Add value.
Inspire trust.

Case Study: Roche Diagnostics International AG

ISO/IEC 27001: Certification that creates trust. For years, Roche Diagnostics International AG has been committed to information security – particularly when it comes to protecting sensitive patient data.

Business challenge

"When it comes to sensitive data, 'Trust & Transparency' is our guiding principle," explains Reto Weber, ISMS Officer at Roche Diagnostics International AG. Roche Diagnostics is one of two business divisions within the pharmaceutical company Roche, specialising in products and services for the prevention, diagnosis and treatment of diseases.

Analysis of tissue, blood and other patient samples provides important information about diseases, risks and a patient's response to certain treatments. This can be used to prevent a disease from progressing, and even stop its onset in some cases. As the information is derived from a large volume of highly sensitive data, it must be protected as effectively as possible. "Long-term success is only possible if people can be assured that we are highly committed to IT security," Weber notes.

Specific impetus for a third-party IT security assessment at the company's Rotkreuz site was given by the public health service system in Great Britain and Northern Ireland, the National Health Service (NHS). The NHS recommended that Roche Diagnostics obtain independent certification to validate its protection of patient data. Weber explains: "It was something we already had on our agenda, as we were reviewing

OVERVIEW	
Client name	Roche Diagnostics International AG
Industry	Diagnostics
Profile	Roche Diagnostics International AG provides products and services related to illness prevention, diagnostics and treatment for researchers, medical personnel, patients, hospitals and laboratories worldwide.
Business challenge	Sensitive patient data requires specific protection – in addition to the commitment of the provider, an independent seal of approval is needed.
Our solution	An information security management system based on ISO/IEC 27001, with a structured and systematic approach for the optimised protection of sensitive data.
Business benefits	A certification such as ISO/IEC 27001 creates customer trust, confirming the effective implementation of a highly professional, responsible system for securing sensitive patient data.

several cloud solutions." For Roche, the highest priority when it comes to security is creating trust among customers. "Whether it is in relation to patients, hospitals or labs, our stakeholders need to know that we take information security very seriously."

Our solution

Roche Diagnostics International chose to implement an Information Security Management System (ISMS) based on ISO/IEC 27001, which is the leading global standard for ISMS.

The first step was to gather all stakeholders around one table – no easy task, since a wide range of departments from the global group were involved, as well as various business partners. Nonetheless, stakeholder alignment proved to be a central component on the path to certification. In contrast to the internal complexity, the choice of service provider for the certification was clear. "We enjoy a long-standing partnership with TÜV SÜD – they also handle our ISO 13485 certification. Our co-operation has always been highly satisfactory and we were happy to extend it," says Weber. One particular advantage of TÜV SÜD is the prominence of its certification mark, which is recognised as a symbol of quality and reliability globally, across all industries and even among consumers. "A seal of approval awarded by a German industry expert such as TÜV SÜD brings a distinct credibility," explains Weber. "It can really help you stand out from the competition."

Business benefits

During the ISO/IEC 27001 certification process, it became clear that information security is not solely an IT issue, but also needs to be managed across business operations. "This aspect was particularly appealing to the decision-makers," recalls Weber. "And for our customers, a certification is the best possible mark of confidence." A total of seven sites in Germany, Switzerland, Spain and the USA have been certified on a gradual basis. "The certification was definitely worth it, even just for the change of mindset within the business," says Weber. He goes on to point out that: "At product level, the ISMS enabled a fast and easy migration to cloud solutions." One example is the seamless data migration to the 'Tumour Board', a diagnostics and collaboration application in which patient data can be securely stored in the cloud. "Obtaining certification is one thing, retaining it is the next challenge. After all, it is not simply a one-off investment," Weber points out. The ISO/IEC 27001 standard demands continuous improvement, for which the annual visit from an external auditor with broad industry experience and the capacity for benchmarking can be very helpful. "The auditor examines our processes and implementations to evaluate how we are developing in terms of information security," Weber emphasises. "With TÜV SÜD, an audit does not simply consist of a checklist. In fact, the auditor offers input and knowledge from the field which creates true added value for us. During this period, we have made considerable progress." As a result, the ISMS certification is highly valued at Roche Diagnostics International. "We get so much positive feedback. The ISMS is being extended by one to two sites and scopes every year," enthuses Weber.

Weber has also learned from experience that upper management must be on board to ensure effective implementation. He explains: "My advice would be to focus on the issue itself rather than the standard, which is just a means to an end. In our case, the issue was protecting patient data and the importance of our venture was clear to everyone from the onset." Weber concludes: "We are responsible for securing all data, but especially highly sensitive data, as efficiently as possible. The customers place great trust in us, and we want to do justice to that trust. We ensure this by implementing systems that comply with international standards and are certified by industry experts," summarises Weber. "If personal data of myself or my family were to end up in the system at some point, I would like it to be really well protected – that is our daily motivation, and precisely how we approach the data with which we are entrusted. The ISO/IEC 27001 management system perfectly supports us in these endeavours."

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory 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 24,000 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 AG Westendstr. 199, 80686 München, Germany
+49 89 5791-0 systemcertification@tuvsud.com www.tuvsud.com/iso-27001