CBA Information Security Statement

September 2025

Commonwealth Bank of Australia

Table of Contents

1 Purpose and Scope

The Information Security Statement (the Statement) provides a high-level overview of the governance approach and controls implemented by the Commonwealth Bank of Australia and Bankwest (together, 'CBA' for the purposes of the Statement) to manage information security risks.

Drawing on the structure provided by the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0, the Statement sets out CBA's approach to information security management using the six functions of Govern, Identify, Protect, Detect, Respond, and Recover.

This Statement sets out some of the step's CBA takes to help mitigate different types of information security risk in the context of the constantly evolving threat landscape, and the nature of information we hold and services we provide. The mitigation measures outlined in the Statement cannot provide assurance that all information security attacks against CBA will be prevented.

Information contained in the Statement is general in nature and is provided as a guide only. Reasonable steps were taken to check the information contained in this statement prior to publication, however the information is subject to change.

2 Govern

2.1 Structure

The Technology unit comprises various teams responsible for digital delivery, Group data and analytics, technology and technology infrastructure, cyber, fraud, physical security and business resilience for all divisions across CBA. The Group Security function within Technology brings together key security functions, which consists of approximately 700 staff members (as at the time of publication) dedicated to supporting cyber security for CBA, under the leadership of the Chief Security Officer, who reports to the Chief Information Officer.

2.2 Strategy

Cyber security is identified as a material non-financial risk for CBA. To manage cyber security risk, CBA implements a cyber security strategy which focuses on four key priorities:

- To build leading end-to-end cyber capability
- Prioritise protection of critical assets
- Instil discipline to deliver securely at velocity

- Safeguard Australians through industry partnerships.

As cyber threats become more frequent and complex, we collaborate with the Australian Government and industry peers to strengthen collective cyber security resilience. This includes actively participating in initiatives such as the Executive Cyber Council, which was established as part of the 2023-2030 Australian Cyber Security Strategy with the aim of bringing together cyber experts from across Government and industry to co-lead national cyber security priorities.

CBA also invests in strategies, advanced technologies such as AI and GenAI and skilled teams to help protect customers, assets and data.

2.3 Regulatory Obligations

CBA applies a Risk Management Framework (RMF) aligned with industry standards and maintains an information security capability in accordance with domestic and international regulatory obligations. This includes the Australian Prudential Regulation Authority (APRA) standards such as CPS 234 (Information Security), which mandates effective information security controls, governance, and incident response, CPS 230 (Operational Risk Management) which sets the requirements for operational risk management, business continuity, and third-party risk, and CPS 220 (Risk Management) which requires the maintenance of risk management frameworks and practices. CBA also aligns with relevant legislations such as the Security of Critical Infrastructure Act 2018 (SOCI), the Privacy Act 1988, and the Cyber Security Act 2024.

2.4 Privacy

Privacy is identified as a material non-financial risk for CBA. Policies and Standards are in place to manage customers' personal information, according to its privacy obligations. For more information on how we handle and protect personal information, please refer to our Privacy Statement.

2.5 Risk Management Framework

The RMF outlines CBA's expectations on how to identify, measure, monitor and respond to risks. The RMF is comprised of systems, structures, policies, processes and people. They work together to help identify, assess and mitigate internal and external sources of risk.

2.6 Roles, Responsibilities, and Authorities

The Board is responsible for overseeing the RMF and its operations by management and the management of strategic and emerging material risks, including cyber security risks. Key activities in FY25 included:

- Overseeing the execution of our cyber security strategy.
- Receiving updates on cyber security risk from the Board Risk & Compliance Committee (BRCC).
- Continuing focus on cyber security at both the December 2024 and April 2025 strategy deep-dives.

CBA maintains defined roles and responsibilities for the oversight and management of information security operations and risks, including (but not limited to) the Board and its

Committees, senior management and individuals. In particular, roles and responsibilities are reflected in a range of policy documents, including:

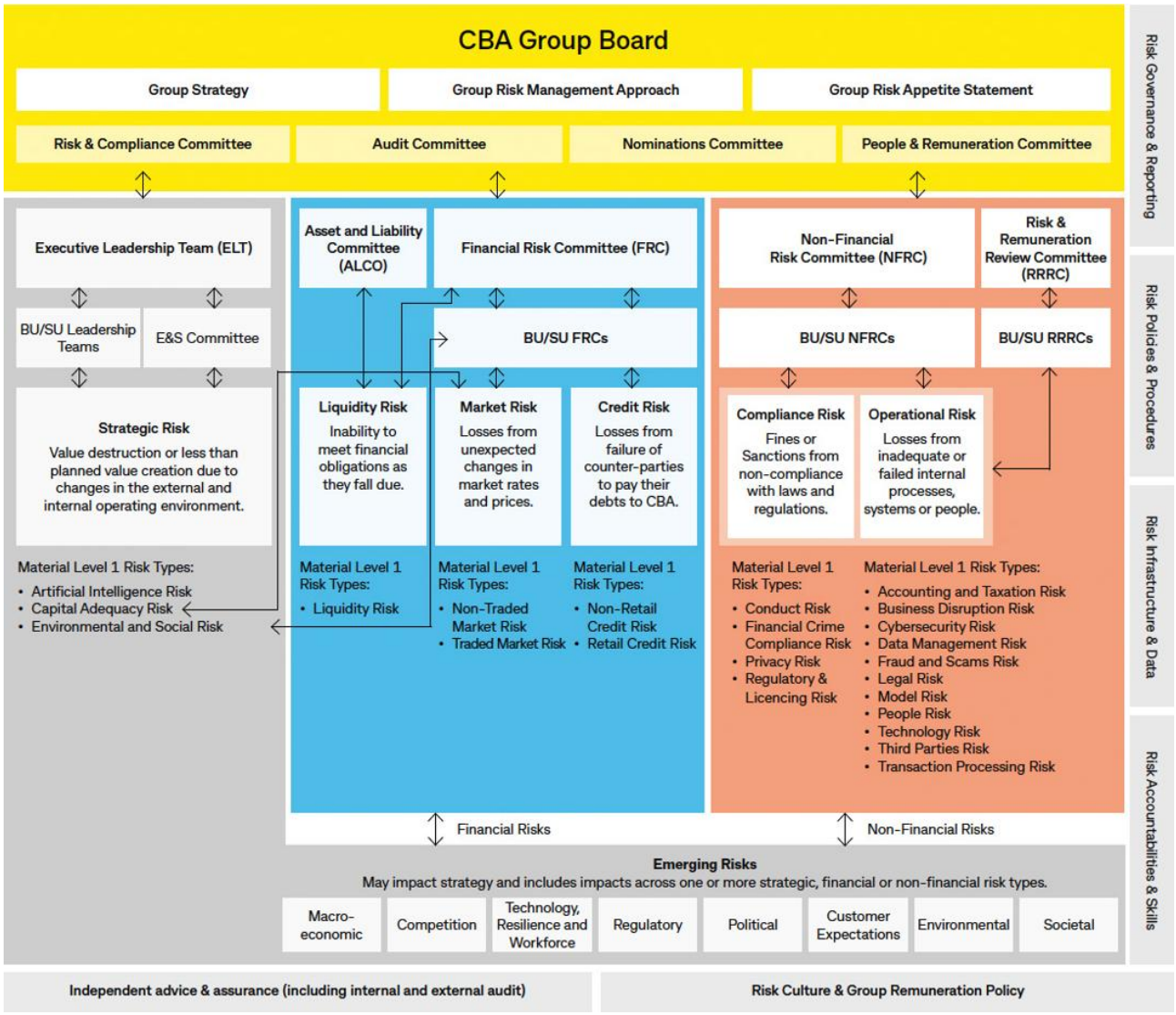
- The Group Information Security Policy Framework;
- Charters for the Board, its Committees, and other governing bodies; and
- The Group FAR (Financial Accountability Regime) Policy.

Each year the Board assesses the maturity of the RMF in managing material risks through the Risk Management Declaration (RMD), and adjusts the RMF as required.

To enable those responsibilities to be discharged, reports are provided to the Board, and to other Committees responsible for overseeing the management of cyber security risks for CBA, on cyber security matters including (but not limited to) the cyber threat landscape, cyber risk management, cyber security posture, and incident management. Cyber security as a risk domain falls within the remit of the BRCC.

In FY25 the BRCC supported the Board by reviewing CBA's risk-based approach to technology and cyber security controls. This included considering the use of risk scenarios to support the assessment of cyber security risk exposure and associated remediation activities.

The framework below provides an overview of organisational and governance structures of CBA, through which various risk types, including cyber security risks, are escalated.



2.7 Policy

The Group Information Security Policy Framework comprises a suite of documents which outline the requirements for managing cyber and information security risk and resilience within CBA.

The Framework is comprised of:

- Policy: concise, high-level policy statements that govern decision making
- Standards: specific rules, expectations or criteria that must be met to comply with a policy
- Guidelines & Resource: supplement the Standards and other resources

The requirements in the Group's Information Security Policy Framework are guided by industry standards and frameworks such as those issued by the International Organization for Standardization (ISO) and NIST CSF 2.0, and covers various information/cyber security domains including (but not limited to):

- Information security policies;

- Organisation of information security;
- Human resource security;
- Asset management;
- Access control;
- Cryptography;
- Physical and environmental security;
- Operations security;
- Communications security;
- System acquisition, development, and maintenance;
- Third party relationships
- Information security incident management;
- Information security business continuity management; and
- Compliance.

2.8 Oversight

CBA monitors and manages its exposure to financial, non-financial and strategic risks, and has risk management policies, processes and practices that support its risk governance. This risk governance approach applies to the management of cyber security related risks, such as the risks associated with internal or external attack, and the risk posed by an attack on a third party of CBA.

2.9 Cyber Security Supply Chain Risk Management

CBA relies upon third parties to provide products or services to meet a range of operational needs. This presents an exposure to potential disruptions, delays, and failures in the supply chain that can impact products, services, and operations.

CBA assesses and manages third party risk, taking into account the relative risk that party represents, considering factors such as:

- The level of cyber inherent risk presented by the third party
- The type of third party CBA is working with
- The nature of CBA's relationship with the third party
- The nature and sensitivity of the information being handled by the third party.

Information security risks associated with the third party are mitigated through the implementation of controls, such as (but not limited to):

- Assessment of the information security controls operated by the third party, or reviews of independent reports evidencing these controls
- Technical security assessments or testing in relation to network or system connectivity between CBA and the third party
- Compliance with relevant approved network connectivity patterns
- Contractual obligations on the third party

- Ongoing governance of the third party

2.10 Board Skills Matrix

The Board recognises the importance of having appropriate skills and experience to support decision making and oversight. The Board skills matrix sets out the skills and experience considered essential to the effectiveness of the Board and its Committees. It is used to guide the Board renewal process. 'Digital and technology' is one of the skills included in the Board skills matrix which describes that a director has experience in technology, use of data and analytics, digital transformation and innovation and their impacts on customer experiences, cyber security and other technology risks. On the digital and technology skill of our 10 Board members, three have been assessed as 'high competency, knowledge and experience.'

For more information on the Board skills matrix and the experience of our directors, see pages 49–53 of our Annual Report 2025.

3 Identify

3.1 Asset Management

CBA maintains an IT asset management inventory and supporting process for the management of assets through their lifecycle.

3.2 Threat Intelligence

Cyber threat intelligence is used to provide awareness and actionable insights to understand the cyber security threats and threat actors in the external environment that may target or impact CBA.

CBA's cyber threat intelligence capabilities include monitoring the external cyber threat landscape, and sourcing of information from a network of trusted industry peers, private sector security groups, intelligence vendors, law enforcement and government agencies.

Tactical, operational, and strategic intelligence produced by the Cyber team provides actionable intelligence that guide CBA's efforts to adapt, detect, and respond to cybersecurity threats.

3.3 Personnel Due Diligence

CBA undertakes personnel due diligence checks on employees, secondees, contractors, service providers and volunteers.

Personnel due diligence can include checks on:

- Right to work;
- Identification verification;
- Background screening;

- Qualification verification; and
- Conflicts of interest

3.4 Information Classification and Handling

CBA classifies the criticality and sensitivity of its information assets, including those managed by third parties, in accordance with the Group Information Security Policy Framework. The classification approach includes:

- Mechanisms to define information assets and tier IT systems and services according to their criticality, considering the inter-relationship between information assets and IT services;
- Mechanisms to tier suppliers according to their criticality, considering the sensitivity and volume of the information assets handled by such third parties; and
- Labelling of information contained in documents and emails.

Information is then stored and handled throughout its lifecycle in accordance with its assigned classification, using tools and processes approved for that classification level.

4 Protect

4.1 Identity and Access Management

Identity and Access Management (IAM) works to prevent unauthorised access to CBA systems and services.

The Group Information Security Policy Framework requires controls to be set in place regarding:

- Identity management: maintaining role creation, modification, review, segregation of duties, and retirement;
- Identity lifecycle management: provision, review, and removal of access;
- Authentication management: implementing steps that require authentication of users that request access to systems and services; and
- Access assurance: having identity and access assurance governance processes in place that monitor and review compliance with CBA standards.

4.2 Cyber Training and Awareness

Staff training and awareness is a foundational component of CBA's cyber security risk framework. The provision of regular training aims to support staff understanding of the current cyber security threat landscape and commonly used techniques, such as social engineering, including phishing, credential compromise, data breaches and ransomware. It also promotes best practices such as using strong passwords, handling sensitive information

securely, and reporting suspicious activity. CBA's information security training and awareness program includes:

- Mandatory induction training upon joining CBA, along with messaging on cyber security best practices, reporting avenues, and available information classification and handling resources.
- Regular communications to staff, such as cyber security intranet articles and awareness sessions. Internal social network groups are also used to address staff queries, share announcements, and provide cyber awareness updates.
- Phishing simulations to all staff, with additional targeted behavioural training for those who indicate the need for additional support.
- Mandatory annual eLearning refresh across CBA on information security that covers topics such as privacy, data breaches, information classification and secure handling, social engineering, and strong passwords.
- Elective technical learning and training for specific role types.

The information security training and awareness program aims to embed a security-conscious culture and to empower staff to be an important line of defence against cyber threats.

4.3 Data Security

4.3.1 Cryptography and Key Management

Cryptography deters and helps prevent unauthorised access or change to data within CBA IT systems and services.

The Group Information Security Policy Framework outlines the requirements for cryptographic algorithms and usage, certificate usage and management, and key management for systems and infrastructure supporting the CBA's business processes. CBA utilises cryptographic controls to help protect information assets.

4.3.2 Secure Information Transmission

The Group Information Security Policy Framework sets out the requirements to securely transmit information electronically based on the classification of the information. Supporting processes and controls help protect information transferred digitally within CBA and with external parties.

4.3.3 Data Loss Prevention

CBA has implemented software and controls to monitor electronic data transfers. This safeguard is known as data loss prevention and assists in keeping CBA and customer data secure. These controls are implemented across CBA to help detect and reduce the exposure of accidental loss or malicious theft of CBA data/information, in particular sensitive customer or commercial data/information, in accordance with the Group Information Security Policy Framework.

4.4 Secure Configuration Management

Secure configuration management provides a technology specific configuration baseline to help prevent the exploitation of assets within the CBA's IT environment throughout their operating lifecycle.

The Group Information Security Policy Framework requires secure configuration baselines to be established, implemented and actively managed throughout an asset's lifecycle. CBA uses baseline compliance scanning solutions to scan assets against established configuration baselines.

4.5 Vulnerability Management

Vulnerability management is used to help prevent or mitigate the successful exploitation of potential vulnerabilities which may exist in IT assets.

The Group Information Security Policy Framework defines the minimum baseline requirements for protecting CBA and its information through identification, prioritisation and management of potential vulnerabilities. The framework requires that security vulnerabilities be identified in a timely manner including by way of maintaining a register of information systems and services, using appropriate discovery methods to identify security vulnerabilities, ensuring availability of scanning targets, and scanning for vulnerabilities using approved scanning services.

4.6 Malware Protection

Endpoints, servers and cloud workloads can be vulnerable to the introduction of malware which can disrupt systems and compromise data. To address risks arising from malware, the Group Information Security Policy Framework requires malware protection activities include monitoring external threat intelligence sources to identify new malware threats and implementing emergency procedures for dealing with malware related incidents.

CBA maintains centrally-managed anti-malware capabilities, which include anti-virus, endpoint detection and response and application allowlisting controls.

4.7 Network Security

Network security helps protect the confidentiality, integrity and availability of the CBA's infrastructure. It works to help prevent the entry or proliferation of malicious threats into or within the CBA's IT environment at the network layer.

The Group Information Security Policy Framework defines the key principles of network security and the respective security controls. These principles provide the guardrails for the design and governance of physical and logical networks to help detect and protect against malicious activity which may be harmful to CBA.

CBA utilises a wide range of technologies to detect and help protect against anomalous traffic, access to inappropriate web content, and restrict insecure or unapproved devices, services and flows into or within the network.

4.8 Device Security

The Group Information Security Policy Framework defines minimum device management requirements to help protect CBA and its information through identification, prioritisation and management. The Group Information Security Policy framework outlines the requirements for network connections and remote access, acceptable use of devices, data storage and encryption, and return/disposal of devices.

4.9 Application Security

Application Security (AppSec) helps to reduce the number of potential vulnerabilities introduced into software developed internally by CBA by seeking to embed security capabilities into the software development lifecycle. The Group Information Security Policy Framework outlines the requirements for developing secure applications.

AppSec capabilities within CBA include:

- Tooling: Governance and support for code scanning tools, which are used to assist developers to self-identify security issues in their code early on in the development lifecycle;
- Training: Providing both informal training, through developer "brown bag" sessions, as well as more formal secure development training content, covering both general security best practice, as well as CBA-platform-specific vulnerabilities; and
- Consulting and code reviews: Performing code reviews and code audits to help identify potential security weaknesses, and providing security consulting to projects to support adoption of secure development practices from the outset.

4.10 Physical Security

To help protect CBA's IT infrastructure and the information it processes and stores, physical safeguards are utilised for facilities which host CBA infrastructure, assets or data. These safeguards are designed to protect against and deter unauthorised access, detect attempted or actual unauthorised access, and activate an effective response if required.

These safeguards also apply in international locations, and extend to facilities and equipment owned and operated by CBA, or on behalf of CBA by an approved third-party vendor.

Physical security measures are designed to reduce a number of risks including theft of CBA's IT assets, physical damage to CBA's IT systems or assets, unauthorised tampering with CBA's systems and unauthorised access to CBA's IT facilities, damage or unavailability caused by environmental factors and compromise of sensitive CBA data contained on IT systems.

5 Detect

5.1 Penetration Testing

Penetration testing aims to evaluate the security posture of a system by simulating an attack by a malicious user. The process involves an active analysis of the system and exploitation of potential vulnerabilities.

CBA undertakes penetration testing both during project/IT change phases as well as on a periodic schedule for production systems. CBA's penetration testing programme, including nature and frequency of testing is informed by various factors such as:

- Specific penetration testing requirements enshrined in legislative or regulatory schemes applicable to the CBA;
- The nature of the information assets including criticality, where continually developed, and where developed in-house; and
- Cyber threat intelligence on the techniques of threat actors and targets.

5.2 User Behaviour Analytics

CBA has implemented software and controls to monitor staff access to customer information and help detect inappropriate access. Instances of suspected unauthorised access are investigated and managed in accordance with CBA's incident response plans and Group Conduct Policy, which may result in disciplinary action.

6 Respond

6.1 Incident Response

CBA maintains various plans, playbooks and capabilities to support the management of technology and operational incidents, including crisis events – which cover:

- Determination of the course of action to be adopted following identification of incidents through monitoring processes;
- Communication of events and alerts to relevant stakeholders;
- Investigation of cause and impacts; and
- Mitigation of risk and impacts to the Group.

These are supplemented by specific information / cyber security incident response plans and capabilities as set out below.

6.2 Incident Response Preparedness and Management

Information / cyber security, data breaches and third party cyber incidents (Incident/s) impacting CBA are managed through dedicated response plans, processes and specialist teams. Response activities across typical Incident phases include:

- Preparation: Establishing and training team members, acquiring necessary tools, and assessing risks for the prevention, detection, and response to Incidents;
- Identification: Potentially adverse events are brought to the team's attention through detection, response and reporting activities within the Group and by third parties;
- Triage: The validity of the initial alert is confirmed and initial response action and priority agreed and committed;
- Investigation: Relevant systems and information is assessed to determine the scope and impacts of the Incidents;
- Remediation: Planning and execution of activities to contain and eradicate the threat and recover from the Incidents; and
- Post-incident: Assessing and documenting lessons learned, sharing outcomes with key governing bodies, and improving capabilities with the aim of enhancing the organisation's ability to prevent, detect, and respond to cyber security incidents.

Where an incident is determined to be a significant event that has the potential to impact CBA, the incident is handled under the Group's Crisis Management Framework, which guides the organisational response to a significant disruptive risk event, with the objective of minimising the impact to staff, customers, business operations and communities.

To keep up with the ever-changing evolution of cyber threats, CBA tests and updates incident response plans, to help them remain fit for purpose. In addition, CBA leverages external expertise and undertakes internal exercises to help build and consolidate readiness for an incident.

Further, in recognition of CBA's role in the broader financial ecosystem, CBA participates in industry-wide exercises in coordination with government and regulatory stakeholders.

6.3 Incident Notifications Reporting

CBA is required to report notifiable data breaches and cyber security incidents to domestic and international regulators. The 2024 Sustainability performance metrics and disclosures which is available on the CBA website, contains the definition and number of data breaches reported (under the 'Governance' tab).

7 Recover

7.1 Cyber Recovery Planning

CBA maintains capabilities to prepare for recovery from major cyber incidents and minimise the impacts to customers and operations. This includes plans and playbooks for coordination of recovery activities, and planning and testing of the restoration of impacted technology.

7.2 Business Continuity Planning

CBA maintains an operational risk management framework that allows for the identification, assessment, and management of risk to critical operations. This includes business continuity plans that the associated tolerance levels for disruption, and the response steps that minimise impact to critical operations. The business continuity plans are tested on a periodic basis through a program that covers a range of scenarios, and the results are reported to senior management.

8 Review

Cyber Security engages external firms and subject matter experts to conduct reviews and provide feedback on the CBA's cyber strategic priorities and provide assurance on an annual basis of compliance with regulatory obligations such as APRA's CPS-234 Information Security. These external audit reports are provided to the Board through governance mechanisms. CBA also participates in external and regulatory reviews which help identify areas for improvement and benchmark CBA against best-in-class and industry peers.