# Westpac Cyber Security Statement

For customers and interested parties.

GROUP

# Table of Contents

# Westpac Cyber Security Statement

## Introduction

This document provides an overview of the management of cyber security and associated controls deployed across Westpac Group (Westpac).

The audience for this document is existing or potential Westpac customers and interested parties.

This document must only be distributed by Westpac employees or authorised third parties to meet Westpac business objectives.

## Security Statement

The security of customer information is critical. Westpac deploys and maintains modern security technologies and procedures to protect information, which are monitored and reviewed to ensure they remain relevant and operate effectively.

Westpac takes all reasonable efforts to ensure that:

- Confidentiality of information is maintained
- Integrity of information is maintained
- Availability of information is maintained
- Our people are appropriately trained to protect the security of information
- Cyber security controls are monitored and reviewed for appropriateness; and
- Policies and standards are maintained to comply with legal and regulatory requirements across all jurisdictions in which Westpac operate.

# Cyber Security Overview

## Cyber Security Organisation

Cyber Security is the responsibility of the Group Chief Information Security Officer (CISO). They are supported through formally documented roles and responsibilities across the organisation and Statements of Accountability, as appropriate. All employees and contractors are responsible for ensuring appropriate cyber security management.

## Non-disclosure and confidentiality agreements

All employees and contractors are required to agree to security responsibilities through the following means:

- Employment contracts
- Confidentiality agreements and/or non-disclosure agreements; and
- Supplier contracts that cover security, confidentiality, and privacy.

## Our Cyber Culture

Westpac promotes education and awareness of cyber security risks to achieve and influence long-term cultural and behavioural change. The Cyber Culture team continues growing a network of cyber champions throughout the organisation to embed awareness and education across all business units. In addition, cyber security awareness events and training sessions support government initiatives such as Safer Internet Day, Scams Awareness Week and Cyber Security Awareness Month.

Customers, employees and contractors are provided with cyber security awareness training at regular intervals to assist them with identifying, managing and monitoring cyber security risks. In addition, Westpac employs qualified cyber security specialists and conducts regular specialist training to ensure skills are maintained and current.

Where required by law, regulations, or to address business needs, additional business unit or role-specific training is provided. Mandatory cyber training is supplemented with regular communications, briefings, and self-paced learning modules and materials.

# Cyber Security Management System

Westpac has multiple policies, standards, guidelines, and procedures which cover the topic of cyber security. The policies are based on ISO 27000 series of Information Security Standards and other local legal, regulatory and industry compliance requirements (such as NIST, CISs, PCI-DSS).

All documents are version controlled and centrally managed, with appropriately assigned owners and sufficient subject matter expertise. Document management follows the Frameworks and Policies Management Procedures with individuals and committees responsible for the material and non-material changes.

Security documents include;

- Group Technology Code of Use
- Group Information Security Policy
- Information Security Framework
- Data Protection Security Standard
- Digital Communications Security Standard
- Enterprise Identity & Access Management Standard
- Information Security Roles & Responsibilities Standard
- Mobile Computing Devices Security Standard
- Third-Party Information Security Standard
- Cryptography and Key Management Standard
- Database Security Standard
- End Point Security Standard
- Security Administration and Configuration Standard
- Network Security Standard
- Secure Software Development Standard
- Security Monitoring and Response Standard
- Security Patch Management Standard
- Security Testing Standard
- Certificate and Key Management Operational Guideline
- Information Security Requirements for Working Abroad Guideline
- Information Security Roles & Responsibilities Guideline
- Network Security Operational Guideline
- QR Code Guideline
- Secure Software Development Guideline; and
- Web Application Masking Guideline.

# Risk Management Framework

Westpac utilises an operational risk management framework to identify, report and manage risk across the organisation. This framework follows the three lines of defence model for implementing risk management across the group. See Diagram 1.

Westpac systems undergo mandatory control self-assessment and governance, ensuring continuous review of the technology controls, associated monitoring procedures and remediation of control gaps.

To protect Westpac assets and customers, Westpac has a mature Cyber Risk Management Framework (CyberRMF) describing the approach to managing cyber risk. This is defined as: "The risk that the Group or its third parties' data or technology are inappropriately accessed, manipulated or damaged from cyber threats or vulnerabilities." This Framework supports the implementation of the Westpac Board approved Risk Management Framework (RMF) and Risk Management Strategy (RMS).

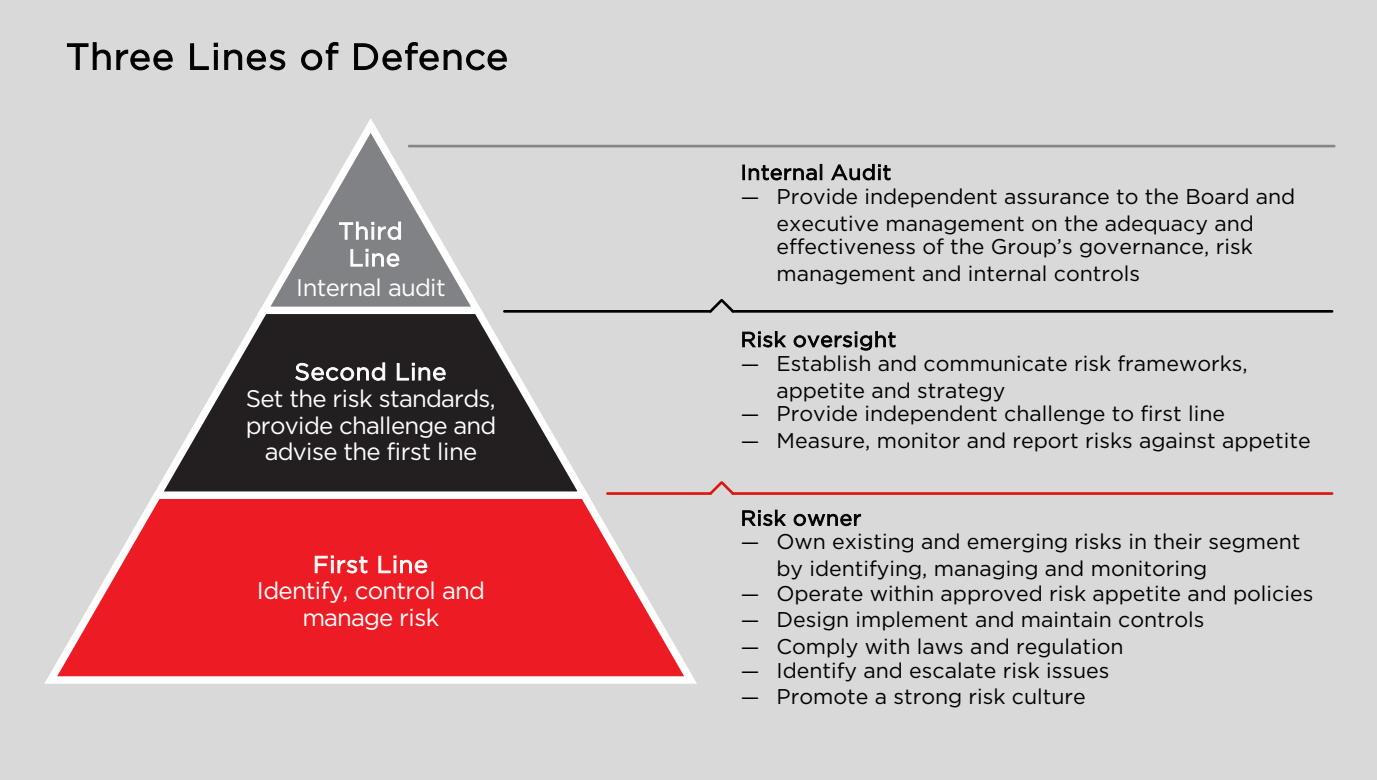


*Diagram 1 – Risk Management Three Lines of Defence*

Westpac monitors a broad set of security controls and their impact on the residual risk level to the organisation through a Technology Control Library.

Risk assessments are performed periodically to address evolving security risk posture changes, security requirements, risk appetite or when significant changes occur. Security-related risk is assessed during the introduction of new implementations (including renewal and changes to systems and infrastructure) through "Secure by Design" (SbD) certification processes. This is undertaken as part of established project life cycle processes.

Westpac performs risk assessments on a variety of assets within the organisation. These assets can include people, processes, facilities, software, hardware, and information.

Regular cyber security risk assessments are performed on application and infrastructure technologies to:

- Define an approach to collaboratively identify, quantify, and manage cyber security risks to achieve business objectives
- Provide means to identify activities and factors which pose the greatest security risks to the Westpac
- Ensure security issues are managed according to their risk rating. Effective controls are therefore, proportional to the level of technology risk discovered
- Provide an enterprise view of cyber security risks and respective remediation plans
- Plan the deployment of resources to areas that provide the greatest reduction in risks to customer and corporate information
- Assess all aspects of cyber security risks, threats and vulnerabilities to Westpac's assets and reputation; and
- Identify any opportunities for improvement.

# Identity and Access Management

Westpac access management controls provide authentication of users and systems to data and information. In addition, processes are in place to ensure that requesting, granting and revoking access to systems is appropriate.

A Privileged Access Management (PAM) solution controls user access privileges and reduces potential attacks by encrypting and changing passwords constantly. This prevents unauthorised transactions alongside ensuring regulatory requirements are met.

Identity & access management operating principles include:

- Users only have access rights that are necessary for executing their roles and responsibilities (need to know principle / Restricted Access)
- Users have access rights that only allow them to perform tasks that are not in conflict with one another (Segregation of Duties) that may otherwise if performed in combination, expose the bank to unchecked financial, reputational or operational risk
- Users' access is reassessed periodically and where necessary, amended or revoked as soon as they move within or leave the organisation
- Access granted to users is periodically revalidated by People Leaders, Business Application Owners and IT System Managers
- IT assets are designed, built, implemented and maintained with sound identity & user access management controls in place
- Database activity monitoring is in place
- Users are aware of and are proactive in managing their access; and
- Privileged Access is only provided temporarily, with a process to request, authorise and monitor access in place.

# Security Certifications

Westpac has developed a project security certification process called Secure by Design (SbD). The SbD processes ensure that all projects are reviewed for security impact and risk, with appropriate security controls implemented.

The SbD certification includes the following activities:

- Architectural alignment and consulting
- Security control design and implementation
- Application security
- Risk identification, recording and management
- Security service design and integration; and
- Security code review and penetration testing.

## External Certifications

Westpac Sarbanes-Oxley (SOX) scoped applications are annually certified to the SOX compliance requirements by independent auditors.

In addition, certain Westpac application systems (such as Corporate Online) and their design, development and operational environment are subjected to SOC2 Type II assessment. These assessments are repeated annually.

Westpac wholly-owned subsidiary Qvalent is independently certified to ISO 27001 and PCI- DSS requirements.

# Application Security

Westpac standards are designed to ensure that applications are developed securely through the software development lifecycle to reduce the likelihood of software vulnerabilities being deployed to production systems. Westpac standards align with the OWASP (Open Web Application Security Project) framework.

Application Security teams are responsible for the following:

- Undertaking application security testing to ensure risks in the use of applications and systems are managed to an acceptable level
- Providing technical and cyber security risk advice to business, project and change initiatives
- Providing input, guidance and recommending changes to the application security standards
- Designing and implementing application system controls
- Conducting application code scanning using automated tools; and
- Web application protection to protect critical internet-facing applications.

## Penetration Testing

Penetration tests are performed against Westpac systems.

Penetration testing is a component of technical security and audit reviews used to validate the security posture of any given technology, system or network.

Unannounced ‘Red Team’ testing is performed to ensure that security testing closely mirrors real-life, malicious actors and an Ethical Hack program is in place and performed using a risk-based approach.

## Physical Security

Physical security countermeasures are implemented to prevent, control and deter unauthorised access to Westpac facilities, resources or information.

Security counter-measures deployed by Westpac may include, but are not limited to:

- Concrete bollards
- Security fencing
- Physical barriers
- Access control and identity passes
- Baggage and vehicle searches
- Security guards
- Closed-circuit television and video
- Surveillance systems
- Intruder alarms; and
- Secured data and network cabinets.

Revalidation reviews of Westpac physical security controls are performed regularly.

# Network Security

## Network Touch Points

Westpac utilises various technologies at strategic internal and external network touchpoints to manage and secure network traffic effectively. Westpac applications are deployed across discretely partitioned security zones based on functions.

## Network Intrusion Prevention Systems and Logging

Network-Based Intrusion Prevention Systems (NIPS) are deployed across the Westpac network. These systems are managed by operational security teams based in a Security Operations Centre (SOC). Infrastructure Security is subject to 24/7 monitoring. Westpac has a robust centralised logging infrastructure that onboards to the Security Information Event Management (SIEM) tooling for consumption by the SOC. Whilst NIPS are placed on traffic aggregation choke points, Westpac uses the IPS function on next-generation firewalls (NGFW) that segregate network topology trust boundaries.

## Data Classification and Cryptography

Westpac classifies data according to sensitivity. Encryption and integrity controls are implemented where industry-recognised security algorithms are required. In addition, Westpac employs several data protection measures, including data masking, database encryption, and mobile intrusion prevention technologies.

Westpac has clearly defined standards covering cryptography requirements to maintain:

- Confidentiality, using symmetric and asymmetric algorithms
- Integrity, using hashing algorithms
- Identity, using asymmetric algorithms; and
- Secure establishment of connections using key exchange protocols.

# Host Security

## Workstations and Laptops

Westpac workstations and laptops have controls to prevent data loss and anti-malware software incorporated into all operating builds. These controls are set to automatically check files as part of regular full-time scanning and obtain updates as they become available. In addition, all desktops have the following:

- Approved, pre-installed images
- Secure Internet and Cloud Access Technology
- USB storage devices disabled to protect against data leakage
- Administrative Control restrictions
- Hard drive endpoint encryption
- Data Loss Protection software; and
- Anti Malware and Endpoint Detection and Response.

## Server Platform

Standardised builds exist for server platforms by covering the following minimum levels of hardening controls during implementation:

- Configuration settings are defined based on the 'least privilege' principle
- Unnecessary and redundant network services, devices, processes, protocols, system and network utilities, programs, and accounts are disabled or removed
- Operations or services are running with the minimum privileges required
- Anti Malware and Endpoint Detection and Response
- Appropriate file system security applied
- Strong user account and password controls (minimum length, maximum length, failed attempts, history, lockout, etc.); and
- Monitoring and reporting of any non-compliance.

## Mobile Devices

Mobile devices with access to Westpac data are managed using Mobile Device Management software with integrated Mobile Threat Defence technology.

This provides security protection to mobile endpoints and applications with a centralised dedicated team managing and monitoring the technology and ensures:

- Remote wipe functionality in the event of device loss
- Complex password enforcement
- Restricted access to approved applications
- Real-time threat analysis and reporting; and
- Secure access to Westpac data to prevent unauthorised exposure.

# Threat Detection and Response

Westpac threat detection and response function leverages multiple security solutions to provide proactive 24/7 security event monitoring, technical analysis support and threat response. These automated solutions enable early threat identification and assessment to formulate consistent response plans for potentially malicious or unauthorised activity.

Threat modelling identifies threat scenarios applicable to the financial services industry that are monitored and tracked.

Intelligence research and information sharing provide a wide range of information sources to detect new threats and enable swift response quickly.

Services provided include:

- Forensic technical analysis of digital media and electronic artifacts
- Data leakage monitoring
- Domain-based message authentication
- Safe Internet access via whitelisting DNS destination domains and sanitising content
- Security Information and Event Management (SIEM) to analyse events
- Security Orchestration Automation & Response (SOAR) to correlate and act on events
- Security Operations Centre, providing personnel to manage events 24/7
- Cyber threat hunting, targeted attack assessment and remediation
- Malware and virus mitigation
- Emerging technology threat management
- Investigation of suspicious system access attempts; and
- Cybercrime response.

# Incident Management

Westpac incident management processes ensure cyber incidents are managed promptly, efficiently, and thoroughly. The objectives of these processes are to:

- Ensure that all appropriate personnel are notified of a cyber incident on a timely basis
- Co-ordinate centralised cyber incident management to ensure that all required tasks are completed and that duplicative and/or contradictory efforts are avoided
- Ensure that the cyber incident is investigated in a timely manner
- Ensure that the risk associated with an incident is appropriately identified, measured, and controlled
- Ensure that required internal and/or external reporting and/or notification is completed
- Ensure all cyber incidents are centrally tracked for trend analysis; and
- Facilitate consolidated reporting to management.

Regular simulated cyber incident exercises are completed to test the efficacy of implemented processes. These exercises simulate common cyber incidents and threats. Upon completion, time is taken to reflect and review, detailing areas of good practice and recommendations to improve capability.

## Data Breach Notification

Westpac has internal and third-party data breach management policies that govern the processes for assessing, remediating, and managing data breach incidents impacting customer information, whether on Westpac or third-party systems.

Westpac complies with data breach obligations and disclosure laws mandated by applicable regulatory bodies worldwide. Data breach notification processes are continually reviewed to ensure appropriate response in the event of an incident.

Contractual obligations with third parties require immediate notification to Westpac of suspected or actual incidents that involve Westpac data.

When suspected or actual incidents occur in Westpac systems involving customer or third party data, Westpac will endeavour to notify impacted parties as soon as practicable. This is part of the activated cyber incident response plans to support the rapid and effective response to an information security incident.

Additionally, Westpac completes due diligence activities to investigate major incidents in the global landscape regardless of contractual relationships or likelihood of impact.

## Patch and Vulnerability Management

Westpac has in place a patch management program supported by dedicated resources. Vendor patch and end-of-life updates are received as they become available and prioritised for deployment across the environment.

Patches are tested in non-production environments before deployment into production systems. All patch deployments are managed by following change management processes and are prioritised by criticality.

Westpac utilises automated tools to scan internal and external facing assets. Any discovered vulnerabilities through this process form an input into the patch management and vulnerability remediation processes.

# Governance and Reporting

Internal and external functions regularly review Westpac systems and processes. Additionally, reviews are undertaken by the Information Security Group across all business units, with regular reporting detailing the security state of the environment.

# Third-Party Supplier Security Management

Westpac has a third-party supplier security assurance framework and supplier risk assessment process that governs the process for employees to identify and control risk with a third-party vendor contract, including cyber security risks. All third parties are mandated to complete an assessment for any new agreement and when directed to by Westpac for ongoing checks.

Third party suppliers are required to meet Westpac standards, including legal and regulatory requirements that apply to information accessed or processed in the provision of goods or services. This includes but is not limited to, Anti-Monetary Laundering (AML) and Counter-Terrorism Financing (CTF). You can read more about how Westpac meet AML and CTF obligations at westpac.com.au/about-westpac/westpac-group/corporate-governance/aml-counter-terrorism/

Third parties with access to Westpac information are subject to security due diligence review, assessment, and monitoring. Specific security obligations are included in contract terms and conditions, enabling Westpac the right to undertake audits of physical and logical third-party security controls.

# Regulatory Compliance

Security of information assets and customer privacy are paramount to Westpac delivering on strategy.

Where applicable, Australian and international regulatory legislation shape our approach to data security and handling of personal information, such as but not limited to:

- Privacy Act 1988 (Cth)
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- APRA CPS 234 (Information Security)
- International regulatory bodies such as the National Futures Association (NFA) in the USA or the Monetary Authority of Singapore (MAS).

Westpac has established governance practices with third parties to ensure mutual compliance with all applicable regulatory laws, and obligations are included in agreement terms to ensure ongoing compliance.