Question 1

What are the three (3) different factors that are used for authentication?

For each factor, give an example.

Finally, describe a situation where a combination of at least two factors is necessary and briefly explain why

Three diff factors

1. Sth a person knows (Pwd Pin)
2. Sth a person has (Token)
3. Sth a person is (Biometrics Thumbprint, Thumb, Iris)

Two Factors Necessary (Choose 2 from above)

* Companies Card access and Biometrics to verify identity
* Companies Pin and Thumbprint
* Internet Banking Pin and Message sent to phone

**Question 2**

One important requirement when assigning value to an identity is that the value must be non-descriptive.

Explain (Provide Definition) what it means by ‘‘non-descriptive” and why (Give Example) it is required so.

Neither piece of the cred set shld indicate the purpose of the acct

Eg. user id not (backup op, ceo, administrator) - does not show who it belongs to

**Question 3**

Describe 描述 two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry 普通的电脑室免遭未经授权的进入.

(Find Two out of Five Types of Technical controls from the chart. Examples listed have to be relevant to the question. (In this case: Physical Building access))

Preventive Technical controls include Access cards, biometrics, Pin (personal id number)

Detective Technical controls include CCTV.

Low security - Biometrics, Pin, Access Card,

\* Need to write what type of biometrics

**Question 4**

Auditing is used for multiple purposes in a security system. Describe three major security issues addressed by the use of auditing. (Describe : Definition, Describe three issues addressed: Give the reasons why auditing is important WHY)

审计在安全系统中被用于多种目的。描述通过使用审计解决的三个主要安全问题。

To be able to:

Detect intrusion

reconstruct events and system conditions

provide legal recourse material

**Question 5**

Physical controls are often neglected when security systems are developed but nonetheless they are a critical component of an effective security solution. (Statement)

Describe two physical preventive types of controls as well as two physical detective types of controls and specify a scenario in which a combination of the two is necessary.

在开发安全系统时，物理控制往往被忽视，但它们是有效的安全解决方案的重要组成部分。描述两种物理预防类型的控制和两种物理检测类型的控制，并说明在什么情况下需要结合这两种控制。

Physical Preventives

* Turnstiles
* Automated barriers
* Bollards

Physical Preventive controls include turnstiles, automated barriers and bollards.

Physical Detectives

* Cctv
* smoke detector

Scenario (Physical)

CCTV and Biometrics (Data Centre)

A data centre will have to have CCTV and Biometrics in place.

Hospital

School

Research Lab

Technical Real Life examples:

* Online banking includes the:
* technical preventive controls such as (Passwords)

密码

* Technical deterrent (Message on website to prevent people from hacking)

网站上的信息，以防止人们的黑客行为

* Technical detective (Audit)

审计

* School security system
* Technical preventive (Passwords)

密码

* Technical deterrent (Message on website to prevent people from hacking)

网站上的信息，以防止人们的黑客行为

* Technical detective (Antivirus software)

杀毒软件

* Technical Corrective (Recycle bin)

回收站

* Technical Recovery (Recovery technologies)

恢复技术

Administrative Real life examples:

* Big organisations:
* Administrative deterrent (Penalty and termination policy)

处罚和解雇政策

* Administrative preventive (Security awareness and training)

安全意识和培训

* Administrative detective (Security reviews, performance evaluations)

安全审查、绩效评估

* Administrative Corrective (Incident handling procedures)

事故处理程序

* Administrative recovery (Contingency plans and Disaster recovery plans)

应急计划和灾难恢复计划

**Question 6**

When developing a security system, it is important to plan for cases which the preventive measures in place fail and, consequently, the system integrity is compromised. From a security perspective what are the two main avenues that are generally considered for continuity/restoration of services? (Recovery)

在开发一个安全系统时，重要的是要对预防措施失败的情况进行规划，从而使系统的完整性受到损害。从安全的角度来看，通常考虑的两个主要途径是什么，用于服务的连续性/恢复？

Access controls fail

If fail and integrity is compromised:

(Backup - offsite storage backups(Offline)

Ensure restoration of services, test the backup so that the backup will not fail (once in 6 months or once a year)

(Under the 5th stage of Security Controls: Recovery, list out 2 examples)

**Question 7**

The integrity principle in the context of data security deals with the correctness of the data and the aim is to prevent damage from personnel inside or outside the organization. What is the first measure that needs to be put in place to help with the data integrity protection?

数据安全方面的完整性原则涉及到数据的正确性，其目的是防止组织内部或外部人员的破坏。为帮助保护数据的完整性，首先需要采取的措施是什么？

Implement access controls. Users will only have limited access, this reduces the chance that a basic mist can result in a major damage to the data that is being protected.

**Question 8**

Explain the difference between corrective and recovery controls.

Compare

Explain the similarities (Definition of both, both is \_\_\_\_)

(Definition of both, description, Advantage and Disadvantage, Examples)

解释纠正性控制和恢复性控制之间的区别。

Definition: Recovery controls are for recovering more serious situations from damage.

**Corrective control**

Example:

Recycle bin in Windows helps to correct accidental deletion. When an item is accidentally deleted, it goes into the recycle bin and users are still able to retrieve the files within a specific amount of time.

**Recovery control**

Example:

Chkdsk which helps to recover files that have been erased.

**Question 9**

Many organizations develop security systems which are focused entirely on physical and technological security controls. Explain why this is insufficient and provide examples how the security could be compromised. (Explain why it is insufficient: Find what is missing and list why it is important to have the missing item)

许多组织开发的安全系统完全集中在物理和技术安全控制上。解释为什么这是不充分的，并举例说明安全可能受到损害。

Cyber security has 3 main aspects: People, Process, Systems

We need **Administrative Controls** as well.

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

Thus an attacker may not need to break into the better protector systems as the access to confidential information is unlikely to be thoroughly control.

Example of lack of **Administrative Control**

Email to all users instead of only those that should have access to it.

Disposal of older hardware is not done in a secure manner and harddrives are simply thrown into a bin in from which an attacker can extract critical information such as passwords or confidential records.

**Question 10**

What is CERT-Australia? What is AusCERT? What is ASD? Why is it important from a data security point of view to know about each of them?

**C.E.R.T -** Computer Emergency Response Team

**CERT Australia** is the national computer emergency response team. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

**AusCERT** is a non-profit organisation that provides advice and solutions to cybersecurity threats and vulnerabilities. The organisation covers their costs through member subscriptions, attendees to the annual AusCERT conference and service contracts.

CERT educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Knowing about each of them allows us to be better prepared in tackling cyber-security threats.

**Question 11**

What is sender policy framework (SPF)? Explain the type of attacks that SPF addresses.

The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to stop phishing attacks. It allows your company to specify who is allowed to send email on behalf of your domain.

This is useful because in a typical phishing attack, the threat actor spoofs the sender address to look like an official business account or someone the victim may know.

**Targets**

* Email spoofing
* Phishing attacks

**How**

The protection of your outbound email is implemented by configuring a TXT record in your public DNS which lists the servers that are allowed to send email from your mail domain. Nothing is configured on the mail server itself.

The Sender Policy Framework (SPF) email authentication method aims to reduce spam and fraud by making it harder for email senders to hide their identity. SPF detects email spoofing by providing a process to verify who is permitted to send emails on your behalf.