REFERENCE SHEET

USING THIRD-PARTY SERVICES

Purpose of the document

Provide tips and tools to organizations that outsource some of their activities to at least one third party.

These services refer solely to hosting services, namely IT system-related services (e.g., infrastructure services, software services, data management).

Types of services

Infrastructure services	Application services	Data management
• Virtualization • Hosting • Maintenance • Identity and access management • Server monitoring	• Application development • Application support • Change management	• Computer backup • Data migration and integration • Implementing storage and archiving solutions

Risks related to outsourcing

Here is a non-exhaustive list of the risks related to outsourcing:

- Unsatisfactory or non-compliant service
- Inadequate or no support
- Inadequate framework
- Non-compliance with organizational framework
- Incompatible software or hardware
- Deliberate or accidental data loss, theft, corruption or leakage
- Service interruption or degradation due to a failure
- Inadequate service quality

By using third-party services, the organization also exposes itself to a loss of control of its IT system and a certain technological dependence.

Recommendations

Carry out security measures throughout the outsourcing process:

Call for tenders and request for proposals

- Identify and quantify the risks related to outsourcing the service in question
- Obtain a formal commitment from subcontractors that they will not disclose any of the organization's information classified as confidential, private, or secret
- Include risk-proportionate security requirements in the specifications for any call for tenders or request for proposals
- Evaluate the provider's security practices
- Assess the risk of gaps between the organization's obligations and the supplier's measures
- Adopt a response strategy (accept, reduce, transfer, refuse).

New contracts and renewal or modification of existing contracts

- Identify and quantify the risks related to outsourcing the service in question
- Obtain a formal commitment from subcontractors that they will not disclose any of the organization's information classified as confidential, private, or secret
- Assess the supplier's security practices before signing a contract
- Include in the contract the security measures proportionate to the risk based on the nature of the contract
- Analyze the risk associated with a supplier's refusal to include or modify a security requirement.

Security requirements

Here's a list of security requirements that must be included in your contracts based on the nature of the contract and proportionate to the risk:

- Confidentiality
- Responsibilities
- Penalties in the event of a breach
- Supplier and client obligations
- Data location (main site and backups)
- Third parties involved
- Security screening
- Service agreement (service availability rate, maximum monthly unavailability, average time between two failures)
- Contact information of the person responsible for security
- Security incident management (detect, respond, restore, and monitor)
- Contract cancellation or termination (information recovery and destruction)
- Security audit