Homework due **Sunday, December 4 at 11:55 PM** (Required)

1. Check your Understanding:

2. Access control - It is the restriction of access to information and information resources to only those who are authorized by role or other means

Access safeguards. - It is being able to identify which employees should have access to what data.

ARRA - American Recovery and Reinvestment Act

Authentication - It is the act of verifying a claim of identity.

CBAC - Context-based access control

Encryption - It is a method of encoding data, converting them to a jumble of unreadable scrambled characters and symbols as they are transmitted through a telecommunication network so that they are not understood by persons who do not have a key to transform the data into their original form.

Edit check - This helps to ensure data integrity by allowing only reasonable and predetermined values to be entered into the computer.

Data availability - Making sure the sure the organization can depend on the information system to perform as expected, and to provide information when and where it is needed.

Data integrity - This means that data are complete, accurate, consistent, and up-to-date so it is reliable.

IDS - Intrusion Detection System

ITAD - Information Technology Asset Disposition

HIPAA Security Rule - This requires the enforcement of information governance, which is the protection of information and access by authorized individuals only.

Impact analysis - It is what the impact of threats on information assets might be.

Decryption - It is the use of special algorithm that takes a message from one computer and encodes it in a form that only the receiving computer can decode.

Edit check - This helps to ensure data integrity by allowing only reasonable and predetermined values to be entered into the computer.

Firewall - it is a computer system or a combination of systems that provides a security barrier or supports an access control policy between two networks or between a network and any other traffic outside the network.

Network controls - These are essential to prevent the threat of hackers.

Password - It is a series of characters that must be entered to authenticate user identity and gain access to a computer or specified portions of a database.

Security breach - This is an unauthorized data or system access

Risk analysis - It is the process of identifying possible security threats to the organization’s data and identifying which risks should be proactively addressed and which risks are lower in priority.

Risk management - This is a comprehensive program of activities intended to minimize the potential for injuries to occur in a facility and to anticipate and respond to ensuring liabilities for those injuries that do occur.

RBAC - Role-based access control

PKI - Public Key Infrastructure

UBAC - User-based access control

e-PHI - Unsecured electronic protected health information

Single - key encryption - It is when two or more computers share the same secret key and that key is used to both encrypt and decrypt a message

Single sign on - It allows a user to log in one time and be able to access the many systems

Trigger events - It is the review of access logs, audit trails, failed logins, and other reports generated to monitor compliance with the policies and procedures.

3.  **Name and describe** 4 examples of malware.

Trojan horse: It is a program that gains unauthorized access to a computer and masquerades as a useful function.

Spyware: It is a computer program that tracks an individual’s activity on a computer system.

Computer worm: It is a program that copies itself and spreads throughout a network.

Computer virus: It is a program that reproduces itself and attaches itself to legitimate programs on a computer.

4. **Name  and describe** 4 Access Safeguards

Identification: It is the basic building block of access control used in blocking imposters who pose as legitimate users and enter a system illegitimately.

Authentication: It is the act of verifying a claim of identity.

Passwords: They are series of characters that must be entered to authenticate use identity and gain access to a computer or specified portions of a database.

Smart Cards and Tokens: These are small plastic cards with embedded microchips that can store multiple identification factors for a specific user.

5. HIPAA Security provisions:  **Name and describe**   3 Administrative safeguards.

Inappropriate sharing: Employees must not be allowed to share passwords

Prohibition of employees from accessing the Internet for purposes that are not work related.

Employees must log off the computers when they are not using them.