

## HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

### REVIEW OF THE FOUR MAJOR BANKS (SECOND REPORT)

#### Commonwealth Bank of Australia

**CBA87QW:**

***How regularly and with what specific frequency does the Bank's senior executives formally meet to address risk factors and ensure the implementation of risk mitigation factors?***

***Who is accountable at a senior executive level for the implementation of such risk mitigation mechanisms?***

**Answer:**

Commonwealth Bank's highest management committee is the Executive Committee and includes the CEO, the Group Chief Risk Officer, all Group Executives with responsibility for business units and all other Group Executives. It meets regularly (generally weekly) and agenda items include consideration of risk matters where relevant. A standing agenda item is major operational risk events.

The Executive Committee is supported by a structure of sub-committees aligned to various risk types and separate leadership committees within the business units. Each business unit has its own risk governance forum which considers risk pertinent to that business unit. These committees meet regularly (generally monthly).

The various committees perform monitoring of risk profiles, including incidents and issues, in accordance with the relevant frameworks. Actions arising from these committees, including any risk mitigation actions, are allocated to the appropriate specific members of the committees.

Each month the CEO meets with the Chief Risk Officer and Chief Financial Officer to review compliance, conduct and operational risk matters.

The CEO also has visibility of key risk issues in each business unit through his regular meetings with each of the Group Executives. Group Executives notify the CEO of relevant risk incidents as they arise.

We believe that the global best practice approach to managing risk in financial institutions is through the Three Lines of Defence model which Commonwealth Bank has adopted. Under this approach:

- Group Executives, who report to the CEO, own the risks within their business unit and are accountable for the effective implementation of the Group risk frameworks (Line 1);
- business units are overseen by an independent risk function, reporting to the Group Chief Risk Officer, who establish and maintain the risk frameworks and provide review and challenge to their deployment (Line 2); and
- there is further independent assurance provided by Group Audit and Assurance (Line 3).