Assignment 4 Task 1 December 20, 2020

Summary Report for ISO/IEC 27002

Chapter 5 – 9

Yuyao Duan

5. Information security policy

The objective of information security is to provide a management direction and to support information security for the focal organization fulfilling both business requirements and laws/regulations. There are two important parts of this management direction: 1) policies for information security and 2) review of the policies for information security.

Regarding policies for information security, in order to realize **control**, a set of polices for information security should be defined, approved by management, published and communicated to all stakeholders. The **implementation guidance** for this control includes the highest level's "information security policy" which is approved by the management to reach information security objectives. The policies should address the requirements of business strategy, all sorts of legislation, and information security threat environment.

6. Organization of information security

There are two main aspects of organization's information security: internal organization and mobile devices and teleworking. The aim of the first aspect is to establish a management framework to initiate and control the implementation and operation of information security within the organization. The objective of second aspect is to secure teleworking and use of mobile devices.

Regarding the **first aspect**, it includes five important parts: 1) information security roles and responsibilities aims to define and allocate all the responsibilities of information security. Responsibilities of information security should be allocated in accordance with information security policies. 2) Segregation of duties aims to reduce the chances when unauthorized or unintentional modification or misuse of the organization's assets occur which is due to conflicting duties and areas of responsibility. Even it is difficult, small organizations should also apply this principle as far as possible and practicable. When it is difficult to segregate, the control such as monitoring of activities, audit trails and management supervision should be considered. 3) Contact with authorities emphasizes that organizations should maintain appropriate contacts with relevant authorities. When to contact whom under what procedure should be considered. 4) Organizations should maintain appropriate contacts with special interest groups or other specialist security forums and professional associations. 5) Information security in project management should be addressed in project management, regardless of the type of the project. This asks that the organization should integrate information security in their project management methods. In terms of the **second aspect**, it includes two important parts: 1) mobile device policy emphasizes the organization should consider seriously about using mobile devices in the work environment, typically in the unprotected environments such as all kinds of public places. Using cryptographic techniques and enforcing use of secret authentication information are critical. 2) In terms of teleworking, the organizations should implement related policy and security measures for protecting information accessing, processing and storing at teleworking sites.

7. Human resource security

Three stages of human resource security should be considered: prior to employment→during employment→termination and change of employment. The objective of the **first stage** is to make sure the employees and contractors understand their responsibilities, and helping the organization to identify the suitable persons. The organization should pay attention to the candidates' background checking (screening). Furthermore, the organization should clearly claim the responsibilities (terms and conditions of employment) for information security to the employees/contractors. The aim of the

second stage is to ensure that the employees and contractors are aware of and fulfil their information security responsibilities. To do this, employees should apply information security with established policies; the organization should periodically educate its employees regarding security awareness; the organization should set up disciplinary process when employees violate security information breach. The **third stage** aims to protect the organization's interests when changing or terminating employment. The organization should communicate with employees if certain information security responsibilities will remain valid after termination or change of employment.

8. Asset management

Asset management concerns the following three management aspects: responsibility for assets, information classification, and media handling. For the **first management aspect**, the organizations should identify what are the assets and then come up with appropriate protection responsibilities. To achieve this, the organization should create inventories of assets to protect information and information processing facilities. Furthermore, the maintained assets should be assigned with ownership. Moreover, the rules for acceptable use of information and of assets related to information and information processing facilities should be identified, documented and implemented. When termination of the employment happening, the users should return their possession of different types of assets. Regarding the **second management objective**, the organization should give different information with appropriate level of protection by its organizational importance. Under this management objective, the information should be properly classified, labeled, and handled by organizational procedures. In terms of **media handling**, the organization should prevent unauthorized disclosure, modification, removal or destruction of the information stored on media.

9. Access control

Access control is important for organizational information security which includes business requirements of access control, user access management, user responsibilities, and system and application access control. For the **first management aspect**, the organization should establish an access control policy to manage the specific user roles accessing their assets, and only authorized users should have access to the organizational network and network services. The organization should come up with effective **user access management** mechanism to differ the authorized user access and unauthorized access to the systems and services. The organization should utilize user registration and de-registration process to assign access rights, which the privilege access rights should be restricted and controlled. Assets owner should regularly review the users' access rights to make in time adjustment. Regarding the **third management aspect**, users should be required to follow the organizations' requirements in the use of secret authentication information. With respect to **system and application access control**, the related access should be restricted in accordance with the access control policy and the requirements of business application. Secure log-on procedures should be applied such as cryptographic means, smart cards, tokens or biometric means etc. Furthermore, the organization should implement interactive and qualified password management systems which should enforce the use of individual user IDs and passwords. Due to the demand of preventing the introduction of unauthorized functionality, unintentional changes, and protecting intellectual property, the organization should restrict the access to source code.

Questions/Requests for Loco News:

Information Security Policy:

- What information security policy has Loco News applied to handle the external stakeholders?
- Does the current information security policy fulfill the latest GDPR regulations?

Organization of information security:

- What extra information security responsibilities do Loco News allocate to the "trusted employees" currently?
- Does Loco News consider the principle of "segregation of duties" for the "trusted employees"? Please provide their duties and responsibilities.
- Does Loco News apply any cryptographic strategy to protect mobile devices when employees are on travels?

Human Resource Security:

- What human resource security policies have Loco News applied in order to identify the "trusted employees" who have the access to the servers?
- Does Loco News offer periodically education regarding security awareness?

Asset Management:

- What strategies/policies has Loco News previously applied in order to manage the ownership of the organizational assets, typically the shared devices?
- Since the servers have important information and records, has Loco News applied any policy for information protection in terms of different level?

Access control:

- Does Loco News apply any access control in terms of *user role access management*, *authentication information control*, *cryptographic log-on methods*, and *password management system*? (If so, what industrial standards have been applied?)