EUROPEAN
COMMISSION

Brussels, 13.12.2017
C(2017) 8841 final

COMMISSION DECISION

of 13.12.2017

laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission

COMMISSION DECISION

of 13.12.2017

laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission

THE EUROPEAN COMMISSION,

Having regard to Commission Decision 2017/46, and in particular Article 13 thereof,

Whereas:

(1) It is necessary to review, update and consolidate the standards and guidelines developed on the basis of Decision C(2006) 3602 and to provide for a new set of rules implementing Decision 2017/46.

(2) The implementing rules related to the scope of this Decision to Commission Decision C(2006) 3602 should therefore be repealed.

(3) This Decision is based on international standards and IT Security good practices including ISO/IEC 27001, 27002, 27005, 27035 and the project methodology PM^2.

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1) The subject matter and scope of this Decision are provided in Article 1 of Decision (EU, Euratom) 2017/46.

2) The provisions in this Decision apply to all communication and information systems (hereafter CIS). However, the responsibilities defined in this Decision shall not apply to CISs handling EU classified information. The relevant responsibilities for these systems shall be determined in line with Decision (EU, Euratom) 2015/444 by the System Owner and the Commission Security Authority.

3) Chapter 2 of this Decision presents an overview of the additional organisation and responsibilities[1] relating to IT security. Chapter 3 presents an overview of the main processes involved in IT security, covering the essential parts of the lifecycle of a CIS. Due to the complexity of the subject matter, this Decision does not include all detailed procedures and rules, which are published in the related IT Security Standards. Additional guidance could be published in some domains as IT Security Guidelines.

Article 2

Definitions

For the purposes of this Decision, in addition to the definitions in Article 2 of Decision (EU, Euratom) 2017/46 the following definitions also apply:

1) 'Business Impact Assessment' or 'BIA' means the activity to identify immediate or future impact of losing security (confidentiality, integrity, availability) on the business of the organisation.
2) 'Exception' means an instance where a decision was taken at appropriate level not to implement a security measure that is based on a rule or on legislation;
3) 'IT asset' means a technical asset as part of an IT system;
4) 'IT asset management inventory' means a repository for information technology installations which holds data relating to the collection of IT assets, as well as descriptive relationships between such assets;
5) 'IT service' means the services provided by an IT system or IT Service Provider to support the functionality or operations of a CIS;
6) 'IT system' means the technical assets of a CIS, that is to say supporting information, hardware, software and/or a network, other digital information handling components or a combination of those, which may be dedicated for one CIS or shared between multiple CISs;
7) 'Outsourced Commission CIS' means a Commission CIS that is housed on non-Commission premises on the basis of a contract with a third party contractor, and includes the outsourcing of individual or multiple CISs or other IT services, data centres on non-Commission premises, and the handling of Commission data sets by external services;
8) 'Outsourced IT System' means an IT system as part of an outsourced Commission CIS.
9) '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.
10) 'Residual risk' means the risk remaining after risk treatment;
11) 'Risk treatment' means the process of mitigating risk, which may include risk avoidance, risk reduction, removing the source of the risk, changing the likelihood of risk, changing the consequences of risk, sharing the risk, and retaining the risk;
12) 'Segregation of duties' means sharing responsibilities within a key process and dispersing the critical functions of that process to more than one person or department.

[1] See Appendix 1 for an overview of the main responsibilities per process.

13) ‘Technical specification’ means the detailed description of a requirement, typically used in the software design process.

CHAPTER 2

ORGANISATION AND RESPONSIBILITIES

Article 3a

Assignment and delegation of roles

The main roles and responsibilities related to the security of communication and information systems are described in the Decision (EU, Euratom) 2017/46. The System Owner, having the overall responsibility for the IT security of the CIS, may delegate part of the IT security operational activities and their associated responsibilities to more specific operational roles. The delegation shall be in line with the principles of segregation of duties and be formally documented. For complex IT systems, multiple instances of those specific operational roles may exist. Ultimately, the System Owner remains responsible for those delegated responsibilities in accordance with Article 9(3) of Decision 2017/46.

Article 3b

The specific operational roles shall be the following:

1) ‘Project Manager’ or ‘PM’: manage the daily progress of the project to deliver the outputs within the agreed constraints;

2) ‘System Manager’ or ‘SM’: manages and/or operates the IT system on behalf of the System Owner and ensures proper access management, backup, logging, monitoring, vulnerability and patch management, and change management;

3) ‘System Security Officer’ or ‘SSO’: advises the System Owner, System Manager and Project Manager on the IT security approach and takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security;

4) ‘System Supplier’ or ‘SS’: implements the technical architecture and security measures of a system based on the IT security requirements, supports in developing those security requirements and performs appropriate security testing;

5) ‘IT Service Provider’ or ‘ITSP’: provides a range of structured and managed IT services.

CHAPTER 3

IT SECURITY PROCESSES

Article 4

IT security governance

1. The governance of IT security is the process of establishing and maintaining a framework to support management structure and processes to provide assurance that IT security strategies are aligned with and support the Commission’s objectives. The effective governance of IT security ensures that the governing body receives relevant reporting - framed in a business context - about IT security-related activities. This enables pertinent and timely decisions about IT security issues in support of the strategic objectives of the Commission.

2. The processes related to governance of IT security shall be carried out through the following:

(a) ‘evaluate’: the governance process that considers the current and planned achievement of security objectives based on current processes and planned changes, and determines where any adjustments are required to optimise the achievement of strategic objectives in the future;

(b) 'direct': the governance process, by which the Governance Body gives direction about the IT security objectives and strategy that needs to be implemented; direction may include changes in prioritisation of activities, and endorsement of policies, material risk acceptance and IT security plans;

(c) 'monitor': the governance process that enables the Governance Body to assess the achievements of strategic objectives;

(d) 'communicate': the bidirectional governance process by which the Governance Body and stakeholders exchange information about IT security, appropriate to their specific needs;

(e) 'assure': the governance process by which the Governing Body commissions independent and objective audits, reviews or certifications which shall identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security.

3. The roles relating to IT security governance shall be defined in accordance with the RASCI model as follows:

(a) the Corporate Management Board (CMB) is responsible[2] for IT security governance and ensures that the necessary IT security governance processes are performed;

(b) the Information Security Steering Board (ISSB) and Directorate-General for Informatics are Responsible for the implementation of the IT security governance processes;

(c) the Directorate-General for Informatics and Directorate-General for Human Resources and Security shall support the ISSB in the implementation of its responsibilities, additionally Human Resources and Security has responsibilities related to the governance process in relation to Article 6 of Decision (EU, Euratom) 2017/46;

(d) the Commission Departments and their Local Information Security Officers (LISO's) shall support the ISSB and the Directorate-General for Informatics in performing their IT security governance responsibilities and shall be consulted where appropriate;

(e) the Commission Departments shall be kept informed.

4. The main activities related to the process of IT security risk management shall be the following:

(a) the Directorate-General for Informatics shall develop and maintain the overall Commission's IT security strategy with long term objectives, including activities to be performed in the years ahead. These activities shall support the Commission's priorities, be prioritised on the basis of past performance reviews, audits and incidents and receive sufficient investment and resources;

(b) the Directorate-General for Informatics shall, in close cooperation with the Directorate-General for Human Resources and Security, support the IT Security Policy, and develop and maintain standards and guidelines aligned with Annex A of the ISO 27001 standard and other corporate frameworks of the Commission. The IT security policy shall be adopted by the Commission based on a recommendation from the ISSB;

(c) the Directorate-General for Informatics shall provide advice and support on the implementation of the IT security policy, as well as on standards and guidelines and offer methodologies, templates and tools;

(d) the ISSB shall respond to IT security performance issues and initiate required actions when the residual risk level is deemed too high;

(e) the ISSB shall monitor the IT security strategy effectiveness, key performance indicators on preventive and reactive measures, the risk landscape, compliance with security policies and significant incidents on a quarterly basis and shall report biannually on these topics to the CMB;

(f) the Directorate-General for Informatics shall report to the ISSB on a quarterly basis on the progress of the implementation and the effectiveness of preventive, detective and corrective IT security measures, as well as on significant IT security threats, exceptions to the security policies, incidents, risks and IT security strategy implementation. On an annual basis, the IT security report shall summarise the threats, IT security incidents, preventive, detective and corrective measures relevant for the previous year, draw conclusions and highlight the future outlook on IT security;

[2] As defined in C(2017)6915.

(g) the Directorate-General for Informatics shall review the IT security policy, standards and guidelines whenever there are significant changes in the organisational or technical environment, in the legal conditions or when new or changing threats are identified. It may recommend changes to the ISSB;

(h) the Directorate-General for Informatics shall monitor the implementation of the IT security policies, standards and guidelines to ensure ongoing compliance. It shall issue annual security evaluation forms or questionnaires on chosen topics of interest that shall be used to update the IT security strategy and IT security policy on those topics;

(i) the Commission Departments and their LISO shall respond to annual security questionnaires and evaluation forms issued by the Directorate-General for Informatics;

(j) the Directorate-General for Informatics shall monitor relevant internal or external trends or developments including threats, vulnerabilities, security techniques or products, insofar as they have an impact on the Commission's IT security policy or IT security strategy;

(k) the ISSB shall evaluate the residual risk levels related to the Commission's CIS as reported by the Directorate-General for Informatics. The ISSB may issue formal recommendations to Heads of Commission Departments in case of persistent failure to properly treat risks and enforce appropriate measures. Those requests shall include targets for residual risk levels and a timeline for remediation.

Article 5

IT security risk management

1. The IT security risk management process shall identify, assess and implement a set of cost-effective security measures for an IT system to reduce risks to an acceptable level. The process shall be applied to all IT systems.

2. The IT security risk management process shall consist of the following phases:

(a) 'context establishment': the external and internal context for IT security risk management is established; it involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organisation operating the IT security risk management;

(b) 'risk assessment': risks are identified, quantitatively or qualitatively described, and prioritised against risk evaluation criteria and objectives relevant to the organisation;

(c) 'risk treatment': controls to reduce, retain, avoid, or share the risks are selected and a risk treatment is defined in the IT security plan;

(d) 'risk acceptance': the decision to accept the risk and the responsibility for the decision are made and are formally recorded;

(e) 'risk monitoring and review': risks and their factors, including values of assets, impact, threats and the likelihood of their occurrence are monitored and reviewed to identify any changes in the context of the organisation at an early stage, and to maintain an overview of the complete risk picture;

(f) risk communication: information about risks is exchanged between decision-makers and other stakeholders.

3. The roles relating to IT security risk management shall be the following, in accordance with the RASCI model:

(a) the Head of a Commission Department shall be accountable for IT security risk management;

(b) the System Owner shall be responsible for IT security risk management, but may delegate certain responsibilities;

(c) the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall take delegated responsibility for the activities in this process;

(d) the LISO and the Data Owner shall provide support and be consulted;

(e) the Directorate-General for Informatics shall provide support and be consulted;

(f) the Commission Departments shall be kept informed;

(g) the System Suppliers, if the appropriate powers are delegated to them by the System Owner, support the System Owner to perform the IT security risk management process.

4. The main activities related to the process of IT security risk management shall be the following:

(a) as part of the IT risk assessment, the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall perform, in collaboration with the relevant stakeholders, in particular the Data Owner or other linked System Owners, a business impact assessment to identify the IT security needs based on the required levels of confidentiality, integrity and availability of the IT system. Security measures shall be selected to mitigate identified risks, be aligned with the business needs of the IT system and comply with rules and legislation;

(b) the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall draw up security plans that shall contain the key output of the IT risk management process, in particular, the IT security needs, IT security measures and selection rationale, residual risks, risk acceptance criteria and exceptions with a timespan of their validity;

(c) the System Owner shall formally approve the security plans and residual risks; the residual risks shall be formally accepted by the Head of the Commission Department concerned while using criteria documented in the security plan; major residual risks shall be escalated to the ISSB and may have to be flagged in the Directorate-General's Annual Activity Report;

(d) the System Owner shall monitor and review at least once a year, the IT security needs and risk assessments' results, the residual risks, exceptions and the identified acceptable levels of risks, taking into account changes to the organisation, technology, business objectives and processes, identified threats, effectiveness of the implemented security measures and external events, such as changes to the legal, contractual or regulatory environment or changes in the Commission's IT security policy. The security plan must be updated accordingly after each major change;

e) the System Owner shall report on the IT risk management process to the Directorate-General for Informatics in order to enable that Directorate-General to assess the IT risk management methods and identify potential improvements;

(f) the Directorate-General for Informatics shall provide guidance and coaching on risk assessments and on the creation of security plans to facilitate compliance with the IT security policy and standards and support the System Owners in managing IT security risks;

(g) the Directorate-General for Informatics shall monitor Commission-wide IT security risks and IT security measures implemented and report to the ISSB on a quarterly basis and System Owners shall communicate the information required for the Directorate General of Informatics to report to the ISSB in a timely manner.

Article 6

Secure IT operations

1. Secure IT operations management shall comprise planning and sustaining the day-to-day processes for maintaining the security of the Commission's IT environments.

2. The roles relating to secure IT operations shall be the following, in accordance with the RASCI model:

(a) the Head of a Commission Department shall be accountable for secure IT operations;

(b) the System Owner shall be responsible for secure IT operations, but may delegate responsibilities to the System Manager and the IT Service Provider;

(c) the System Manager and IT Service Provider, if the appropriate powers are delegated to them by the System Owner, shall take delegated responsibility for the activities in the secure IT operations management process;

(d) the Directorate-General for Informatics and the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall be consulted and the Commission Departments shall be kept informed about it.

3. The main activities related to the secure IT operations management process shall be the following:

(a) the System Owner shall identify responsibilities and priorities for managing the operation and continuous improvement of security measures, taking into account the business impact of their system, and the Commission Department's budget and priorities;

(b) the System Manager and the IT Service Provider, if the appropriate powers are delegated to them by the System Owner, shall implement the operational IT security measures identified for the IT system in the IT security plan, and in particular perform and test backups according to agreed schedules, system monitoring and logging as well as vulnerability and patch management;

(c) the System Manager, if the appropriate powers are delegated to him by the System Owner, may request an exception to the planned measures if approved by the System Owner and if the related residual risk is formally accepted by the Head of Commission Department; this shall be documented in the security plan;

(d) the System Owner shall formally approve the implementation of the IT security plan before the IT system is taken into production based on predefined acceptance criteria;

(e) the System Manager, if the appropriate powers are delegated to him by the System Owner, shall:

(i) manage the operation of the IT system on behalf of the System Owner. The System Manager, if the appropriate powers are delegated to him by the System Owner, may manage the specific IT security measures directly, or subcontract the management to an IT Service Provider; in the latter case, the System Manager shall conclude a formal agreement with the IT Service Provider to ensure that the security measures for which they are responsible are implemented;

(ii) ensure IT asset registration is done and kept up to date in the relevant IT asset management inventory;

(iii) maintain a register of user access rights including approvals, enforce and monitor access control mechanisms and review access periodically, in particular privileged access;

(iv) ensure that logging and monitoring solutions are in place and relevant security logs and alerts are shared with the Directorate-General of Informatics if requested.

Article 7

IT security incident management

1. IT security incident management shall aim at minimising the direct negative impact of IT security incidents by detecting, stopping and containing, eradicating, analysing and reporting, and following them up; to that effect related artefacts and evidence are collected and handled.

2. The IT security incident management process shall consist of the following five distinct phases:

(a) 'prepare and plan': the process phase by which an organisation completes a number of preparatory activities after the necessary planning to put in operational use an efficient and effective IT security event and incident management process;

(b) 'detect and report': the process phase that involves the detecting of, collecting information associated with, and reporting on, occurrences of IT security events, by human or automatic means;

(c) 'assess and decide: the process phase that involves assessing information associated with the occurrence of IT security events and making a decision in the event of an IT security incident;

(d) 'respond' is the process phase that involves the implementation of responses to IT security incidents in accordance with the actions agreed in the assessment and decision phase;

(e) 'lessons learnt': the process phase that follows when IT security incidents have been resolved or closed, involving learning lessons from how incidents have been handled and dealt with.

3. The roles relating to IT security incident management shall be the following, in accordance with the RASCI model:

(a) the Head of a Commission Department shall be accountable for IT security incident management;

(b) the System Owner and the Directorate-General for Informatics shall be responsible for IT security incident management; the System Owner may delegate responsibility to IT Service Providers;

(c) the System Manager and the System Security Officer, if the appropriate powers are delegated to them by the System Owner, shall support the System Owner. The LISO shall be consulted and informed where appropriate and within a reasonable amount of time;

(d) the ISSB and the Commission Departments shall be kept informed;

(e) the Directorate-General for Human Resources and Security shall be informed and shall be responsible and accountable for forensic analysis regarding cyber security, formal inquiries and relations with law enforcement and intelligence services as provided for in Article 15(2) of Decision 2017/46. The System Manager, the LISO, the Directorate-General for Informatics and the IT Service Providers shall support the Directorate-General for Human Resources and Security in these activities.

4. The main activities related to the IT security incident management process shall be the following:

(a) the System Owner shall provide information and support to handle IT security incidents;

(b) the Directorate-General for Informatics shall take the lead in handling all IT security incidents for those IT systems that are not outsourced and shall in its role as the internal incident management IT Service Provider:

(i) maintain tools and procedures for incident handling (detection, triage, analysis, response);

(ii) assess incidents and make decisions about how they are to be addressed by categorising and prioritising incidents;

(iii) respond to incidents, i.e. investigate them and contain them;

(iv) identify lessons to be learned from incidents.

(c) all access to information in IT systems for the purposes of IT security incident management shall be proportionate to the severity of the IT security incident concerned and compliant with the principles laid down in Regulation (EC) No 45/2001 of the European Parliament and of the Council and with the principle of professional secrecy;

(d) all personnel involved in the IT security incident management process shall receive prior and adequate training in the relevant procedures;

(e) the Directorate-General for Informatics may access, acquire and process relevant information held in IT systems when necessary for the IT security incident management process in accordance with the following:

(i) for sensitive non-classified information, explicit prior approval shall be obtained from the System Owner or the Head of the Commission Department concerned;

(ii) for access to user information or Commission information stored on end user devices, such as e-mails or documents, prior approval shall be obtained from end users on a case-by-case basis;

(iii) for access to other information, including system log files, operating system files, system configuration information and potentially suspicious executable file, approval shall not be required.

(f) the Directorate-General for Informatics shall lay down detailed procedures for IT security incident management that shall provide for a transparent audit trail, appropriate management supervision and security measures to ensure the confidentiality of any information acquired during and after the handling of IT security incidents. The audit trail shall be available for consultation by the System Owner of the affected CIS;

(g) information that is accessed, acquired or processed during an IT security incident response shall not be used for any other purpose and shall not be shared with any other party without authorisation from the Data Owner, except the Security Directorate of the Directorate-General for Human Resources and Security, IDOC and OLAF;

(h) the LISO, the SSO, the System Manager, the Data Owner and the Data Protection Coordinator shall support the incident management process.

Article 8

Secure IT system development and acquisition

1. IT security shall be sufficiently considered in the development or acquisition of all IT systems and shall be built into every phase of the IT System Development Lifecycle, including system conception, design and development, build and construction, testing, deployment, ongoing maintenance and distribution.

2. The roles relating to secure IT system development and acquisition shall be the following, in accordance with the RASCI model:

(a) the Head of a Commission Department shall be accountable for secure IT system development;

(b) the System Owner shall be responsible for secure IT system development, but may delegate responsibilities to the Project Manager and the System Supplier;

(c) the System Security Officer, if the appropriate powers are delegated to him by the System Owner, and the Directorate-General for Informatics shall support the System Owner;

(d) the Commission Departments shall be kept informed.

3. The main activities related to the secure IT system development and acquisition process shall be the following:

(a) the System Owner shall bear responsibility for the specification of IT security requirements;

(b) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall ensure the specification of the IT security requirements on the basis of the IT security needs as identified in the business impact assessment and shall apply the security measures based on the Commission's standards and other regulations and legislation;

(c) the System Owner shall approve the IT security requirements as part of the security plan approval;

(d) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall:

(i) ensure that the security measures are implemented in the IT system or in the infrastructures that support it, whether local or centralised;

(ii) ensure that the design, installation and implementation of the system are in accordance with the IT security requirements of the IT system and the IT security standards;

(iii) bear responsibility for the deployment and hand-over of the IT system to the System Owner;

(iv) evaluate the cost of the required IT security measures and may request not to implement measures if approved by the System Owner and if the related residual risk is formally accepted by the Head of Commission Department; these expectations shall be documented in the security plan.

(e) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall provide operating manuals and instructions for the System Manager;

(f) the Directorate-General for Informatics shall provide recommended tools and services to help development teams to identify and assess source code vulnerabilities in the earliest stages of the development life cycle;

(g) the Directorate-General for Informatics shall provide secure development guidelines, including fundamental practices to support developers in their day-to-day work with the aim of avoiding security weaknesses in the early stages of the system's development;

(h) when an IT system is acquired from a third party (Commercial Off-The-Shelf), the functionality and security of the system shall be assessed against the IT security requirements and the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall provide assurance on the quality of the development process;

(i) when an IT system is developed for the Commission, the following activities shall be performed:

(i) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall define the technical architecture and draw up technical specifications for the implementation of the IT security requirements as defined by the Project Manager, if the appropriate powers are delegated to him by the System Owner;

(ii) the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall support the specification of IT security requirements, the definition of IT security architecture, and the implementation and verification of security measures during the IT project;

(iii) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall construct and ensure the development of the IT system in accordance with the IT security requirements;

(iv) the Project Manager, if the appropriate powers are delegated to him by the System Owner, shall ensure that a secure system development lifecycle is applied and that the necessary IT Security clauses are included in contracts with external parties;

(v) the System Supplier, if the appropriate powers are delegated to him by the System Owner, shall ensure good quality by performing code reviews and security tests of applications prior to their deployment in production.

Article 9

IT security training, awareness and communication

1. IT security is as much a human issue as it is a technology issue. IT security training, awareness and communication shall:

(a) determine the necessary competences of individuals working within their remit that affects the IT security performance of the Commission;

(b) ensure that these individuals are competent on the basis of appropriate education, training, or experience;

(c) take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, where applicable;

(d) retain appropriate documented information as evidence of competence;

(e) ensure awareness of:

(i) the IT security policy;

(ii) these individuals contribution to the effectiveness of improvements in IT security performance;

(iii) the implications of not conforming to the IT security policy.

(f) communicate appropriately and in a timely manner, both internally and externally with relevant stakeholders and target groups, using suitable content and defined processes, communication channels and spokespersons.

2. The roles relating to IT security training, awareness and communication shall be the following, in accordance with the RASCI model:

(a) the Commission Departments shall be accountable for IT security training, awareness and communication;

(b) the Directorate-General for Informatics and the Directorate-General for Human Resources and Security shall be responsible for performing the activities in this process;

(c) the LISOs shall be consulted and shall support the Directorate-General for Informatics in this process;

(d) the ISSB shall be kept informed of the process.

3. The main activities related to the IT security training, awareness and communication process shall be the following:

(a) the Directorate-General for Informatics shall define the training needs and coordinate training programmes on IT security in cooperation with the Directorate-General for Human Resources and Security;

(b) the Directorate-General for Informatics shall organise IT security trainings both online and offline in cooperation with the Directorate-General for Human Resources;

(c) the Directorate-General for Informatics shall coordinate awareness-raising activities on IT security in close cooperation with the Directorate-General for Human Resources, targeting different audiences such as management, IT professionals and users within the Commission;

(d) the Directorate-General for Informatics shall coordinate communication to ensure that System Owners, Data Owners and other roles with IT security responsibilities in Commission Departments are made aware of the IT security policy, standards and guidelines and shall maintain a corporate website dedicated to IT security;

(e) the Directorate-General for Informatics shall organise regular meetings of the LISO network and support LISOs in carrying out their duties where coordination and exchange of information and best practice between security stakeholders shall take place;

(f) the Commission Departments shall organise specific awareness-raising or training activities for all personnel, in collaboration with the Directorate-General for Human Resources and Security and the Directorate-General for Informatics and they shall ensure alignment between local IT security information and corporate IT security information;

(g) the Commission Departments shall ensure and monitor that the System Owner, Data Owner, System Manager, System Security Officer, LISO and Project Manager have a sufficient level of IT security awareness and training to perform their assigned duties;

(h) the Commission Departments shall ensure that users take at least one training session or follow one awareness activity on IT security every three years and that all new staff take IT security induction training when joining the Commission; all training, awareness and communication activities related to IT security shall be performed in close cooperation with Directorate-General for Informatics.

Article 10

IT security compliance and continuous improvement

1. IT security compliance and continuous improvement shall involve the proper implementation and regular update of IT security policy, IT security standards and IT security plans to meet the changing needs of the Commission. This process is there to ensure the recurring activities to enhance performance of the implementation of IT Security.

2. The roles relating to IT security compliance and continuous improvement shall be the following, in accordance with the RASCI model:

(a) the Head of Commission Department shall be accountable for IT security compliance and continuous improvement;

(b) the System Owner, the Directorate-General for Informatics and the LISO are responsible for performing the activities in this process;

(c) the System Security Officer, if the appropriate powers are delegated to him by the System Owner, shall support the process and be consulted and the ISSB shall be kept informed.

3. The main activities associated with the IT security compliance and continuous improvement process shall be the following:

(a) the System Owner shall ensure continuous improvement for activities within his responsibility;

(b) the System Owner shall take into account lessons learnt from the experience of past IT security incidents and where appropriate, the Directorate-General for Informatics shall organise 'lessons-learnt' sessions with the relevant stakeholders, in particular those involved in IT risk management; the goal of those sessions shall be to identify ways to improve the existing security controls or processes in order to prevent or reduce the impact of future incidents;

(c) the System Owner shall monitor compliance with the Commission IT security policies and standards, in order to detect errors or potential breaches of compliance, to take appropriate corrective or preventive action and to assess the effectiveness and efficiency of the action taken; System Suppliers and IT Service Providers, if the appropriate powers are delegated to them by the System Owner, shall provide assurance to the System Owner of their compliance with the IT security policy;

(d) the Directorate-General for Informatics shall verify the implementation of the Commission IT security policy on the basis of information in the IT security plans, the results of the annual IT security questionnaires and evaluation forms, exception reports, identified and reported IT security incidents and other relevant information; System Owners shall communicate to the Directorate-General for Informatics in a timely manner the information required to perform those activities;

(e) the LISO shall inform the Directorate-General for Informatics about any findings which may require changing or improving the Commission IT security policy, standards and guidelines.

(f) The ISSB may request the Internal Audit Service to perform IT security audits on the Commission's CIS if it deems it necessary.

CHAPTER 4

MISCELLANEOUS AND FINAL PROVISIONS

Article 11

Transparency

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

Article 12

Standards

1. The provisions of this Decision shall, where necessary, be further detailed in standards and/or guidelines to be adopted in line with Decision (EU, Euratom) 2017/46. IT security standards and guidelines shall provide further details on these implementing rules and Decision (EU, Euratom) 2017/46 for specific security domains according to ISO 27001:2013 Annex A. These standards and guidelines are based on industry best practices and are selected to suit the Commission's IT environment.

2. Standards shall, where necessary, be developed according to ISO 27001:2013 Annex A in the following domains:

1. Organisation of information security
2. Human resources security
3. Asset management
4. Access control
5. Cryptography
6. Physical and environmental security
7. Operational security
8. Communications security
9. System acquisition, development and maintenance
10. Supplier relationships
11. Information security incident management
12. Information security aspects of business continuity management
13. Compliance

3. Additional technical standards or technical guidelines that focus on more specific aspects of IT security shall, where necessary, be developed.

4. The ISSB shall approve the standards referred to in paragraph 1 and 2 of this Article before their adoption.

5. The implementing rules to Commission Decision C(2006) 3602 related to the scope of this Decision are hereby repealed.

6. The standards and guidelines adopted under Decision C(2006) 3602 of 16 August 2006 shall remain in effect, insofar as they do not conflict with these implementing rules, until they are repealed or replaced by standards or guidelines to be adopted under Article 13 of Decision (EU, Euratom) 2017/46.

Article 13

Entry into force

This Decision shall enter into force on the twentieth day following that of its adoption.

Done at Brussels, 13.12.2017

For the Commission

Gertrud Ingestad
Director -General

Appendix 1: Roles & Responsibilities (RASCI)

Role: / Process:	ISSB	Commission Departments	System Owner	System Manager	System Supplier	IT Service Provider	Project Manager	System Security Officer	LISO	DIGIT[3]	HR(DS)[4]	CMB
IT Security Governance	R	C/S/I							C/S	R	S	R[5]
IT Security Risk Management		A/I	R					R(D)[1]	C/S/I	C/S		
Security IT Operations		A/I	R	R(D)[6]		R(D)[4]		C		C		
IT Security Incident Management	I	A/I	R	S		R(D)[4]		S	C/S	R	I[7]	I
Secure IT System Development and Acquisition		A/I	R		R(D)[4]		R(D)[4]	S		S		
IT Security Training, Awareness and Communication	I	A/I							C/S	R	R	
IT Security Compliance and Continuous Improvement	I	A/I	R	S	S	S		C/S	R	R		

[3] Directorate-General for Informatics
[4] Directorate-General for Human Resources and Security
[5] As defined in C(2017)6915.
[6] R(D) is Delegated responsibility by the System Owner.
[7] HR.DS has additional responsibilities regarding forensic analysis, formal inquiries and relations with law enforcement and intelligence services as defined in 2017/46 Article 15.2.