Press Release

White Paper 9 January 2023

New version of ISO/IEC 27001 for more information security and cybersecurity

Munich. The universal presence of cyberthreats has become one of the most serious risks facing companies today. After revision, the internationally established ISO/IEC 27001 standard for information security now contains new measures designed to improve cybersecurity and data protection. The transition period for certification ends in autumn 2025. TÜV SÜD's latest White Paper provides an overview of the new elements.

"An information security management system (ISMS) can help companies of any size to protect themselves effectively against cyberattacks and other forms of malicious data manipulation. ISO/IEC 27001 certification enables companies to strengthen their protection against cyberattacks and prevent loss of sensitive information", says Alexander Häußler, Global Product Performance Manager IT and Lead Auditor at TÜV SÜD.

The ISO/IEC 27001 standard is the foremost international standard for information security management systems (ISMS), and accordingly also for cybersecurity. After revision in October 2022, the new ISO/IEC 27001:2022 has replaced the previous ISO/IEC 27001:2013. The new version contains long-awaited amendments with respect to IT security measures, data protection and concrete cloud security measures.

New controls

The main changes in the new ISO/IEC 27001:2022 compared to its predecessor involve the controls defined in Annex A, which have been reduced in number from 114 to 93 and reclassified into four groups: Organisational Controls (37 controls), People Controls (8 controls), Physical Controls (14 controls), Technological Controls (34 controls). 11 new controls have been added, addressing issues including data masking (a method of rendering data unusable for hackers), monitoring activities (to detect unusual IT activities) and information security for use of cloud services.

Transition period ends in autumn 2025

A transition period of 36 months applies from the time of publication of the new standard; this means that existing certificates must be transitioned to the new ISO/IEC 27001:2022 standard by autumn 2025. Companies that already hold ISO/IEC 27001:2013 certification thus have around three years to complete the transition of their certificates. Nevertheless, TÜV SÜD advises companies to begin addressing the changes in the new standard as soon as possible, given their crucial importance for information security.

The White Paper published by TÜV SÜD provides an up-to-date overview of ISO/IEC 27001, its development and the concrete steps involved in gaining certification. It can be downloaded free of charge at: https://www.tuvsud.com/en/resource-centre/white-papers/iso-iec-27001-information-security-management.

For more information on certification under ISO/IEC 27001, visit: https://www.tuvsud.com/en/services/auditing-and-system-certification/iso-27001.

Media Relations

Sabine Krömer TÜV SÜD AG Corporate Communications Westendstr. 199, 80686 Munich	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 Email sabine.kroemer@tuvsud.com Internet www.tuvsud.com

Founded in 1866 as a steam boiler inspection association, the TÜV SÜD Group has evolved into a global enterprise. More than 25,000 employees work at over 1.000 locations in about 50 countries to continually improve technology, systems and expertise. They contribute significantly to making technical innovations such as Industry 4.0, autonomous driving and renewable energy safe and reliable. www.tuvsud.com