Technologies

Audit, Risk and Security Committee Terms of Reference

July 2025

1. Introduction

The Audit Risk and Security Committee (Committee) is a committee of the Board of Directors of CEA Technologies Pty Limited (Company).

The Board established the Committee under the Company's constitution.

These Terms of Reference set out the scope of the Committee's responsibilities in relation to the Company.

2. Purpose

The purpose of the Committee is to assist the Board in fulfilling its corporate governance and oversight responsibilities in relation to corporate reporting processes, including the financial reporting process, risk management and internal control, external audit, internal audit and compliance (including but not limited with, the security provisions and standards of the Defence Industry Security Program, Australian Signals Directorate, Australian Security Intelligence Organisation, the Vice Chief of the Defence Force Group and the Australian Government Security Vetting).

In carrying out its role, the Committee has authority from the Board to review and investigate any matter within the scope of this Charter and make recommendations to the Board in relation to the outcomes. The Committee has no delegated authority from the Board to determine the outcomes of its reviews and investigations; with the Board retaining its authority over such matter.

3. Financial reporting

The Committee is responsible for:

a. receiving, reviewing and recommending for adoption by the Board of:
   i. annual budgets for their appropriateness and consistency with the Company's strategic objectives;
   ii. quarterly, or more often if required, monitoring of the Company's expenditure and revenue against the budget; and
   iii. all expenditure submitted for Board approval (i.e. where the proposed expenditure exceeds the Chief Executive Officer's level of delegated financial authority).

b. examining and assessing:
   i. the appropriateness of accounting and financial reporting policies, systems and processes;
   ii. the annual financial statements, focusing on changes to accounting policies, significant audit adjustments and compliance with accounting standards and legal requirements; and
   iii. the annual report, including compliance with the Public Governance, Performance and Accountability (PGPA) Act 2013 and PGPA Rules.

4. Risk management and internal control

The Committee is responsible for:

a. assessing and prioritising the areas of greatest potential financial risk, including:
   i. safeguarding assets;
   ii. litigation and claims;
   iii. non-compliance with laws, regulations, standards and best practice guidelines that may result in significant financial loss;
   iv. important judgments and accounting estimates; and
   v. maintenance of proper accounting records.

b. assessing the internal process for determining areas of greatest potential financial risk;

c. assessing and monitoring the management of areas of greatest potential financial risk;

d. reporting to the Board on the adequacy of the financial risk management;

e. assessing and recommending to the Board for adoption the scope, cover and cost of insurance;

f. reviewing management's processes for assessing and monitoring compliance with applicable laws, regulations and other requirements relating to:
   i. the security provisions and standards of Defence, as promulgated in the Defence Security Principles Framework; and
   ii. the external reporting of financial and non-financial information (including, among other things, preliminary announcements, interim reporting, open or one-on-one briefings and continuous disclosure).

g. overseeing the establishment and implementation of risk management and internal compliance and control systems and ensuring there is a mechanism for assessing the efficiency and effectiveness of those systems;

h. approving and recommending to the Board, policies and procedures on risk oversight and management to establish a system for:
   i. identifying, assessing, monitoring and managing risk; and
   ii. disclosing any material change to the Company's risk profile.

i. regularly reviewing and updating the Company's risk profile;

j. assessing the adequacy of the internal risk control system with management and internal and external auditors;

k. monitoring the effectiveness of internal risk control systems;

l. satisfying itself that the risk management system takes into account all material risks, including risks arising from:
   i. strategic risk;
   ii. operational risk;
   iii. security risk;

iv. legal risk;
v. reputational risk;
vi. credit risk
vii. market risk; and
viii. liquidity risk.

m. confirming the Company has the controls and processes in place for transactions that may carry more than an acceptable degree of risk;
n. confirming the internal process for determining, monitoring and managing areas of greatest legal and regulatory risk;
o. receiving reports from management of any actual or suspected fraud, theft or other breach of the law;
p. reporting and making recommendations to the Board regarding:
    i. the management of areas of greatest legal and regulatory risk (including fraud and theft); and
    ii. compliance with legal and regulatory obligations.
q. reporting to the Board on the effectiveness of the management of the Company's material business risk exposure including assurance and audit activities undertaken which may impact the Company's risk profile.

5. Security

The Committee is responsible for:

a. security risk oversight of all aspects of security within the Company in order to ensure all necessary authorities and compliance are maintained as it relates to:
    i. the Company's policies, plans, metrics and programs relating to the physical security of the Company's facilities and employees as well as enterprise cybersecurity and data protection risks associated with the entirety of the Company's security-related infrastructure and related operations; and
    ii. the effectiveness of the Company's programs and practices for identifying, assessing and mitigating such risks across the entirety of the Company's business operations.
b. overseeing the Company's cyber crisis preparedness, security breach and incident response plans, communication plans, and disaster recovery and business continuity capabilities with respect to the forgoing;
c. oversight of safeguards used to protect the confidentiality, integrity, availability, safety and resiliency of the Company's employees, facilities, intellectual property and business operations;
d. oversight of the Company's compliance with all applicable information security and data protection direction from the Commonwealth of Australia and industry standards, new or updated legal or operative implications of security, data privacy, and/or other regulatory or compliance risks to the Company or the Company's employees, facilities and business operations and the threat landscape facing the Company and the Company's business operations;

e. strategic oversight of the Company's physical and cybersecurity strategy, crisis or incident management and security-related information technology planning processes and review the strategy for investing in the Company's security systems;

f. overseeing the Company's public disclosures in reports filed with all regulatory bodies and the Commonwealth of Australia, relating to all aspects of security including privacy, network security and data security; and

g. regularly reviewing the security risks, and in particular the cybersecurity risks, associated with the Company's outside partners (such as stakeholders, vendors, suppliers, operations partners).

6. External audit

The Auditor General is the external auditor of the Company. As permitted the Auditor-General Act 1997, the Australian National Audit Office may engage third parties under contract to assist with the conduct of the audit. The Committee is responsible for:

a. approving and recommending to the Board for acceptance, the terms of engagement with the external auditor at the beginning of each financial year;

b. regularly reviewing with the external auditor:

   i. the scope of the external audit;

   ii. identified risk areas; and

   iii. any other agreed procedures.

c. regularly reviewing the effectiveness and independence of the external auditor taking into account:

   i. the length of appointment;

   ii. the last dates lead engagement partners were rotated;

   iii. an analysis and disclosure of fees paid to external auditors, including the materiality of fees paid for non-audit services and the nature of those services; and

   iv. any relationships with the Company or any other body or organisation that may impair or appear to impair the external auditor's independence.

d. meeting periodically with the external auditors and inviting them to attend Committee meetings to:

   i. review their plans for carrying out internal control reviews;

   ii. consider any comments made in the external auditor's management letter, particularly, any comments about material weaknesses in internal controls and management's response to those matters; and

   iii. make recommendations to the Board.

e. that acceptable provision is made for the accounting of intellectual property and research and development;

f. asking the external auditor if there have been any significant disagreements with management, whether or not they have been resolved;

g. monitoring and reporting to the Board on management's response to the external auditor's findings and recommendations; and

h. receiving and reviewing the reports of the external auditor.

7. Internal audit

The Committee is responsible for:

a. overseeing the scope of the internal audit, including reviewing the internal audit team's mission, Terms of Reference, qualifications and resources;

b. reviewing and approving the scope of the internal audit plan and work programme;

c. overseeing the liaison between the internal audit team and the external auditor; and

d. confirming the internal audit team reports directly to the Committee.

8. Committee composition

The Committee must comprise:

a. at least three Directors; and

b. at least one Director appointed by each shareholder.

The Committee will appoint a Chair and Deputy Chair. The Chair and/or Deputy Chair may not be the Board Chair.

The roles of Chair and Deputy Chair may rotate between two Committee members appointed as Chair of the Audit and Risk and Chair of Security in accordance with the structure outlined in Section 9.

The Company Secretary is secretary (but not a member) of the Committee.

The Committee must be of sufficient size and technical expertise to effectively discharge its mandate.

Each member of the Committee must be able to read and understand financial statements and at least one member must be a qualified accountant or other financial professional with experience of financial and accounting matters.

Each member of the Committee should have an understanding of the industry in which the Company operates.

9. Committee meetings

The Committee will meet as often as it considers necessary but at least three times per calendar year.

A quorum for a Committee meeting is three Committee members (of which one must be appointed by the Shareholder Ministers and one must be appointed by Ian Croser).

Committee meetings will be conducted in two distinct parts to reflect the Committee's responsibilities:

- Part A – Audit and Risk: This portion of the meeting will focus on matters relating to audit, risk, compliance, physical security and financial oversight. It will be chaired by the Chair of Audit and Risk, with the Chair of Security acting as Deputy Chair.
- Part B – Security: This portion of the meeting will focus on all matters relating to security, including enterprise cybersecurity and data protection, security-relating infrastructure, business continuity planning and related operational matters. It will be chaired by the Chair of Security, with the Chair of Audit and Risk acting as Deputy Chair.

Committee meetings may be held by any technological means allowing its members to participate in discussions even if all of them are not physically present in the same place. A member who is not physically present but participating by technological means is taken to be present.

Questions arising at a meeting of the Committee are to be determined by a majority of votes of the members of the Committee present and voting. The Chair of that part of the meeting has a casting vote, unless only two members of the Committee are present and entitled to vote on the question.

The Committee may invite other persons it regards appropriate to attend Committee meetings.

10. Minutes of Committee meetings

The Committee must keep minutes of its meetings.

Minutes of each Committee meeting must be included in the papers for the next full Board meeting after each meeting of the Committee, except if there is a conflict of interest.

Minutes must be distributed to all Committee members, after the Committee Chair has approved them.

The agenda and supporting papers are available to Directors upon request to the Committee secretary, except if there is a conflict of interest.

11. Reporting to the Board

The Committee Chair must report the Committee's findings to the Board after each Committee meeting.

12. Access to information and independent advice

The Committee may seek any information it considers necessary to fulfil its responsibilities.

The Committee has access to:

a. management to seek explanations and information from management; and

b. internal and external auditors to seek explanations and information from them, without management being present.

The Committee may seek professional advice from employees of the Company and from appropriate external advisers. The Committee may meet with these external advisers without management being present.

13. Review and changes to these Terms of Reference

The Committee will review these Terms of Reference annually or as often as it considers necessary and submit any proposed revisions to the Board for consideration and approval.

The Board may change these Terms of Reference from time to time by resolution.

14. Approved and adopted

These Terms of Reference were approved and adopted by the Board on 30 July 2025.