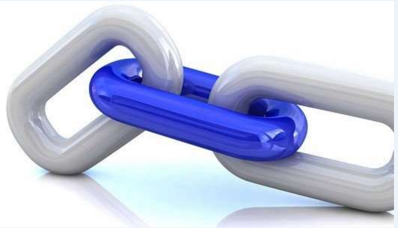
ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

Security category – 15.1. Information security in supplier relationships

Control – 15.1.1. Information security policy for supplier relationships
The organization needs to agree with its suppliers and to document the requirements for information security needed to mitigate risks that may arise from the supplier's access to its assets.

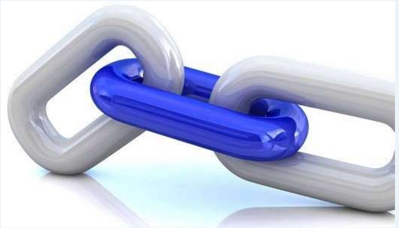


If a supplier is accessing the organization's assets there are risks involved.

There have to be rules and procedures specifying:
- what the supplier is allowed to do and to access,
- what are the obligations of the suppliers;
- how security incidents are to be handled;
- awareness of the organization's personnel involved in acquisition;
- documenting the security requirements in contracts.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

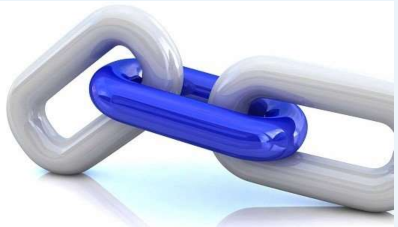
Control – 15.1.2. Addressing security within supplier agreements
The contracts signed with the suppliers should include all relevant information security requirements.



The contracts signed with supplier depend on the risks involved but the best practice is to make the contracts as detailed as possible in terms of information security.

Suppliers should not be allowed access to the organization's assets before the contracts are not agreed and signed and any other controls agreed by the parties are not implemented.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

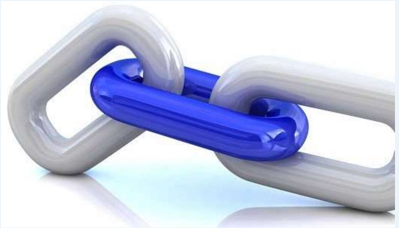


Guidance of ISO/IEC 27002 on elements to be included in supplier agreements:

- obligation of the supplier to comply to the organization's policies;
- information to be provided to or accessed by the supplier and how;
- the classification of information used within the agreement;
- any legal requirements applicable to the relations between the parties;
- what controls are to be implemented by each party;
- the list of supplier's personnel to access the organization's assets or a system to authorize personnel for the access including here the possibility to perform screening of suppliers personnel before granting access;
- how incidents are to be handled and how conflicts are to be resolved;
- rules and conditions for subcontracting by the supplier;
- if the parties agree that the organization can audit the supplier.

ISO/IEC 27001:2013 Information security management systems
-Information security in supplier relationships-

Control – 15.1.3. Information and communication technology supply chain
The organization should include in its agreements with suppliers requirements related to the supply chain for IT&C products and services.



This is meant to address the risks associated with the suppliers' sub-suppliers.

So the organization should investigate its IT&C supply chain and document in the contracts with its suppliers some aspects on this topic, like:

- asking the supplier to propagate the organization's security requirements throughout the supply chain;
- getting assurance that critical components origin can be traced throughout the supply chain;
- how the supplier evaluates its own suppliers and how it chooses them.