

CISSP Certification Exam Study Guide

Physical Security

1. Introduction

1.1 **Physical security** addresses the physical protection of the resources of an organization, which include people, data, facilities, equipment, systems, etc. It concerns with people safety, how people can physically enter a facility, and how the environmental issues affect equipment and systems. **People safety** always takes precedence over the other security factors.

1.2 Physical security is the **first line of defense**.

1.3 Major sources of physical security threats are:

- **Weather**, e.g. temperature, humidity, water, flood, wind, snow, lightning, etc.
- **Fire and Chemical**, e.g. explosion, smoke, toxic material, industrial pollution, etc.
- **Earth movement**, e.g. earthquake, volcano, slide, etc.
- **Object movement**, e.g. building collapse, falling object, car, truck, plane, etc.
- **Energy**, e.g. electricity, magnetism, radio wave anomalies, etc.
- **Equipment**, e.g. mechanical or electronic component failure, etc.
- **Organism**, e.g. virus, bacteria, animal, insect, etc.
- **Human**, e.g. theft, fraud, strike, war, sabotage, etc.

1.4 Like the other types of security controls, physical security controls can be classified as:

- **Administrative controls**, e.g. facility selection, facility construction and management, personnel control, evacuation procedure, system shutdown procedure, fire suppression procedure, handling procedures for other exceptions such as hardware failure, bomb threats, etc.
- **Physical controls**, e.g. facility construction material, key and lock, access card and reader, fence, lighting, etc.
- **Technical controls**, e.g. physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup, etc.

- 1.5 A "**layered**" approach (from the physical security perspective) should be adopted to protect a facility. It means that multiple layers of physical security controls (e.g. fences for protecting the perimeter, card access control system for protecting building entry points, office doors are locked, servers are located in a data center with 7x24 access control, etc.) should be implemented to protect sensitive areas so that an intruder cannot successfully break into such areas even if some of the physical security controls have been compromised or circumvented.
- 1.6 Some physical security controls are required by laws, e.g. fire exit door, fire alarm, etc.
- 1.7 **Crime Prevention Through Environmental Design** (CPTED) is an approach to deter an offender from committing criminal activities by manipulating the physical environment to increase the offender's perceived risk of being detected and caught. It also makes the legitimate users feel safe.
- 1.8 CPTED is based on three major environmental strategies:
- **Territorial Reinforcement** - It defines public, semi-public and private space, and express ownership using fences, pavements, signs, landscaping, etc.
 - **Surveillance** - It increases the likelihood that criminal activities will be observed by using proper lighting designs, landscape designs, windows, closed-circuit television (CCTV), etc.
 - **Access Controls** - It controls and limits access by using entrances, exits, fencing, landscaping, etc.

2. Facility Requirements

- 2.1 Factors that should be considered when selecting a site are:
- **Visibility**, e.g. surrounding terrain, markings and signs, etc.
 - **Local considerations**, e.g. crime rate, adjacent neighbors, proximity to police and fire station, etc.
 - **Transportation**, e.g. road access and traffic condition, proximity to airport and train station, etc.
 - **Natural threats**, e.g. likelihood of flood, earthquake, hurricane, or other natural threats.

Depending on the needs of a business, some of the above concerns may be more important than the others.

- 2.2 A **data center** or **server room** should be located:

- Not on the top floor (for fire consideration).
- Not in the basement (for flooding consideration).
- In the core of a building (for providing protection from natural disasters or bomb attacks).
- Not close to a public area (for security consideration).

2.3 When designing and building a facility, the following items should be considered:

- **Wall** - fire rating (level of fire protection and combustibility), load (the maximum weight it can hold), floor to ceiling barrier, reinforcement for secured area, resistance to attacks and disasters (e.g. earthquake, hurricane, etc.).
- **Partition** - considerations similar to those of wall, plus the requirement of extension above drop ceiling (if there is no extension, an intruder can lift the ceiling panels and climb above the partition).
- **Door** - fire rating (should be equal to that of the surrounding walls), resistance from being forced open, intrusion detection alarm, fail-soft vs fail-safe lock (i.e. lock that is unlocked or locked in a power outage respectively), directional opening, emergency exit, emergency marking, and placement of doors.
- **Window** - characteristics of windows material (opaque, translucent, transparent, shatterproof, bulletproof), wire-mesh windows, intrusion detection alarm, placement of windows.
- **Entry point** - security controls (e.g. key and locks, intrusion detection sensors, etc.) are required to protect both official entry points (e.g. doors and gates) and other potential entry points (e.g. windows, roof access, fire escapes, ventilation ducts, utility tunnels, etc.).
- **Ceiling** - fire rating, load, waterproof (preventing water leakage from the upper floor), drop ceiling.
- **Floor** - fire rating, load, raised floor, electrical grounding (for raised floor), non-conducting material.
- **Heating, ventilation, and air conditioning (HVAC)** - independent power source, positive air pressure (i.e. air will flow out of a room when the door is open, for avoiding contamination of the room), protected intake vents to prevent tampering, monitoring of environmental condition, emergency power off, placement of HVAC system.
- **Power supplies** - backup power supply, clean power supply, circuit breaker, access to power distribution panels, placement of power sockets.
- **Liquid and gas line** - shutoff valve, leakage sensor, placement of liquid and gas lines.
- **Fire detection and suppression** - fire or smoke detector and alarm, sprinkler, gas discharge system, placement of detectors and sprinkler heads.

- **Lighting** - all areas where individuals may walk, and all potential entry/exit points for a facility, should be properly lit. No dead spot (unlit area) should exist between the lights.

2.4 There are several major types of **building construction material**:

- **Light frame** - used by most houses, with 30-minute fire survival ability.
- **Heavy timber** - structural elements with a minimum thickness of four inches and 1-hour fire survival ability.
- **Incombustible** - steel constructed, which is incombustible but will be weakened under very high temperature and may even cause the structure to collapse (like the World Trade Center in the September 11, 2001 terrorist attack).
- **Fire resistant** - structural elements are incombustible and concrete encases steel for added protection.

2.5 In general, a wall should have **1-hour fireproof rating**. For data center or room which stores paper document, magnetic media, etc., the walls should have a minimum of **2-hour fireproof rating**.

2.6 Windows can be made of the following materials:

- **Standard glass** - It is commonly used in residential homes and is easy to break.
- **Tempered glass** - It is around five to seven times stronger and more difficult to break than standard glass.
- **Standard Acrylic** - It is a type of plastic, and is stronger than standard glass. However, it produces toxic fumes if burned. It is also easy to be scratched.
- **Polycarbonate acrylic** - It is much stronger than standard acrylics (around 20 times).
- **Glass-clad polycarbonate** - It is the strongest windows material, and can resist different types of threats (e.g. fire, chemical, breakage). It is more expensive than the other types of windows materials.
- **Wired glass** - It consists of a continuous sheet of wire mesh embedded between two sheets of glass. The wire mesh makes it more difficult to break the window. It also prevents the window from shattering if broken.
- **Laminated glass** - It consists of a layer of plastic between two sheets of glass. The plastic sheet makes it more difficult to break the window, and prevents the window from shattering if broken.
- **Solar window film** - A transparent film that is affixed to a window to filter ultraviolet rays and prevent people outside from viewing activities on the inside.
- **Security film** - A transparent film that is affixed to a window to increase its strength.

2.7 It is essential that window frames are securely anchored in the wall, and windows can be locked from the inside.

2.8 **Lighting** (e.g. streetlight, floodlight and searchlight) is a good deterrent for unauthorized access. It can also provide safety for personnel. There are several common types of security lighting systems:

a. **Continuous lighting**

- It consists a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light.
- It is the most common type of security lighting systems.
- There are two primary methods of using continuous lighting:
 - Glare projection - Glare of lights is directed across the surrounding territory. Guards are protected by being kept in comparative darkness. In addition, they can observe intruders at a considerable distance beyond the perimeter.
 - Controlled lighting - The width of the lighted strip is controlled and adjusted to fit particular needs, such as outside the perimeter or along a highway.

b. **Standby lighting**

- Similar to continuous lighting. However, the luminaries are not continuously lit.
- They are either automatically or manually turned on when suspicious activity is detected.

c. **Movable lighting**

- It consists of manually operated, movable searchlights.
- It is normally used to supplement continuous or standby lighting.

d. **Emergency lighting**

- It is used during a power failure or other emergencies that render the normal system inoperative.
- It should be powered by essential power supply (e.g. backup generator) and/or batteries for emergencies that render the normal power supply inoperative.

2.9 A **gaseous discharge lamp** (e.g. high-pressure sodium and mercury vapor lamp) has the following security weaknesses:

- It can take several minutes to re-ignite after a power interruption.
- It usually contains a photo-voltaic sensor so that it can automatically turn on at dusk and off at dawn. An intruder can make use of this feature to turn off the light by pointing an invisible infrared beam at the sensor for a certain period of time.

3. Perimeter Security

- 3.1 **Perimeter security controls** are used to prevent unauthorized access to a facility. They deal with access control, access monitoring, intrusion detection and response.
- 3.2 All servers and communications equipment (e.g., bridges, routers, switches, etc.) should be located in data centers, closets, etc., with proper physical security controls.
- 3.3 The perimeter security requirements when a facility is in operation should be different from those when the facility is closed.

Access Control

- 3.4 **Physical access control mechanisms** include:
- Lock and key.
 - Access card and reader.
 - Fence and gate.
 - Doorway and Man-trap.
 - Safe.
- 3.5 **Lock and key** is the most inexpensive physical access control mechanism. It is a deterrent and delaying device to intruders. Since most locks can be defeated or picked, they should only be used as one of the many physical controls.
- 3.6 There are several types of locks as follows:
- **Preset lock**
 - Typical door lock, which needs to be replaced if the key needs to be changed.
 - **Deadbolt lock**
 - A bolt is inserted into the frame of the door for added security.
 - **Combination lock**
 - Lock with a wheel, which can be turned through a sequence of numbers in a specific order to open the lock.
 - **Programmable lock** or **Cipher lock**
 - Lock with a key pad. It requires a combination of keys to open the lock.
 - Some programmable locks also have card readers and require valid access cards for opening the locks.
 - It may have special options such as:
 - Hostage alarm (support a key combination to trigger an alarm).
 - Master-keying (support key combinations to change the access code and

configure the functions of the lock).

- Key-override (support key combinations to override the usual procedures).
- **Smart lock**
 - Lock that permits a user to enter a certain door only at certain time periods.
- **Device lock** (for locking a device, e.g. laptop, rather than for perimeter security):
 - Slot lock - secure a device to a stationary component (e.g. steel cable with lock, which is commonly used for locking a laptop).
 - Cable trap - secure a peripheral by locking its cable to a stationary component.
 - Power switch lock - lock the on/off power switch of a device (e.g. key-switch).

3.7 A **fail-soft lock** is unlocked in a power interruption.

A **fail-safe** (or **fail-secure**) **lock** is locked in a power interruption.

3.8 Proper control procedures for **key handling** (e.g. key access record, key storage, dealing with lost keys, etc.) should be well documented and enforced.

3.9 A **master key system** can be used in a large organization or facility. There are a "master key" and a number of "sub-master keys" in the system. The master key can open all the locks within the facility, although each lock also has its own unique key. A sub-master key can open one or more locks. This type of system allows supervisory or emergency access to locked rooms, cabinets, etc.

3.10 Since the master and sub-master keys are powerful, they must be properly protected, and the function of each key and who is in charge of the key must be well-documented.

3.11 **Access card** and **reader** can also be used as an access control mechanism (details can be found in Chapter 5).

3.12 **Fence** is another physical access control mechanism. Some of the considerations when designing a fence are as follows:

- Fabric specification. For example, chain-link fences should be constructed with 9-gauge (i.e. 0.148-inch diameter) or heavier wire, and with mesh openings smaller than 2x2 inches.
- Height of the fence. Fences of different heights can serve different purposes:
 - 3 - 4 feet - deter casual trespassers.
 - 6 - 7 feet - deter general intruders.
 - 8 feet with strands of barbed wire (slant at a 45° angle) - deter more determined intruders.
- It should be fastened to steel or concrete posts set in concrete or buried deep enough

to compensate for the shifting or erosion of soil.

- CCTV for monitoring the fence.
- Pipes and wires that pass through the fence should be closely monitored. They may be used by intruders to gain unauthorized access.

3.13 **Gate** is used to control entrance and exit of persons and vehicles. There are 4 classes of gates:

- **Class I** - residential usage.
- **Class II** - commercial usage, where general public access is expected (e.g. gates for a parking lot).
- **Class III** - industrial usage, where limited access is expected (e.g. gates for a warehouse, factory, loading dock, etc.).
- **Class IV** - restricted access that requires supervision by security personnel (e.g. gates for a prison, police station, airport security area, etc.).

Each gate classification has its implementation and maintenance guidelines to ensure the necessary level of protection. These guidelines are developed by the **Underwriters Laboratory** (UL), an independent, not-for-profit product-safety testing and certification organization.

3.14 Some considerations for designing and implementing a gate are as follows:

- Prevent **tailgating** or **piggybacking** (i.e. one vehicle follows another closely through the gate, even the vehicle does not have the necessary authorization).
- Trigger an alarm if it is forcibly opened.
- Provide the same level of protection as the adjacent fences (e.g. fabric material).
- Prevent **entrapment** (i.e. an object is caught by the gate such that it may cause injury to someone).

3.15 **Bollards** are small and round concrete pillars for use in traffic control. For example, it can be placed around a property to protect it from being damaged by someone running a vehicle into it. Bollards with lights can also illuminate surfaces and provide lighting for parks, paths, etc.

3.16 There are two major types of **doors** :

- **Hollow-core** door - Most commonly used. It can be broken in easily.
- **Solid-core** door - Recommended for sensitive area such as data center. It should be mounted in a strong doorframe as it is usually the weakest point in a door assembly.

3.17 **Door** for a secured area should have the following characteristics:

- Use solid-core door.

- Have the same fire rating as that of the surrounding walls.
- Be self-closing and have no hold-open feature.
- Trigger an alarm if it is forcibly opened or have been held open for a long period of time (door delay trigger).
- Use a fail-secure lock, if necessary.
- Have similar appearance as the other doors to avoid catching the attention of intruders.

3.18 **Emergency exit bar** (also known as **panic bar**) is a door-locking device that allows exit by pressing the bar to release the lock, but prevent entrance unless the door is properly unlocked.

3.19 A **man-trap** is an area with double doors. There is a security guard or another mechanism to identify and authenticate an individual before opening the second door. This control can solve the **piggybacking** problem of access control (one following another closely through a door).

3.20 Visitor access to restricted areas requires special security controls such as **visitor registration** and **escort**.

3.21 An **audit trail** should be maintained for every entrance of a restricted area. It can be used for auditing whether the access controls are properly enforced, and for incident investigation in case an incident occurs. It should contain the following information for every access attempt:

- Timestamp of the access attempt.
- Username.
- Result of the access attempt (successful or unsuccessful).
- Departure time of the user.

3.22 A **safe** or a locked cabinet should be used to store highly sensitive documents or objects. Security considerations for a safe include:

- Its body and door should be made of steel or other metal that can resist attack by tools, or even explosives.
- It should be protected by a combination lock, electronic combination lock, or equivalence. In addition, a good combination should be used, and it should be changed regularly.
- It should be fire-proof.
- If it is lightweight, it should be installed in reinforced concrete or to the wall.
- CCTV or security guard should be deployed to watch for unauthorized access.

- A relocking device (a mechanism inside a lock that will be activated to provide additional protection if a forced entry is attempted) should be installed for better security protection.

3.23 For **portable** or **mobile** devices, laptops, or similar equipment (especially if sensitive data is stored in the device) that cannot be protected by the perimeter security controls, other security measures and **user responsibilities** become more important. Some of the recommended protection measures are listed below:

- Don't leave the device unattended.
- Don't check the device as luggage when flying.
- Use a device lock (e.g. a slot lock with a steel cable) to lock the device to a stationary object.
- Password protect the BIOS.
- Harden the operating system.
- Backup all important data on a separate computer or backup media.
- Encrypt all sensitive data.
- Record the serial number of the device. Report it to the police and vendor if the device is stolen, so that the device can be properly identified if recovered (for example, if the stolen device is sent to the vendor for repairing).

Access Monitoring and Intrusion Detection

3.24 Physical access monitoring controls include patrol force, security guards and dogs.

3.25 **Patrol force** / **security guard** is a good deterrent to intrusion and can provide flexible security and safety response, but it has the following drawbacks or implementation considerations:

- It is expensive.
- The reliability of security guards is an issue. Pre-employment screening and other background checking are required.
- Security guards should be fully trained on the activities they are expected to perform in different situations.
- Human is subject to social engineering. Training against social engineering attacks is required.
- Security guards should be equipped with the necessary equipment, e.g. two-way radio, whistle, flashlight, weapon (must be licensed by the appropriate government authority), etc.
- It should be accompanied by other surveillance and detection mechanisms, e.g. CCTV.

3.26 A **guard station** should be a specially constructed enclosure (which may require higher level of security controls, e.g. bullet-proof windows and doors, etc.) for security guards to monitor the security of the facility through TV monitors, alarm systems, radio devices such as walkie-talkies, etc.

3.27 **Dogs** are very effective in detecting intruders and other exceptions because they have good sight, hearing and smelling capabilities. Moreover, they are loyal, intelligent, and can be trained to recognize specific smells, e.g. smoke.

3.28 Technical access monitoring or intrusion detection controls include:

- **Dry contact switch** uses metallic foil tape as a contact detector to detect whether a door or window is opened.
- **Electro-mechanical detection system** detects a change or break in a circuit. It can be used as a contact detector to detect whether a door or window is opened.
- **Vibration detection system** detects movement on walls, ceiling, floors, etc., by vibration.
- **Pressure mat** detects whether there is someone stepping on the mat.
- **Visual recording device**, e.g. camera and Closed Circuit TV (CCTV), records the activities taking place in a particular area. It should be used together with security guards to detect for anomalies.
- **Photoelectric or photometric detection system** emits an invisible (unless the intruder is wearing an infrared or night-vision goggle) beam of light and monitors the beam to detect for motion and break-in.
- **Wave pattern motion detector** generates microwave or ultrasonic wave, and monitors the emitted wave to detect for motions. Since microwave uses a much higher frequency than ultrasonic wave, it can detect some motions even through walls. In addition, it is not affected by noise and air current. However, it is difficult to confine the coverage of a microwave motion detector to a specific area.
- **Passive infrared (PIR) detection system** detects for changes of heat wave generated by an intruder.
- **Audio or Acoustical-seismic detection system** listens for changes in noise level.
- **Proximity detector or capacitance detector** emits electrostatic magnetic field and monitors the field to detect for any interruption. It is especially useful for protecting specific objects (e.g. a safe).

3.29 **Perimeter intrusion and detection assessment system (PIDAS)** is a fencing system with mesh wire and passive cable vibration sensors that can detect if an intruder is approaching and damaging the fence. However, it may generate many false alarms.

3.30 A CCTV system may consist of the following components:

- **Camera**
 - It captures optical images and converts them into video signals that are then transmitted to a remote monitor display.
 - It has an iris to control the amount of light that enters into its lens.
 - A manual iris should be used in an area that has fixed lighting.
 - An auto iris should be used in an area that the light intensity will change (e.g. outdoor environment).
 - CCTV cameras have specific requirements on the light intensity (or illumination) of the area to be monitored. Illumination is measured in the unit of lux or footcandle. (1 fc = 10.76 lux).
 - Some cameras have zoom lens to provide both wide scenes and close-up captures.
 - Most CCTV cameras nowadays use light-sensitive chips called charged coupled devices (CCDs), which are also commonly used in digital cameras and recorders, to capture images. This technology allows for the capturing of very detail and precise images.
- **Transmission media**
 - It transmits video signals from the camera to the remote monitor display.
 - The most common transmission medium is coaxial cable. Other feasible media include fiber-optic cable, wireless transmission, etc.
 - The transmission media must be properly protected from tampering (e.g. by intrusion detection sensors), as the most common attacks to a CCTV system is to tamper the transmission media and play the video recording from the day before to cheat the security guards who monitor the CCTV display.
- **Monitor Display** - It converts video signals into display images.
- **Pan and tilt unit** - It controls the positioning of the camera in both the horizontal (pan) and vertical (tilt) planes.
- **Infrared illuminator** - It is used in low-light conditions to provide greater viewing capability.
- **Multiplexer** - It multiplexes the video signals from several cameras onto a single line, and allows selected viewing of the signals from different cameras on the monitor display either manually or automatically.
- **Time/date generator** - It automatically inserts the date and time onto the video film.
- **Videotape recorder or Digital recorder** - A digital recorder uses hard drives or compact disks for film storage. It also offers enhanced search features.
- **Control system** - It remotely controls the operation of the pan and tilt unit, lenses, infrared illuminators, etc.

3.31 When the access monitoring controls detect an exception or intrusion, an alarm system can be used to alert the relevant parties to take the necessary response actions. There are several types of **alarm systems**:

- **Local system** - The alarm system only rings locally.
- **Central station system** - Alarms (and CCTV) are monitored by a central station. The central station should be located within 10-minute travel time from the customer site.
- **Proprietary system** - Similar to a central station system except that the monitoring facilities are owned and operated by the customer.
- **Auxiliary system** - The alarm system rings local fire station and/or police station. Many central station systems have this feature.

3.32 Other issues related to intrusion detection and alarm systems are:

- An intrusion detection system may generate a lot of false alarms.
- An intrusion detection/alarm system should have emergency backup power supply to prevent intruders from disabling the system by cutting the normal power supply.
- An intrusion detection/alarm system and the signal transmission medium should be protected and monitored against tampering.
- For simplicity, different detectors (e.g. intrusion, fire, water, etc.) should be connected to a central alarm system rather than using multiple alarm systems.
- An alarm should be audible for at least 400 feet.
- Human intervention (e.g. security guard) is required to respond to an alarm.

4. Fire Protection

Combustion Elements and Fire Types

4.1 Combustion elements which can sustain a fire are:

- **Fuel**, e.g. wood, paper, wiring, etc. (can be suppressed by CO₂ or Soda acid).
- **Oxygen** (can be suppressed by CO₂ or Soda acid).
- **Temperature** (can be reduced by water).
- **Chemical** (can be suppressed by Halon, which interferes with the chemical reaction).

4.2 There are four types of fire:

Class	Description	Element of fire	Suppression method
A	Common combustibles	Miscellaneous, e.g. wood, paper, etc.	Water, Soda acid

B	Liquid	Petroleum products, coolants, etc.	Halon, CO ₂ , Soda acid
C	Electrical	Electrical equipment, wires, etc.	Halon, CO ₂
D	Combustible metal	Magnesium, sodium, etc.	Dry powder

4.3 The **flash point** is the lowest temperature at which a Class B fire will continue to burn.

Fire Prevention

4.4 Doors, partitions, false ceiling, and other construction material should be **flammable** and **fireproof** up to a specific time limit. Floor-to-ceiling walls should be installed to prevent rapid spread of fire.

4.5 Since magnetic tapes will produce toxic gas when they burn, they should be stored in a fireproof room or container.

4.6 **Fire drills** should be performed regularly to ensure all people know how to safely exit the building. In addition, if some staff are required to shut off the power supply or perform other emergency response procedures, they should know how to perform the tasks while safely exiting the building.

Fire Detection

4.7 There are several types of fire detectors:

- **Heat detector**, which is based on a temperature threshold or the rising rate of temperature.
- **Flame detector**, which detects infra-red energy or pulse of flame (expensive but fast response).
- **Smoke or Combustion particle detector**, which emits a light beam and uses a photoelectric device to detect if the beam is obstructed.

4.8 **Fire detectors** and **alarms** should be installed with the following considerations:

- Fire detectors should be installed above ceiling, below raised floor (where wires can start an electrical fire), and in air vents (where smoke spreads), in addition to open areas.
- A fire alarm system should be configured to dial-up to a fire station and police station automatically.
- If a fire alarm will trigger automatic system shutdown (or some other emergency

procedures), there should be a warning before the shutdown, and there should be some methods to override the shutdown.

- There should be some manual methods to trigger a fire alarm.

Fire Suppression

4.9 A **heating, ventilation, and air conditioning** (HVAC) system has to be stopped automatically (e.g. trigger by the fire alarm system) when there is a fire because it can supply oxygen to the fire and spread smoke to the other areas.

4.10 A **portable fire extinguisher** (or hand-held fire extinguisher) should be used with the following considerations:

- It should have marking which indicates the type of fire it is designed for. Most portable fire extinguishers are filled with CO₂ or Soda acid.
- It should be placed within 50 feet of electrical equipment or at an exit.
- It should be easily reached and can be operated by an average-sized person.
- It should be inspected by licensed personnel regularly, e.g. quarterly.

4.11 A **gas discharge system** uses pressurized gas, e.g. CO₂ or Halon, to extinguish a fire. It is recommended for unmanned computer facilities, as the gas will not damage computer equipment, but may be dangerous to people. In a manned area, a gas discharge system should have built-in delay (after the fire alarm is triggered) before releasing gas. It allows enough time for staff to evacuate, or to disable the discharge system if it is a false alarm or it is a small fire that can be put out without discharging gas.

4.12 **CO₂** is colorless, odorless and can cause suffocation. It is more suitable for unattended facilities.

4.13 **Halon** is harmless to people in small quantity. It should be used with 5% concentration. If the concentration is above 10%, it can be dangerous to people. It can also deplete ozone. In an extremely hot fire (> 900°C), it will even degrade into toxic chemicals. Because of these problems, it is no longer manufactured since 1990s by international agreement. Extinguishers using Halon are not allowed to be refilled (or can refill only from a recycling bank). However, it is not necessary to replace them immediately.

4.14 Halon 1211 is a liquid agent used mainly in portable extinguishers. Halon 1301 is a gas agent used mainly in flooding systems, and it requires sophisticated pressurization.

4.15 **FM-200** is a common replacement for Halon. FM-200 should be used with 7% concentration. Other replacements for Halon include Argon, Inergen, CEA-410, FE-13 and NAF-S-III.

4.16 A **water sprinkler system** is an inexpensive fire suppression mechanism. There are four main types of water sprinkler systems. They are:

1. **Wet pipe system (or Closed head system)**

- All the pipes are filled with water.
- When the temperature increases above a certain threshold, the links melt and water is released from the sprinkler heads.
- Water in the pipes may freeze in cold area, which may break the pipes.

2. **Dry pipe system**

- All the pipes are filled with air under pressure, and water is held back by valves in a water tank.
- If a fire is detected, water will fill the pipes and then begin to sprinkle. During the time delay when water is filling the pipes, someone can shut down the sprinkler system, if necessary (e.g. for a false alarm).
- It is suitable for cold climate countries (where water would freeze in pipes if a wet pipe system is used).
- It does not react as fast as a wet pipe system.

3. **Pre-action system**

- Water is not held in the pipes in a normal situation.
- When the temperature exceeds a certain threshold, water is released into the pipes, but is not yet released from the sprinkler heads until the links melt (combine the features of a wet pipe system and a dry pipe system).
- It is designed for equipment that is costly such that water damage should be avoided in a small fire (leaving it to hand-held fire extinguisher).
- It is suitable for data processing environment.

4. **Deluge system**

- It is similar to a dry pipe system except that all the sprinkler heads are opened, so that a larger volume of water can be released over a large area in a short period of time.
- It is not suitable for data processing environment.

4.17 A water sprinkler system should be used with the following considerations:

- Water can increase the fire intensity in an electrical fire (because it can work as conductor for electricity). Therefore, electrical power should be shut down automatically (e.g. trigger by the fire alarm system) before water is discharged from the sprinkler heads.

- Sprinkler heads in different zones should be activated separately to avoid wide-area water damage. It requires fire detectors to be installed in each zone, such that the system can locate which zone is on fire.
- To prevent a false alarm from causing water damage, the system should discharge water only if a fire is detected by multiple sensors, and/or it has been detected for a certain period of time (so that there is sufficient time for someone to disable the sprinkler system if it is a false alarm, or if it is a small fire that can be put out without discharging water).

5. Power Protection

5.1 Power protection controls include:

- **Uninterrupted Power Supply (UPS)** to protect against a short duration power failure, or to provide enough time for system administrators to shut down the systems and equipment orderly. There are two types of UPS:
 - **Online UPS** - It is in continual use because the primary power source goes through it to the equipment. It uses AC line voltage to charge a bank of batteries. When the primary power source fails, an inverter in the UPS will change DC of the batteries into AC.
 - **Standby UPS** - It has sensors to detect for power failures. If there is a power failure, the load will be switched to the UPS. It stays inactive before a power failure, and takes more time than online UPS to provide power when the primary source fails.
- **Backup power source** (e.g. motor generator, another electrical substation, etc.) to protect against a long duration power failure.
- **Voltage regulator** and **line conditioner** to protect against unstable power supply.
- **Proper grounding** (e.g. by using 3-prong outlets) for all electrical devices to protect against short circuit and static electricity.
- **Cable shielding** to avoid interference.
- **Power line monitor** to detect for changes in frequency and voltage amplitude.
- **Emergency power off (EPO)** switch to shut down the power quickly when required.
- Electrical cables should be placed away from powerful electrical motors and lighting to avoid **electromagnetic interference**.
- Electrical cables should be placed away from powerful electrical cables and fluorescent lighting to avoid **radio frequency interference**.

5.2 UPS has several attributes:

- Electrical load it can support (measured in kVA).

- Length of time it can support.
- Speed of providing power when there is a power failure.
- Physical space it occupies.

5.3 UPS and backup power source should be tested periodically.

5.4 **Clean power** refers to stable power with no voltage fluctuation or interference. It is necessary for power-sensitive equipment.

5.5 **Interference** or **noise** is a random disturbance of power. There are two types of interference:

- **Electromagnetic interference (EMI)**
 - created by the charge difference between the 3 electrical wires (hot, neutral and ground).
 - induced by motors, lightning, etc.
- **Radio frequency interference (RFI)**
 - created by the components of an electrical system, and electrical cables.
 - created by fluorescent lighting, radio stations, cellular phones, etc.

5.6 There are several types of electrical voltage fluctuations:

- Excess power - "**Spike**" for momentary high, "**Surge**" for prolonged high.
- Power degradation - "**Sag**" or "**Dip**" for momentary low, "**Brownout**" for prolonged low.
- Power loss - "**Fault**" for momentary outage, "**Blackout**" for prolonged outage.

5.7 **In-rush current** refers to the initial surge of current required by some electrical equipment (e.g. motor) before it reaches normal operation. This increased current to the device may cause a sag to the other devices in the same electrical segment. Therefore, any device that would cause a dramatic in-rush current should not be connected to an electrical segment which supports critical computer equipment.

6. General Environmental Protection

6.1 A **HVAC** system is a control system which governs **heating, ventilation and air conditioning**. It can be used to control the temperature, humidity and contamination (e.g. dust, dirt, smoke, gas, etc.) of a facility.

6.2 A HAVC system should be installed in a data center with the following security

considerations:

- Physical access control to the system.
- Logical access control on remote access to the system (many modern HVAC systems are networked for remote control, monitoring, and maintenance).
- HVAC system for the data center should be independent of the central air-conditioning system for the building (with separate power source), so that failure of the central air-conditioning system would not cause the server equipment in the data center from being overheated.
- A backup HVAC system should be installed in the data center to prevent a single point of failure. Proper maintenance and periodical checking are also required for the systems.
- It can distribute toxic gas (in a terrorist attack) or smoke (in a fire) throughout the data center quickly. It should be stopped in case of such emergencies.

6.3 The **temperature** of a data center should be maintained between **21 - 23 °C** or **70 - 74 °F** ($^{\circ}\text{C} = 5 / 9 \times (^{\circ}\text{F} - 32)$). If the temperature is too low, it may cause some mechanisms to slow down. If the temperature is too high, it may cause equipment damage. The damaging points for different products are as follows:

- Magnetic media - 38 °C or 100 °F
- Computer hardware - 80 °C or 175 °F
- Paper products - 175 °C or 350 °F

6.4 The **relative humidity** of a data center should be maintained between **40 - 60%**. If the humidity is too low, there may be excessive static electricity. If the humidity is too high, there may be condensation and corrosion. The humidity can be monitored by a **hygrometer**.

6.5 To avoid contamination and to maintain **air quality**, a data center should use a closed-loop re-circulating air conditioning system and maintain **positive air pressure** inside the center (i.e. when the door is open, air will not flow in the room because of the higher pressure inside).

6.6 **Liquid** and **gas lines** must have **shut-off valves** and **leakage sensors**. The lines and valves should be protected from unauthorized access. However, the shut-off valves should also be easily accessible such that the liquid or gas supply can be shut off quickly in case of emergency.

6.7 **Water damage**, caused by leaks or condensation, can cause damage to computer equipment. Common sources of water problems are broken pipes, fire-suppression

systems, air conditioners, washrooms, etc. A data center should not be located below or next to such water sources.

- 6.8 Water damage in a data center may lead to problems with mold and mildew which could affect the proper functioning of computer equipment. It may be required to use industry-strength dehumidifiers, water movers, and sanitizers to handle a water damage for minimizing the potential problems.
- 6.9 **Static electricity** or **electrostatic discharge** can be prevented by using anti-static floor, anti-static carpet (or not use carpet), and anti-static armband or wrist strap (for grounding a person). Proper humidity and grounding are also required.

7. Equipment Failure Protection

- 7.1 There are several types of controls for protecting against equipment failure:
- **Hardware maintenance**, including service level agreements (SLAs) with the maintenance service suppliers.
 - **Hardware redundancy**, e.g. RAID disk, clustering, spare equipment, link redundancy, etc.
 - **Regular backup** of data and systems (Details can be found in Chapter 10).
 - **Alternate site** or Disaster Recovery (DR) site (Details can be found in Chapter 11).
- 7.2 There are two important concepts when determining the requirement of controls for protecting against equipment failure:
- **Mean-Time-Between-Failure (MTBF)** - expected time a device can function before failure.
 - **Mean-Time-To-Repair (MTTR)** - expected time required to repair a device.
- 7.3 Hardware redundancy can be classified as follows:
- **Hot Spare** - the redundant device can instantly take over the service if the primary device fails.
 - **Cold Spare** - the redundant device is onsite, but some manual configuration steps are required before it can take over the service if the primary device fails.
- 7.4 Availability of disk storage can be increased by:
- **Disk mirroring** or **shadowing** - Real-time duplication of data between the primary disk and a mirror disk. Both disks are attached to the same disk controller. Data access will not be affected if only one disk fails.

- **Disk duplexing** - Disk mirroring plus redundant disk controller.
- **Redundant Array of Inexpensive Disks (RAID).**

7.5 **Redundant Array of Inexpensive Disks (RAID)** makes use of redundant physical hard disks to increase the availability of a logical disk. There are several levels of RAID.

The common RAID levels are listed below:

- **RAID 0**
 - Stripping, i.e. a large logical disk which has data been divided into equal-sized blocks and spread over several physical disks evenly.
 - It can improve the logical disk performance by spreading the reads/writes over multiple physical disks.
 - It provides no redundancy. Failure of one physical disk will make the whole logical disk fails.
- **RAID 1**
 - Disk mirroring, i.e. all data on a primary physical disk are duplicated to a mirror physical disk, and all modifications are made to both disks simultaneously.
 - Data access will not be affected if only one physical disk fails.
- **RAID 2**
 - Stripping plus hamming code parity at bit level for redundancy (a logical disk consists of 32 physical disks for storage and 7 physical disks for parity).
 - Data access will not be affected if only one disk fails, as the data can be rebuilt from the information stored on the remaining disks.
 - This level is seldom used in the real world as it is complex and expensive to implement.
- **RAID 3**
 - Byte level stripping plus parity (a logical disk consists of N physical data disks and 1 physical parity disk).
 - The effective capacity of the logical disk = N x size of a physical disk.
 - Data access will not be affected if only one physical disk fails, as the data can be rebuilt from the information stored on the remaining physical disks.
- **RAID 4**
 - Block level stripping plus parity (N data disks and 1 parity disk).
 - The effective capacity of the logical disk = N x size of a physical disk.
 - Data access will not be affected if only one physical disk fails.
- **RAID 5**
 - Block level stripping plus interleaved parity, i.e. parity information is interleaved across all physical disks (N+1 disks).
 - The effective capacity of the logical disk = N x size of a physical disk.
 - Data access will not be affected if only one physical disk fails.

- The logical disk performance is better than that of Levels 3 and 4 because of the distribution of parity information.
- It is the most widely used RAID level.
- **RAID 6**
 - Block level striping plus two sets of parity (N+2 disks).
 - The effective capacity of the logical disk = N x size of a physical disk.
 - Data access will not be affected even if at most two physical disks fail.
- **RAID 10**
 - RAID 1 + RAID 0, i.e. striping across multiple RAID-1 disk pairs.
- **RAID 01**
 - RAID 0 + RAID 1, i.e. 2 x RAID-0 disk groups, each disk group is a mirror of the other.
- **RAID 15**
 - RAID 1 + RAID 5, i.e. striping with interleaved parity across multiple RAID-1 disk pairs.
- **RAID 51**
 - RAID 5 + RAID 1, i.e. 2 x RAID-5 disk groups, each disk group is a mirror of the other.

7.6 Some RAID systems support one or both of the following two features:

- **Hot swapping**, i.e. replacement of a failed hard disk and reconstruction of the contents of the failed disk onto the replacement disk can be done even if the system is running.
- **Hot sparing**, i.e. a spare disk can be pre-installed such that reconstruction of the contents of the failed disk will be started automatically once a disk fails.

7.7 RAID can be implemented on hardware level or software level:

- **Hardware RAID**
 - A dedicated RAID controller is used to manage the RAID array.
 - The operating system sees the RAID array as a single disk. The individual physical disks are invisible to the operating system.
 - It has the advantage of better performance, but requires extra cost to acquire the necessary hardware.
- **Software RAID**
 - Regular hard disks and disk controller are used, without any special hardware.
 - A software, usually part of the operating system, is used to create and manage the RAID array.

7.8 The RAID Advisory Board introduced the concept of **Extended Data Availability and**

Protection (EDAP) in 1997, which is a classification system for the resilience of an entire storage system rather than just a disk-based storage as in the RAID classification. The classification system contains the following classes:

- **FRDS (failure-resistant disk system):**
 1. Protection against **data loss** and **loss of access** due to disk failure.
 2. Ability to reconstruct the contents of a failed disk onto a replacement disk.
 3. Protection against **data loss** due to the failure of a system component.
 4. Active component monitoring and failure indication.
- **FRDS+:**
 5. Features 1-4.
 6. Hot swapping.
 7. Protection against **data loss** due to cache, power and other environmental failures.
- **FTDS (failure-tolerant disk system):**
 8. Features 1-7.
 9. Protection against **loss of access** due to device channel and controller failure.
- **FTDS+:**
 10. Features 1-9.
 11. Protection against **loss of access** due to bus and power failure, and component replacement.
- **FTDS++:**
 12. Features 1-11.
 13. Protection against **data loss** and **loss of access** due to multiple disk failures.
- **DTDS (disaster-tolerant disk system):**
 14. Features 1-11.
 15. Protection against **data loss** due to complete failure of one zone (distance between two zones > 1 km).
- **DTDS+:**
 16. Features 1-11.
 17. Protection against **data loss** due to complete failure of one zone (distance between two zones > 10 km).

7.9 A **Storage Area Network** (SAN) is composed of storage systems and servers connected by switching fabric, such that multiple servers can share the same storage systems. Redundancy and fault tolerance can be built into the switching fabric to increase the availability of access to the storage systems.

7.10 **Fault tolerance** means that a system can detect if there is a fault and can correct it or work around it automatically.

7.11 **Clustering** is a fault tolerant server technology. A group of servers working together as a logical unit to provide load balancing, redundancy and fail-over functions. If any one server fails, the other servers will pick up the load of the failed server.

Table of Contents of CISSP Certification Exam Study Guide

CHAPTER 1. INTRODUCTION	1
1. Common Body of Knowledge (CBK)	1
2. Certification and Re-certification	1
CHAPTER 2. INFORMATION SECURITY MANAGEMENT	3
1. Introduction	3
2. Risk Management	7
3. Data Classification	13
4. Security Policies, Standards, Baselines, Guidelines, and Procedures	14
5. Personnel Security Policies and Practices	16
CHAPTER 3. SECURITY ARCHITECTURE & MODELS	19
1. Introduction	19
2. Computer Architecture	19
3. Operating System Architecture	23
4. Security Architecture	29
5. Security Models	32
6. Security Evaluation	38
7. Certification and Accreditation	46
CHAPTER 4. PHYSICAL SECURITY	49
1. Introduction	49
2. Facility Requirements	50
3. Perimeter Security	53
4. Fire Protection	61
5. Power Protection	65
6. General Environmental Protection	66
7. Equipment Failure Protection	68
CHAPTER 5. ACCESS CONTROL SYSTEMS & METHODOLOGY	73
1. Introduction	73
2. Identification and Authentication	73
3. Single Sign-On (SSO)	82
4. Authorization	86
5. Accountability	87
6. Access Control Models	88
7. Access Control and Monitoring Mechanisms	90
8. Threats and Countermeasures	97
CHAPTER 6. TELECOMMUNICATIONS & NETWORK SECURITY - I	100
1. Introduction	100

2. Open System Interconnect (OSI)	101
3. Transmission Control Protocol / Internet Protocol (TCP/IP)	106
4. Network Communication Characteristics	112
5. Network Types and Topologies	114
6. Network Media	117
CHAPTER 7. TELECOMMUNICATIONS & NETWORK SECURITY - II	125
1. LAN Technologies - Media Access	125
2. LAN Technologies - Protocols	128
3. LAN Technologies - Devices	132
4. WAN Technologies - Basics	137
5. WAN Technologies - Protocols and Services	140
6. Wireless Technologies	149
7. Network Services	157
8. Firewall and Virtual Private Network (VPN)	166
CHAPTER 8. CRYPTOGRAPHY	174
1. Introduction	174
2. Encryption Algorithm Basics	177
3. Symmetric Encryption	179
4. Asymmetric Encryption	183
5. Message Authentication	186
6. Public Key Infrastructure (PKI)	189
7. Key Management	191
8. Cryptography Applications	193
9. Attack Methods against Cryptographic Systems	200
CHAPTER 9. APPLICATIONS & SYSTEMS DEVELOPMENT SECURITY	204
1. Introduction	204
2. System Development Life Cycle and Software Process Management	204
3. Application Development Technologies	213
4. Database and Data Warehousing	220
5. Application Security Threats and Malicious Codes	228
CHAPTER 10. OPERATIONS SECURITY	236
1. Introduction	236
2. Roles and Responsibilities	236
3. Backup and Recovery	238
4. Other Operation Controls	242
5. Threats and Countermeasures	243
CHAPTER 11. BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING	250
1. Introduction	250
2. Business Continuity Planning (BCP)	251

3. Disaster Recovery Planning (DRP)	254
CHAPTER 12. LAW, INVESTIGATIONS & ETHICS	261
1. Laws related to Computer Crime	261
2. Computer Fraud and Abuse	268
3. Incident Handling and Evidence Control	271
4. Ethical Conduct	277
APPENDIX	279
1. British Standard 7799 (BS7799)	279
2. Useful Websites	280
3. Commonly Used Well-known TCP and UDP Ports	281

CISSP Certification Exam Study Guide

Copyright©2006 by the KP Lab Limited. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN-13 978-988-97323-5-6
ISBN-10 988-97323-5-1
Publisher KP Lab Limited
Author K. Wan
Web Site www.kp-lab.com
e-mail kplab@pacific.net.hk

About the Author

K. Wan, MSc., CISSP, CCNP, CCSE, MCSE, MCDBA, SCSA, SCNA, SCJP, has over ten years' experience in system and security administration on various computing platforms. He is currently an IT infrastructure and security manager working in Hong Kong.

IT Certification Examination Study Guides published by KP Lab:

1. CISSP Certification Exam Study Guide
ISBN: 988-97323-5-1, 978-988-97323-5-6
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$19.99):
<http://www.kp-lab.com/cissp.htm>

2. CCNA 640-801 Exam Notes
ISBN: 988-97323-2-7
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$10.39):
<http://www.kp-lab.com/ccna.htm>

3. CCNP BSCI 642-801 Exam Notes
ISBN: 988-97323-3-5
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$16.95):
http://www.kp-lab.com/ccnp_bsci.htm

4. CompTIA Network+ Exam Notes
ISBN: 988-97323-4-3, 978-988-97323-4-9
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$16.95):
http://www.kp-lab.com/comptia_network.htm