ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Security category – 14.1. Security requirements of information systems

Control – 14.1.1. Information security requirements analysis and specification
The organization should include security related requirements in its requirements for new information systems or enhancements to existing information systems.

The organization needs to recognize information security requirements from the first stages of information systems acquisition or development.

There are 2 different situations:
- the information system is developed specifically for the organization, or by the organization itself;
- the system is acquired as a commercial product not personalized.

The level of security requirements and controls should reflect of course the business value of the information involved and the potential negative impact over the business in case this information is not adequately protected.

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Control – 14.1.2. Securing application services on public networks
Information from application services that are passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

E-commerce.

Many security requirements can be addressed by using cryptography:

- encryption to ensure the confidentiality of information like billing details and personal information;
- digital signatures to ensure the integrity of electronic transactions and to authenticate the partners in the transaction;
- both encryption and digital signatures to achieve non-repudiation that may be needed in case of disputes on the occurrence or non-occurrence of a certain event.

ISO/IEC 27001:2013 Information security management systems

-Security requirements of information systems-

If the organization is using or providing application services over public networks it should have clear regulations that define:

- who is allowed to carry out electronic commerce activities and what is the employee authorized to do;
- how segregation of duties is ensured - activities that in combination can be used to commit fraud should not be performed by the same person;
- what controls are in place to monitor activities and ensure protection of the information involved.

ISO/IEC 27001:2013 Information security management systems
-Security requirements of information systems-

Control – 14.1.3. Protecting application service transactions
Information used for transactions has to be protected against incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

The security considerations provided by ISO/ IEC 27002 refer to:

- the use of electronic signatures;
- aspects on the transaction - privacy of the parties, confidentiality of the transaction, verification and validation of the user's authentication information;
- encryption of the communications between parties;
- the use of secure protocols for communication between the parties involved in the transaction;
- storage of the transaction details outside any publicly accessible environment;