What is ISO 27001 Gap Analysis?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

Organizations seeking a high level of security and protection for their IT Infrastructure need to get ISO27001 Accreditation. ISO 27001 is a globally-recognized standard that organizations use as a benchmark to audit and certify their Information Security Management System (ISMS). Achieving ISO 27001 accreditation simply demonstrates that the organization has a robust management framework in place to protect the confidentiality, integrity, and availability of the organization's IT infrastructure. But when the organization commits to this standard of excellence, ensuring continuous compliance is critical. Conducting a thorough Assessment and Gap analysis of the organization's IT Infrastructure and its ISO 27001 Compliance requires commitment and exceptional expertise. In today's article, we discuss what an ISO27001 Gap Analysis is and why is it an essential part of the ISO27001 Audit process. So let us first quickly understand what is an ISO 27001 Gap Analysis is.

What is ISO27001 Gap Analysis?

An ISO 27001 Gap Analysis also known sometimes as Compliance Assessment or Pre-Assessment is an assessment that provides a high-level overview of your organization's current security posture. The assessment and report serve as a guide to organizations for achieving ISO27001 certification. The assessment involves comparing the organization's existing information security controls against the requirements of ISO 27001. The Gap Analysis measures the current state of compliance against the Standard and also scopes the organization's ISMS parameters across all business functions. It provides companies with the necessary information and recommendations of controls that may need to be implemented to close the gaps. The Gap Analysis helps companies understand the best way to improve and streamline their internal information security management systems to ensure they meet the requirements of the ISO 27001 standard.

When is an ISO27001 Gap Analysis performed?

ISO27001 Gap Analysis is a professional assessment that is performed between stage 1 and stage 2 of the ISO 27001 Audit process. The assessment helps bridge the gap between stage 1 and stage 2 of the ISO 27001 Audit. The objective is to ensure that any ISMS gaps that were identified in stage 1 are addressed appropriately. It further helps companies prepare for stage 2 and the ISO 27001 certification process. However, it is important to note that gap analysis is mandatory in ISO 27001, but only after an organization has developed its Statement of Applicability. It details the security posture on each of the 114 information security controls that are outlined in Annex A of ISO 27001. So, ISO 27001 gap analysis should be performed only for the controls from Annex A of the ISO 27001 standard and is also done before it starts the ISO 27001 implementation to get a perspective on the current standing of the organization and the quantum of work involved.

What to expect from an ISO27001 Gap Analysis?

Companies hire professional consultancies to perform the ISO 27001 gap analysis. During this course of analysis, the auditors will assess the existing information security processes, procedures, and documentation of the organization and compare those against the requirements of the ISO 27001 standard. This is done to identify areas that require improvement in their existing information security processes and procedures. The report of the analysis performed will highlight deficits in systems against the requirements of the ISO 27001 standard, and further help address the identified issues. Conducted by an ISO 27001 specialist, the analysis gives a detailed assessment and analysis reports detailing the findings which include-

- The current state and maturity of the information security processes and procedures.
- The compliance gaps as against the requirements of the ISO 27001 standard.
- The scope of the organization's ISMS.
- Details about the internal resource requirements for achieving compliance.
- An outline plan of action indicating the level of effort required to implement an ISO 27001.
- The tentative timeline to achieve certification readiness.

What are the benefits of ISO27001 Gap Analysis?

Given below are listed benefits of ISO27001 Gap Analysis-

- You will get an overview of the organization's current security posture against the requirement of ISO 27001.
- It guides the organization in its efforts of achieving ISO27001 certification.
- The gap analysis scopes your ISMS parameters across all business functions.
- The analysis gives clarity on what needs to be included in the scope of ISMS and controls that need to be implemented
- Helps estimate the resources and budgetary needs of the ISO 27001 project.
- Ensures translation of cybersecurity into business policies procedures and framework.
- The valuable insight obtained from the analysis enables the organization to plan a strategic roadmap for the implementation of necessary cybersecurity controls.
- It also provides you with a potential timeline for achieving ISO27001 certification.
- The gap analysis will help the organization get closer to achieving the accredited certification.

Final thought

For those organizations looking to seek high-level security for their IT infrastructure must comply with the ISO 27001 and perform at least Gap Analysis. It allows you to benchmark the organization’s existing policies and controls against the ISO27001 standard. It will allow you to identify gap areas in the organization’s processes, policies, and controls and highlight weak areas in the system. So, to strengthen the organization's security posture, businesses should consider performing an ISO27001 audit and gap analysis to develop a strong business case for implementing an ISO 27001-compliant ISMS.

Original Published on:- ISOUpdate
Written By:- VISTA InfoSec

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA +1-415-513 5261 | INDIA +91 73045 57744 | SINGAPORE +65-3129-0397 | UK +447405816761