# ISO27002

# Clause 7 - Physical Controls

# Focus:
# Physical, Environmental, Geographic

# ISO27001
# [Strategic]

Disruption to business from natural disasters can cause potential high financial losses in terms of revenue and reputational damage.

**We must minimise the risk and impact of business disruption and potential loss of revenue, reputation from natural disasters, by implementing physical security.**

# ISO27002 - 7.5 Control [Tactical]

# ISO27002 - 7.5 scope

# Control

# Purpose

**Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.**

# Guidance

- Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals.

- Necessary safeguards should be implemented and changes to threats should be monitored.

- Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

**Physical premises location and construction should take account of:**

a) **local topography, such as appropriate elevation, bodies of water and tectonic fault lines;**
b) **urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.**

**Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:**

**a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);**

**b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;**

**c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;**

**explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.**

# Other information

Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

# How to implement the control?

1. **Regular risk assessments on threats**

# 2. Monitor and implement safeguards

# 2. Specialist advice on how to manage risks from physical and environmental threats

# How to make a revision?

According to the ISMS frequency & methods in ISO27001 clause 9.2.2

# Conduct GAP Analysis

**Ask the employees / the responsible persons about the controls implemented.**