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 certain business units.

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

Govern

The Cyber Risk Management Framework defines Westpac's approach to identifying, assessing and managing cybersecurity risk across the Group and is applied through a three lines of defence model. This framework establishes governance arrangements, roles and responsibilities, and aligns cybersecurity risk management with the Group's overall risk appetite and enterprise risk management practices.

The Group Chief Information Security Officer (CISO) is responsible for leading and managing the cybersecurity function, setting cybersecurity strategy and direction, and overseeing the implementation and operation of cybersecurity policies, standards, controls and capabilities, including those relating to third party service providers. The CISO is a member of key governance forums and provides updates to senior management and relevant Board committees at least quarterly.

As part of its cybersecurity risk management approach, Westpac uses a range of mitigants to manage residual cybersecurity risk within risk appetite, which may include risk transfer arrangements such as cyber insurance.

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, education and awareness, data and platform security that are commensurate to the risk and nature 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.