

Fundamental Concepts of Data Security

ISEC2001

Security Controls I

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.

Question 2

One important requirement when assigning value to an identity is that the value must be non-descriptive. Explain what it means by “non-descriptive” and why it is required so.

Question 3

Describe 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.

Question 4

Auditing is used for multiple purposes in a security system. Describe three major security issues addressed by the use of auditing.

Question 5

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

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?

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?

Question 8

Explain the difference between corrective and recovery controls.

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.

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?

Question 11

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