

RISK COMMITTEE TERMS OF REFERENCE

- PURPOSE:** The Risk Committee (“the Committee”) is established by the Board to assist with oversight of the Trustee’s risk management and operational resilience arrangements. The Committee provides independent oversight of whether enterprise and material risks are being managed within the Board-approved risk appetite and in accordance with applicable prudential and regulatory requirements. In fulfilling this purpose, the Committee will have oversight of:
 - Trustee’s Risk Management Framework and Risk Appetite Statement
 - CSC’s Risk Culture
 - Enterprise and material risks across all aspects of the business including operational resilience and crisis management, fraud and compliance, investment, Information and Communications Technology (ICT) and information security, data governance, and corporate sustainability
 - Compliance with relevant prudential standards (including SPS 220, CPS 230 and CPS 234)
 - Material risk incidents, breaches and complaints
 - Emerging and systemic risks
 - Make recommendations to the Board, Audit Committee, People and Governance Committee on matters within its remit.

2. RESPONSIBILITIES

The Committee will provide input to the Audit Committee in relation to the Audit Committee’s obligation to review the appropriateness of CSC’s ‘system of risk oversight and management’ and ‘system of internal control’ under *Public Governance, Performance and Accountability Act 2013* before the Trustee makes its annual Risk Declaration under SPS 220. To facilitate this, the Risk Committee will have oversight of the matters outlined below:

CSC Risk Culture

The Committee will have oversight of:

- The development and effectiveness of the Trustee’s risk culture, including whether behaviours support sound risk management and decision making
- Executive leadership in relation to risk culture
- Risk culture indicators and insights, including survey outcomes, themes from incidents and regulatory feedback, to identify material concerns or trends
- Material risk culture issues for escalation to the Board and oversee management’s response where risk culture may undermine the Risk Management Framework or risk appetite

Risk Management Framework

The Committee will:

- Consider changes and updates to CSC Risk Management Framework, including the Risk Management Strategy
- Review CSC’s Risk Appetite Statement and recommend changes to the Board
- Monitor the external environment impacting on CSC’s Risk Management Framework including relevant regulatory requirements and expectations
- Update CSC’s Risk management structures (Line 1) through Line 2 reporting and deep dives from time to time as requested by the Committee
- Examine CSC’s enterprise risk operating systems
- Review and endorsement of CSC’s risk policies and related control reporting, and recommendations to the Board for approval
- Management’s identification, monitoring, assessment and treatment of Strategic and Operational risks in relation to CSC
- Oversee the identification, assessment and management of material corporate sustainability risks, including climate related risks and opportunities, insofar as they may impact CSC’s operations, risk profile and long-term sustainability

Incidents, Breaches and Systemic matters

Oversight of incidents and breaches including:

- Material breaches, loss and complaints with risk implications
- Root cause analysis and adequacy of remediation actions for significant matters
- Trends and systemic issues arising from incidents and complaints

Fraud and AML/CTF

Oversee CSC's financial crime governance for adequacy and effectiveness of:

- The Fraud Control Plan and key AML/CTF activities, including alignment with the Board's risk appetite and compliance with statutory reporting obligations
- Management's capacity for identifying material breaches, suspicious matter reporting trends, and the progress of remediation for identified control weaknesses
- The Trustee's approach to identifying and managing fraud risk, and escalating matters to the Audit Committee as appropriate

Business Continuity Management & Crisis Management; and Material Service Providers (CPS 230)

The Committee will:

- Monitor The effectiveness of governance and risk management frameworks
- Review CSC's operational resilience, crisis management arrangements and compliance with CPS 230
- Monitor the management of risks related to critical operations and Material Service Providers (MSP), including significant incidents or disruptions and ongoing monitoring of MSP performance

Information and Communication Technology, Data Governance and Cybersecurity Risk

The Committee will:

- Oversee the Trustee's compliance with CPS 234
- Governance arrangements for information security and technology risk and data governance frameworks
- Monitor material ICT and cyber risks, incidents and control weaknesses, including matters with potential operational, regulatory or member impact
- Receive and consider reporting on ICT risk and information security assessments, reviews and remediation activities, escalating material matters to the Board as appropriate

Remuneration and Risk Adjusted Performance Input

The Committee will have oversight of CSC's Remuneration framework review to provide input to the People and Governance Committee on whether:

- Executives and 'material risk takers' operated within CSC's Board approved Risk Appetite for the purposes of CPS 511 Remuneration and Financial Accountability Regime (FAR)
- To recommend any specific reductions or forfeiture of variable pay for conduct in line with CSC's Consequence Management Framework and FAR requirements
- To seek input from the Chief Risk & Compliance Officer on their independent assessment, where appropriate
- Incentive design is aligned with CSC's Risk Appetite Statement

Annual Risk Management Declaration

The Committee will have oversight of:

- Evidence that CSC's risk management framework and internal controls are appropriate for the Trustee's complexity and operated effectively, in all material respects, throughout the year
- Inputs across the three lines of defence to satisfy itself that the annual declaration is supported by robust evidence before recommending to the Audit Committee, and subsequently the Board, for approval
- Advice to the Audit Committee of any matters that should be disclosed as qualifications, limitations or areas of heightened risk in the declaration and recommend to the Audit Committee and the Board whether it is appropriate for the Board to execute the annual Risk Management Declaration

Interaction with other Committees

The Committee will:

- Coordinate with the Audit Committee to assess and recommend the approval of CSC's RMD by the Board
- Provide input to the People and Governance Committee for risk conduct matters relating to CPS 511 Remuneration requirements
- Consult with the People and Governance Committee on changes to, or implementation under, the Remuneration Policy Framework to oversee appropriate reflection and management of risk outcomes
- Provide input to the Audit Committee on systemic issues in relation to internal controls.

3. MEETING GOVERNANCE

Membership:

- Members of the Committee and the Chair of the Committee are appointed by the Board
- In the absence of the Committee Chair, the meeting may elect one of its members to chair the meeting
- The Committee will have at least four members
- A quorum of the Committee is formed when at least 70% of the Committee members are present

Meetings:

- The Committee will meet at least 4 times a year or as otherwise required
- Meetings may be held in person, by telephone or by video conference, or by any combination of these media
- The Committee Chair may convene special meetings when necessary
- The Company Secretary or their delegate will act as Secretary to the meeting
- The Chief Executive Officer, Chief Risk and Compliance Officer and are standing attendees. A delegate of these officers may also attend Committee meetings, subject to prior approval of the Committee Chair.

4. AUTHORITY

The Committee is authorised by the Board, within the scope of its responsibilities, to:

- Do anything necessary for the performance of its functions
- Seek any information it requires from any internal or external party
- Obtain external professional advice as required, including to support and enhance the Committee's performance of its duties from time to time
- Request and/or permit the attendance of any external party as required.

5. REPORTING AND REVIEWING

- The Committee Chair or their delegate will provide updates (including minutes) to the Board at the following Board meeting
- The Committee will consult with other relevant Committees as necessary to make informed decisions and recommendations to the Board
- The Committee will conduct an annual self-assessment, generally as part of the Board performance assessment process, to assess discharge of its responsibilities under these Terms of Reference and the adequacy of its reporting to the Board, and will report its findings to the Board
- These Terms of Reference will be reviewed at least biennially or earlier if required, with recommendations for changes made to the Board for approval.