Ekaterina Simakina/Assignment 3/Task 1/Computer security

ISO/IEC 27002. This standard contains 14 security control clauses. I have written a summary of four of them: human resource security, asset management, access control and cryptography.1. Human resource security. It includes several stages: prior to employment, during employment, termination and change of employment.

1.1 *Prior to employment.* A company should ensure that employees and contractors acknowledge their responsibilities and they are appropriate for the roles which they are being considered for. Before making an offer to an employee a company needs to ensure the following actions: background checks of all the applicants must be carried out in accordance with laws and regulations; make sure that declared academic and professional qualifications correspond to reality; make independent verification of identity (with a passport or a similar document). Responsibility of information security must be stated in contractual agreements with employees and contractors. All employees and contractors who are given access to confidential information must sign confidentiality or nondisclosure agreement prior to gaining access to information processing assets.

1.2 During employment. During employment. During this stage a company needs to require all managers and contractors to apply information security in accordance with the organization's established policies and procedures. All employees of an organization as well as the contractors should be provided with relevant information through educational facilities and on-the-job-training, as well as regular with a regular update of organizational policies and procedures related to their professional duties.

If someone has made a mistake or violated the information security rules, a company has to investigate the case. It is necessary to reveal the reason of violation, in other words - if it happened by negligence or was done intentionally. The disciplinary process should not begin without first checking if an information security breach has occurred. This procedure should also be applied as a deterrent to prevent further employee misconduct.

1.3 Termination and change of employment. A company needs to protect the interests of the organization in case of changing or terminating employment. The company should notify the employee of the responsibilities and obligations in the field of information security that remain in effect after termination or change positions.

2.Asset management.

*2.1 Responsibility for asset*s. Responsibility for assets. A company should identify the assets of the organization and determine the appropriate responsibility for their protection. All information assets should be inventoried and identified. An owner must be assigned for each identified asset, and a classification must be made. In the event of a termination of employment, employees and external users must return all of the organization's assets to its disposal at the end of the employment contracts, or any other contracts and agreements signed with the organization.

2.2 Information classification. A company should ensure that information has a level of protection corresponding with its significance to the organization. Information should be classified in accordance with the level of confidentiality. Thereafter the information should be labelled by its owners according to the security protection required and handled appropriately.

2.3 Media handling. A company needs to prevent unauthorized disclosure, modification, movement or destruction of information stored on the carrier. Procedures should be in place to manage removable media in accordance with the organization's classification scheme. For example, all media should be stored in a safe, secure location in accordance with the manufacturer's requirements. If the data is confidential, cryptographic methods should be applied to protect the data on removable media. Copies of important data should be saved on separate media, as this will help reduce the risk of data loss or damage.

3. Access control. Access control is a big area of control including business requirements of access control, user access management, user responsibilities, system and application access control.

3.1 The aim of business requirements is to limit access to information and information processing facilities. Business requirements include the following aspects:

Access control policy which should be established, documented and reviewed based on business and information security access. Access control rules, access rights and restrictions for specific user roles have to be determined. A person gets access to the information which he or she needs to do a job with and therefore he or she is limited to a certain degree of access to information processing facilities.

Access to networks and network services. Users should only be given access to the network and network services they were specially authorized to use. Unauthorized and insecure connections to network services can badly affect an entire organization.

3.2 The aim of **user access management** is to ensure authorized user access and to prevent unauthorized access to systems and services. It includes the following: user registration and de-registration which is essential to control the process of registration and deregistration of a user and to assign an access right. User access provisioning: the process of granting access to users or revoking access rights. Management of privileged access rights: the distribution and use of privileged access rights should be limited and controlled, that is, privileged access rights should be allocated to users based on the purpose of use. Review of user access rights: user access rights have to be reviewed regularly when a person moves from one position to another, as well as privilege allocations have to be checked regularly.

3.3 User responsibilities. Users should be responsible for protecting their authentication data and have to keep it protected and secure, that is, use quality passwords, not share individual user's secret authentication information; and don't use the same secret authentication information for business and non-business purposes.

3.4 System and application access control. A company needs to prevent unauthorized access to systems. To do this a company should consider the following areas: ensure information access restriction; control the access rights of users (read, delete etc); access to systems and applications should be controlled by a secure log-on procedure; password management system must be interactive and provide quality passwords; enhance the use of privileged utility programs that can override system and application controls.

4. Cryptography.

The task is to ensure the proper and effective use of cryptography for protection confidentiality, authenticity or integrity of information. A policy of using cryptographic methods to protect information should be developed and implemented. Cryptographic methods can be used to achieve goals related to information security, for example: confidentiality, integrity, irrefutability, authentication. The policy should contain requirements for the management of cryptographic keys throughout their entire life cycle: generation, storage, archiving, recovery, distribution, revocation and destruction of keys. All cryptographic keys must be protected from modification or loss. Secret and private keys require protection from unauthorized use and disclosure. The equipment used for generating, storing and archiving keys must be physically protected.

Questions:

1.How does a company control access to corporate networks, IT systems, information, and applications? Is it based on user roles or organizational procedures?
2.Are user accounts locked out after a specified number of failed login attempts?
3.Do workstations automatically disconnect users from the network after a period of inactivity?
4.Does the company restrict access to the network depending on the position?
5.Are privileged access rights checked? (That is, access rights for administration, management, security and monitoring of IT systems.)
6.Does the company check network access for employees who change roles or positions in the organization?
7.Does the company prevent users from sharing their logins?
8.How does the company ensure the secure use of passwords? How does the company verify if this person is the declared person?
9. Do employees of the organization sign nondisclosure and confidentiality agreements?
10. Does the employee who is about to leave the company give back access cards, keys, IT equipment, storage devices and all other company assets?