CBA Information Security Statement

July 2024

Commonwealth Bank of Australia

Contents

1 Purpose and Scope of Statement

This information security statement provides a broad overview of the controls and capabilities adopted by the Commonwealth Bank of Australia (CBA) and Bankwest (together, the 'Group' for purposes of this statement) in managing information security risk across those businesses.

Drawing on the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), this statement sets out the Group's approach to information security management in the frame of the six NIST CSF functions i.e. Govern, Identify, Protect, Detect, Respond, and Recover.

This statement sets out the steps taken by the Group to mitigate the different types of cyber risk that are anticipated to continue growing due to the fast-evolving nature of the cyber threat landscape and nature of the information we hold and services we provide. The mitigation measures outlined in this statement cannot provide assurance that all cyber attacks against the Group will be prevented.

Information contained in this 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 its publication, however the information is subject to change.

2 General

2.1 Strategy and Team Structure

The Group's Technology Business Unit comprises various teams providing technology and digitisation capability, and otherwise supporting the Group's Retail, Business, Institutional, and Market operations. The Group Security function within Technology brings together key security functions for the Group, including Cyber Security which supports the management of information security risk and resilience for the Group. The Group has appointed personnel into key roles with formalised accountability for management of information security risk and resilience, in particular the Chief Information Officer (CIO) and the Chief Security Officer (CSO).

Technology maintains a strategy that sets out the overarching key pillars which include, security, resiliency and reliability. The Group's cyber security strategy in turn expands on the Technology strategy and sets out the Group's strategic priorities for the management of cyber security risk and resilience. These strategies guide ongoing initiatives and prioritisation decisions.

As at the time of publication, the Cyber Security function is comprised of approximately 700 staff.

2.2 Privacy

Privacy and data management is a material non-financial risk to the Group and is subject to continual investment and uplift. For more information on how we seek to mitigate our material risk types, please refer to our risk disclosures in our latest Annual Report on our Investor Centre.

3 Govern

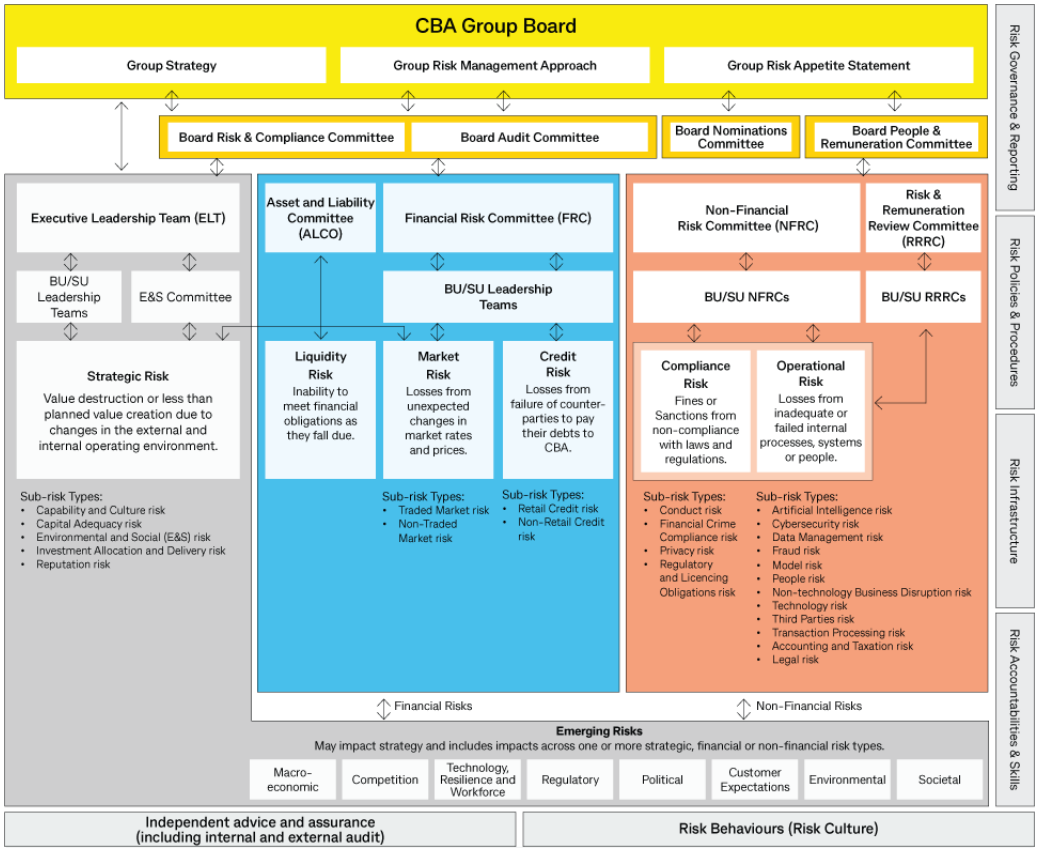
3.1 Roles, responsibilities, and authorities

The Group maintains defined roles and responsibilities for information security, including (but not limited to) the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.
In particular, roles and responsibilities are reflected in:

- The Group Information Security Policy Framework;
- Charters for the Board and other governing bodies; and
- The Financial Accountability Regime (FAR) which establishes obligations and clarifies accountabilities for the Group and its accountable persons.

To enable execution of responsibilities with respect to information security, reports are provided to the Board, and other governing bodies responsible for maintaining cyber security for the Group, 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 CBA Board Risk and Compliance Committee (BRCC).

The following provides an overview of organisational and governance structures, including key information security governing bodies up to the Board within which Cyber Security operates.



3.2 Oversight

The Group 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 encompasses 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 the Group.

3.3 Risk Management Framework

The Group Risk Management Framework comprises the systems, structures, policies, processes, and people that identify, measure, evaluate, control, monitor and report on both internal and external sources of material risk.

The Group manages cyber risk as a non-financial risk type and employs various controls to govern how these risks are managed. Controls are both technical and non-technical in nature and are tested and assessed for design and operational effectiveness.

3.4 Cyber Security Supply Chain Risk Management

The Group relies upon suppliers to provide products or services to meet a range of operational needs. Suppliers that hold or manage the Group's information assets are subject to contractual obligations in respect of information security management, in addition to periodic assessments of the cyber security capability and controls applied to Group information assets, and ongoing governance activities commensurate with the nature of the services provided to the Group.

3.5 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 the Group. The Framework is comprised of:

- Information security policy, which provides high-level policy statements that govern decision making;
- Standards, which provide specific rules, expectations or criteria that must be met to comply with a policy; and
- Guidelines and resources, which supplement the Standards and other resources to support compliance.

The Group's Information Security Policy Framework is informed by industry standards and frameworks such as the International Organization for Standardization (ISO) and NIST CSF, 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;
- Supplier relationship;
- Information security incident management;
- Information security business continuity management; and
- Compliance.

4 Identify

4.1 Threat Intelligence

Cyber threat intelligence is information used to understand the cyber security threats and threat actors in the external environment that may target or impact the Group.

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

Tactical, operational, and strategic intelligence obtained through these channels in turn informs efforts to adapt, detect, and respond to cyber security threats faced by the Group.

4.2 Personnel Due Diligence

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

Personnel due diligence can include checks on:

- Pre-employment medical declarations;
- Rights to work;
- Identification verification;
- Background screening;
- Qualification verification; and
- Conflicts of interest.

4.3 Information Classification and Handling

The Group 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 is inclusive of:

- 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 of the information assets handled by such third parties; and
- Labelling of information contained in documents and emails.

4.4 Asset Management

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

5 Protect

5.1 Cyber Training and Awareness

The Group maintains an information security training and awareness programme that involves participation from personnel to reinforce their information security roles and responsibilities.

This programme is inclusive of online mandatory training to be completed upon joining the Group, and thereafter on an annual basis. The mandatory training aims to help provide personnel with adequate knowledge to prevent, detect and escalate cyber risks appropriately. Non-completion of mandatory training may result in disciplinary action.

The Group also offers a suite of voluntary online and seminar-style training, including for specific role types, to further educate personnel on managing information security risks relevant to them through secure information handling practices both on and off Group premises.

Training is further supported through other awareness initiatives including simulated exercises and publication of intranet articles and newsletters, which promote secure information security practices across key topics such as (but not limited to) ‘phishing’ and ‘spear phishing’ attacks, password security, and secure information transfer and storage.

5.2 Identity and Access Management

Identity and Access Management (IAM) works to prevent unauthorised access to Group 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;
- 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 Group standards.

5.3 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 the Group 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.

5.4 Secure Configuration Management

Secure configuration management provides a technology specific configuration baseline to help prevent the exploitation of assets within the Group'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. The Group uses baseline compliance scanning solutions to scan the Group's assets against established configuration baselines.

5.5 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.

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

5.6 Network Security

Network security helps protect the confidentiality, integrity and availability of the Group's infrastructure. It works to help prevent the entry or proliferation of malicious threats into or within the Group'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 aim to provide the guardrails required for the design and governance of physical and logical networks to detect and protect against malicious activity which may be harmful to the Group.

The Group 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.

5.7 Device Security

The Group Information Security Policy Framework defines the minimum device management requirements for protecting the Group 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.

5.8 Application Security

Application Security (AppSec) helps to reduce the number of potential vulnerabilities introduced into software developed internally by the Group 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 the Group 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.

5.9 Data Security

5.9.1 Cryptography and Key Management

Cryptography deters and helps prevent unauthorised access or change to data within Group 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 Group's business processes. The Group utilises cryptographic controls to help protect Group information assets.

5.9.2 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 the Group and with external parties.

5.9.3 Data Loss Prevention

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

5.10 Physical Security

To help protect the Group's IT infrastructure and the information it processes and stores, physical safeguards are utilised for facilities which host Group 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 the Group, or on behalf of the Group by an approved third-party vendor.

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

6 Detect

6.1 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.

The Group undertakes penetration testing both during project/IT change phases as well as on a periodic schedule for production systems. The Group'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 Group;
- 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.

6.2 User Behaviour Analytics

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

7 Respond

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

- 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 frameworks interlock with specific information / cyber security incident response plans and capabilities as set out below.

7.1 Incident Response Preparedness and Management

Information / cyber security, data breaches and third party cyber incidents (Incidents) impacting the Group are managed through dedicated response plans, processes and 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 Incident;
- Remediation: Planning and execution of activities to contain and eradicate the threat and recover from the Incident; and
- Post-incident: Assessing and documenting lessons learned, sharing outcomes with key governing bodies, and improving capabilities to enhance 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 the Group, 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 advancement of cyber threats which are ever-changing, the Group regularly tests and updates incident response plans, to ensure they remain fit for purpose. In addition, the Group leverages external expertise and undertakes internal exercises to help build and consolidate readiness for an incident.

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

7.2 Incident Notifications Reporting

The Group is required to report notifiable data breaches and cyber security incidents to domestic and international regulators. The 2023 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).

8 Recover

8.1 Cyber Recovery Planning

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

8.2 Business Continuity Planning

Business continuity and crisis management capabilities aim to support the Group's resilience to disruption events. The Group monitors the health of systems and performs security risk reviews, threat monitoring, and business continuity planning for disruptions to critical systems and business processes.

The Group's IT Service Continuity processes are in place to support the Group's compliance with Prudential Standard CPS 232 on Business Continuity Management. The Group is also assessing

and revising processes to comply with the new APRA Prudential Standard CPS 230 Operational Risk Management (effective 1 July 2025) which will include updated requirements for operational risk, business continuity and service provider management.

9 Review

Cyber Security periodically engages external firms and subject matter experts to conduct reviews and provide feedback on the Group's cyber strategic priorities. The Group also participates in external and regulatory reviews which help identify areas for improvement and benchmark the Group against best-in-class and industry peers.