IT Security Management

ISO 27001 & IT-Grundschutz

The implementation of IT security controls is common practice in numerous companies. The question, however, is whether these measures are sufficient and appropriate. ISO 27001, developed by the International Organisation for Standardisation, as well as the IT-Grundschutz Catalogues by the German Federal Office for Information Security (BSI) provide frameworks for the selection of appropriate controls for typical IT configurations. The objective of these recommendations is to help companies apply suitable standard security measures regarding organisation, personnel, infrastructure, and technology in order to create and maintain an IT system security level appropriate and suitable for normal security needs and capable of serving as a basis for highly vulnerable IT systems and applications. No matter which standard you follow as a company – a successful certification audit entitles you to an internationally accepted ISO 27001 certificate.

Objective

Our ISO 27001 auditors assist you with the creation of a security concept based on ISO 27001/IT-Grundschutz and guide you on your way to the ISO 27001 certificate. Thanks to many years of experience in this area, plan42 helps you complete your project in a cost- and time-effective way.

The IT-Grundschutz Methodology

1. **Initiating the Security Process** – We help you identify your needs and define general security goals; a security guideline and your security organisation are established.
2. **Analysing Your IT Structure** – The project's scope is determined. We collect information about the technology used in your environment.
3. **Assessing Your Protection Requirements** – Which level of protection is required for your IT and applications? The assessment provides answers to this question and thus helps you select appropriate security controls for your individual IT components.
4. **Modelling the Components** – In this step, we help you model your IT network and its individual components by means of modules/controls defined in ISO 27001 or the IT-Grundschutz Catalogues.
5. **Performing a Basis Check** – The security measures already implemented are compared to the ISO 27001/IT-Grundschutz Catalogue recommendations in order to identify the achieved security level, find potential for improvement and initiate implementation planning. Security measures are not limited to technical aspects, but also include aspects such as organisation, personnel, and physical infrastructure.
6. **Identifying Additional Measures** – The controls provided by ISO 27001 or the IT-Grundschutz Catalogues may not suffice for critical communication channels and highly vulnerable IT systems or rooms. A supplementing security analysis helps you identify any additional security controls required for these critical IT components.
7. **Implementing Your Strategy** – We help you deploy any missing security controls and are glad to assist you with both the technical implementation and the development of security guidelines and concepts.
8. **Audit** – We prepare for you all the documents required for the audit and are happy to assist you during the remaining steps to certification.

Result

In accordance with the ISO 27001/IT-Grundschutz Catalogue recommendations we summarise the results from the individual project steps in detailed documents. This provides you with all the risk management documentation demanded by law and allows you to have an optional ISO 27001 certification carried out.

plan42

plan42 is a consulting firm specialised on IT Service Management, IT Security Management & Business Solutions. Process analysis, consulting, conception, and implementation – plan42 combines technical expertise and best-practice concepts of IT Service & Security Management.