
CISSP Exam Notes - 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 an environment 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, lightening, 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. strike, war, sabotage, etc.

1.4 There are three major types of control mechanisms for physical security:

- **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 Some physical security controls are required by laws, e.g. fire exit door, fire alarm, etc.

2. Facility Requirement

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, 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** 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.
- **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), emergency marking, directional opening, 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), placement of doors.
- **Window** – characteristics of windows material (opaque, translucent, transparent, shatterproof, bulletproof), intrusion detection alarm, placement of windows.
- **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, which can avoid 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, positive flow (i.e. liquid or gas should flow out of a building, not in), 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.
- **Emergency lighting** – essential power supply and battery for emergency lighting.

2.4 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.

3. Perimeter Security

3.1 **Perimeter security controls** are used to prevent unauthorized access to a facility. They deal with access control, auditing and monitoring; intrusion detection and response.

3.2 The perimeter security requirements when a facility is in operation should be different from those when the facility is closed.

Access Control and Auditing

3.3 Physical access control mechanisms include:

- Lock and key.
- Access card and reader.
- Fence.
- Lighting.
- Doorway and Man-trap.

3.4 **Lock and key** is the most inexpensive physical access control mechanism. It is a deterrent and delaying device to intruders. 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.
- **Programmable lock** or **Cipher lock** – Lock with key pad which requires a combination of keys to open the lock, or lock with reader which requires an access card to open the lock. 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).
- **Device lock** (for locking a device rather than for perimeter security):
 - Slot lock – secure a device to a stationary component (e.g. steel cable with lock).
 - 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).

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

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

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

3.7 **Fence** is another physical access control mechanism. 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.

3.8 **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.

3.9 **Bollards** are small and round concrete pillars that are constructed and placed around a building to protect it from being damaged by someone running a vehicle into the side of the building.

3.10 **Lighting** (e.g. streetlight, floodlight and searchlight) is a good deterrent for unauthorized access. It can also provide safety for personnel. The National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power.

3.11 **Doors** to secured areas should have the following characteristics:

- Have similar appearance as the other doors to avoid catching the attention of intruders.
- Be self-closing and have no hold-open feature.
- Trigger alarms if they are forcibly opened or have been held open for a long period

of time (door delay trigger).

- Use fail-secure locks, if necessary.

3.12 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).

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

3.14 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 after an incident happens. It should contain the following information for every access attempt:

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

3.15 For mobile devices, laptops, or similar equipment that cannot be protected by the perimeter security controls, other security measures (e.g. device lock and data encryption) and user responsibilities become more important.

Access Monitoring and Intrusion Detection

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

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

- It is expensive.
- The reliability of security guards is an issue. Pre-employment screening and other background checking are required.
- Human is subject to social engineering. Training against social engineering is required.

3.18 **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.

3.19 Technical access monitoring 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 a 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 motion.
- **Passive infrared 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 magnetic field and monitors the field to detect for any interruption. It is especially useful for protecting specific objects.

3.20 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.

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

- An intrusion detection system may generate a lot of false alarms.
- 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 system should have emergency backup power supply to prevent intruders from disabling the system by cutting the normal power supply.

- An alarm system and the signal transmission medium should be monitored to detect for tampering.
- An alarm should be audible for at least 400 feet.
- An alarm requires a security guard to respond to locally.

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 Detection

4.4 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.

4.5 **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).

- 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, 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

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

4.7 A **portable 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.

4.8 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, so that people have enough time to evacuate.

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

4.10 **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 1994 by international agreement. Extinguishers using Halon are not allowed to be refilled. However, it is not necessary to replace them immediately.

4.11 Halon 1211 is a liquid agent used mainly in portable extinguishers. Halon 1301 is a gas agent used mainly in flooding systems. Halon 1301 requires sophisticated pressurization.

4.12 **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.

4.13 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.
- 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 false alarm).
- It is suitable for cold climate.
- It does not react as fast as the wet pipe system.

3. **Pre-action system**

- Water is not held in the pipes in 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 wet pipe system and dry pipe systems).
- 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 the 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.

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

- Water can increase the fire intensity in an electrical fire. Therefore, electrical power should be shut down automatically (e.g. by connecting it to the fire alarm system) before water is discharged from the sprinkler heads.
- Each sprinkler head should be activated individually to avoid wide-area water damage.

5. Power Protection

5.1 Power protection controls include:

- **Uninterrupted Power Supply (UPS)** to protect against a short duration power failure. 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** to protect against a long duration power failure, e.g. motor generator, another electrical substation, etc.
- **Voltage regulator and line conditioner** to protect against unstable power supply.
- **Proper grounding** for all electrical devices to protect against short circuit and static electricity, e.g. by using 3-prong outlets.
- **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 is designed for protection against a short duration power outage, or for providing enough time for system administrators to shut down the systems and equipment orderly. Backup power source such as motor generator is designed for protection against a long duration power outage.

5.4 UPS and backup power source should be tested periodically.

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

5.6 **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, truck ignition, etc.

5.7 There are several types of electrical voltage fluctuations:

- Excess power – **“Spike”** for momentary high, **“Surge”** for prolonged high.
- Power degradation – **“Sag”** for momentary low, **“Brownout”** for prolonged low.
- Power loss – **“Fault”** for momentary outage, **“Blackout”** for prolonged outage.

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 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 mechanisms to slow down. If the temperature is too high, it may cause equipment damage. The temperature damaging points of 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

6.3 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**.

- 6.4 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).
- 6.5 **Liquid and gas lines** must have **shut-off valves** and **leakage sensors**. The lines should maintain **positive flow** (i.e. liquid or gas should flow out instead of flow in a building).
- 6.6 **Static electricity** can be prevented by using anti-static floor, anti-static carpet (or not use carpet) and anti-static band. Proper humidity and grounding are also required.

7. Equipment Failure Protection

- 7.1 There are several types of controls for ensuring system availability:
- **Hardware maintenance**, with service level agreements (SLAs) with the maintenance service suppliers.
 - **Hardware redundancy**, e.g. RAID disk, clustering, spare equipment.
 - **Regular backup** of data and systems (Details can be found in Chapter 9).
 - **Alternate site** or Disaster Recovery (DR) site (Details can be found in Chapter 10).
- 7.2 There are two important concepts when determining the requirement of controls for system availability:
- **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 Availability of disk storage can be increased by:
- **Disk mirroring** or **shadowing** – Real-time duplication of data on a mirror disk.
 - **Disk duplexing** – Disk mirroring plus redundant disk controller.
 - **Redundant Array of Inexpensive Disks** (RAID).
- 7.4 **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:
- Level 0 – Stripping, i.e. a large logical disk which has data being divided and written over several physical disks. It can improve the logical disk performance, but has no redundancy. Failure of one physical disk will make the whole logical disk fails.

- Level 1 – Disk mirroring, i.e. all data on a physical disk are duplicated to a mirror disk, and all modifications are made to the both disks simultaneously.
- Level 2 – Striping plus hamming code parity at bit level for redundancy (32 disks for storage and 7 disks for parity). This level is seldom used in the real world.
- Level 3 – Byte level striping plus parity (N data disks and 1 parity disk).
- Level 4 – Block level striping plus parity (N data disks and 1 parity disk).
- Level 5 – Block level striping plus interleaved parity, i.e. parity information is interleaved across all physical disks (N+1 disks). 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.
- Level 6 – Block level striping plus two sets of parity (N+2 disks). A logical disk can operate without data loss even if at most two physical disks failed.
(For Levels 1-5, a logical disk can operate without data loss if at most one physical disk failed.)
- Level 10 – Level 1 + Level 0, i.e. striping across multiple RAID-1 disk pairs.
- Level 01 – Level 0 + Level 1, i.e. 2 x RAID-0 disk groups, each disk group is a mirror of the other.
- Level 15 – Level 1 + Level 5, i.e. striping with interleaved parity across multiple RAID-1 disk pairs.
- Level 51 – Level 5 + Level 1, i.e. 2 x RAID-5 disk groups, each disk group is a mirror of the other.

7.5 Most RAID systems support **hot swapping** disks, i.e. replacement of a failed hard disk and reconstruction of the contents of the failed disk onto a replacement disk while the system is running.

7.6 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 failed disk contents 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).

7.7 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.

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

7.9 **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 Exam Notes

CHAPTER 1. INTRODUCTION.....	1
1. COMMON BODY OF KNOWLEDGE (CBK).....	1
2. CERTIFICATION AND RE-CERTIFICATION	1
CHAPTER 2. SECURITY MANAGEMENT PRACTICES	3
1. SECURITY MANAGEMENT	3
2. SECURITY PRINCIPLES AND DEFINITIONS.....	5
3. RISK MANAGEMENT	6
4. DATA CLASSIFICATION.....	10
5. SECURITY POLICIES, STANDARDS, GUIDELINES, AND PROCEDURES.....	11
6. EMPLOYMENT POLICIES AND PRACTICES.....	12
CHAPTER 3. SECURITY ARCHITECTURE & MODELS	15
1. COMPUTER ARCHITECTURE.....	15
2. OPERATING SYSTEM ARCHITECTURE	18
3. SECURITY ARCHITECTURE DEFINITIONS.....	20
4. SECURITY MODELS.....	23
5. SECURITY EVALUATION	26
6. CERTIFICATION AND ACCREDITATION	33
CHAPTER 4. PHYSICAL SECURITY.....	35
1. INTRODUCTION.....	35
2. FACILITY REQUIREMENT	36
3. PERIMETER SECURITY	37
4. FIRE PROTECTION.....	41
5. POWER PROTECTION	44
6. GENERAL ENVIRONMENTAL PROTECTION	45
7. EQUIPMENT FAILURE PROTECTION	46
CHAPTER 5. ACCESS CONTROL SYSTEMS & METHODOLOGY.....	49
1. INTRODUCTION.....	49
2. IDENTIFICATION.....	49
3. AUTHENTICATION.....	51
4. AUTHORIZATION	58
5. ACCOUNTABILITY.....	59
6. ACCESS CONTROL MODELS.....	60

7.	ACCESS CONTROL AND MONITORING MECHANISMS	62
8.	THREATS AND COUNTERMEASURES.....	67
CHAPTER 6. TELECOMMUNICATIONS & NETWORK SECURITY.....		69
1.	NETWORKING BASICS.....	69
2.	LOCAL AREA NETWORK (LAN) TECHNOLOGIES	74
3.	METROPOLITAN AREA NETWORK (MAN) AND WIDE AREA NETWORK (WAN) TECHNOLOGIES.....	81
4.	WIRELESS TECHNOLOGIES.....	88
5.	NETWORK DEVICES.....	92
6.	NETWORK SERVICES	99
CHAPTER 7. CRYPTOGRAPHY.....		104
1.	INTRODUCTION.....	104
2.	ENCRYPTION ALGORITHM BASICS.....	107
3.	SYMMETRIC ENCRYPTION	108
4.	ASYMMETRIC ENCRYPTION	111
5.	MESSAGE AUTHENTICATION	113
6.	PUBLIC KEY INFRASTRUCTURE (PKI).....	115
7.	KEY MANAGEMENT	117
8.	CRYPTOGRAPHY APPLICATIONS.....	119
9.	ATTACK METHODS TO CRYPTOGRAPHY	126
CHAPTER 8. APPLICATIONS & SYSTEMS DEVELOPMENT SECURITY.....		129
1.	INTRODUCTION.....	129
2.	SYSTEM DEVELOPMENT LIFE CYCLE AND SOFTWARE PROCESS MANAGEMENT	129
3.	APPLICATION DEVELOPMENT TECHNOLOGIES.....	135
4.	DATABASE AND DATA WAREHOUSING.....	141
5.	THREATS, MALICIOUS CODE AND ATTACK METHODS.....	146
CHAPTER 9. OPERATIONS SECURITY.....		152
1.	INTRODUCTION.....	152
2.	ROLES AND RESPONSIBILITIES.....	152
3.	BACKUP AND RECOVERY	153
4.	OTHER OPERATION CONTROLS.....	157
5.	THREATS AND COUNTERMEASURES.....	158
CHAPTER 10. BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING.....		162
1.	INTRODUCTION.....	162
2.	BUSINESS CONTINUITY PLAN (BCP).....	163
3.	DISASTER RECOVERY PLAN (DRP).....	164

CHAPTER 11. LAW, INVESTIGATIONS & ETHICS	170
1. LAWS RELATED TO COMPUTER CRIME	170
2. COMPUTER FRAUD AND ABUSE	175
3. INCIDENT HANDLING AND EVIDENCE CONTROL	177
4. ETHICAL CONDUCT	181
APPENDIX	183
1. BRITISH STANDARD 7799 (BS7799).....	183
2. USEFUL WEBSITES.....	184
3. COMMONLY USED WELL-KNOWN TCP AND UDP PORTS.....	185
INDEX	186

CISSP Exam Notes – All you need to pass the exam

Copyright©2003 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 988-97323-1-9
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 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 Exam Notes
ISBN: 988-97323-1-9
Free Chapter:
<http://www.kp-lab.com/download.htm>
Complete Book (\$16.80):
<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>
Complete Book (\$9.74):
<http://www.kp-lab.com/ccna.htm>