Managing information security in the ICT supply chain

ISO 27002 Control 5.21

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain

Purpose

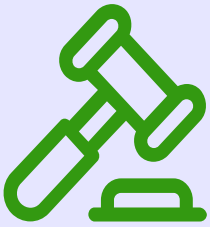
To maintain an agreed level of information security in supplier relationships

Why is it important ?

- To address the risk associated with acquiring vulnerable, malicious, or altered products from external sources
- To ensure security requirements flow down from the primary supplier to component providers and sub-contractors.

What could happen if badly implemented ?

- Introduction of vulnerable, malicious, or altered products or components into the organization's environment
- Security requirements failure to propagate down to sub-contractors, creating protection gaps
- Lack of traceability for critical components
- Disruption due to component obsolescence or unavailability if risks are not managed



How can it be audited ?

By providing evidence of :

- The obligation to propagate security requirements to provider
- Software component details (SBoM)
- Records of requests for information regarding software components and security functions sent to suppliers

Link with other frameworks

- NIST 800-53 rev5 : SR-3, SR-5
- NIST CSF 2.0 : GV.OC-05, GV.RM-05, GV.SC-01, GV.SC-05, GV.SC-06, GV.SC-09, GV.SC-10

Renaud Dardenne
Asphalia Consulting