

Information security in supplier relationships

ISO 27002 Control 5.19

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services

Purpose

To maintain an agreed level of information security in supplier relationships



Why is it important?

- To establish clear instructions on how personnel should act when dealing with information assets, guaranteeing confidentiality, reliability and accessibility of the organization's data security assets

To which information assets is it applicable ?

- Hardware : computers, mobile devices, and phones
- Software : operating systems, applications, utilities, firmware
- Data : relational databases, flat files, NoSQL data, text documents, spreadsheets, images, video, and audio files
- Networks : both wired and wireless systems, telecommunications, and Voice over Internet Protocol (VoIP) services
- Cloud services, email accounts and other hosted services



How is it achieved ?

By defining contractually :

- An acceptable use policy
- What is permitted and prohibited
- The monitoring activities
- Access restrictions

Link with other frameworks

- NIST 800-53 rev5 : SR-1
- NIST CSF 2.0 : GV.RM-05, GV.SC-01, GV.SC-05, GV.SC-06, GV.SC-09, GV.SC-10, ID.AM-08, PR.PS-02



Renaud Dardenne
Asphalia Consulting