Addressing information security within supplier agreements

ISO 27002 Control 5.20

Control

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship

Purpose

To maintain an agreed level of information security in supplier relationships

Who should be involved ?

- The management
- The Procurement department
- The IT departement
- Legal
- Data Protection Officer

Which Topics should be addressed ?

- Legal, statutory, regulatory and contractual requirements
- Personally identifiable information (PII)
- Intellectual property rights
- Incident management requirements and procedures
- A change management process
- Termination clauses
- Assurance (e.g., third-party attestations or right to audit)

Implementation best practices

- Document supplier agreements detailing information security requirements.
- Define minimum information security requirements
- Establish and maintain a register of external parties

Link with other frameworks

- NIST 800-53 rev5 : SA-4, SR-3
- NIST CSF 2.0 : GV.RM-05, GV.SC-01, GV.SC-05, GV.SC-06, GV.SC-09, GV.SC-10

Renaud Dardenne
Asphalia Consulting