Cyber and Information Security

Legal & General Group operates and oversees Cyber and Information Security according to a governance framework that is overseen by the Group Board.

Governance and oversight

The Legal & General Group Board resolved to appoint a Data and Technology Committee whose primary role is to provide oversight of, and guidance to, the Board with regards to all aspects of information technology, cyber security (including IT and information security) and data & analytics across the Group. The Committee is chaired by an independent Non-Executive Director and membership comprises a minimum of three independent Non-Executive Directors of the Company. The Committee normally meets four times per year to be briefed on all matters relating to Information Security. The Terms of Reference for this Committee are available here. The Group Chief Technology Officer and Group Chief Information Security Officer attend all meetings to brief the Board.

In addition, the Technology and Data Risk Committee, a sub-committee of the Executive Risk Committee (ERC), maintains oversight of the Group's exposure to information and technology risk, and has day-to-day accountability and responsibility for all cyber and information security matters, to ensure it is controlled in line with the Group's risk appetite. The committee is chaired by the Group Chief Risk Officer (CRO) and has delegated responsibility for the oversight of technology risk from the Group Risk Committee (GRC).

Information security framework

Legal & General has established a security framework, which comprises a suite of policies, standards and controls that apply across the Group, with oversight of implementation through governance processes. The Group's compliance, risk and audit teams regularly monitor, test, and assure the controls with metrics reported to management on a regular basis. This ensures that controls remain robust and the Group continues to operate within risk appetite. Legal & General's risk appetite for IT and cyber security is as follows:

"Legal & General has a very low tolerance for threats to the confidentiality and integrity of its data, due to the potential disruption to business operations, adverse customer impacts and potential damage to our reputation. We will seek to minimise the risks of unauthorised access to or modification of data by enforcing a structured framework of controls, process and culture which ensures the necessary standard of behaviour and controls to prevent as well as detect current and emerging threats, and will maintain business plans that enable business operations to recover from security events and incidents. In addition, Legal & General has a very low tolerance for threats to its financial and data assets from the disruption of its business operations, by the actions of external parties, such as denial of service attacks, ransomware or infiltration. We seek to ensure that, alongside deploying appropriate processes and technology 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, Legal & General received ISO/IEC 27001 certification with a recertification audit against the updated ISO/IEC 27001:2022 standard scheduled for 2024. This assessment provides independent assurance that industry-standard security management practices are followed. Commitment has been made by Legal & General to maintain certification for the foreseeable future.

N.B The certification does not apply to subsidiaries of Legal & General Capital or Legal & General America.

Cyber security strategy

Given the nature of cyber threats, the Legal & General cyber security strategy is an evolving direction to match the constantly evolving cyber threats as necessary. The strategy is reviewed on an annual basis to ensure that the correct priorities are being addressed to meet existing and evolving threats. The objectives of the Legal & General cyber security strategy are:

- drive digital trust, promote innovation and competitiveness using technology, whilst remaining secure
- ensure the confidentiality, integrity, and availability of data and systems held in digital environments owned by Legal & General, or of those entrusted to host Legal & General data
- prevent, detect, and respond to cyber-attacks from malicious actors considering different geographic threats and regulations
- enhance the resilience and recovery capabilities of critical Legal & General infrastructure and services

- promote cyber awareness and individual responsibility among Legal & General staff, and its partners. Where applicable, provide digitally vulnerable customers with cyber security advice and, for Legal & General's wider customer base, help them to determine and report cyber enabled fraud when it is encountered
- foster a cyber community through a culture of collaboration and knowledge sharing across divisional security teams
- cooperate and collaborate with relevant stakeholders at a national and international level with the aim of reducing cyber risk to Legal & General entities and customers.

Security awareness and training

An annual information security training course is completed by all Legal & General employees, and managed service providers with access to Legal & General systems, to support and equip them 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 programme of simulated phishing testing.

Last updated: June 2024