CBA Information Security Statement

October 2023

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 the organisation.

Noting that the Group's cyber security controls and capabilities are broadly aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), this statement sets out the Group's approach to information security management across the five NIST CSF functions i.e. identify, protect, detect, respond, and recover.

This statement is intended to serve as reference material for third parties such as customers, investors, and regulatory authorities. Information contained in this statement is general in nature and provided as a guide only based on CBA's current operating conditions, knowledge and understanding. It has been prepared in good faith and should not be relied on for any purpose other than for information gathering purposes. To the fullest extent allowable by law, the Group does not make any representations, express or implied, and cautions placing reliance on this information statement. Every effort has been made to ensure the information contained in this statement is current as at the time of its publication.

2 General

2.1 Strategy and Team Structure

The Group's Technology Business Unit provides leading technology and digitisation capability, and comprises various teams aligned to and otherwise supporting the Group's retail, business and 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), Chief Security Officer (CSO), and Chief Information Security Officer (CISO).

Technology maintains a strategy that sets out the key pillars and levers through which the Group's strategic technology priorities, including security, resiliency and reliability are delivered. In keeping with this, the Group's cyber security strategy sets out the team's purpose, priorities, objectives and the enablers. The strategy in-turn guides ongoing initiatives and prioritisation decisions.

The Group's central Cyber Security team comprises approximately 650 cyber security professionals predominantly based in Australia, and some team members based internationally supporting the Group's international operations. Cyber Security and supporting teams are generally organised in line with NIST CSF, and consist of the following functions (with some leveraged across Group Security more broadly):

- **Cyber Identity and Protection Management**: Proactively designs, metricises, governs and reports on Group cyber security controls to ensure that the Group has secure networks, applications, and systems;

- **Cyber Intelligence, Resilience and Recovery**: Scans the external environment for cyber security threats to the Group, and works closely with partners in industry and government on proactive management of cyber risks, response to data breach and third party security incidents, and establishes in-house capabilities for recovery from a cyber security incident;
- **Cyber Governance, Compliance, Education and Outreach**: Maintains the Group Information Security Policy Framework, undertakes compliance assessments, monitoring and reporting and executes information security governance, and manages engagement with business and external stakeholders (including regulators) for the Group. In addition, the team educates Group personnel on their cyber security accountabilities and provides cyber security education and awareness to customers and the community by collaborating across industry and government;
- **Cyber Defence Operations**: Responsible for detecting and responding to cyber-attacks against Group systems, and cybercrime against customers. This function executes cyber-attack and vulnerability assessments against Group assets to mitigate the risk of a cyber attack, and further includes a detection engineering function, and capability to perform real-world red, purple and open-source intelligence team testing to continuously improve detective capability.
- **Office of the Chief Security Officer**: Ensures timely and transparent reporting of security risk is provided to the Group board ('Board') and executives via regular reporting;
- **Group Security and Engineering**: End-to-end technology function for Group Security encompassing design, build and run for technology and responsible for defining security architecture. In addition, the team is responsible for selecting the right technologies, building new security solutions and overseeing the engineering, delivery and performance of security tools and services and leading testing and certification of new products and major releases;
- **Cyber Delivery and Transformation**: Focuses on the prioritisation, design, planning, and execution of change programs at high velocity leveraging best practice and implementation disciplines across the Group. The team works closely with all teams across Technology and the businesses to interlock and sequence core foundational cyber technology change Group-wide; and
- **Group Security Performance**: Drives a centralised view of operating performance across Group Security to ensure the function runs as an efficient and effective business with a continuous improvement mindset.

2.2 Privacy

The Group takes the responsibility to protect the personal information and privacy of customers seriously. To keep customer's safe, the Group applies security and privacy controls to the way personal information is handled. The Group Privacy Statement sets out publicly how the Group collects and handles personal information, as well as how individuals may exercise their privacy rights.

Personal information is kept in accordance with the Group's retention policies. The Group's approach is to keep personal information only for as long as it is needed – for business, regulatory, tax or legal reasons. When information is no longer needed, reasonable steps are taken to destroy or de-identify it. The Privacy Act 1988 (Cth) informs the Group's obligation to destroy or de-identify personal information when it is no longer required for the purpose for which it was collected.

Refer to the Group Privacy Statement for more information.

3 Identify

3.1 Threat Intelligence

Cyber threat intelligence is the information an organisation uses to understand the threats that have, will, or are currently targeting the organisation.

The Group's Cyber Intelligence team monitors the external cyber threat landscape to provide tactical and strategic intelligence on the cyber threats and/or threat actors relevant to the Group. The team provides confidential and time sensitive intelligence sourced from a network of trusted industry peers, private sector security groups, law enforcement and government agencies.

Threat actor motivations, infrastructure and tactics, techniques and procedures are collected, analysed and disseminated to relevant teams to uplift existing cyber defences and drive priorities in threat hunting, detection engineering and red teaming.

The team produces strategic threat reporting for senior stakeholders which provides longer term analysis to enable the Group to proactively adapt, detect and respond to cyber security threats in accordance with the Group's Information Security Policy Framework.

3.2 Personnel Due Diligence

The Group is aware that internal cyber threats exist via personnel action. To manage insider threat activity, the Group is committed to recruit, select, appoint, and maintain the most suitable candidates for any vacant position, and ensuring that due diligence is conducted on applicants and all processes undertaken are free from actual or potential conflicts of interest. The Group's recruitment, selection, and appointment practices is applicable to Group personnel, secondees, contractors, service providers and volunteers within Australia.

Personnel due diligence checks are conducted for every appointment and encompass the following:

- Pre-employment medical declaration;
- Right to work in Australia;
- Identification check;
- Background screening check;
- Qualification check; and
- Conflicts of interest check.

All offers of employment, as well as continuing employment are subject to and conditional on the candidate satisfactorily completing the required checks.

3.3 Risk Management

The Group monitors and manages its exposure to financial, non-financial and strategic risks, and is committed to having risk management policies, processes and practices that support a high standard of 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 of attack to a third party supplier to the Group.

3.3.1 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. It incorporates three key documents:

- The Group's Business Plan (consisting of the Group Strategy and the Financial Plan) that sets out the approach to implementing the Group's strategic objectives;
- The Group Risk Appetite Statement (RAS), that establishes the type and degree of risk the Board is prepared to accept and the maximum level of risk that the Group must operate within; and
- Group Risk Management Approach (RMA) that sets out the Board and the Executive Leadership Team's expectations regarding the Group's approach to managing risk and the key elements of the Risk Management Framework that give effect to this approach.

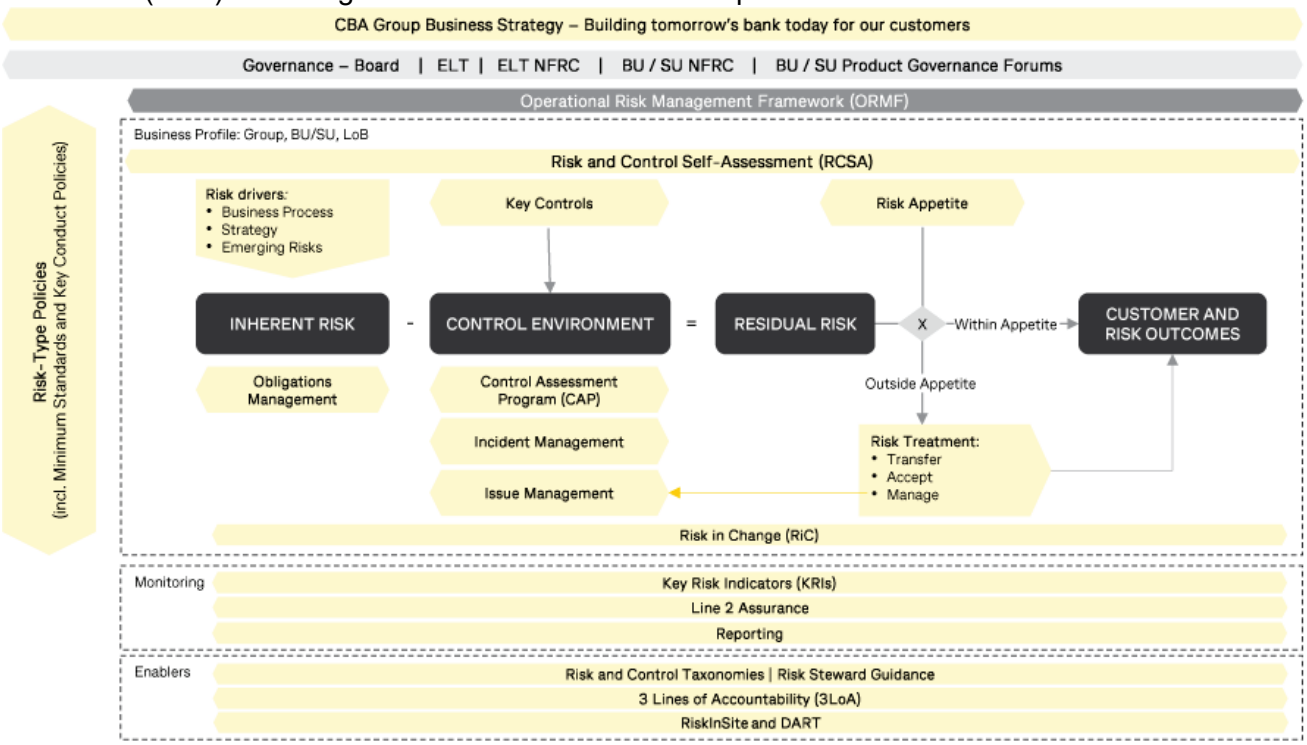
The Board is ultimately responsible for the Group Risk Management Framework and for overseeing its operation by management. As required by APRA's Prudential Standard CPS 220 Risk Management, the Board:

- Sets the Group RAS and the Group RMA, and ensures that these are consistent with the policies and processes developed to support appropriate levels of risk-taking;
- Ensures that the Group Risk Management Framework is appropriate for the size, business mix and complexity of the Group, and is reviewed annually by Group Audit & Assurance, and triennially by operationally independent persons;
- Receives regular management reporting to monitor that material risks are managed within approved appetite;
- Forms a view on the risk culture of the Group and oversees relevant improvement action plans; and
- Delivers an annual Risk Management Declaration to APRA on the adequacy of design and operating effectiveness of the Group Risk Management Framework.

3.3.2 Controls

The Group's Operational Risk Management Framework (ORMF) covers the structures, policies, systems, processes, and people within the Group that identify, measure, evaluate, control / mitigate, monitor, and report internal and external operational risks. The ORMF is a sub-framework within the Group Risk Management Approach (RMA) and aligns with the Group's Risk Appetite

Statement (RAS). The diagram below sets out each component of the ORMF.



As noted above, controls form a key component of the ORMF in managing existing and emerging inherent risks. In particular, the Group employs various controls to oversee risks associated with cyber security, which include:

- Privileged access management;
- Network protection;
- Multifactor authentication;
- Email filtering and web security;
- Detection and response;
- Secure configuration;
- Third party security;
- Cyber training and awareness;
- End of support;
- Vulnerability and patch management; and
- Recovery and backup.

Key controls are assessed periodically in accordance with the Group's control assessment program and where identified, control weaknesses are managed in accordance with the Group's risk management framework, including the issue management process.

3.4 Governance

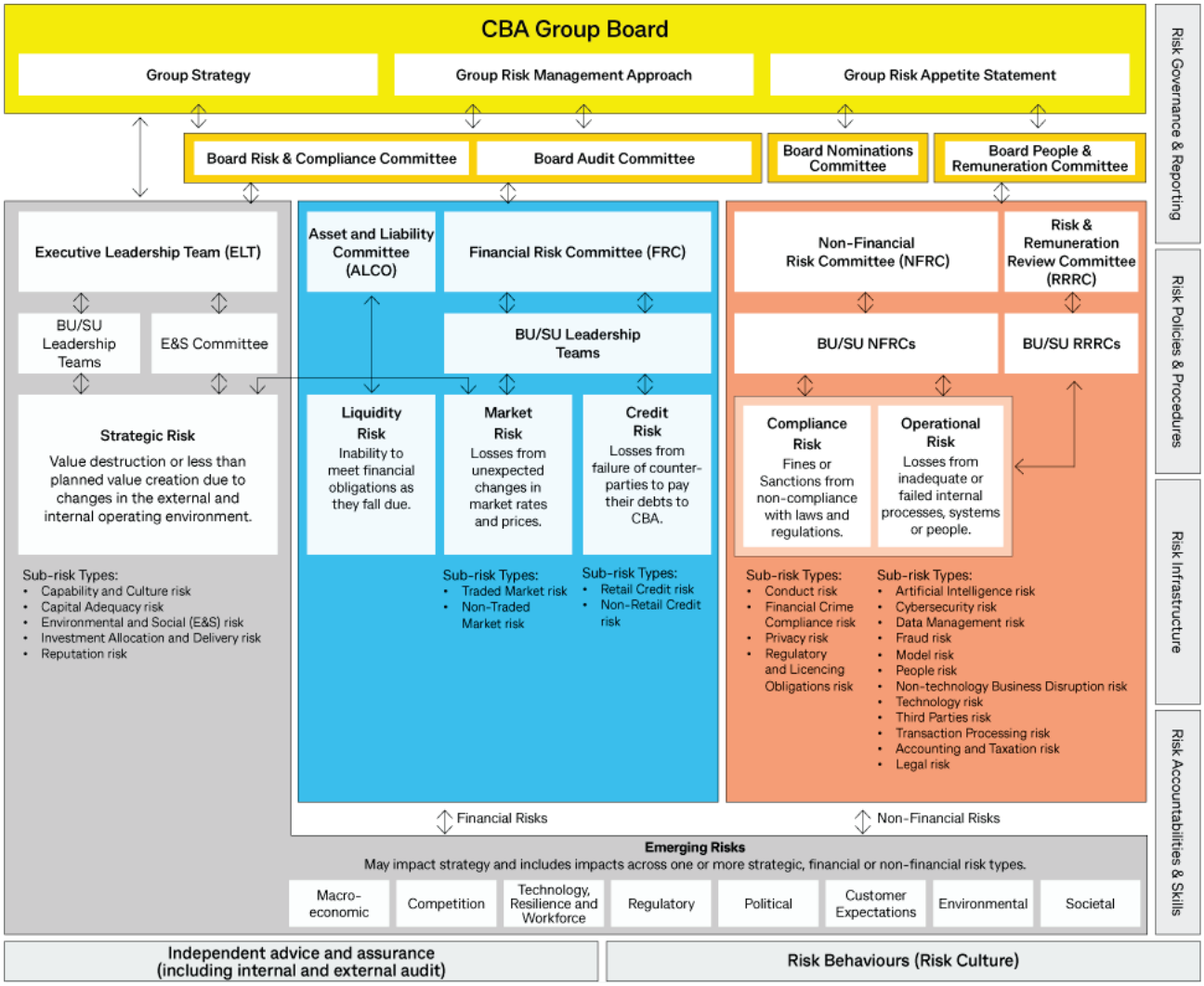
The Group maintains defined roles and responsibilities for information security, including (but not limited to) the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.
In particular,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

- The Group Information Security Policy Framework;
- Charters for the Board and other governing bodies; and

- Banking Executive Accountability Regime statements.

To enable execution of responsibilities with respect to information security, the Board, and other governing bodies responsible for maintaining cyber security for the Group, are provided regular reporting in respect of cyber security matters including (but not limited to) the cyber threat landscape, strategy, risk management, security posture, and incident management. Cyber security as a risk domain falls within the remit of the CBA Board Risk and Compliance Committee (BRCC).

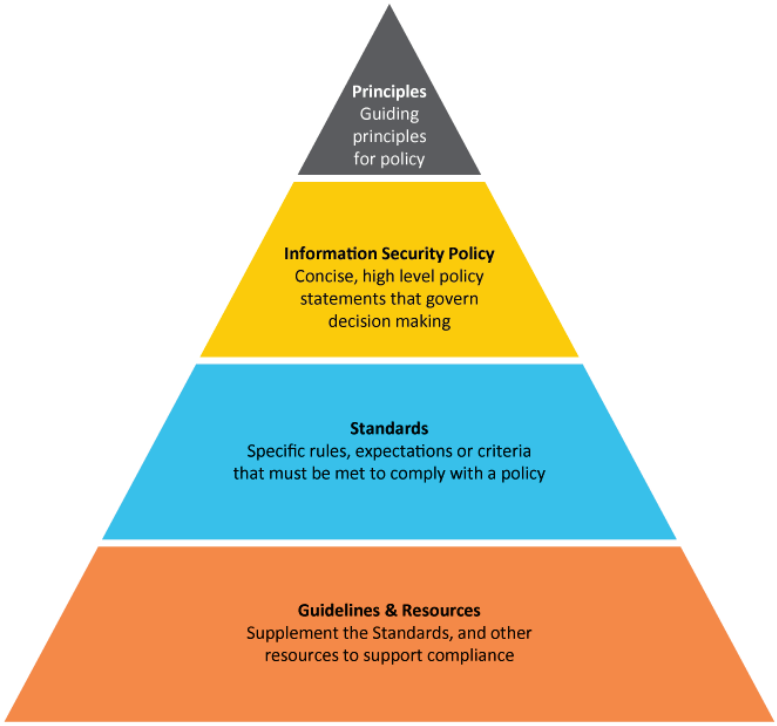
The following provides an overview of organisational and governance structures, including key information security governing bodies up to the Board within which Cyber Security operates.



3.5 Policy

3.5.1 Group Information Security Policy Framework

The Group Information Security Policy Framework is comprised of a suite of documents which outline how cyber and information security risk is managed at the Group. The Framework includes requirements and supporting resources for securing the Group's information assets and is comprised of the following:



The Group's Information Security Policy Framework covers a wide range of areas including, but not limited to:

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

The Group is committed to complying with all domestic and international regulatory obligations, and where appropriate aligning to industry frameworks, best practices and standards. To ensure this, the Group regularly reviews and uplifts internal policy documents, maintains a compliance framework which is embedded in the way the Group conducts business, and defines the requirements for the secure design of systems and processes.

The Group Information Security Policy and Standards are aligned to industry best practices and standards such as, International Organization for Standardization (ISO) and NIST.

The Group's Information Security Policy Framework also interfaces with policy documents across other key risk domains such as privacy, physical security, people and business continuity management.

3.5.2 Policy Exceptions Management

Exceptions to the Group Information Security Policy and Standards are managed via the Group's authorised tracking system. Exceptions are risk-assessed, and mitigating controls applied to manage cyber security risk to the Group pending return to compliant state.

Reporting on non-compliances is provided to senior management on a periodic basis through governing bodies such as non-financial risk committees, in addition to self-service reporting available to stakeholders on the tracking system.

3.6 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 comprised of the following:

- The Group's Information Security Policy Framework, which defines the requirements to ensure the Group's information is accurately classified and handled. This ensures that the appropriate layered security controls, both technical and procedural, are applied to protect the information and conform with applicable policy, regulatory and legislative requirements;
- 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. These mechanisms consume the information classification scheme to drive application of commensurate controls; and
- Mechanisms to tier suppliers according to their criticality, considering the sensitivity of the information assets handled by such third parties. This tiering drives corresponding risk assessments and the application of commensurate controls.

To ensure information contained in documents and emails are appropriately classified, the Group has implemented a data classification tool that requires Group personnel to label documents and emails with the relevant information classification.

3.7 Supplier Security

The Group relies upon suppliers to provide products or services to meet a range of operational needs. The Group governs and manages suppliers to safeguard the Group from a range of supplier-driven risks.

In accordance with the Group's ORMF and Supplier Lifecycle Frameworks, the Group undertakes periodic assessments of the cyber security capability and controls of suppliers that manage information assets on behalf of the Group.

Suppliers that hold or manage the Group's information assets are subject to contractual obligations in respect of information security management, which are reviewed periodically.

4 Protect

4.1 Cyber Training and Awareness

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

This programme is inclusive of online mandatory training to be completed on joining the Group, and thereafter on an annual basis. The mandatory training is based on regulatory guidance and best practices to ensure adequate knowledge to prevent, detect and escalate cyber risks appropriately. Non-completion of mandatory training may result in disciplinary action, including termination of employment.

The Group also has a suite of voluntary online and seminar-style training, including for specific role types, to further educate personnel about managing information security risks relevant to them through secure information handling practices both at work and at home.

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.

In addition, the Group provides awareness and obligations among personnel on usage of social media channels and posting on social media environment via clearly documented policies. The learning is supported by the Cyber Security Champions Programme, which has representation from across the Group, providing grass-roots involvement to ensure security-minded operations and thinking are embedded throughout the organisation.

4.2 Identity and Access Management

Identity and Access Management (IAM) proactively prevents unauthorised access to the Group’s systems and services and ensures that the processes providing access entitlements are complete, consistent and auditable.

The Group manages access to information and systems for appropriate personnel based on their business role and with appropriate privilege for that role, via the following services:

- Identity lifecycle management: Setting up access for new users, modifying access for existing users and removing access;
- Privileged access management: Controls for users with elevated privileges;
- Authentication management: Mechanisms for proving who you are; and
- Identity and access assurance: Ensuring that lifecycle controls in IAM processes remain in place and effective.

4.3 Vulnerability Management

Vulnerability management is a control used to proactively prevent or mitigate the successful exploitation of 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 vulnerabilities. The framework requires that security vulnerabilities must 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 vulnerabilities using approved scanning services.

The Group's Vulnerability Management (VM) team identify security weaknesses and vulnerabilities including within operating systems, applications and work with patch management across Group technologies to ensure remediation through assessment, reporting and governance. The VM team provide internal, external, local and network-based vulnerability scanning, identification of Common Vulnerabilities and Exposures (CVEs) and support a wide range of technologies. Services include:

- Performing ad-hoc scanning if required due to business requirements;
- Generating data for reporting purposes;
- Provide consultation and advice on vulnerabilities and their remediation; and
- Consult with appropriate teams to investigate and approve false positives.

4.4 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 by ensuring they are securely configured throughout their operating lifecycle.

The Group Information Security Policy Framework requires secure configuration baselines to be established, implemented and actively managed throughout a baseline's lifecycle. The Group uses baseline compliance scanning solutions to ensure that the Group's assets are scanned against established configuration baselines.

4.5 Malware Protection

Endpoints, servers and cloud workloads are vulnerable to the introduction of malware which can disrupt systems and compromise data. To appropriately address risks arising from malware, the Group Information Security Policy Framework requires malware protection activities to 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 such as anti-virus, endpoint detection and response, application control and exploit protection across the Group's assets.

4.6 Network Security

Network security protects the confidentiality, integrity and availability of the Group's infrastructure. It prevents the entry or proliferation of malicious threats into or within the Group's IT environment at a 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 is harmful to the Group.

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

4.7 Device Security

4.7.1 Device Management

Mobile computing device management ensures that the configuration, use and monitoring of mobile computing devices, such as laptops, tablets, mobile phones and portable media devices, is managed appropriately to protect Group information assets.

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

4.7.2 Remote Access

Remote access enables users to connect to the Groups' digital resources when external to the network. The Group supports remote access to its protected corporate network to facilitate flexible working arrangements. Users can only connect remotely to the network after validating their identity via multi-factor authentication and that the mobile computer device is Group authorised and has security configurations implemented in accordance with the Group's network access policies including mandatory multi-factor authentication to access the device.

These controls apply to Group personnel, suppliers and service providers with Group identities. The Group ensures that the configuration, use and monitoring of remote access is managed appropriately to protect Group information assets.

4.8 Application Security

Application Security (AppSec) helps to reduce the number of vulnerabilities introduced into software developed internally by the Group by empowering engineers to write secure code and embedding security capabilities into the system development lifecycle. The Group Information Security Policy Framework outlines the requirements for developing secure applications.

AppSec capabilities are provided by the AppSec team and include:

- Tooling: Governance and support for code scanning tools, which are used to allow 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 identify security weaknesses, and providing security consulting to projects, with a focus on early engagement of security, to ensure that secure development practices are in place from the beginning.

4.9 Data Security

4.9.1 Cryptography and Key Management

Cryptography deters and prevents unauthorised access or change to data within Group IT systems and services, and the Group utilises cryptographic controls protect Group information assets.

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. These requirements are regularly reviewed to ensure they align with industry best practice.

4.9.2 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. The processes and controls in place to ensure the protection of information transferred digitally within the Group and with external entities include:

- Information transfer controls and procedures: Protection from threats such as interceptions, eavesdropping, copying, modification, misrouting and destruction;
- Digital communications: This includes protecting communications and helping to protect customers from attacks;
- Agreements on information transfer: A legal agreement in place between the Group and an external party when information is transferred to third parties for handling, processing or storage; and
- Confidentiality or non-disclosure agreements.

4.9.3 Data Loss Prevention

The Group has implemented software and controls to monitor electronic data transfers. This safeguard is known as data loss prevention and plays an important role 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.

4.10 Physical Security

To ensure protection of the Group's IT infrastructure and the information it processes and stores, physical safeguards are utilised for all facilities which host Group infrastructure, assets or data, in order to protect against and deter unauthorised access, detect attempted or actual unauthorised access, and activate an effective response.

These safeguards apply to all locations where the Group's IT infrastructure or assets are located, including international locations, and all 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.

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.

The Group executed penetration testing both during project/IT change phases as well as on a periodic schedule for production systems thus ensuring that the Group is compliant with all external and internal regulatory and compliance requirements.

The Group's penetration testing programme includes the following five key streams, that address different drivers for testing of the Group environment:

- Regulatory and compliance: Addresses specific penetration testing requirements enshrined in legislative or regulatory schemes such as (but not limited to), SWIFT Customer Security Programme, New Payments Platform security requirements, and Payment Card Industry Data Security Standard (PCI DSS);
- Applications: Tests critical, continually developed, in-house developed products;
- Internet perimeter: Discovery and target testing of the Group's internet-facing technology assets;
- IT platforms and systems: Security review of each platform and their systems full stack IT environment; and
- Threat-based: Security assessments that respond to cyber security concerns and intelligence on the techniques of threat actors.

5.2 Intrusion Detection and Logging

The Group has established minimum requirements for Information Technology Service Management (ITSM) Monitoring and event management in accordance with Control Objectives for Information and Related Technologies (COBIT) and Information Technology Infrastructure Library (ITIL) service management guidelines. These requirements support the Group IT Service Support and Management Policy by ensuring IT services and service components are monitored to detect, report on, and manage significant changes of state.

In addition, the Group has relevant controls in place to help detect, analyse and respond to cyber threats. Some of the controls in place include, firewalls, host-based or network-based Intrusion Detection or Intrusion Prevention Systems (IDS/IPS), Endpoint Detection and Response (EDR), authentication servers, anti-virus, messaging proxy servers to detect and log events indicative of malicious activity.

5.3 User Behaviour Analytics

CBA 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.

6 Respond

The Group maintains a comprehensive framework of plans, playbooks and capabilities to support the management of technology and operational incidents, including crisis events, which:

- Determine the course of action to be adopted following identification of incidents through monitoring processes;
- Communicate events and alerts to relevant stakeholders in a timely manner;
- Facilitate efficient investigation of cyber incidents with the relevant resolver groups; and
- Identify the risks associated with incidents appropriately and accurately to support effective risk mitigation.

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

6.1 Incident Response Preparedness and Management

Information security incident management and response (through all stages of an incident) is managed through multiple incident response plans and teams, which address different types of incidents such as cyber security, data breach and third party incidents. The response activities include:

- Preparation: Establishing and training the Cyber Defence Operations (CDO) team, acquiring necessary tools, and assessing risks for the prevention, detection, and response to cyber security incidents;
- Identification: The process through which potentially adverse events are brought to the CDO team's attention;
- Triage: Confirming the validity of the initial alert and determining the initial response action and priority based on the other queued alerts;
- Investigation: Analysing systems and information to determine the scope of a cyber security incident;
- Remediation: Planning and executing activities to contain and eradicate the threat and recover from the cyber security 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 elevated to 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 the community.

The cyber security threat landscape is ever changing and requires organisations to be prepared for and respond to potential attacks when they arise. To keep up with the advancement of cyber threats, the Group regularly tests and updates incident response plans, to ensure they remain fit for purpose. In addition, the Group consults global experts and leverages external expertise to undertake regular internal exercises with key audiences including technology and cyber security teams, legal and communications, and the executive cohort to build and consolidate readiness for a genuine incident.

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

6.2 Digital Forensic Evidence Collection and Analysis

As computer and network attacks grow in frequency and sophistication, the ability to collect, examine and preserve digital forensic evidence becomes increasingly important to support the Group's ability to respond to incidents.

The Group Information Security Policy Framework outlines the requirements for collection, acquisition, storage and preservation of information that can serve as evidence in the event of an IT security incident that may require forensic investigation and provides the minimum baseline requirements required for forensic digital evidence protection in relation to:

- Digital forensic evidence collection: Detailing the collection process within the Group for the purpose of investigation within the relevant jurisdiction. Actions taken are documented in a detailed acquisition log or investigation journal;
- Digital forensic evidence analysis: Data obtained must be processed to extract meaningful information and analysed to draw conclusions about the events leading up to the IT security investigation;
- Chain of custody; and
- Digital forensic evidence handling and preservation.

6.3 Data Breaches

The Group is committed to dealing with any potential, suspected, imminent or actual data breaches in a robust and timely manner. Failure to deal effectively with data breaches creates a compliance and legal risk for the Group which may have an adverse impact on all stakeholders which includes, but is not limited to customers, policyholders, investors, personnel, and regulators as well as the Group's brand and reputation.

The Group is required to report notifiable data breaches and cyber security incidents to domestic and international regulators. See the 2023 Sustainability performance metrics and disclosures (Governance tab) for the definition and number of data breaches reported.

7 Recover

7.1 Cyber Recovery Planning

Cyber recovery planning supports the planning and implementation of cyber resilience and recovery capabilities to help the Group respond to major cyber incidents, including supporting the restoration of impacted technology in a timely fashion to minimise the impacts to our customers from cyber-triggered disruptions.

The Cyber Recovery Planning team supports these activities, and acts as subject matter advisors (and in a coordination capacity where needed) of the recovery activities undertaken by technology (e.g. backup restoration, technical recovery, system rebuilds, data restoration), recommendations for activation of contingency plans and supporting business efforts/processes.

7.2 Business Continuity

Effective business continuity and crisis management capabilities allow the Group to remain resilient to disruption and can minimise customer, community, financial, legal, regulatory, reputation impacts and other material consequences. 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 ensure the Group's compliance with Prudential Standard CPS 232 on Business Continuity Management. The Group is also assessing and revising processes to ensure compliance 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.

7.3 Cyber Insurance

The Group maintains cyber insurance cover to manage costs arising from cyber risk effectively. It is one of the many components in CBA's strategy for managing cyber risk and may be required or expected by many of the Group's industry bodies and regulators.

8 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.