# Information security for use of cloud services

ISO 27002 Control 5.23

## Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements

## Purpose

To specify and manage information security for the use of cloud services

## Why it is an important control ?

- It addresses the crucial concept of shared responsibility inherent in cloud services, preventing security gaps
- It mandates defining exit strategies to manage data portability and asset return upon conclusion of the service

## How can it be implemented ?

- Establish and communicate a topic-specific policy on the use of cloud services
- Define and communicate all relevant information security requirements associated with the service use
- Review cloud service agreements (even if pre-defined) against the organization's requirements
- Conduct relevant risk assessments and ensure management acceptance of residual risks
- Define procedures for monitoring, reviewing, and evaluating the ongoing use of cloud services

## Dangers to avoid

- Believing the CSP assumes all information security responsibility - responsibility is typically shared and must be clearly allocated
- Assuming the agreement is easily negotiable - often, agreements are pre-defined and must be reviewed against organizational needs

## Link with other frameworks

- NIST 800-53 rev5 : SA-1, SA-4, SA-9, SR-5
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting