Council of the European Union
General Secretariat

Brussels, 11 September 2024

WK 10603/2024 INIT

LIMITE

CSC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Security Committee
Subject:	Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union – concept paper on Risk Management provisions

1. At its last meeting on 11 July, the Council Security Committee (CSC) decided to start the examination of the EUCI related articles within the review of the Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union ('the Proposal', doc. 7760/22) at the next meeting on 19 September.

2. In **Annex I** to this concept paper delegations will find the main provisions of the Proposal related to Risk Management (Article 4, 5, 21, 44) and in **Annex II** the proposed definitions (Article 3 on Definitions).

3. The main provisions relating to Information Security Risk Management are covered in *Article 5 Information Security Risk Management process of Chapter 1 - General provisions*, and specifically in the area of EUCI in *Article 21 EUCI Security Risk Management process of Chapter 5 EUCI Section 1 - General Provisions*.

4. The GSC considers that most of the provisions of Article 21 are actually not specific to EUCI and proposes to cover them in Articles 4 and 5, in order that they apply to **both non-classified information and EUCI**.

5. Moreover, the GSC proposes to use **the concept agreed in the context of the review of the Council Security Rules (cf. ST 8852/24) and adjust or complement the provisions relating to the Information Security Risk Management in this Proposal**.

6. Delegations are invited to discuss the following questions at the next CSC meeting on 19 September 2024:

   a) Should provisions on Risk Management in the Proposal be the same for both non-classified and classified information (and if not, what should remain specific for classified information)?

   b) Should the concept agreed on Risk Management within the CSR review be used to adjust or complement the relevant provisions of the proposal?

ANNEX I

Provisions concerning Risk Management in the Proposal

Article 4 **General Principles**
1. Each Union institution and body shall be responsible for the implementation of the provisions of this Regulation within its organisation taking account of its own information security risk management process. 2. For each communication and information system under their responsibility, the Union institutions and bodies shall identify the highest confidentiality level that such communication and information system can handle and store, carry out an information security risk assessment and regularly monitor the security needs and the correct implementation of the identified protective measures.
Article 5 **Information security risk management process**
1. Each Union institution and body shall establish an information security risk management process for the protection of the information they handle and store. 2. The information security risk management process shall include the following steps: (a) threat and vulnerability identification; (b) risk assessment; (c) risk treatment; (d) risk acceptance; (e) risk communication. 3. The information security risk management process shall take account of all factors relevant for the institution or body concerned, in particular: (a) the confidentiality level of the information and the related legal obligations; (b) the form and the quantity of the information and the facilities or CISs where the information is handled and stored; (c) the persons accessing the information on sites or remotely;

(d) the surrounding environment and the structure of the buildings or areas storing the information,

(e) the threats targeting the Union, the Union institutions and bodies or the Member States from cyberattacks, supply chain attacks, espionage, sabotage, terrorist, subversive or other criminal activities;

(f) business continuity and disaster recovery;

(g) the results of inspections, audits or assessment visits, where applicable.

Article 21

EUCI security risk management process

1. The security Authority of each Union institution and body shall approve the security measures for protecting EUCI throughout its life-cycle in accordance with the outcome of a risk assessment performed by the respective Union institution or body.
2. The security measures taken by each Union institution and body shall be commensurate with the classification level of the information handled and stored, its form and volume, and the location and protective features of the facilities where EUCI is handled and stored and the locally assessed threat of malicious or criminal activities.
3. All Union institutions and bodies shall establish:

   (a) contingency plans to ensure EUCI security during emergencies;

   (b) business continuity plans including preventive and recovery measures to minimise the impact of major failures or security incidents on the handling and storage of EUCI.

Article 44

Accreditation process of a CIS handling and storing EUCI

1. All CISs handling and storing EUCI shall undergo an accreditation process, based upon the principles of information assurance, the level of detail of which shall be commensurate with the level of protection required.
2. The accreditation process shall result in an accreditation statement determining the maximum classification level of the information that may be handled and stored in a CIS as well as the corresponding terms and conditions. The accreditation statement shall be based on the formal validation of the risk assessment and of the security measures implemented for the CIS concerned, providing assurance on the following elements:

(a) the information security risk management process has been properly carried out;

(b) the system owner or risk owner has knowingly accepted the residual risk;

(c) a sufficient level of protection of the CIS, and of the EUCI handled and stored in it, has been achieved in accordance with this Regulation.

ANNEX II

Definitions concerning Risk Management in the Proposal	
Information security risk management process	The entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of the systems it uses; it covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication.
Asset	Anything that is of value to a Union institution or body, its operations and their continuity, including information resources that support their mission.
System Owner	The individual responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of a communication and information system.
Threat to information security	An event or agent that can reasonably be expected to adversely affect information security if not responded to and controlled.
Vulnerability	A weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by one or more threats.
Risk	The potential adverse effect of a given threat, possibly exploiting internal and external vulnerabilities of a Union institution or body or of the systems it uses, causing harm to the legitimate public and private interests, measured as a combination of the likelihood of threats occurring and their impact.
Residual risk	The risk which remains after security measures have been implemented.
Risk assessment	Identifying threats and vulnerabilities and conducting the related risk analysis, there is to say the analysis of probability and impact.
Risk treatment	Mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.
Defence in depth	A type of security which uses several independent layers of security controls to ensure that where one fails another will be operative.