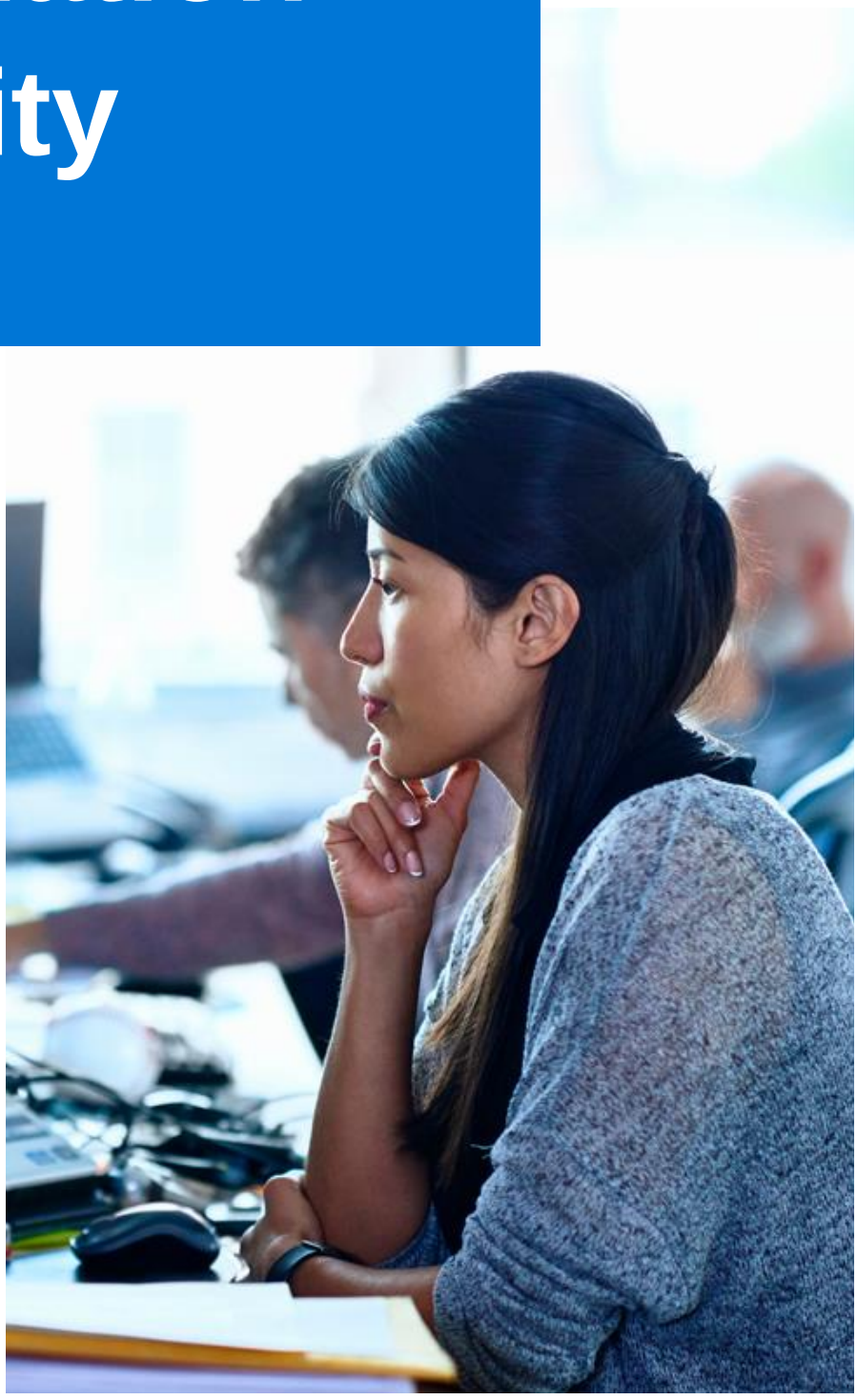
Cyber and Information Security

April 2022



Cyber and Information Security

Legal and General operates and oversees cyber and information security according to a governance framework that is overseen by the Group Board as follows:

Governance and oversight

The Legal & General Group Board has a Technology Committee which is responsible for oversight of Information and Cyber Security. The Committee is chaired by the Group Chairman and membership comprises a minimum of three independent Non-Executive Directors of the Company. The Committee typically meets four times per year to be briefed on all matters relating to Information Security. The Terms of Reference for this Committee are available on our website here. The Group Chief Technology Officer and Group Chief Information Security Officer attend all meetings to brief the Board.

There is also an Executive Security Committee chaired by our Chief Risk Officer that has day-to-day accountability and responsibility for all cyber and information security matters at Legal & General.

Information security framework

Legal & General has established an Information Security Framework, which comprises a suite of policies, standards and guidance that apply across the company, with oversight of implementation through governance processes.

As with many organisations, Legal & General faces an on-going threat of cybersecurity attacks. Cyber resilience is complex yet critical. We do our utmost to ensure minimal disruption to our business operations and to reduce any risks facing our customers and employees.

We have a very low tolerance for the leakage, theft, or corruption of data through weakness in the controls around our IT systems. This is due to the potential disruption to business operations, adverse customer impacts and potential damage to our reputation. Alongside setting a framework to prevent and detect unauthorised access attempts to our business systems, we are committed to ensuring our systems are resilient to current and emerging threats. In the event of an incident, we have robust business continuity plans in place to ensure our business operations recover quickly from security events and incidents and business disruption is minimised.

In addition, we also have a very low tolerance for any disruption of our business operations, as defined by the businesses, or the integrity of our data being compromised by the actions of external parties, such as denial of service attacks, ransomware and infiltration. We seek to ensure that, alongside deploying appropriate IT security tools to protect our digital systems, we have arrangements to enable the early detection and mitigation of threats, and an effective response capability should the need arise.

ISO certification

In September 2021, we received ISO/IEC 27001 certification. This assessment provides independent assurance that we follow industry-standard security management practices. We are committed to maintaining our certification for the foreseeable future.

N.B The ISO certification does not apply to subsidiaries of Legal & General Capital (e.g. CALA and Modular Homes) or our Legal & General America business.

Cyber security strategy

The Legal & General Cyber Security Strategy, first issued in December 2017 provides the roadmap for implementation of changes and improvements to our cyber and information security controls. The strategy is refreshed and approved annually by the Group Board's Technology Committee.

Security awareness and training

A mandatory Information Security Training Course is in place for Legal & General employees. It aims to support and equip our people with the necessary knowledge to identify and respond to security threats, as well as how to operate in a secure manner. This is supported by regular communication on security good practice and an ongoing rolling programme of phishing testing.

Last updated: April 2022