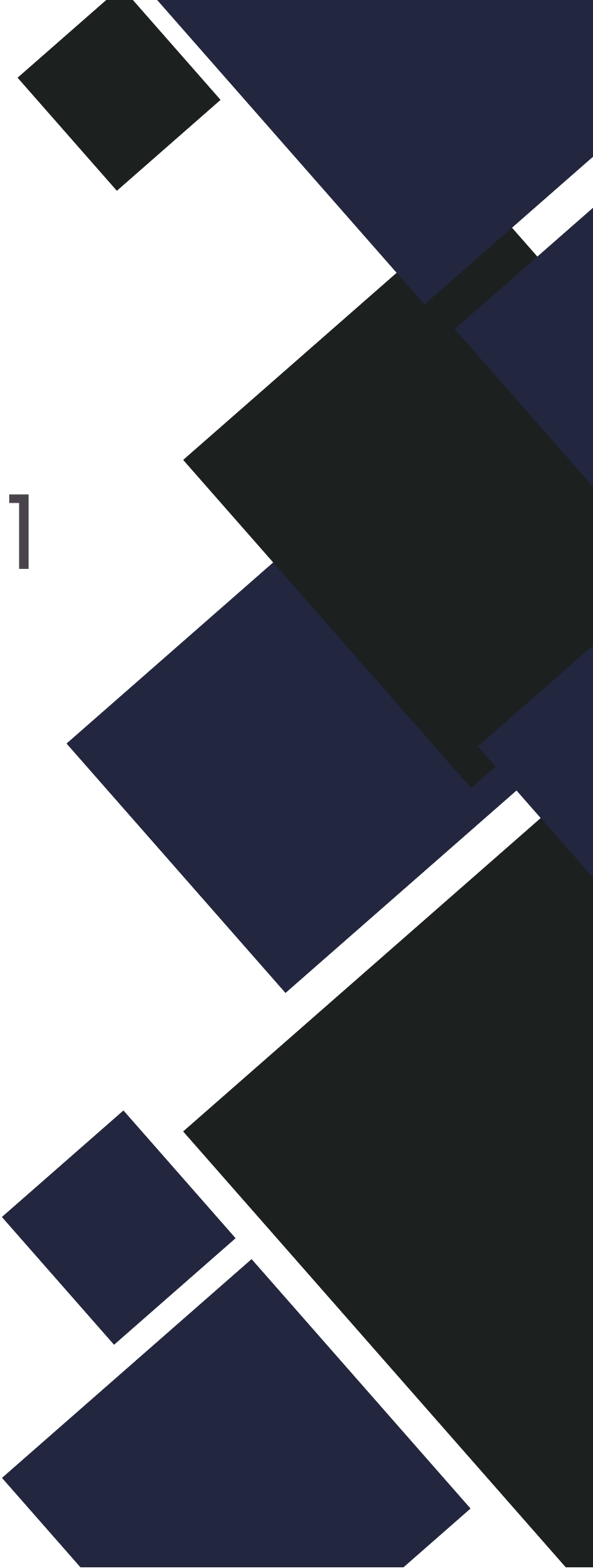
ISO 27001

E-BOOK



accorp

Introduction

ISO 27001 is an international standard for information security management that establishes a risk-based, six-step methodology for effectively managing an organization's information security risks. Without proper implementation of ISO 27001, an organization's security controls may be unproductive and disorganized. Your donation will help fund the development and implementation of ISO 27001 so that organizations can protect their information more effectively.

The six steps of ISO planning are as follows: -

- Establishing a security policy.
- Defining the scope of the information security management system (ISMS).
- Conducting a risk assessment.
- Managing identified risks.
- Selecting the objectives and controls accordingly for implementation.
- Creating a statement of applicability.

Data Security

ESTABLISHING AN ISMS

While ISO 27001 is just one standard of many in the 2700 family, it is still a critical one. This standard provides guidance for businesses who wish to establish an Information Security Management System. Specifically, ISO 27001 establishes requirements for maintaining and improving an organization's information security.

An ISMS is a set of processes and systems that an organization uses to keep information safe. ISO defines it as "a systematic approach to managing sensitive company information so that it remains secure." This approach includes people, processes, and IT systems, and uses risk management to protect information. The specifics of an ISMS will depend on the size and needs of the organization, but a strong ISMS will generally involve all aspects of the organization in data security.

There is no definitive checklist of requirements for ISO 27001 certification, but organizations seeking to comply with this standard must create a number of documents regarding their ISMS policies, such as :

- The scope of the ISMS
- Information security policy and objectives
- Risk assessment methods, definition of security roles and responsibilities, internal audit methodology
- Access control policy
- Legal and regulatory requirements
- Incident management procedure
- Business continuity procedures

PLAN, DO, CHECK, ACT (PDCA)

PLAN

When an organization is planning its security measures, it takes into account the risks and needs present in its current security framework. This establishes security guidelines that are then implemented into the organization's ISMS. By doing this, the organization creates clear and consistent policies surrounding data security.

DO

Guidelines set during the planning phase for an ISMS are put into place during the implementation phase, in order to test out the system's efficacy.

CHECK

Guidelines set during the planning phase for an ISMS are put into place during the implementation phase, in order to test out the system's efficacy.

ACT

The "Act" phase of PDCA (Plan-Do-Check-Act) is when an organization takes corrective action based on its check of the ISMS. Implementing necessary changes is the first step of successful continual maintenance of the ISMS.

CERTIFICATION PROCESS

Once an organization decides that they would like to become ISO certified, they must select an individual to manage the process and ensure that all requirements are met. It is also crucial to develop a comprehensive Information Security Management System (ISMS). The next step is to undergo an internal audit by the assigned ISO manager. The final audit is conducted by a certification registrar. It is important to keep in mind that ISO does not conduct audits for certification purposes.

Once a company has selected an ISO representative, they can begin to conduct a risk analysis to identify which security gaps need to be closed within the organization. After the risk analysis is complete, the company can start to develop the scope of the needed ISMS and create an implementation plan. The next step is to compile the necessary documentation to support the planned ISMS. The amount and type of documentation required will depend on the risk analysis as well as other variables, such as the size and industry of the company applying for certification.

An internal check by a designated auditor should be carried out to assess the controls put in place before a final audit by a certified registrar. If the latter is successful, a company will receive its formal certification.

Other Resources

BUILD TRUST WITH SOC

In current scenario of emerging technologies, most of the organizations outsource few aspects of their business to vendors which can either include performing a specific task or replacing an entire business function.

PCI DSS E-BOOK

PCI DSS audit, or the Payment Card Industry Data Security Standard, is a set of requirements designed to protect credit and debit card information from being compromised by businesses.

HIPAA E-BOOK

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress in 1996 and signed into law by then President Bill Clinton.