ISO 27001 certification

What are the steps to become ISO 27001 certified?

ISO/IEC 27001 is an internationally supported basis for information security. This standard specifies a management system with the intend to bring information security under control of the management by specifying controls required to secure information.

The ISO 27001 certificate is recognized worldwide as a basis for data security. The guidelines and requirements from the standard enable organisations to regulate information security on a structural basis. That makes ISO 27001 certification a solid foundation for securing business information. Certification is of added value for every organization that has to deal with financial risks and risks in the area of privacy-sensitive information.

Many organizations already have some form of controls in place to manage information security, but with ISO 27001 this can be formalized. With ISO 27001 certification, organizations not only demonstrate customers, partners and suppliers that they handle sensitive information accordingly, but also that they safeguard the privacy of their employees. This will increase stakeholders' confidence in interacting with these organizations and provides ease of mind around the business' security risks.

Although every implementation of ISO 27001 differs this whitepaper provides a guideline on some of the mandatory steps which should be included in every implementation.

Create business case
Every implementation of ISO27001 starts with a business case. The business case describes the benefits the organization hopes to achieve by implementing a management system for information security.

Management support
Involvement from top management is critical to the design and effectiveness of any information security program. Having management support further ensures information security is aligned with enterprise strategy and governance and helps with allocating the right resources for the project

Inventory information assets
When implementing ISO 27001 an inventory is needed of the information assets that require protection. These information assets will be the subject of a risk analysis in a later stage. Information assets can include digital and physical sources, applications, IT hardware, etc.

Define risks analysis method
Before you can conduct a risk analysis, rules needs to be defined on how risk management is going to be performed and to ensure this process is conducted in the same way throughout the organization. Choosing a risk assessment methodology is a crucial part of the risk management process.

Risk analysis
Risk analysis if one of the most important steps of the ISO 27001 process. The main purpose of ISO 27001 is to determine which incidents could occur and implement controls to prevent them. During a risk analysis not only the risks are determined but also their importance and impact.

Statement of Applicability
The statement of Applicability links the risk assessment and risk treatment to the implementation of your information security controls. It identifies the selected controls required to address identified risks, explains why these are needed and if they are implemented.

Risk treatment plan
After the risk analysis has been conducted a risk treatment plan should be created. The risk treatment plan document determines who is responsible for the implementation of controls to mitigate risks.

ISMS implementation program
When the information to be protected is identified, a risk analysis has been conducted, the scope is clear and controls have been identified, it is time to implement the Information Security Management System (ISMS). The ISMS contains documents describing policies, procedures, processes, standards and guidelines. It is the framework for an organization's information security policy.

Internal audits
ISO 27001 is all about plan-do-check-act and the internal audit is a core function to achieve this. The main purpose of the internal audits is to determine if the ISMS meets to both the organization's requirements as well as to the requirements of the ISO 27001 standard.

Corrective action procedure
Once a non-conformance is identified as part of the audit process there needs to be a procedure to correct the finding. The main aim of the procedure is not only to solve a non-conformance but also to take away the root cause.

Document control
The purpose of a good document control procedure is to ensure control over the creation, approval, distribution and usage of documents created as part of the ISMS in a ISO 27001 implementation.

Documents
Part of the ISMS is a set of documents concerning procedures, logs, compliance and audit reports as an evidence to demonstrate the working of the ISMS. Having a proper structure on how to store these documents is essential, since they have to be accessible to relevant employees as well as external auditors.

Pre-audit / baseline audit
Before entering the actual certification process, the baseline audit is a useful instrument to assess to what extend the organization complies with the organizational requirements and the requirements set by the ISO 27001 standard.

Certification
Once all steps have been taken and the ISMS is up and running, the organization is ready for certification, which will ultimately lead to an advise given by the external auditor. He determines whether or not the organization can be certified.

NEN 7510
The NEN 7510 is a Dutch standard specifically aimed at healthcare organizations. It relies heavily on the ISO 27001 but requires some additional controls around the handling of patient information.