St.George Bank Cybersecurity Statement

You've got questions? We've got time to talk.

Ask at any branch

13 33 30
8.00am to 8.00pm
Monday to Friday (AEST)

stgeorge.com.au

Accessibility support

If you are deaf, hard of hearing, or have speech/communication difficulty, you can message us within the St.George App or communicate with us using the National Relay Service.

If English is not your preferred language, contact us and we can arrange a language interpreter.

Visit St.George Accessibility for further information on the accessible features on our products, services and accessible collateral for people with disability, who are neurodivergent or where English is not your preferred language.

St.George Bank Cybersecurity Statement

Westpac Banking Corporation and its Australian related body corporates (the Westpac Group, we, us, our) align to international and industry standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and maintain 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 the Westpac Group'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) reports to the Chief Information Officer (CIO) and 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 and cybersecurity team have relevant expertise and experience across strategy, governance, risk management, threat intelligence, incident response, security operations, architecture, engineering, testing and awareness, and regularly participate in training and development to keep pace with the evolving cybersecurity landscape. The CISO is a member of key governance forums and provides updates to senior management and relevant Board committees at least quarterly.

The CISO escalates key cybersecurity risk and control issues, as appropriate, to the Technology Risks Committee (TRC), which reports to the Group Executive Risk Committee (GRISKCO). The Board of Directors are ultimately responsible for oversight of cybersecurity risk management, with certain responsibilities delegated to the Board Risk Committee.

The Westpac Group engages third parties, including external auditors, industry bodies, consultants, and specialists, for independent reviews and assessments of its cybersecurity policies, standards, controls, and capabilities. As part of our cybersecurity risk management approach, we use 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

The Westpac Group 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. This includes regular network and endpoint monitoring, vulnerability assessments, penetration testing and annual information security training for employees. Internal and external functions regularly test and provide assurance and audit for systems and processes.

Detect

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

Respond

The Westpac Group 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. This is guided by an Incident Response Plan which sets out the processes to triage, investigate, contain, and remediate an incident. Tabletop cybersecurity incident response exercises are conducted to test readiness. Processes are in place to manage communications relating to cybersecurity incidents with internal and external stakeholders.

Recovery

The Westpac Group's incident recovery processes are designed to restore services in order of criticality to customers. This is supported by a Business Continuity Plan which maintains the continuity of critical business processes in the event of business interruption, including those involving cybersecurity incidents. We have defined processes to communicate to internal and external parties about recovery of operational services should this occur.

St.George acknowledges the Traditional Owners as the custodians of this land, recognising their connection to land, waters and community. We pay our respects to Australia's First Peoples, and to their Elders, past and present.