Westpac Cybersecurity Statement

Westpac Group (Westpac) aligns to international and industry standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and maintains certifications including ISO 27001, PCI-DSS and SOC2 Type 2 within specific business units.

This statement summarises the management of cybersecurity risks according to the key functions outlined in the NIST CSF.

Govern

The Westpac Board approves the Risk Management Strategy and Framework. The Board Risk Committee receives quarterly updates for cybersecurity strategy, developments and performance. The Cyber Security Risk Management Framework defines our risk management approach, including a proactive and structured cybersecurity risk strategy, policy and controls (and is applied throughout the three lines of defence model implemented by management). This framework defines the Board's commitment to cybersecurity governance. The Group Chief Information Security Officer (CISO) reports to the Chief Information Officer and is a member of key cybersecurity governance forums. The CISO is responsible for leading and managing the cybersecurity function, setting the cybersecurity strategy and direction, and overseeing the implementation, operation and execution of the cybersecurity policies, standards, controls, and capabilities, including for third parties who are engaged to manage Westpac's information assets.

Identify

A structured and integrated approach is used to identify, measure, and evaluate existing and emerging cybersecurity risks, including collaboration with industry peers and government agencies. Risk assessments are performed periodically including to address evolving cybersecurity risks, security controls and risk appetite.

Protect

Westpac implements security measures which are aimed to protect against cybersecurity threats. These measures include identity and access management, training and awareness, data and platform security that are commensurate to the risk and importance of information assets. Internal and external functions regularly test and provide assurance and audit for systems and processes.

Detect

Westpac has in place systems and processes aimed to find and analyse possible cybersecurity attacks and compromises. Westpac's threat detection and response function leverages multiple security solutions to provide proactive 24/7 security event monitoring, technical analysis support and threat response.

Respond

Westpac has incident response processes which have the objective of responding to cybersecurity incidents in a structured manner to reduce the impact to customers, systems and data. Processes are in place to manage communications relating to cybersecurity incidents with internal and external stakeholders.

Recovery

Westpac's incident recovery processes are designed to restore services in order of criticality to customers. Westpac has defined processes to communicate to internal and external parties about recovery of operational services should this occur.