1.
Security

2.
information security

3.
computer security

4.
network security

5.
Asset

6.
Control, safeguard, or countermeasure

7.
C.I.A. triad

8.
Access

9.
Exposure

10.
Exploit

1.
A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

2.
Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

3.
In the early days of computers, this term specified the need to secure the physical location of computer technology from outside threats. This term later came to represent all actions taken to preserve computer systems from losses. It has evolved into the current concept of information security as the scope of

4.
A subset of communications security; the protection of voice and data networking components, connections, and content.

5.
The organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible object. Assets, particularly information assets, are the focus of what security efforts are

6.
Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization.

7.
The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

8.
A subject or object’s ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers must gain illegal access to a system. Access controls regulate this ability.

9.
A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker.

10.
A technique used to compromise a system.

11.
Loss

12.
Protection profile or security posture

13.
Risk

14.
Threat

15.
Subjects and objects of attack

16.
Availability

17.
Threat source

18.
Threat event

19.
Threat agent

20.
confidentiality

12.

The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although a security program often comprises managerial

11.

A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. When an organization's information is stolen, it has suffered a loss.

14.

Any event or circumstance that has the potential to adversely affect operations and assets.

13.

The probability of an unwanted occurrence, such as an adverse event or loss. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk they are willing to accept.

16.

An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

15.

A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity, as shown in Figure 1-8. A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other

18.

An occurrence of an event caused by a threat agent.

17.

A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents.

20.

An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

19.

The specific instance or a component of a threat.

21.
Authenticity

22.
accuracy

23.
personally identifiable information (PII)

24.
integrity

25.
utility

26.
possession

27.
McCumber Cube

28.
top-down approach

29.
Physical security

30.
bottom-up approach

22.
An attribute of information that describes how data is free of errors and has the value that the user expects.

21.
An attribute of information that describes how data is genuine or original rather than reproduced or fabricated.

24.
An attribute of information that describes how data is whole, complete, and uncorrupted.

23.
Information about a person’s history, background, and attributes that can be used to commit identity theft. This information typically includes a person’s name, address, Social Security number, family information, employment history, and financial information.

26.
An attribute of information that describes how the data’s ownership or control is legitimate or authorized.

25.
An attribute of information that describes how data has value or usefulness for an end purpose.

28.
A methodology of establishing security policies and/or practices that is initiated by upper management.

27.
A graphical representation of the architectural approach widely used in computer and information security; commonly shown as a cube composed of 3×3×3 cells, similar to a Rubik’s Cube.

30.
A method of establishing security policies and/or practices that begins as a grassroots effort in which systems administrators attempt to improve the security of their systems.

29.
The protection of physical items, objects, or areas from unauthorized access and misuse.

31.
information system (IS)

32.
systems development life cycle (SDLC)

33.
software assurance

34.
methodology

35.
waterfall model

36.
Data owners

37.
project team

38.
chief information officer (CIO)

39.
chief information security officer (CISO)

40.
Data custodians

32.

A methodology for the design and implementation of an information system. The SDLC contains different phases depending on the methodology deployed, but generally the phases address the investigation, analysis, design, implementation, and maintenance of an information system.

31.

The entire set of software, hardware, data, people, procedures, and networks that enable the use of information resources in the organization.

34.

A formal approach to solving a problem based on a structured sequence of procedures.

33.

A methodological approach to the development of software that seeks to build security into the development life cycle rather than address it at later stages. SA attempts to intentionally create software free of vulnerabilities and provide effective, efficient software that users can deploy with confidence.

36.

Individuals who control, and are therefore responsible for, the security and use of a particular set of information; data owners may rely on custodians for the practical aspects of protecting their information, specifying which users are authorized to access it, but they are ultimately responsible for it.

35.

A type of SDLC in which each phase of the process “flows from” the information gained in the previous phase, with multiple opportunities to return to previous phases and make adjustments.

38.

An executive-level position that oversees the organization’s computing technology and strives to create efficiency in the processing and access of the organization’s information.

37.

A small functional team of people who are experienced in one or multiple facets of the required technical and nontechnical areas for the project to which they are assigned.

40.

Individuals who work directly with data owners and are responsible for storage, maintenance, and protection of information.

39.

Typically considered the top information security officer in an organization. The CISO is usually not an executive-level position, and frequently the person in this role reports to the CIO.

41.
communities of interest

42.
Data users

43.
communications security

42.

Internal and external stakeholders (customers, suppliers, and employees) who interact with information in support of their organization’s planning and operations.

41.

A group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives.

43.

The protection of all communications media, technology, and content.