POL00083966

AUDIT CHARTER

Branch and Cash Centre Audit Activity, Post Office Ltd

POL00083966

Section		Page
1.	Introduction	3
2.	Organisational standards	4
	2.1 Structure 2.2 Purpose and scope of audit role 2.3 Independence 2.4 Relationship with Audit Committee 2.5 Relationships with management, other auditors and review bodies 2.6 Resourcing, training & development	
3.	Operational standards	6
	3.1 Auditing Strategy 3.2 Audit Planning 3.3 Management of audit assignments 3.4 Due professional care 3.5 Reporting process 3.6 Quality Assurance	
4.	Code of ethics	8
5	Appendix A – Service Portfolio	10
6.	Appendix B - Internal Audit Standards – Published by the Institute of Internal Audit (IIA)	12

POL00083966

Section 1 - Introduction

This Charter interprets recognised standards (from the Institute of Internal Auditors) for use in Post Office Ltd, in order that clear guidance is provided to both staff and customers.

This policy document sets out the standards and code of ethics that apply to those staff performing audits of branches and cash centres within Post Office Ltd.

This policy supports the following more details process documents:

- Audit Process Manual

  Chapter 1 Risk Model Operations
  Chapter 2 Audit Planning and Scheduling
  Chapter 3 Performing a Branch Audit
  Chapter 4 Transfers
  Chapter 5 Closures
  Chapter 5a Network Change Closures
  Chapter 6 Robbery & Burglary Audits
  Chapter 7 Cash Centres
  Chapter 8 Annual Certificate of Compliance (Crown Offices)
  Chapter 9 Retention of Working Papers
  Chapter 10 Health & Safety
  Chapter 11 Quality Assurance
  Chapter 12 Continuity Plan

- Compliance Audit Test (CAT) programmes

  <u>Foundation</u>

  Procedural Security
  Financial Controls
  Information Security
  Restrictions Policy
  Data Protection

  <u>Pillars</u>

POL00083966

Financial Services
Government Services
Mails
Telephony

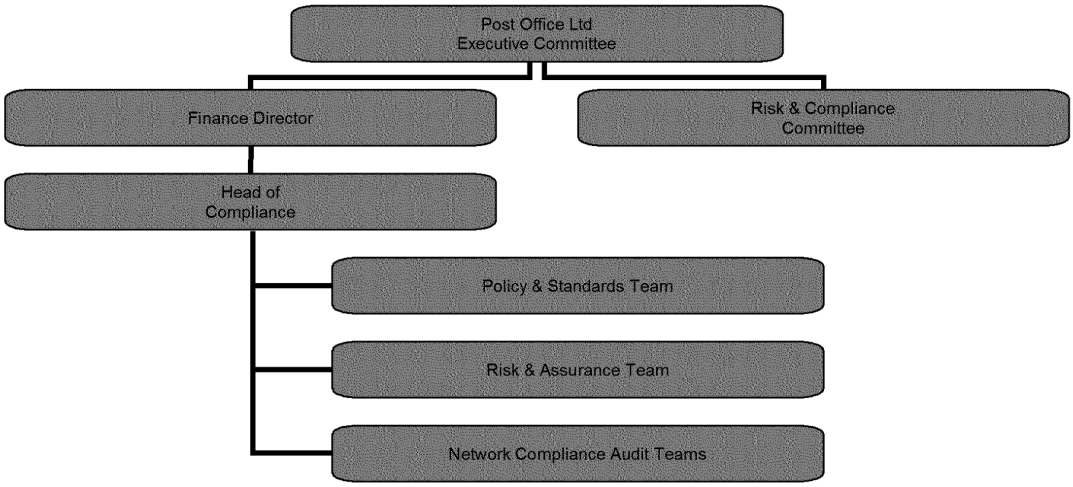
The Risk & Assurance Manger is responsible for periodic reviews of this Charter to ensure it reflects changes in business policies, team roles or internal auditing standards.

POL00083966

Section 2 – Organisational Standards

2.1 Structure

There are three regional network compliance audit teams (referred to as audit teams in this document), which work within a national Compliance Team, reporting up to the Finance Director. These teams perform audit activities within Post Office Ltd.



2.2 Purpose and Scope of Audit Role

The primary purpose of branch and cash centre audit activity is to provide an independent assurance to Post Office Ltd that:-

- Its assets exist at Post Office® branches and cash centres
- There is compliance to relevant policies, processes, regulations and standards

This is delivered through a risk prioritised audit programme, with a percentage of activity selected through pure random methods, covering: -

- Unannounced combined asset verification and compliance audits
- Unannounced compliance only audits
- Verification of assets at transfers and closures of branches
- Verification of assets and procedural security reviews, following robbery and burglary incidents
- Management of an annual certification programme for crown offices

POL00083966

The role ***is not*** an investigative one nor is its primary function to detect fraud. The investigation of fraud is the responsibility of Post Office Ltd Security team. While it is not a primary function of the audit teams to detect fraud, it is not uncommon for system control weaknesses to be exploited for fraudulent gain. Where auditors identify or suspect fraud, processes exist to escalate the matter.

POL00083966

Audit teams have unrestricted access to all Post Office branches and cash centres in order to review, appraise, advise and report on: -

- the extent to which the assets are safeguarded from losses of all kinds arising from inefficient administration, fraud or other cause;
- the extent of compliance with Post Office Ltd's financial and operating procedures for the network of post offices;
- the adequacy of follow-up action taken to remedy weaknesses identified by Internal Audit review, ensuring that good practice is identified and communicated widely.

2.3 Independence
The independence of audit activities within Post Office Ltd is achieved through its organisational structure and the objectivity its auditors.

Operating as three regional teams, with a national team structure (and the management of audit scheduling controlled centrally), the audit teams are independent of the activities it audits in order to ensure the unbiased judgement essential to its proper conduct and impartial advice to management. They have no executive responsibilities. If auditors form non-audit work, e.g. on secondment or as part of the Rapid Deployment Team (RDT), it should be understood that they are working separately from the audit teams.

All work undertaken is complementary to, and not in substitution of, the responsibilities of line management. Line management is responsible for exercising proper and effective internal control. Audit teams may advise, but do not develop or install controls itself.

Any recommendations on, or involvement in improvements of, existing procedures are made without prejudice to the audit teams' right to evaluate these procedures at a later date.

It is incumbent on all auditors to inform their line manager of any circumstances which create a conflict of interest with their Post Office duties, and seek advice if they are unsure. The Risk Reporting Advisor maintains a register of any declared interests.

2.4 Relationship with Audit Committee
Post Office Ltd's audit teams indirectly report to Royal Mail's Audit & Risk Committee via Royal Mail Internal Audit & Risk Management. Monthly

POL00083966

reports, detailing aggregated findings from branch audit activities are circulated to Royal Mail Internal Audit & Risk Management.

POL00083966

2.5 Relationships with management, other auditors and review bodies

The role of audit activities within Post Office Ltd is to provide support to the auditee and add value to management, by providing both individual audit reports (for each audit assignment) and aggregated MI and reports, with trend data.

Post Office Ltd does not have its own audit committee but has a Risk & Compliance Committee, a sub committee of Post Office Ltd's Executive Team (ET), which meets on a quarterly basis (ahead of its ET meetings). This committee provides oversight to audit plans and actions prompted by aggregated findings.

2.6 Staffing, training & development

There is an aim to provide an employee environment, which attracts, develops and retains the required quality and quantity of staff to deliver an effective Internal Audit service to Post Office Ltd.

It is the responsibility of the Head of Compliance, with support from network compliance audit managers to:

- Identify and implement an appropriate staffing structure and balance of skills to enable network audit objectives to be met and to ensure that resources are efficiently and effectively employed;
- Select auditors whose background and personal attributes indicate that they have, or will be able to acquire, the knowledge and skills required to meet Internal Audit standards
- Ensure that staff receive appropriate training and practical experience sufficient to enable them to carry out their duties effectively.

Auditors should have, or be supported in obtaining, the knowledge and skills as described by documented job descriptions. This is achieved through the Performance & Development Reviews (PDR) process, where individual training and development needs for team members are addressed.

New recruits to the team are usually recruited internally and, generally, have an operational background (i.e. working at a branch or cash centre). Each new recruit receives a formal induction and on the job training.

While formal qualifications are not required for team members, those at management level are encouraged to attain the Practitioner in Internal

POL00083966

Audit qualification (accredited by the Institute of Internal Audit), where training funds allow.

POL00083966

Section 3 – Operational Standards

3.1 Auditing Strategy
The network compliance audit managers set strategic direction for the audit teams in line with Business strategy and in agreement with Head of Compliance.

Audit teams perform audits through compliance auditing techniques. The concept of compliance auditing is based on the assumption that the mandatory system and laid down procedures are in operation. Compliance tests are designed to ensure that controls are operating as intended by checking for evidence of adherence to the approved system. The auditor's role in compliance auditing is to undertake sufficient testing in order to be able to confirm with reasonable assurance that the controls, which should be present in a system, are functioning effectively.

3.2 Audit Planning
The Head of Compliance is responsible, with delegated authority to Alvin West, Network & Compliance Audit Manager, for preparing an annual audit plan and quarterly updates (for oversight and approval by the Risk & Compliance Committee).

The following risk models, refreshed monthly, are used by the Network Risk Manager to help inform network compliance audit teams which branches provide the greatest risk and, therefore, help prioritise audit activities that appear in audit plans.

- Financial Audit Risk Model (FARM)
  A range of data from internal financial systems focusing on identifying abnormal trends in cash flow and cash reporting as well as highlighting reported errors and losses. The outputs of the model are a list of branches in score order, with the score representing the value of funds at risk in £000.
- Profiling Model
  Directly linked to FARM, this focuses on the profile of the branch (e.g. size, length of service and history of loss in last four years) to suggest that the branch has the potential to cause future concern.
- Compliance Audit Risk Model (CARM)
  The focus of this model is to highlight those branches, which provide the greatest risk of regulatory compliance failures. The overall model output is a list of branches in risk order. This outputs is based upon four separate models (anti-money laundering, financial services, HomePhone and Mails Integrity models), which focus on recorded failures (e.g. audit findings, failures to obtain

POL00083966

identification for Bureau products, complaints etc) and are weighted by the levels of sales.

3.3 Management of audit assignments

The scheduling advisor assigns an audit leader for each individual audit. The audit leader is responsible for:

- Planning the audit
- Cascading plans to other auditors
- Allocating responsibilities to other auditors
- Coordinating activities on the day of the audit
- Reporting findings

POL00083966

In addition, the audit leader is responsible for ensuring that the audit is carried out in accordance with defined process, set out in the Audit Process Manual.

3.4 Due Professional Care
Team members demonstrate due professional care by:-

- Following laid down processes, set out in the Audit Process Manual
- Applying techniques providing in training sessions
- Being aware of current Business risks and priorities
- Being alert to situations where fraud may be being perpetrated and concealed from immediate view (e.g. not taking figures or comments at face value, without sight of evidence)
- Ensuring that findings are reported promptly and objectively

3.5 Reporting Process
Each individual audit is concluded with a closing meeting with the auditee.

Documented audit findings for written for each individual assignment with a report sent to the auditee and copied to their line manger.

An escalation process exists for reporting serious financial irregularities on the day of an audit, to enable a decision to be made in respect of suspension or conduct code, while the auditor is still on site.

Aggregated MI and audit reports are generated each month and used to influence Business wide change.

3.6 Quality Assurance
A documented process exists to ensure that audit work is performed to the required standard. Network compliance audit managers are responsible for the effective and proper execution of an assignment to the standards defined in the Audit Process Manual and supporting manuals/procedures/tools.

Section 4 – Code of Ethics

The Code of Business Standards and Post Office Ltd Behaviours and Values apply to all Post Office Ltd employees, outlining the responsibility for carrying out activities in a way, which reflects positively on the business.

POL00083966

While all members of audit teams should be conversant with these standards, the following areas from Part 2 of these standards, personal behaviour, are highlighted due to the nature of the role of the team's activities: -

Personal Conduct
Audit activities are usually performed in the presence of non Post Office Ltd employees (i.e. agents). It is important that they view our operation as efficient and professional.

POL00083966

Behaviour towards colleagues
Team members work closely with different colleagues on a day-to-day basis. These relationships should be based on mutual respect.

Security and trust
Team members have access to confidential information (e.g. details of cash holdings, branch audit findings, robbery/burglary details). To ensure safeguarding of such information, they must ensure that it is not disclosed to unauthorised sources. In particular, details should not be discussed with colleagues in the presence of agents.

Team members are provided with computers and are responsible for ensuring that computers are afforded adequate security (in line with Business instructions, including the use of passwords and storage) and are kept up to date with anti virus software (as informed by IT). The personal use of computers, including installation of non-authorised software is not permitted.

Conflicts of interest
If members of the team are related to, or have close friendships with, Post Office Ltd employees, agents or any staff working in a Post Office branch or cash centre, who may be subject to audit, the line manager and Risk Reporting Advisor must be informed. The Risk Reporting Advisor will maintain a record of these relationships, in a log known as “Declaration of Interests”, in order to avoid compromising the audit plan.

Gifts
Team members should not accept any gift, payment or favour from auditees and if such an offer is made, it should be reported to their line manager.

Courtesy and personal appearance
Team members, who come into contact with both employees and agents on a daily basis, should be aware of the importance that high standards of behaviour and present a smart and clean appearance. Name badges must be worn at all times.

POL00083966

APPENDIX A - SERVICE PORTFOLIO (DUE TO BE REPLACED BY SLA)

Purpose of Audit teams

The primary purpose of audit activity is to provide assurance to its stakeholders that:-

- Post Office Ltd's assets, declared at branches and cash centres, exist. This is delivered through a programme of independent financial audits.
- Business policy, process, procedures and regulatory requirements are being complied with at branches and cash centres. This is delivered through compliance auditing techniques, using agreed compliance programmes, and self-assessment programmes.

Audit Plan

The Audit Plan, endorsed by Post Office Ltd's Risk & Compliance Committee, focuses on a risk-based programme of audits. These audits are based on the outputs of risk models, which provide indications where assets are most at risk. All these audits are undertaken without prior notice to the auditee.

Requests for special audits

Although the majority of audits are based on risk model indicators, there is the facility for management concerns to be raised. This has the effect of either prioritising existing audit plans or considering new audit activity. As any new audit activity will replace an audit prompted by risk models, monitoring of specially requested audits is undertaken to both ensure that these audits are providing value and to help identify any gaps in the indicators of risk models. In the case of requests to audit a crown office, it is important to note that a financial audit will not be undertaken as a substitution for a branch manager's own supervisory checks.

Special requests for audits should be made to the network compliance audit manager (by e-mail or telephone) but please note that we do not perform audits at the request of a subpostmaster, franchisee or branch manager nor do we provide a chaperone service for third party auditors.

Audit Reporting

Each audit is concluded with an individual audit report, containing an action plan to remedy any non-compliance or non-conformance issues. The report is sent by hard copy (to the subpostmaster) or by e-mail (to the agreed representative of a National Multiple or crown office branch

POL00083966

manager). The recipient is required to return a signed section of the report (a compliance certificate) to confirm that the report has been read and that actions have been addressed. An electronic copy of the report is sent to the Business Development Manager and the Outlet Intervention Team.

Financial irregularities that are revealed at audits of agency or franchise branches are escalated to the Contract & Service Manager as a matter of urgency, as these will require a decision on a suspension. Where financial irregularities above £5k do not result in a suspension, the decision will require endorsement by a more senior manager (depending on the value of irregularity revealed).
A summary of the results of audit activity is provided monthly (with more detailed MI reports for those who have requested them) to summarise findings of audits and highlight common issues that require addressing across Post Office Ltd.

Planned branch transfers and closures
We attend transfers or closure of an agency branch, to undertake an independent verification of assets prior to the transfer to the incoming subpostmaster or the final remittance. Other agreed activity is also performed e.g. removal of old accounting records.

These activities are arranged by either Agency Recruitment or the National Equipment Implementation team, with transfers and closures booked on a first come first served basis. Any queries relating to transfers or closures should be addressed initially with Audit Admin Support using the published contact points.

Support is also given for on-site crown office conversions. Audit teams do not provide support for relocation of branches (where a final account is not needed).

Response to robbery & burglary incidents
An audit is arranged for all incidents where a loss of greater than £1k has occurred. Where an auditor attends, a financial audit is performed to establish the loss and arrangements made to clear the loss from the account. In addition, a post incident report is completed and, if the loss is more than £5k or there is evidence of negligence, a procedural security inspection is performed. Serious incidents are also attended by the Security Team.

POL00083966

Annual Certificate of Compliance
Each crown office is required to undertake a self-assessment against key controls. This programme of self-assessments is managed by Network Risk Team. Failures to submit an assessment, in spite of reminders, or failures to remedy non-compliance, noted at subsequent audits, are reported to the Business Development Manager.

Audits of Cash Centres
Audit teams have full responsibility for auditing cash centres and are required to meet minimum auditing requirements stipulated by the Bank of England.

Feedback
Each auditee is provided with a questionnaire, to provide feedback on the audit approach.

All stakeholders of audit teams are invited to provide feedback on a range of attributes within an annual customer satisfaction survey.

POL00083966

Appendix B - Internal Audit Standards (Published by Institute of Internal Audit)

1000 – Purpose, Authority, and Responsibility
The purpose, authority, and responsibility of the internal audit activity should be formally defined in a charter, consistent with the *Standards*, and approved by the board.

> **1000.A1** - The nature of assurance services provided to the organization should be defined in the audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances should also be defined in the charter
>
> **1000.C1** - The nature of consulting services should be defined in the audit charter.

1100 – Independence and Objectivity
The internal audit activity should be independent, and internal auditors should be objective in performing their work.

1110 – Organizational Independence
The chief audit executive should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.

> **1110.A1** - The internal audit activity should be free from interference in determining the scope of internal auditing, performing work, and communicating results.

1120 – Individual Objectivity
Internal auditors should have an impartial, unbiased attitude and avoid conflicts of interest.

1130 – Impairments to Independence or Objectivity
If independence or objectivity is impaired in fact or appearance, the details of the impairment should be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

> **1130.A1 –** Internal auditors should refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an auditor provides assurance services for an activity for which the auditor had responsibility within the previous year.
>
> **1130.A2 –** Assurance engagements for functions over which the chief audit executive has responsibility should be overseen by a party outside the internal audit activity.
>
> **1130.C1** - Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.
>
> **1130.C2** - If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure should be made to the engagement client prior to accepting the engagement.

1200 – Proficiency and Due Professional Care
Engagements should be performed with proficiency and due professional care.

1210 – Proficiency
Internal auditors should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

> **1210.A1** - The chief audit executive should obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.

POL00083966

1210.A2 – The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1210.C1 - The chief audit executive should decline the consulting engagement or obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1220 - Due Professional Care
Internal auditors should apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 - The internal auditor should exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of risk management, control, and governance processes.
- Probability of significant errors, irregularities, or noncompliance.
- Cost of assurance in relation to potential benefits.

1220.A2 – The internal auditor should be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1 - The internal auditor should exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- Relative complexity and extent of work needed to achieve the engagement's objectives.
- Cost of the consulting engagement in relation to potential benefits.

1230 – Continuing Professional Development
Internal auditors should enhance their knowledge, skills, and other competencies through continuing professional development.

1300 – Quality Assurance and Improvement Program
The chief audit executive should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness. The program should be designed to help the internal auditing activity add value and improve the organization's operations and to provide assurance that the internal audit activity is in conformity with the *Standards* and the *Code of Ethics.*

1310 – Quality Program Assessments
The internal audit activity should adopt a process to monitor and assess the overall effectiveness of the quality program. The process should include both internal and external assessments.

1311 – Internal Assessments
Internal assessments should include:

POL00083966

- Ongoing reviews of the performance of the internal audit activity; and

- Periodic reviews performed through self-assessment or by other persons within the organization, with knowledge of internal auditing practices and the *Standards*.

1312 – External Assessments
External assessments, such as quality assurance reviews, should be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization.

1320 – Reporting on the Quality Program
The chief audit executive should communicate the results of external assessments to the board.

1330 – Use of "Conducted in Accordance with the Standards"
Internal auditors are encouraged to report that their activities are "conducted in accordance with the *Standards for the Professional Practice of Internal Auditing*." However, internal auditors may use the statement only if assessments of the quality improvement program demonstrate that the internal audit activity is in compliance with the *Standards*.

1340 – Disclosure of Noncompliance
Although the internal audit activity should achieve full compliance with the *Standards* and internal auditors with the *Code of Ethics*, there may be instances in which full compliance is not achieved. When noncompliance impacts the overall scope or operation of the internal audit activity, disclosure should be made to senior management and the board.

PERFORMANCE STANDARDS

2000 – Managing the Internal Audit Activity
The chief audit executive should effectively manage the internal audit activity to ensure it adds value to the organization.

2010 – Planning
The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

> **2010.A1** - The internal audit activity's plan of engagements should be based on a risk assessment, undertaken at least annually. The input of senior management and the board should be considered in this process.
>
> **2010.C1** - The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Those engagements that have been accepted should be included in the plan.

2020 – Communication and Approval
The chief audit executive should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and to the board for review and approval. The chief audit executive should also communicate the impact of resource limitations.

2030 – Resource Management
The chief audit executive should ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

2040 – Policies and Procedures
The chief audit executive should establish policies and procedures to guide the internal audit activity.

2050 – Coordination
The chief audit executive should share information and coordinate activities with other internal and

POL00083966

external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

2060 – Reporting to the Board and Senior Management
The chief audit executive should report periodically to the board and senior management on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting should also include significant risk exposures and control issues, corporate governance issues, and other matters needed or requested by the board and senior management.

2100 – Nature of Work
The internal audit activity evaluates and contributes to the improvement of risk management, control and governance systems.

2110 – Risk Management
The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.

2110.A1 - The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management system.

2110.A2 - The internal audit activity should evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the

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

2110.C1 - During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and should be alert to the existence of other significant risks.

2110.C2 – Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.

2120 – Control
The internal audit activity should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2120.A1 - Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems. This should include:

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

2120.A2 - Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

POL00083966

2120.A3 - Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

2120.A4 - Adequate criteria are needed to evaluate controls. Internal auditors should ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors should use such criteria in their evaluation. If inadequate, internal auditors should work with management to develop appropriate evaluation criteria.

2120.C1 - During consulting engagements, internal auditors should address controls consistent with the engagement's objectives and should be alert to the existence of any significant control weaknesses.

2120.C2 – Internal auditors should incorporate knowledge of controls gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.

2130 – Governance
The internal audit activity should contribute to the organization's governance process by evaluating and improving the process through which (1) values and goals are established and communicated, (2) the accomplishment of goals is monitored, (3) accountability is ensured, and (4) values are preserved.

2130.A1
Internal auditors should review operations and programs to ensure consistency with organizational values.

2130.C1 – Consulting engagement objectives should be consistent with the overall values and goals of the organization.

2200 – Engagement Planning
Internal auditors should develop and record a plan for each engagement.

2201 - Planning Considerations
In planning the engagement, internal auditors should consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's risk management and control systems compared to a relevant control framework or model.
- The opportunities for making significant improvements to the activity's risk management and control systems.

2201.C1 - Internal auditors should establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding should be documented.

2210 – Engagement Objectives
The engagement's objectives should address the risks, controls, and governance processes associated with the activities under review.

2210.A1 - When planning the engagement, the internal auditor should identify and assess risks relevant to the activity under review. The engagement objectives should reflect the results of the risk assessment.

POL00083966

2210.A2 - The internal auditor should consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing the engagement objectives.

2210.C1 – Consulting engagement objectives should address risks, controls, and governance processes to the extent agreed upon with the client.

2220 – Engagement Scope

The established scope should be sufficient to satisfy the objectives of the engagement.

2220.A1 - The scope of the engagement should include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.C1 – In performing consulting engagements, internal auditors should ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations should be discussed with the client to determine whether to continue with the engagement.

2230 – Engagement Resource Allocation

Internal auditors should determine appropriate resources to achieve engagement objectives. Staffing should be based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

2240 – Engagement Work Program

Internal auditors should develop work programs that achieve the engagement objectives. These work programs should be recorded.

2240.A1 - Work programs should establish the procedures for identifying, analyzing, evaluating, and recording information during the engagement. The work program should be approved prior to the commencement of work, and any adjustments approved promptly.

2240.C1 - Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

2300 – Performing the Engagement

Internal auditors should identify, analyze, evaluate, and record sufficient information to achieve the engagement's objectives.

2310 – Identifying Information

Internal auditors should identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

2320 – Analysis and Evaluation

Internal auditors should base conclusions and engagement results on appropriate analyses and evaluations.

2330 – Recording Information

Internal auditors should record relevant information to support the conclusions and engagement results.

2330.A1 - The chief audit executive should control access to engagement records. The chief audit executive should obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

2330.A2 - The chief audit executive should develop retention requirements for engagement records. These retention requirements should be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

POL00083966

2330.C1 - The chief audit executive should develop policies governing the custody and retention of engagement records, as well as their release to internal and external parties. These policies should be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2340 – Engagement Supervision
Engagements should be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

2400 – Communicating Results
Internal auditors should communicate the engagement results promptly.

2410 – Criteria for Communicating
Communications should include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

2410.A1 - The final communication of results should, where appropriate, contain the internal auditor's overall opinion.

2410.A2 - Engagement communications should acknowledge satisfactory performance.

2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

2420 – Quality of Communications
Communications should be accurate, objective, clear, concise, constructive, complete, and timely.

2421 – Errors and Omissions
If a final communication contains a significant error or omission, the chief audit executive should communicate corrected information to all individuals who received the original communication.

2430 – Engagement Disclosure of Noncompliance with the *Standards*
When noncompliance with the *Standards* impacts a specific engagement, communication of the results should disclose the:

- Standard(s) with which full compliance was not achieved,
- Reason(s) for noncompliance, and
- Impact of noncompliance on the engagement.

2440 – Disseminating Results
The chief audit executive should disseminate results to the appropriate individuals.

2440.A1 - The chief audit executive is responsible for communicating the final results to individuals who can ensure that the results are given due consideration.

2440.C1 - The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, risk management, control, and governance issues may be identified. Whenever these issues are significant to the organization, they should be communicated to senior management and the board.

2500 – Monitoring Progress
The chief audit executive should establish and maintain a system to monitor the disposition of results communicated to management.

POL00083966

2500.A1 - The chief audit executive should establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity should monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

2600 – Management's Acceptance of Risks

When the chief audit executive believes that senior management has accepted a level of residual risk that is unacceptable to the organization, the chief audit executive should discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive and senior management should report the matter to the board for resolution.