Protecting your data

To maintain customer trust in the security of our services, we work continuously to mitigate the risks of cyber-attack, exposure or manipulation of confidential data, and against unauthorised access to information. We continue to improve and invest in our detective, preventative and responsive security controls, recognising the evolution of security threats and the increased focus on digital capabilities. Our SOC (Security Operations Centre) operates 24 hours a day, every day, to monitor security alerts, and has powerful protocols in place to respond to any potential incident identified.

What we're doing

Our strategy is aligned to the NIST (National Institute of Standards and Technology) Framework and CIS (Center for Internet Security) Controls which provide a set of safeguards to mitigate risk. Our Information Security Policy Framework contains four Information Security Standards which apply to all job roles and a further eleven Standards relating to technology job roles. The Standards set out our minimum control requirements and are aligned to ISO270001:2013 and CIS Critical Security Controls version 8.

We perform regular targeted internal and external audits of our systems and processes throughout the year. We independently test the effectiveness of our security controls using specialist organisations to support.

Our corporate governance framework oversees the management of information security risk in accordance with our risk appetite. Operational governance is provided across 3 Lines of Defence, with continuous monitoring and oversight that allows for timely actions to be taken whenever industry or regulatory requirements change – or in response to new security threats.