Monitoring, review and change management of supplier services

ISO 27002 Control 5.22

Control

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery

Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements

Why should it be implemented ?

- To ensure the supplier complies with the terms and conditions of the agreement continuously
- To ensure that supplier changes do not negatively affect service delivery

How can it be implemented ?

- Assigning responsibility for relationship management and ensuring sufficient technical resources are available
- Establishing procedures for monitoring service performance
- Defining processes for reviewing service reports and conducting regular progress meetings
- Defining procedures for conducting audits

What are common misconceptions ?

- That monitoring is purely contractual; it must include technical review and evaluation of information security levels
- That audit reports are sufficient; the organization must follow up on issues identified in audits

Link with other frameworks

- NIST 800-53 rev5 : RA-9, SA-9, SR-6, SR-7
- NIST CSF 2.0 : GV.OC-02, GV.OC-05, GV.RM-05, GV.SC-01, GV.SC-06, GV.SC-09, GV.SC-10, ID.AM-08, PR.PS-02, DE.CM-06

Renaud Dardenne
Asphalia Consulting