In order to achieve this goal, ECHA has implemented a formal IT Security Management System which is described in this section.

IT Security Management System is a systematic approach to manage security risks related to IT systems. It is implemented as an efficient and effective set of procedures, rules and controls, and strongly supported by the IT security service.

ECHA IT Security Management System is applicable to all ECHA's IT systems and IT governance processes. Also, the risk-driven methodology defined in this document is followed when an IT-service is outsourced or planned to be outsourced.

The entire life cycle of IT systems, services, and processes is within the scope of ECHA's IT Security Management System. Thus, the risk driven approach is used, for example, when

- new IT systems and solutions are designed, procured, developed[1], tested and released
- a new IT infrastructure is designed or existing one changed, or other architectural and major changes are designed, planned and implemented
- IT services and processes are designed, changed, managed and run
- the existing IT systems and solutions are maintained and changed, and when the data media are disposed in the end of their life cycle

While all IT systems are in scope of the IT Security Management system, it is not necessary feasible or even doable to change all legacy applications or systems to be fully compliant with the requirements defined in the system. Thus, the risks related to incompliance are assessed and the decisions are made based on the cost-benefit - assessment[2], as a part of requirement specification of a new version of the application/system.

3.13.1. Overall Description of IT Security Management System

3.13.1.1. Characteristics and Objectives

The Main characteristics of the IT security management system are the following:

Risk driven approach. Instead of strictly following any formal security standard or best practice, ECHA's IT security is based on identifying, assessing and mitigating security risks; the security measures are grounded on the risk management decisions. The risk driven approach is followed to ensure that IT security focuses on the relevant security risks and in order to keep the security controls and risks in balance.

Proactive attitude. Usually, it is costly, difficult or even impossible to implement security later if it was not considered at the right time. The ECHA IT security management system supports initiating and taking the correct security actions at the right time, for example ensuring that security is considered in requirement

[1] "Secure Application Design and Development Guideline" describes in more detail security practices and procedures for application development
[2] Risk assessment and cost-benefit assessment will be discussed later in this document