**CYB0103: Cybersecurity Design Principles**

**Question Bank**

**Chapter 1**

Prepared by: Rana Al Haj Fakeeh

**Part I: multiple choice questions:**

1. \_\_\_\_\_\_ means keeping things secret that shouldn’t be made known to the public:
2. Confidentiality.
3. Availability.
4. Traceability
5. Integrity.

**Answer:** A

1. \_\_\_\_\_\_ means that the information doesn’t change or is only allowed to change in specific, authorized ways:
2. Confidentiality.
3. Availability.
4. Traceability
5. Integrity.

**Answer:** D

1. \_\_\_\_\_\_ means data is at hand in a timely manner:
2. Confidentiality.
3. Availability.
4. Traceability
5. Integrity.

**Answer:** B

1. \_\_\_\_\_\_ means the need for knowing who changed or accessed what data when:
2. Confidentiality.
3. Availability.
4. Traceability
5. Integrity.

**Answer:** C

1. Which one of the following is NOT one of the security concerns:
2. Connectivity.
3. Availability.
4. Traceability
5. Integrity.

**Answer:** A

1. What is the Information Security definition:
2. Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
3. It is a broader category that protects all information assets, whether in hard copy or digital form.
4. It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
5. It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

**Answer:** B

1. What is the Cybersecurity definition:
2. Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
3. It is a broader category that protects all information assets, whether in hard copy or digital form.
4. It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
5. It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

**Answer:** D

1. What is the Traditional Approach to software security definition:
2. Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
3. It is a broader category that protects all information assets, whether in hard copy or digital form.
4. It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
5. It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

**Answer:** A

1. What is the Design definition:
2. Security should be a top priority when developing and writing code and everyone involved in the process should be trained and experienced in software security.
3. It is a broader category that protects all information assets, whether in hard copy or digital form.
4. It is the guiding principle for how a system is built and is applicable on all levels, from code to architecture
5. It is protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible.

**Answer:** C

1. Which one of the following is NOT true about the Design Approach to software security:
2. Design is a natural part of software development.
3. Business concerns and security concerns become of equal priority.
4. Non-security experts can naturally write secure code.
5. Developers should know about things like cross-site scripting (XSS) attacks, be aware of vulnerabilities in low-level protocols, and know the OWASP Top 10 like the backs of their hands.

**Answer:** D

**Part II: true / false questions:**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 1 | The design approach to software security is better than traditional approach. | T |
| 2 | The traditional approach considered problematic because it requires every developer to be a security expert. | T |
| 3 | Integrity concern captures the need for knowing who changed or accessed what data when. | F |
| 4 | Security is a natural part of software development. | F |
| 5 | One advantage of design approach is that business concerns and security concerns become of equal priority. | T |
| 6 | One advantage of design approach is that non-security experts naturally write secure code. | T |
| 7 | A strong design focus lets you create code that’s less secure compared to the traditional approach to software security. | F |
| 8 | A strong focus on traditional approach lets you create code that’s less secure compared to the traditional approach to software security. | T |
| 9 | Login Page, Encryption, Firewall, and Antivirus are considered security concerns rather than security features. | F |
| 10 | Confidentiality, Integrity, Availability, and Traceability are considered security concerns rather than security features. | T |
| 11 | Implementing a login page to an application is enough to meet the information confidentiality concern. | F |
| 12 | Even when security features address a specific security problem, your concern about security may not have been met. | T |
| 13 | It’s better to view security as a feature to implement than to view it as a concern to be met. | F |
| 14 | It is easier for developers to achieve security through design because most developers understand and appreciate software design. | T |
| 15 | The design approach creates a conflict between security concerns and business concerns for developers. | F |