Seven Steps on the Path to ISO 27001 Certification

Certification to ISO/IEC 27001 can reduce overall information security risks, ease compliance with applicable security regulations and requirements, and help organizations foster the development of a culture of security. Implementing an Information Security Management System (ISMS) according to the requirements of ISO/IEC 27001, and obtaining certification includes a number of specific steps. The following 7 steps will apply to most organizations, regardless of their industry or level of preparedness.

1 Obtain management commitment

The successful implementation of any management system, including an ISMS, requires a commitment from leadership at the highest level of the organization. Without such a commitment, other business priorities will inevitably erode implementation efforts.

2 Define the information security policy

The organization identifies and defines its information security policy based on the specific goals and objectives that it hopes to achieve. This policy will serve as a framework for future development efforts by establishing a direction and set of principles regarding information security.

3 Define the scope of the ISMS

With its information security policy in place, the organization then identifies those specific aspects of information systems security that can be effectively addressed within the scope of its ISMS.

4 Complete a risk assessment of current information security practices

Applying the most appropriate methodology, the organization then conducts a thorough risk assessment to identify the risks that are currently being addressed, as well as system vulnerabilities and threats that require attention.

5 Identify and implement risk measures and controls

The organization implements measures and practices to mitigate all of the risks identified in the risk assessment. The results of these measures and practices are then monitored and modified as required to improve their effectiveness.

6 Conduct an ISMS pre-audit

With a tested and proven ISMS in place, the organization conducts a certification assessment pre-audit to identify any potential issues that could negatively impact the outcome of the certification audit. Any nonconformities with the requirements of ISO/IEC 27001 are then addressed and/or corrected.

7 Conduct surveillance audits

Organizations that achieve ISO/IEC 27001 certification are subject to yearly surveillance audits to confirm continued compliance with the requirements of the standard. A full recertification audit is required every third year following certification.

About TÜV SÜD

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions, specializing in testing, certification and auditing services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology-related risks. Through more than 25,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

TÜV SÜD America

Learn more about TÜV SÜD's ISO 27001 Certification Services:

www.tuvsud.com/en-us/iso-27001
systemcertification@tuvsud.com