Internal Audit Charter

1 Introduction

This charter describes the mission, independence and objectivity, scope and responsibilities, authority, accountability and standards of Castle Trust Bank's Internal Audit function ("CTIA").

2 Mission

The primary role of the Internal Audit function is to help protect Castle Trust's assets, reputation and sustainability by assessing whether all the risks faced by Castle Trust Bank are understood and effectively managed.

3 Independence and objectivity

To safeguard independence, CTIA reports directly to the Chair of the Audit Committee on functional and professional matters. CTIA reports administratively to the Chief Executive Officer. To maintain objectivity, CTIA is not involved in day-to-day control procedures. Each business function is responsible for its own risk management, internal control and efficiency.

4 Scope and responsibilities

5 The scope of internal audit work covers the activities of the whole of the organisation and includes: Purpose, strategy and business model; Organisational culture; Internal governance; The setting of, and adherence to risk appetite; Key corporate and external events; Capital, interest rate and liquidity risks; Risks of poor customer treatment, giving rise to conduct or reputational risk; Environmental sustainability, climate change risks and social issues; Financial crime, economic crime and fraud; Technology, cyber, digital and data risks; Risk management, compliance, finance and control functions; and Outcomes of processes

The work involves periodic appraisal of the process for risk identification and assessments and the design operation of controls. Internal Audit will also undertake periodic testing of transactions and continuous assessments of control operation. The scope of work extends to key process and controls undertaken on behalf of Castle Trust Bank by third parties

.

To fulfil its responsibilities, CTIA will:

- Identify and assess potential risks to Castle Trust's operations – CTIA's view of risk is informed by, but not determined by management's view of risk;
- Review the design and operating effectiveness of the internal governance structures and processes of the organisation;
- Assess the completeness, accuracy and representativeness of information presented to the board and executive management;
- Assess whether the risk appetite is established, reviewed and adhered to;
- Assess whether processes and observed behaviours are consistent with Castle Trust bank values, especially the 'customer first' value:
- adequacy of controls established to ensure compliance with policies, plans, procedures and business objectives;
- Review the adequacy of product governance controls;
- Review the process and models used to manage capital and liquidity risk;

- Assess the means of safeguarding assets;
- Challenge and influence senior management to improve the effectiveness of governance, risk management and internal controls, including identifying efficiencies and removing duplicative and / or redundant controls;
- Regularly consider new and emerging risks, particularly arising from projects and other Castle Trust bank's business initiatives and report the outcome of that consideration in its update to Audit Committee;
- Review the adequacy and effectiveness of the Castle Trust bank's Risk Management, Compliance and outsourced third party assurance functions and place reliance on those functions as a proxy for direct internal audit work, where it is reasonable and appropriate to do so, and where CTIA is satisfied on the reliability of underlying processes;
- Agree SMART and fully costed actions with management to resolve and issues and follow up to confirm that actions have been implemented effectively; and
- Carry out ad hoc appraisals, investigations, or reviews requested by Castle Trust Management.

6 Authority

Internal Audit aims to promote effective control at reasonable cost. To achieve this, CTIA is authorised, in the course of its activities to:

- Have access to all people, systems, documents and records considered necessary for the performance of its functions. This extends to all third parties to whom Castle Trust bank has outsourced significant activities, subject to access protocols as set out in the contractual arrangements with each third party; and
- Require all colleagues to supply such information and explanations as may be needed within a reasonable period of time.

Castle Trust bank Executives should inform CTIA without delay of any significant incident concerning security and/or compliance with policies and procedures and risk management/control failures.

7 Accountability

CTIA will provide its assurance by way of individual assignment reports to management and quarterly summary reports to Executive Committee and to Audit Committee. The Head of Internal Audit will also provide an annual report to Audit Committee on the overall effectiveness of the system of internal control. In this annual report the Head of Internal Audit will provide specific conclusions and observations on:

- The scope areas selected and covered in the year:
- the risk and control culture within the organisation, particularly whether observed behaviours are in line with espoused values and ethics;
- any thematic and systemic issues arising from CTIA's work;
- insights on significant control weaknesses and breakdowns together with a robust root cause analysis, particularly any 'lessons learned' analysis of any significant adverse event;
- management's record of implementing actions agreed in response to issues raised by internal audit and other assurance providers; and
- insights on areas where governance, risk management and internal controls are effective, and where internal audit has identified efficiencies, including the removal of duplicative and / or redundant controls; and

- an assessment of the overall effectiveness of the governance, and risk and control framework of and whether Castle Trust bank's risk appetite is being adhered to.

CTIA will produce a risk based annual audit plan which it will discuss with Castle Trust Executives and present to Audit Committee for approval at its September meeting. Subsequent significant changes to the plan will be presented at each subsequent meeting for review and approval.

CTIA is responsible for planning, conducting, reporting and following up on audit tasks included in the audit plan, and decides on the scope and timing of audits. The details of these processes are defined in the Internal Audit Manual.

Audit fieldwork will be conducted in a professional and timely manner. Reporting of results will include a process to agree on the facts and the validity of any audit issues and actions required to resolve issues. In all cases, follow-up work will be undertaken to ensure adequate implementation of agreed actions.

Where appropriate, details of audit results will be included in support of the quarterly summary reports provided to Audit Committee.

All internal audit work will be carried out either by Castle Trust Bank's in house internal audit function, or, under a co-source arrangement, by a specialist internal audit service provider, particularly for the audit of technology controls and management of capital, liquidity and interest rate risks..

CTIA will coordinate with the Compliance function and external audit to ensure proper coverage and avoid duplication of effort.

8 Standards

CTIA conforms to the International Standards for the Professional Practice of Internal Auditors, the UK's Internal Audit Code of Practice and mandatory internal audit requirements for authorised firms in the UK financial services sector. In the event of conflict between International Standards and UK regulatory requirements, the latter shall prevail in order of importance.