Suitable for
customers and investors



Quilter's cyber security statement

Our approach to cyber security

The security and safety of our clients' investments and data is of the utmost importance at Quilter.

We operate on the principle of "defence in depth" – meaning we have multiple layers of technical security controls and experienced people in place. This strategy helps us protect your data and reduces the chance that a cyber-attack would be successful.

Artificial intelligence (AI) is changing how many organisations work, including those who try to commit cybercrime. Like other financial firms, we are keeping a close eye on these developments, in line with guidance from UK regulators and best practice across the industry, and we continue to adapt our defences.

Our controls are aligned with the industry-recognised National Institute of Standards and Technology's Cyber Security Framework. This framework comprises the following areas: Govern, Identify, Protect, Detect, Respond & Recover, explained further below.

Our security framework

Govern: We document, report on and regularly review our security controls so that we have a clear understanding of how effective they are. This gives our management and board confidence, and the opportunity to review and challenge how we manage both long-standing and emerging risks, including those arising from new technologies such as AI.

Identify: We proactively monitor for and research potential threats using credible threat intelligence. This tells us what attackers around the world are doing and how their methods are evolving. It also alerts us to new and emerging cyber threats and vulnerabilities. We assess this information against our own environment and the suppliers and software we rely on, and take action where required.

Protect: We limit access to your data to only those who need it to perform their role, and use additional measures such as encryption and Multi Factor Authentication to further protect it. We keep our systems secure and up to date, regularly testing them with the same techniques an attacker would use so that we can find and fix weaknesses first. As attackers use AI to find weaknesses more quickly, we are evolving our processes to do the same. We ensure all staff are regularly trained so that they are aware of the latest threats.

Detect: A suite of sophisticated security tools, increasingly supported by automation and AI, monitor our systems for unusual behaviour. This allows us to quickly spot and remove potentially harmful software, and identify unauthorised access, attempts to steal data and other malicious activity. Our Security Operations team continuously monitor our systems for signs of active attacks and act quickly when something doesn't look right.

Respond: Tried and tested "runbooks" and regular scenario training mean we can be confident in how we react to a wide range of potential security incidents. Tests are conducted against Quilter's environment and performed jointly with key suppliers where possible. Specialist incident response capabilities support our teams in taking prompt action to contain threats and minimise potential harm to our clients and their data.

Recover: Our environment is designed to reduce the chances of a successful attack, but we are also prepared should one occur. We have documented the key steps to recover our environment and bring our systems back safely and securely, reducing the impact on our clients. We regularly test these steps through planned recovery exercises, including restoring from secure backups and rehearsing realistic cyber-attack scenarios such as a Ransomware event.

Protecting yourself from AI-enabled scams

Criminals are increasingly using AI to impersonate trusted people and organisations, including financial firms. An email, text message, phone call or even a video call may look and sound genuine, use your name and personal details, and appear to come from your financial adviser or from Quilter.

If you receive an unexpected or urgent request to make a payment, change bank details, move your investments or share passwords or security codes, please stop and check. **Contact Quilter using contact details you already hold**, rather than any number or link in the message. **Quilter will never ask you to share your passwords or one-time security codes**.

If you think you may have been targeted, please contact us straight away by calling 0808 171 2626.

You can also forward suspicious emails to report@phishing.gov.uk, forward suspicious text messages to 7726, and report fraud to the police through Report Fraud at reportfraud.police.uk or on 0300 123 2040 (in Scotland, call Police Scotland on 101).

quilter.com

This communication is issued by Quilter, a trading name of Quilter Investment Platform Limited.

Quilter Investment Platform Limited is registered in England and Wales under number 01680071.

Registered office at Senator House, 85 Queen Victoria Street, London, EC4V 4AB.

Quilter Investment Platform Limited is authorised and regulated by the Financial Conduct Authority under reference number 165359.

Quilter uses all reasonable skill and care in compiling the information in this communication and in ensuring its accuracy, but no assurances or warranties are given. You should not rely on the information in this communication when making investment decisions. Nothing in this communication constitutes advice or a personal recommendation. This communication is for information purposes only and is not an offer or solicitation to buy or sell any Quilter product.

Approver: Quilter, November 2026.

QIP 24386/206/19761/B