of internal audit charters and policies completed			

Appendix I - Definitions

Risk:	Risk is defined as anything that prevents an organisation from achieving its objectives.
Risk Identification:	The process of determining what risks might happen, why and how
Risk Policy	The risk policy sets out the position with regard to the standards for identification, assessment, tolerance, mitigation, monitoring and reporting of risk as set out by the communication of the risk appetite.
Risk Management	Risk Management is the process by which risks are identified, assessed, managed and controlled.
Risk Assessment	Risks are assessed and prioritised by the Senior Management Team on the combined basis of their likelihood of occurrence and the resulting impact should they materialise.
Risk Exposure	The chance or possibility of loss or harm arising from a failure in business operations. An exposure has two dimensions: • The magnitude of the loss or harm (impact); and • The vulnerability of the organisation to a process failure arising (likelihood).
Risk Impact	A measure of the damage/harm arising from the adverse consequence suffered by an organisation as a result of an operational failure. The impact on the organisation if the risk actually happens is estimated using a scale of 1 - 5, where 1 is insignificant and 5 is catastrophic.
Risk Likelihood	The degree of possibility of a business operational failure occurring in an organisation. The likelihood of occurrence is estimated using a scale of 1 – 5 where 1 is rare and 5 is almost certain.
Risk Appetite	Risk appetite is the level of risk a business is willing to accept based on the accepted return of the activity in question.

Risk Mitigation	The strategies and controls including all the policies, procedures, practices and processes in place that are used to prevent or limit the damage caused by a risk materialising.

Appendix 2 - Considering the Likelihood of the Risk

Rating	Category	Description	% likelihood
1	**Rare**	May only occur in exceptional circumstances; simple process; no previous incidence of non-compliance.	0-20%
2	**Unlikely**	Could occur at some time; less than 40% chance of occurring; non-complex process &/or existence of checks and balances.	21-40%
3	**Possible**	Might occur at some time; 41%-60% chance of occurring; complex process with extensive checks & balances; impacting on factors outside control of organisation.	41-60%
4	**Likely**	Will probably occur in most circumstances; 61% – 80% chance of occurring; complex process with some checks & balances; impacting factors outside control of organisation.	61-80%
5	**Almost certain**	Can be expected to occur in most circumstances; more than 81% chance of occurring; complex process with minimal checks & balances; impacting factors outside control of organisation.	81-100%

Appendix 3 - Considering the Impact of the Risk

Level & Description	Financial - % of Net Assets	Reputation and image per issue	Critical services interruption	Organisational outcomes/ objectives	Non-compliance
Insignificant (1)	0-20%	Non-headline exposure Not at fault No impact	No material disruption	Little impact	Innocent procedural breach Little impact
Minor (2)	21-40%	Non-headline exposure Clear fault settled quickly Minor impact	Short term temporary suspension Backlog cleared < 1 day	Inconvenient delays	Breach Minor harm with investigation
Moderate (3)	41-60%	Repeated non-headline exposure Slow resolution	Medium term temporary suspension Backlog cleared by additional resources	Material delays, marginal under-achievement of target performance	Negligent breach Performance review initiated
Major (4)	61-80%	Headline profile Repeated exposure At fault or unresolved complexities	Prolonged suspension of work Additional resources required Performance affected	Significant delays performance significantly under target	Deliberate breach or gross negligence Disciplinary action
Extreme (5)	81-100%	Maximum high level headline exposure Loss of credibility	Indeterminate prolonged suspension of work Non performance	Non achievement of objective/outcome Performance failure	Serious, wilful breach Criminal negligence or act; prosecution Dismissal

Appendix 4 – Incident and Near-Miss Report Form

poistphoiblí publicjobs

Incident & Near-Miss Report

This form is to be completed as soon as possible following the occurrence of any incident or near miss that has been rated as "3" in terms of impact by the relevant senior manage (see page 3).

An incident includes any errors, process failures, etc. which has impacted on the delivery of services to any of our customers.

A near-miss includes any errors, process failures, etc. which could have impacted on the delivery of services to any of our customers.

All items completed should be based on information that is currently available.

This form may be updated and modified if necessary.

CONTACT INFORMATION	
Name	
Title	
Role in Incident/Near-Miss Resolution	

INCIDENT / NEAR MISS SUMMARY
Summary Description of Incident/Near-Miss

How was the incident/near-miss discovered?	
Date the incident/near-miss was discovered	
Date the incident/near-miss is thought to have occurred/started	
Processes affected/potentially affected by the incident/near-miss	

Approximate numbers & types of customers affected/potentially affected by the incident/near-miss	
Is the issue resolved?	
Resolution Date	

INCIDENT / NEAR-MISS DETAILS

Description of Incident / Near-Miss
Please provide a description of the incident / near-miss including how it was identified
Impact of Incident / Near-Miss
Please provide a description of the impact/potential impact of the incident/near-miss including processes and/or campaigns affects/potentially affected
Cause of Incident
Please detail how/why the incident / near-miss occurred

INCIDENT / NEAR-MISS RESOLUTION
Resolution of Incident/Near-Miss
Please detail any steps taken to mitigate against or resolve the issue and who was involved in problem-solving activities
Additional Information
Please provide any additional information that you feel is important but has not been provided elsewhere on this form
Remaining Risks
Please provide details of any risks or issues that remain unresolved
Additional Required Action
Please provide details of any further action or risk mitigation strategies that need to occur

Consequences	**Likelihood**
1 - Negligible	1 - Rare
2 - Minor	2 - Low
3 - Moderate	3 - Medium
4 - Significant	4 - High
5 - Substantial	5 - Very High

Appendix 5 – Risk Appetite Statement

1. Introduction

The purpose of the organisation is set out in the primary legislation which establishes us[1]. The Act states that the core role of the organisation is to be "*the centralised recruitment, selection, and assessment body for the Civil Service and to provide a similar service, where requested, to the local authorities and Health Boards, the Garda Siochana and any other public service body*" (s.34(I)(a) of the Act). Under the Act, we may also provide recruitment-related advisory and related services to the Civil Service, Local Authorities, the Health Service Executive, the Education Sector, An Garda Síochána, other public bodies and non-commercial semi-state agencies, when requested (s.34(I)(f) of the Act).

The ability of the organisation to effectively fulfil this mandate rests, among other things, on its reputation as an organisation of the highest integrity and professionalism.

This Statement considers the most significant risks to which we are exposed and provides an outline of the approach to managing these risks. All strategic plans and business plans for functional areas must be consistent with this Statement.

2. General Statement of Appetite

The organisation faces a broad range of risks reflecting its responsibilities as a central provider of recruitment and selection services to the public service.

Reputational risks (particularly those for areas which are not fully within the control of the organisation) can be significant. These risks are managed through detailed processes that emphasise the importance of integrity, maintaining high quality, and public accountability.

[1] Public Service (Recruitment and Appointments) Act, 2004 – hereinafter referred to as "The Act".

In terms of operational and quality related issues, we have a low appetite for risk. We make resources available to control operational risks to acceptable levels. We recognise that it is not possible or necessarily desirable to eliminate some of the risks inherent in its activities. Acceptance of some risk is often necessary to foster innovation within business projects (particularly those risks related to the increase in use of technology).

Where we do not have control over the full recruitment to appointments process (e.g. State Boards) we have a willingness to accept a medium level of risk which will be carefully managed through adherence to the appropriate Guidelines or Codes in place. Where risks are necessary to introduce innovations to the business (we will accept a medium level of risk. We will adopt an integrated approach to risk management across digital transformation, business continuity, use of AI and automation, cyber security and data protection. Before any new process or technology is introduced, we will complete a thorough risk assessment process to ensure these risks are effectively controlled or mitigated. This will include discussions at Management Board in terms of risk appetite for digital transformation while balancing the requirements around data protection and cyber security. We will ensure that relevant experts in these areas are involved in the discussions in order to ensure Management Board have the appropriate guidance to make evidence-informed decisions. A detailed analysis of the risk appetite for various aspects of work is set out in the Chart below.

3. The Risk Management Framework

The risk management framework seeks to ensure there is an effective process in place to manage risks across the organisation. Risk management is integral to all aspects of our activities and is the responsibility of all staff. Managers have a particular responsibility to evaluate their risk environment, and put in place appropriate controls and to monitor the effectiveness of those controls. The risk management culture emphasises careful risk analysis and management of risk in all business processes.

Risks are identified, assessed and managed at both business level and at a strategic level. The Risk Management Committee has oversight of these processes and conducts a "deep dive" into all risk registers on an annual basis. The Committee meet regularly during the year and provide an update on its activities to the Management Board after each Risk Management meeting. The annual plan for the Risk Management Committee is submitted to the Management Board and the Board for approval.

4. Coverage

Our attitude towards its key strategic, reputational, financial, and operational risks is described below.

4.1 Strategic Risks

We aspire to be the recruitment provider of choice in the public service measured by the quality and effectiveness of our operations. This requires on-going development and innovation in its operations through strategic business projects and initiatives. We have a low appetite for threats to the effective and efficient delivery of these initiatives. It recognises that actual or perceived inability to deliver strategic initiatives could have a significant impact on its ability to achieve its objectives as well as its reputation.

The Management Board meet regularly to discuss these strategic projects. A framework is in place to ensure these initiatives are prioritised appropriately and are managed and reported on a consistent basis.

4.2 Financial Risks

We are responsible for the effective use of public funds and takes this responsibility very seriously. We have a high level of controls in place in order to manage all financial resources and to reduce the risk of fraudulent activities. Expenditure is monitored on a monthly basis by the Senior Management Team.

4.3 Operational Risks

Risks to the operations are carefully analysed in all operational activities.

IT

We have a low appetite for risks to the availability of systems to support critical business functions; the maximum recovery times have been identified and agreed with the recruitment and selection units. We have a low appetite for threats to operations arising from external malicious attacks. To address this risk, we aim for strong internal control processes and the development of robust technology solutions. We are greatly dependent on the internet and email to communicate with candidates and therefore cannot completely mitigate this risk. The implementation of new technologies creates new opportunities and new risks. We have a low appetite for IT system-related incidents that are generated by poor change management practices.

Fraud and Corruption

We have no appetite for fraud or corruption perpetuated by its staff. We take all allegations of suspected fraud or corruption very seriously and respond fully and fairly as set out in the Anti-Fraud and Corruption Policy.

Physical Security

We strive to provide a highly secure environment for its staff and customers by ensuring its physical security measures meet high standards. We have a very low appetite for failure of physical security measures.

Compliance

We are committed to a high level of compliance with relevant legislation, regulation, CPSA Codes and similar guidelines for campaigns outside of the codes, Codes of Standards, in addition to internal policies and sound corporate governance principles. Identified breaches of compliance will be remedied as

soon as practicable. We have no appetite for deliberate or purposeful violations of legislative or regulatory requirements.

Information Management

We are committed to ensuring that information is managed in compliance with Data Protection requirements and that the confidentiality of customers is maintained. We have a very low appetite for risks in relation to breaches of confidentiality.

Protected Disclosures Risk Assessment

This was discussed by Risk Management Committee in 2022. Areas where it was felt there is most potential for protected disclosures are from candidates in relation to cheating at assessments or in relation to board member conflicts of interest. There are procedures in place in relation to both of these areas but any protected disclosure will be investigated as received. We have a low appetite for risks in both of these areas but accepts that it cannot 100% guarantee compliance in relation to candidate behaviour at online assessments despite the controls in place, particularly as technological advancements continue at a rapid rate. We do however make every effort to keep up-to-date on developments and mitigate against them.

4.4. Opportunities

We have identified areas where there are opportunities for improvement and innovation; we are therefore willing to take a carefully managed approach to the risks around these areas in order for us to make the most of these opportunities for change. They include areas such as adopting new approaches, attracting new audiences and markets, using new recruitment models and providing new services to clients. This includes piloting new approaches under the turning insights into action element of our strategy. It also includes the approach to digital innovation and

market positioning. Effective project and change management processes will allow us to take these opportunities while minimising any potential negative impact on reputation.

5. Implementation of the Risk Appetite

The Heads of all Units (at AP level) are responsible for the implementation of, and compliance with, this Statement.

5.1 The Risk Appetite Statement is published on the Intranet and on the Corporate Governance section of publicjobs.ie.

5.2 Risk Assessments

Each unit maintains a Risk Register of the business risks it faces in its day-to-day operations and the control framework which is in place to mitigate risks. These Registers take into account risks from within the organisation and external sources and are reviewed every six months. Risk registers are also updated when there are key changes in policies or procedures or when controls have to be amended as a result of additional risks or an evaluation of "near misses". Any risks which exceed the overall risk appetite should be flagged to the Risk Management Committee during the annual deep dive process.

A Corporate Risk Register which includes all of the major risks facing the organisation is in place and reviewed by the Management Board on a quarterly basis.

Staff can bring new risks or "near misses" to the attention of the Risk Management Committee. Additional controls will be put in place to address such risks and the risk may be escalated to the Management Board depending on the rating of such risk

6. Review

This Risk Appetite Statement will be reviewed on an annual basis in conjunction with the Audit and Assurance Arrangements document. Proposed changes to the Risk Appetite Statement will be agreed by the Management Board and any revisions will be circulated to the Audit Committee. The Audit and Assurance Arrangements will be circulated to the Board on an annual basis.

Chart 1 – Analysis of Risk Appetite

Goal, Activity or Function	1	2	3	4	5	6	7	8	9	10
Strategic Risks										
Economic – Funding						X				
Legal & Regulatory Changes (incl. DP)					X					
Strategic alliances / shared responsibility initiatives					X					
Customer experience				X						
Turning Insights into Action					X					
Disaster Recovery			X							
Financial Risks										
Budget Management			X							
Fraud and Corruption	X									
Procurement			X							
Operational Risks										
Quality of Service Delivery		X								
New methods of Service Delivery						X				
Developing Assessment Approaches						X				
Recruitment processes not within our full control					X					
Digital Innovation							X			
Market Positioning							X			
Business Continuity					X					
Reputational & Compliance Risks										
Compliance with CPSA Codes		X								
Legal & Regulatory Compliance	X									
Legal & Regulatory Compliance not within our full control					X					
Information Security & Governance (Cyber Security and Data Protection)		X								
Governance Compliance			X							
ED&I				X						
Environment and social responsibility				X						
People and Culture										
Physical Security		X								
Capacity & Competence				X						
Engagement & Retention			X							
Health, Safety & Wellbeing		X								

1 – unwilling to take risks (risk averse) – 10 willing to actively pursue opportunities (risk embracing) (1-3 Low; 4-7 Medium; 8-10 High)

Appendix 6 – Statement of Interests

Person/ Organisation	Nature of relationship and/or nature of conflict of interest
e.g. Department of Public Affairs	Employee

Name:

Position:

Signed: