TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

SIEMENS

Setting up an Information Security Management System (ISMS) at SIEMENS AG

Using Information Management Security Systems (ISMS) is now a core element of corporate strategies for cybersecurity and other security issues. That is why more and more Siemens AG business units are now opting for the international ISO/IEC 27001 standard. The company's Corporate Governance department commissioned TÜV TRUST IT to launch an ISO/IEC 27001-based ISMS as an essential foundation for information security within the Siemens Group.

SIEMENS AG is a leading global company that is positioned along the electrification value chain – from conversion, distribution and utilisation of energy to medical imaging and in-vitro diagnostics. Active worldwide, the company has a payroll of over 370,000 employees and earned sales revenues of around € 83 billion in financial year 2017.

To implement its security strategies Siemens uses the services of external experts as required. The Group's Corporate Governance department did precisely that when assistance was required to improve the process maturity of the ISO 27001:2013-based ISMS in preparation for certification. In June 2017 Siemens decided in favour of TÜV TRUST IT as its external partner.

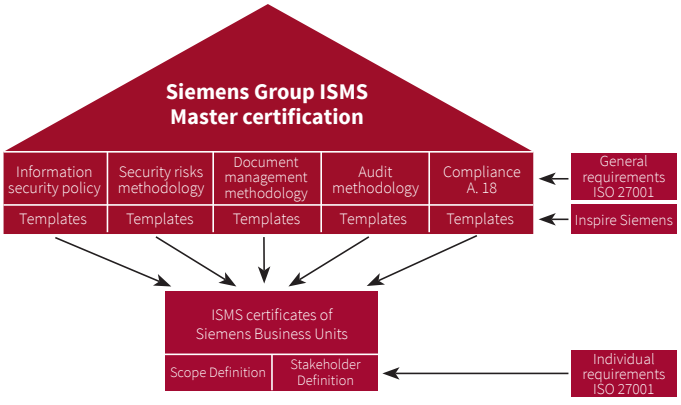
Starting point

The aim of the project was to establish an ISMS at Corporate Governance, one of the Group's key departments. Special attention was to be paid to the individual ISMS sub-processes document control, auditing and risk management. They were to be designed so that they could be used independently of the department to be protected.

A further fundamental requirement added to the complexity. As Siemens has different application areas for its services that each need to be secured by the verifiable implementation of an Information Security Management System a certified ISMS was to be set up in a central department from which the certified sub-processes were to be distributed. The sub-processes were to be mapped in such a way they only needed to be personalised by the requesting business units.

Approach

ISMS inventories and gap analyses had already been undertaken as part of an in-house preliminary project in various organisational areas of the Group. They included identification and factual evaluation of disparities between the existing ISMS status and a status capable of certification in accordance with ISO/IEC 27001:2013. These findings were taken into consideration in the further development of the ISMS.



ISMS development plan

TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

After this detailed research into and evaluation of in-house information security processes they were consolidated and structured using the document templates of the TÜV TRUST IT ISMS framework. Missing relevant methodologies and proofs were drawn up and published in close cooperation with the Siemens project managers. The result was an in-house group ISMS framework that was distributed around the Group in order better to do justice to upcoming certification requirements.

Structured working and creative use of the TÜV TRUST IT ISMS framework made it possible to complete the project within four months and to have the ISMS established at the Corporate Governance department successfully certified by an accredited certification authority.

Benefits

- The central Corporate Governance department now has a certificated ISMS with individual sub-processes designed so that other SIEMENS AG business units can use them.
- Certification testifies that the organisation has a functioning IT security management.
- This IT security system knows the organisation's risks and can derive rules from them. With its assistance processes can be documented and measured.
- Certification enables SIEMENS AG to prove its quality level objectively and convincingly to its customers and business partners.

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

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