Insufficient security in information processing causes millions in damages every year. The reasons for this are manifold: external troubles, technical errors, espionage, or information misuse. In order to implement effective measures, though, you first need to identify the challenges involved.

The objective of an information security management system (ISMS) according to ISO 27001 is to identify corporate risks, to analyze them and to use suitable measures to make them controllable. In its structure, international standard ISO 27001 is aligned with the PDCA cycle of Plan-Do-Check-Act, an approach well known from ISO 9001. Integrating ISMS into an existing management system can therefore be done easily.

Benefit
ISO 27001 specifies the systematic structure of a process-oriented management system for information security. It also specifies the requirements for such a system. This comprehensive approach offers many decisive advantages:

- Increased security awareness among employees and managers
- Safeguarding of the security objectives confidentiality, availability, integrity, authenticity, and reliability of information
- Contribution to safeguarding business continuity
- Legal certainty through systematic adherence to relevant laws on information security and data protection
- Reduced risk of management liability
- Cost savings through security incidents avoided
Getting started:
The DQS multi-level approach to ISMS

DQS was the first German certification body to become accredited for BS 7799-2, the predecessor of ISO 27001, in December 2000. Based on many years of experience, DQS then developed a four-level assessment concept, which can be customized to the security needs and objectives of each individual customer.

With highly qualified auditors and flexible planning, DQS supports their customers on all levels of their development – from the easy first step of self-evaluation all the way to comprehensive certification.

**Step 1**: Self-evaluation of your security aspects based on a short questionnaire

**Step 2**: During a quality management assessment, auditors address security considerations

**Step 3**: Assessment of the most important aspects of an ISMS, subsequent to an assessment to ISO 9001

**Step 4**: Comprehensive assessment of your ISMS and certification to ISO 27001

**Step 5**: Upgrade of the integrated management system with additional IT and information security considerations, such as data privacy or IT service management