Classification of information

ISO 27002 Control 5.12

Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements

Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization

Why is it important?

To ensure that the assets required to deliver services are controlled and that information on these assets is sufficient, accurate and available when necessary.

This information includes details about the configuration of the assets as well as the relationships between them :

- The integrity of the CIs and their configuration must be protected
- All CIs are listed in a configuration management system
- Must effectively support other business processes

What is the usual classification scheme

- Confidentiality : Protecting information from unauthorized access
- Integrity : Ensuring information is accurate and unaltered
- Availability : Ensuring information is accessible when needed
- PII: Personally Identifiable Information : data that can tied to an individual
- Any legal attribute that has associated security requirements

What is the usual process ?

- The asset owner defines the classification
- Consider the business needs
- Consider legal obligations
- Regularly update and review the classification
- Ensure organizational consistency

Link with other frameworks

- NIST 800-53 rev5 : RA-2
- NIST CSF 2.0 : ID.AM-05

Renaud Dardenne
Asphalia Consulting