

Understanding the Differences Between ISO 27001, ISO 27017, and ISO 27018

1 What is ISO 27001?

Code of practice for information security management.

ISO 27001 is the leading international standard for information security which was developed to help organizations protect their information through the implementation of an Information Security Management System (ISMS).



2 What is ISO 27017?

Code of practice for information security controls based on ISO 27002 for cloud services.

ISO 27017 standard provides additional guidance and recommendations for implementing cloud-specific information security controls beyond what was provided in a previous standard (ISO 27002).

3 What is ISO 27018?

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO 27018 was created to specifically address measures to ensure privacy in cloud computing services, helping cloud service providers to process personally identifiable information (PII), as well as to assess risk and implement controls to protect PII.



What Makes Them Different?



Since ISO 27001 is fairly vague regarding the specifics of cloud services, the ISO 27017 standard was created to fill the gap.



The layout of ISO 27017 mirrors that of ISO 27001, but it goes into greater detail about the security of the cloud.

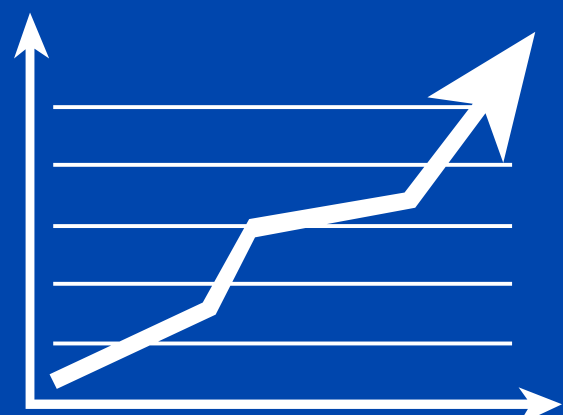


Similarly, ISO 27018 was created to expand on the ISO 27001 standard and address the requirements that the EU General Data Protection Regulation (GDPR) has put into place regarding necessary PII protection measures.

Fast Facts



In 2019, there were over 36,000 valid certificates for ISO 27001 across more than 68,900 sites.



All ISO standards have seen the number of certifications increase by 3.8% from 2018 to 2019.



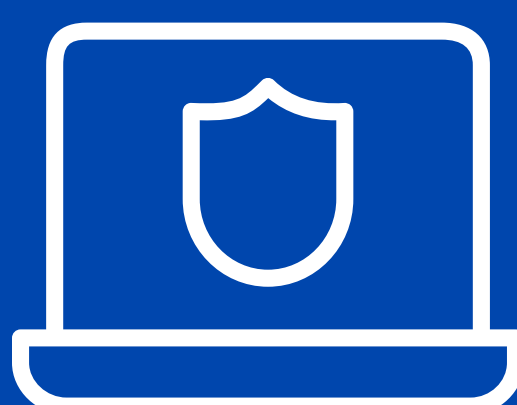
48% of privacy-active respondents to a recent survey indicated they have already switched companies due to lackluster data policies or data sharing practices.



81% of Americans believe that the potential risks of data collection outweigh the benefits an organization can offer.



79% of Americans aren't confident that companies will use and protect their personal data appropriately.



Only 18% of countries have no data protection law implemented in 2020.



America

Learn more about TÜV SÜD's cybersecurity services.

www.tuvsud.com/en-us/cybersecurity