



Compliance Training for IT Managers

DEW21 is a water supply company based in Dortmund, in which the Dortmunder Stadtwerke AG and RWE Deutschland AG are shareholders. With approximately 1,000 employees and an annual turnover of 950 million euro, the Dortmund Energie- und Wasserversorgung GmbH belongs to the largest utility companies in the Ruhr area. Like all organizations operating critical infrastructures (CRITIS), DEW21 is facing major challenges: The regulatory requirements are increasing and the compliance management has to meet ever-increasing expectations from government agencies and business partners, particularly in the IT sector. TÜV Rheinland accompanied DEW21 during the setup of an IT compliance management system (CMS) and trained the IT Compliance Managers for future requirements.

IMPLEMENTATION OF AN IT COMPLIANCE MANAGEMENT

The IT compliance of an organization is subject to self-determined standards as well as legal requirements, such as the German Federal Data Protection Act (BDSG) and the principles for proper keeping and maintaining books,

records and documents in electronic form, as well as data access (GoBD) and internal sets of rules, such as service level agreements (SLA), up to international standards. In this context, special focus is on the IT security law. By May 2018, energy supply companies must demonstrate a minimum level of IT security according to the "current state of the art" – and the certification as per ISO standard 27001 is one of the ideal solutions for this goal. This standard forms the basis for introducing an information security management system (ISMS) which, in turn, demands that the organization knows and complies with its own regulatory requirements. With the implementation of an effective IT compliance management, this requirement can be perfectly met. However, both are tasks that cannot be accomplished overnight. DEW21 knows the importance of an effective compliance management and has already initiated the steps required for it in 2015. The organization is revising its compliance structures and processes, at the same time it also implements an ISMS, with both teams working hand in hand. In this way, Ralf Kohlmann, IT Compliance Manager, supports and relieves the Chief Information Officer.



POINT-TO-POINT ANALYSIS OF STRUCTURES AND PROCESSES

TÜV Rheinland offers training for the demanding role of the IT Compliance Manager. The coaching covers all areas needed for the setup of an effective IT compliance management. The overriding objective is to establish and operate a command center in the organization to control IT compliance topics actively, independently and, as a result, effectively. In the process, relevant areas, such as IT risk management, IT security, information security and business continuity management as well as data protection are also integrated. The coaching defines roles, tasks and processes, and provides long-term support for the implementation.

OUR EXPERTISE IN IT COMPLIANCE MANAGEMENT

Essential questions to be answered during the coaching include:

- Which specifications are relevant overall to the IT of the organization?
- Which processes, systems and applications are affected by it?
- Which requirements apply to the individual areas of IT?
- Which risks are associated with a lack of compliance?
- Which technical, organizational and personal measures are required to assure IT compliance?
- Which references to other topics are important in this context?

“After the coaching, the organization will have knowledgeable employees who can implement a successful IT compliance management and rigorously maintain it,” explains Jörg Stümke, Project Manager and expert on information security at TÜV Rheinland.

PROJECT COURSE AND MILESTONES

The coaching of the IT Compliance Manager takes approximately six months and includes six one-day workshops in monthly rotation. After the common stake-out of objectives and the definition of internal and external requirements on IT compliance, the participants analyze which criteria are important to the organizational structure and the required processes. For this purpose, roles, tasks and relevant contact persons in other departments are identified. IT compliance management does not exist detached from other fields and tasks of the company, but has to fit harmoniously and meaningfully into the overall organization. The effective use of checklists and reporting is also part of the coaching topics.

The IT Compliance Manager can be successful only if he or she has not just the expert knowledge and knows the methods, but also has the required skills for their tasks, such as the power of persuasion and assertiveness. For this reason, the coaching also mediates how the IT Compliance Manager succeeds in being recognized as assistant and partner and achieve their intentions in the organization in the interest of safeguarding the future for everyone. Ralf Kohlmann, IT Compliance Manager of DEW21, draws a positive conclusion: “The coaching by TÜV Rheinland prepared us optimally to successfully master the multitude of challenges in the coming years in the field of IT compliance.”

TÜV Rheinland
Digital Transformation & Cybersecurity
service@i-sec.tuv.com

www.tuv.com/informationsecurity

DEW21



TÜVRheinland®
Precisely Right.