TÜV TRUST IT
TÜV AUSTRIA Group

Certification

Certification in Accordance with ISO/IEC 27001:2013 by TÜV Austria Deutschland GmbH

Information is the basis for the course of business and production processes and for communication with customers and partners. To provide appropriate protection for business information, effective processes, such as those that are mapped in an information security management system (ISMS), are required. The internationally recognised standard for ISMSs is ISO/IEC 27001:2013.

Certification in accordance with ISO/IEC 27001:2013 means that ISMS processes and measures are subject to constant independent review. By means of a certification, companies can additionally demonstrate to their customers and partners the efficacy and efficiency of the ISMS along with the fact that the ISMS is regularly checked by independent auditors such as TÜV TRUST IT's. Using tried and tested methods and tools to assess the management of information security, security concepts and organisational and technical measures, TÜV TRUST IT can identify specific vulnerabilities and highlight improvement potentials.

Approach

For certification in accordance with ISO/IEC 27001:2013 the following procedure is mandatory, focusing in this excerpt on the following aspects:

Stage 1: Checking the ISMS's Certifiability (Document Check)

- Assess the customer's location and his location-specific conditions
- Evaluate the customer's status and his understanding of the standard's requirements
- Collect the necessary information about the scope of the ISMS
- Evaluate the allocation of resources for the Stage 2 Audit
- Specify the focal points for planning the Stage 2 Audit
- Judge whether the internal audits and management appraisals were planned and implemented

On successful completion of this phase the next stage can begin.

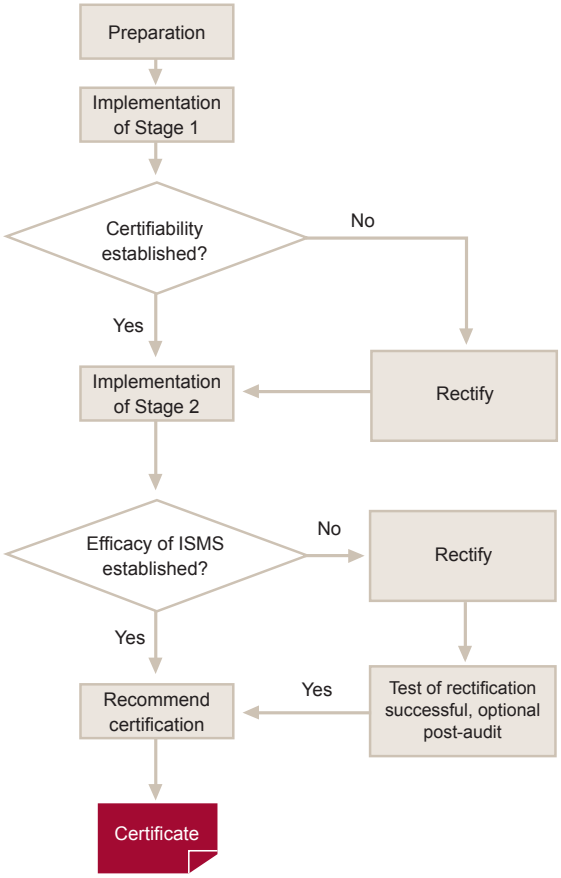
Stage 2: Checking the ISMS's Efficacy

- Assess the information security risks
- Check the documentation required in Chapters 4 to 10 and how it is checked
- Select targets and checks on the basis of the risk assessment
- Check internal ISMS audits and management reviews
- Check the responsibility of the top management
- Implement checks

All audit activity in this phase is based on the ISMS processes that have heretofore been adopted. The audit team analyses all information and audit evidence recorded in stages 1 and 2 in order to assess the audit findings and to agree on audit conclusions. If the audit conclusion is successful, the auditors will recommend to the certifying body that issues the certificate a certification based on the positive findings of their audit.

Certification

An ISO/IEC 27001:2013 certificate is valid for three years. Following the certification audit there are annual review audits and, if required, a re-certification after three years.



Procedure of Certification based on ISO/IEC 27001:2013

Your Benefits

- Independent and internationally recognised proof of appropriate information security for partners and authorities
- Lasting improvement of ISMS processes by means of regular reviews
- Avoidance of unforeseen costs due to security incidents
- Build-up of trustworthiness and security ISMS certification is proof of value promises and ensures lasting maintenance and development of information security
- As a DAkkS-accredited certification body, TÜV Austria Deutschland GmbH is happy to be of assistance with your certification projects

TÜV TRUST IT GmbH
TÜV AUSTRIA Group

Waltherstraße 49–51
D-51069 Köln
Phone: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Phone: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com