ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Security category – 17.1. Information security continuity

Control – 17.1.1. Planning information security continuity
The organization is required to ensure that in case of adverse situations like a crisis or a disaster, information security management is not neglected.

If there is a need for information security when things are ok, then there is a need for information security when things go wrong too.

Information security aspects should be inserted in the planning for business continuity and disaster recovery.

If there is no formal business continuity management implemented :

- either information security applicable in normal conditions remain the same in case of adverse conditions;
- or a business impact analysis is made to determine the requirements for information security in case of a crisis or disaster..

ISO 22301 – Business Continuity Management Systems

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Control – 17.1.2. Implementing information security continuity
The requirement here is for the organization to have processes, procedures and controls in place to ensure the continuity of information security during an adverse situation.

The organization is required to:
- have a management structure in place that will prepare for and respond to an a disruptive event using personnel with sufficient competence and authority;
- nominate personnel with the specific tasks to maintain information security in case of an unexpected event;
- have plans and procedures for response and recovery that include aspects on how to maintain information security while managing the disruptive event.

Normally the information security controls should be able to operate in case of a disruptive event but if not, the organization should plan for other controls that will become effective in this situation to ensure an acceptable level of information security.

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Control – 17.1.3. Verify, review and evaluate information security continuity
The controls implemented for information security continuity need to be verified to ensure they are still valid and effective in case of real adverse situation.

Information security continuity processes, procedures and controls need to be tested for functionality.

Whenever something changes information security continuity measures need to be reviewed and updated as necessary.

ISO/IEC 27001:2013 Information security management systems
-Information security continuity-

Security category – 17.2. Redundancies

Control – 17.2.1. Availability of information processing facilities
Redundancy should be sufficient to meet the requirements for availability.

Redundancy offers availability.

The organization needs to identify the business requirements for availability of information systems, see what the current systems provide and where the existing architecture cannot guarantee availability needed the organization should consider the use redundant components or systems to match the needs for availability.

Redundant should be tested.