TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

Roche

Developing an Information Security Strategy and Setting up an ISMS for Roche Diagnostics

Medical products are subject to strict controls and regulations. Violation of these regulations can lead to severe penalties, including a sales stop. Roche Diagnostics ltd. in Burgress Hill (England) was faced with the challenge of meeting the given national requirements. The company requested support from the global Roche Diagnostics Quality & Regulatory Organisation in Rotkreuz, Switzerland. The organisation commissioned TÜV TRUST IT to identify the information security strategy and to support the implementation of the measures identified.

Initial Situation

The Diagnostics Division of F. Hoffmann-La Roche AG, the world's third-largest pharmaceutical company, supplies products for the prevention, diagnosis and treatment of diseases for scientists, doctors, patients, hospitals and laboratories around the world. The National Health Service in England (NHS) places high demands on companies working with patient data. These requirements also had to be met by Roche Diagnostics' UK subsidiary in order to continue its support and sales operations in the UK. In order to demonstrate a concrete approach, it was first determined which legal entities in Germany and abroad were affected by the NHS requirement. At the same time, the requirements were subjected to an analysis in order to estimate the effort and resources required. It was recognised that the requirements of the NHS are to a large extent congruent with the ISO/IEC 27001 standard. As a result, it was decided to establish and certify a global ISMS.

Hans Georg Seiberlich (Head of Global Customer Support Quality) says: *"Thanks to TÜV TRUST IT, we quickly identified the appropriate strategy for implementation. Above all, it was important to recognise that not only the subsidiary must meet the requirements of the NHS, but also every third party to whom the English subsidiary transmits patient data. In addition to suppliers, these included other Roche Diagnostics companies in various countries."*

Approach

In order not to overburden the entire organisation, a strategy was chosen which provided for gradual implementation per legal entity. This ensured that there was a learning effect and that synergies could be optimally made use of for each subsequent legal entity. A steering committee and central project management were responsible for the coordination and interfaces between the units.

The next step was to use simulated audits (mock audits) to determine the conformity of the legal entities concerned with the requirements of ISO/IEC 27001. On the basis of these audits, the missing requirements were identified and a development plan was drawn up. Not only the implementation of the technical requirements was important. An elementary part of the project was interdisciplinary and organisational.

Since information security can only be achieved sustainably if the acceptance of the organisation is present, a top management commitment was obtained and intensive change management was carried out.

Rob Chapman (project manager): *"Thanks to the qualified consulting of TÜV TRUST IT, we were able to implement the change within the organisation in a sustainable manner. The*

TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

ISMS and the associated information security requirements are now an integral part of our corporate culture."

Another requirement was the design of the processes. Thus, no unnecessary processes designed especially for the ISMS were introduced, but existing processes were adjusted or extended.

Jan Kiefer (Senior Consultant at TÜV TRUST IT): *"We have seamlessly integrated risk and quality management into Roche Global's global system. This has enabled us to ensure that processes are lived sustainably and that no inefficient workarounds occur."*

Benefits

The successful introduction of the ISMS was confirmed with the certification according to ISO/IEC 27001:2013. Locations in Germany, Switzerland and England are now part of the global ISMS. With the successful completion of the project, the foundation stone has been laid for the operation of a sustainable ISMS.

Hans-Georg Seiberlich: *"With the selection of TÜV TRUST IT as a consultant for the information security strategy, we were absolutely right. The pragmatic and competent approach to such a complex project made a decisive contribution to its success."*

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