FCDS Test 2 - Practice Questions:

Security Controls:

1. For each of the following Security controls, place them in the correct category (Physical, Technical or Administrative) and (Deterrent, Preventative, Detective, Corrective or Recovery)
    - Swipe card
    - Barking Dog
    - Fake Security Camera
    - Password policy
    - DRP (Disaster recovery plan)

2. Steve is going to be working from home now onwards and needs to ensure that his home is secure. List 2 security controls (and identify which categories they fit in) that you would suggest Steve to implement at home. Note that he doesn't have much time or money that he can use on this

3. Why is it a good idea to disable inactive accounts after 30-60 day

4. Briefly explain the difference of white listing vs black listing in terms of programs that a company can have installed.

5. Out of the 9 given Security methods. Which do you think would be the cheapest and easiest to implement? Why (You need to explain why you chose that one)?

6. What are the 3 differnet factors that are used for authentication. For each factor give an example.

7. Steve's new fancy flower shop is wanting to get some security. The store is a pure physical shop with no online website. Steve has decided that he is wanting to implement a Defence-In-Depth security method to protect his store. Describe what you think he should do to achieve this and which security controls he should implement.

Risk Management

1. What are 3 steps when it comes to managing risks?

2. List the 5 different ways of addressing a risk

3. Steve is currently using a laptop that has an old version of the Windows operating system and discovered that there is a major vulnerability with it. He has identified that this is a risk and is wishing to address it. He mainly uses the laptop for non-internet uses such as playing solitaire and minesweeper and using it to store photos from his camera. Which of the 5 methods of addressing a risk would you pick for Steve to do. Explain why you chose that one

4. Give an example of a risk that the best cause of action would be to accept it.

5. How does mitigation differ from defend?

6. With the help of an example, explain the principle of Fail Securely.

Change Management

1. What is a benefit is documenting the steps performed when making a change?

2. Why is it important to notify those that are going to be affected by the change?

3. Why doesn't every company do change management properly given all the benefits that it brings?

BCP and DRP

1. What are the main differences between a DRP and a BCP?

2. Which is generally a larger value, the MTD or the RTO?

3. Briefly explain what the RPO is and how the result of it differs from the MTD.

4. List and explain 3 different types of disasters that an impact a company.

5. Given the following table, calculate the SLE, ARO and ALE for each category

Threat	**Cost per incident**	**Occurrence frequency**
Hackers	$10,000	1 per month
Fires	$80,000	1 per 2 years
Theft	$100	1 per week