EUROPEAN
COMMISSION

Brussels, 4.11.2019
C(2019) 8017 final

IT security standard

IT security compliance management

CONTENTS

1. INTRODUCTION

1.1. Legal base

This IT security standard is based on Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission and on the Commission Decision that sets out implementing rules for Articles 3, 5, 7-15 of Decision 2017/46, C (2017) 8841, in particular its Article 12.

It repeals the IT security standard on compliance as addressed in Commission Decision C(2006) 3602.

1.2. Subject matter and scope

1. The subject matter and scope of this IT security standard are presented in Article 1 of Commission Decision (EU, Euratom) 2017/46.

2. The provisions of this IT security standard apply to the IT systems of the European Commission. The responsibilities related to and IT security measures set up for IT systems handling classified EU information shall be in line with Commission Decision (EU, Euratom) 2015/444.

3. The provisions of this IT security standard cover the IT security compliance of Commission IT systems and related processes with the European Commission IT security policies and standards and the specific IT security provisions or requirements included in relevant legislation and contracts.

4. The provisions of this IT security standard cover the following three types of IT security compliance verification:

    a. review of IT security,

    b. IT security compliance review,

    c. IT security technical compliance review.

5. Provisions on IT security audits and IT security inspections fall outside the scope of this standard.

1.3. Definitions

For the purposes of this IT security standard, in addition to the definitions provided in Article 2 of Commission Decision (EU, Euratom) 2017/46 and Article 2 of Commission Decision (EU, Euratom) 2017/8841, the following definitions also apply:

1) A ‘review of IT security’ means a check of the organisation’s approach to managing IT security and its implementation (i.e. IT security controls, policies, processes and procedures) by an actor having no conflict of interest.

2) An ‘IT security audit’ means a systematic, independent and documented process, carried out exclusively by an entity with official IT security audit capability, to obtain audit evidence, objectively evaluate IT security and determine the extent to which the audit criteria have been fulfilled.

3) ‘internal IT security audit capability’ means the Internal Audit Service (IAS) of the Commission and any other internal audit capability.

4) ‘external IT security audit capability’ means the European Court of Auditors (ECA) or the Data Protection Supervisor (EDPS)1.

5) ‘IT security compliance review’ means a regular check of the compliance of information processing and procedures of a particular IT system with the IT security policies, standards and any other IT security requirements, through the following steps:

    a. identification of non-compliance, as well as, the causes of non-compliance;

    b. evaluation of the needs for action to achieve compliance;

    c. review of implementation plan for appropriate correction actions and their effectiveness.

6) An ‘IT security inspection’ is a particular type of IT security review. The Security Directorate of the Directorate-General for Human Resources and Security (HR.DS) carries out IT security inspections.

7) An ‘IT security technical compliance review’ means a regular check that verifies the existence and effectiveness of the technical security measures that are required by security policies, standards, IT security plan(s) and other security requirements.

2. IT SECURITY COMPLIANCE METRICS AND EXCEPTION HANDLING

2.1. Metrics for IT security compliance

IT security compliance metrics provide insight into the effective implementation of IT security measures and correct execution of IT security processes, including IT risk management, IT asset management and IT vulnerability and remediation management.

2.2. IT security exceptions handling

1. This activity covers verifying, registering and maintaining IT security exceptions to ensure their validity and business rationale throughout the IT system lifecycle.

2. IT security exception categories are as follows:

    a. IT security policy exceptions, meaning exceptions made for a part of IT security policy and/or standards due to a particular overall business context. They can be valid for one or multiple IT systems in a department.

    b. Technical IT system exceptions, meaning exceptions to a single mandatory IT security standard rule or requirement due to a technical or financial constraint.

3. All IT security exceptions shall be registered in the IT security plan.

[1] IT security is an integral part of the data protection rules (Article 33 Regulation (EU) 2018/1725), which can be subject to data protection audits as defined in the powers of the EDPS (Article 58 (1) b) of Regulation (EU) 2018/1725).

3. ORGANISATION AND RESPONSIBILITIES

3.1. The 'three lines of defence' operational model

1. A 'three lines of defence' operational model provides for three layers of IT security assurance activities involving different groups of actors:

    a. The first line of defence encompasses IT security risk management. The actors involved are system owners, system managers and heads of department, who are responsible and accountable for operational management.

    b. The second line of defence encompasses of IT security compliance reviews. The actors involved are the Directorate-General for Informatics (DIGIT) and the Human Resources Directorate of Security (HRDS), who monitor and facilitate the implementation of effective IT security compliance management practices and assist in reporting compliance-related information across all levels of the organisation.

    c. The third line of defence encompasses internal IT security audits. The actors involved are entities with official capacity to carry such audits; they provide independent assurance.

2. In complement to the above-mentioned model, external IT security audit capabilities are the only ones authorised to perform external IT security audits.

3.2. Roles and responsibilities

1. The Head of Commission Department is accountable for the compliance of IT systems owned by their department. The compliance shall cover the Commission IT security policy and standards and the specific IT security provisions or requirements included in relevant legislation and contracts.

2. The System Owner, or the System Manager with delegated responsibility, shall:

    a. be responsible for IT security compliance of their IT systems;

    b. identify the applicable legislation and contractual requirements may impact the IT security requirements and shall document them in the IT security plan;

    c. handle IT security exceptions;

    d. ensure that any weaknesses identified by compliance reviews are adequately addressed;

    e. record in the IT security plan the results of compliance checks and corrective actions carried out;

    f. cooperate and share information with actors carrying out IT security audits, inspections and compliance reviews.

3. The System owners of IT systems providing shared IT services shall additionally ensure that:

a. adequate IT security compliance information is provided to System Owners of IT systems using those shared IT services;

b. sufficient information on the IT security controls in place is shared on a per-request basis with System Owners of IT systems using those shared IT services in order to make it possible for them to fulfil their IT security compliance management responsibilities.

4. The LISO, shall:

a. Collect the IT security compliance metrics and the compliance information in the IT security plan and report this information to Directorate-General for Informatics in a timely manner and according to a standard procedure;

b. consider automated measurement and reporting tools, in particular the Commission IT security compliance support tools;

c. communicate to the Directorate-General for Informatics and the Head of Department any IT security policy exceptions.

5. The Directorate-General for Informatics shall:

a. propose to the Information Technology and Cybersecurity Board (ITCB) a list of Commission IT security compliance metrics, after collecting feedback and proposals from LISOs and reviewing them each year;

b. aggregate the IT security compliance metrics and exception information received from the LISOs and report on it to the ITCB each year;

c. set up and maintain the Commission IT security compliance support tools that will facilitate the collection and consolidation of IT security compliance information, in particular metrics, and support System Owners and LISO's to fulfil their responsibilities in IT security compliance management;

d. promote the use of Commission IT security compliance support tools, in particular for technical IT security compliance reviews;

e. provide guidance on how to assess the implementation of security rules, in particular, on how to verify that the rules defined in policies, standards and other applicable regulations have been adequately met.

6. The Information Technology and Cybersecurity Board (ITCB) shall:

a. endorse the list of IT security compliance metrics.

4. MISCELLANEOUS AND FINAL PROVISIONS

4.1. Transparency

This IT security standard shall be brought to the attention of Commission staff and to all individuals to whom it applies.

4.2. IT security standards

1. The provisions of this IT Security Standard shall, where necessary, be further detailed in technical standards and/or guidelines to be adopted in line with Commission Decision (EU, Euratom) 2017/46 and its implementing rules C(2017) 8841. These technical standards and guidelines shall be based on industry best practices and are selected to suit the Commission's IT environment.

2. The standard on compliance and related guidelines adopted under Decision C (2006) 3602 of 16 August 2006 is repealed.

4.3. Entry into force

This standard shall enter into force on the twentieth day following the date of its adoption.

Appendix 1: Roles and responsibilities (RASCI)

Role: / Activity:	Head of Commission Department	System Owner	System Manager	LISO	DIGIT	HRDS	ITCB
IT security compliance management	A	R	R(D)[2]	S	S		
IT security inspection	A	S	S(D)[3]	S		R	
IT security compliance review	A	S	S(D)[2]	S	R		
IT security technical compliance review	A	S	S(D)[2]	S	R		
IT security compliance reporting	A	R	R(D)[1]	S	S		I
IT security compliance metrics reporting	A	S	S(D)[2]	S	R		I
IT security exception handling	A	R	R(D)[1]	S	S		

'RASCI' is an abbreviation for a responsibility assignment based on the following attribution indicators:

(a) 'responsible' (R) means having the obligation to act and take decisions to achieve required outcomes;
(b) 'accountable' (A) means being answerable for actions, decisions and performance;

(c) 'supports' (S) means having the obligation to work with the person responsible to complete the task;

(d) 'consulted' (C) means being sought for advice or opinion;

(e) 'informed' (I) means being kept up to date with relevant information.

[2] Delegated Responsibility from the System Owner
[3] Delegated Support from the System Owner