Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

CHAPTER 5

PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Article 35

Definitions

For the purpose of this Chapter, the following definitions apply:

(a) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the Security Accreditation Authority (SAA) to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation;

(b) 'Accreditation Process' means the necessary steps and tasks required prior to the accreditation by the Security Accreditation Authority. These steps and tasks shall be specified in an Accreditation Process Standard;

(c) 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources;

(d) 'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

(e) 'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

(f) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment;

(g) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

(h) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities;

(i) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

Changes to legislation:
There are currently no known outstanding effects for the Commission Decision (EU, Euratom) 2015/444, Article 35.