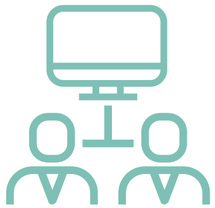
HOW ISO 27001 CAN HELP MEET GDPR REQUIREMENTS

1 Confidence

Certifications do not remove or reduce accountability for data protection - but help demonstrate non-negligence in approaching the Article 32 requirements. The use of certification schemes and best-pratice information security standards such as ISO 27001 provides the necessary assurance that the organisation is effectively managing its information security risks.

2 Control and security framework

GDPR stipulates that organisations should select appropriate technical and organisational controls to mitigate risks. The majority of GDPR's data protection arrangements and controls are also recommended by ISO 27001.

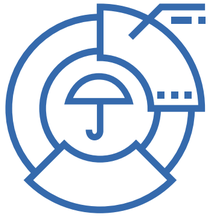


3 Managing people, processes and technology

ISO 27001 encompasses the three essential aspects of information security: people, processes and technology, which means you can protect your business not only from technology based risks but also other, more common threats associated with poorly informed staff or ineffective procedures.

4 Accountability

GDPR mandates clear accountability for data protection throughout the organisation. ISO 27001 requires that security is incorporated into the organisation's culture and strategy. It also requires the appointment of a senior individual who takes accountability for the ISMS.



5 Risk assessments

GDPR specifically requires a risk assessment to ensure an organisation has identified risks that can impact personal data. ISO 27001 compliance means conducting regular risk assessments to identify threats and vulnerabilities that can affect your information assets and to take appropriate steps to protect that data.

6 Continual process of testing, audit and improvement

Being GDPR-compliant means an organisation needs to carry out regular testing and audits to prove that its security regime is working effectively. ISO 27001 requires that your ISMS is constantly monitored, updated, reviewed and regularly assesses against the defined standard.