**DECISION No GB/2023/12**
**of the Governing Board of**
**the European Cybersecurity Competence Centre**

**on the Internal Control Framework**
**for effective management applicable to the**
**European Cybersecurity Competence Centre**

The GOVERNING BOARD,

Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (hereinafter "the constituent act" and "ECCC");

Having regard to Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (hereinafter "Financial Regulation);

Having regard to the Governing Board Decision No/2023/1 on ECCC Financial Rules (hereinafter "ECCC Financial Rules"), and in particular Article 5, 30, 45(2), 48(1)(v) thereof;

Having regard to the Communication to the Commission from Commissioner Oettinger on the Revision of the Internal Control Framework, adopted by the European Commission on 19 April 2017,

Whereas:

1) According to subparagraph (u) of paragraph (2) of Article 17 of the constituent act, the Executive Director shall establish and ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board.
2) Article 30 of the ECCC Financial Rules determines that internal control shall be applied at all levels of management and shall be designed to provide reasonable assurance of achieving five internal control objectives namely (1) effectiveness, efficiency and economy of operations; (2) reliability of reporting; (3) safeguarding of assets and information; (4) prevention, detection, correction and follow-up of fraud and irregularities; (5) adequate management of the risks related to the legality and regularity of the underlying transactions, taking into account the multiannual character of the programmes as well as the nature of the payments concerned.
3) Article 48 of the ECCC Financial Rules states that the Executive Director has the obligation to sign a declaration of assurance in the Annual Activity Report in which he/she states that he/she can provide reasonable assurance that the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.
4) To fulfil these obligations, the ECCC needs to adopt its Internal Control Framework in line with the requirements mentioned above.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

**Article 1**

1. The ECCC's Internal Control Framework in the Annex of this Decision is adopted.

2. The internal control components and principles set out in the Annex of this Decision constitute the minimum standards referred to in Article 45(2) of the ECCC Financial Rules.

3. The Executive Director shall implement this Decision when it enters into force. He/she shall ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board. He/she shall conduct an overall assessment of the presence and functioning of all internal control framework at least once a year in the context of the Annual Activity Report.

**Article 2**

1. This Decision shall enter into force on the date of its adoption.

Done at Bucharest, 6 December 2023

For the European Cybersecurity Industrial,
Technology and Research Competence Centre

*(e-signed)*

Pascal Steichen

Chairperson of the Governing Board

**Annex**
**to the Governing Board Decision of the Governing Board of the European Cybersecurity Competence Centre**

**on the Internal Control Framework for effective management applicable to the European Cybersecurity Competence Centre**

## Scope

The ECCC Internal Control Framework is implemented by adopting, *mutatis mutandis,* the framework of the European Commission which was revised in 2017[1] with a view to align the Commission standards to the international standards set by the Committee of Sponsoring Organizations (COSO) framework.

It is a principle-based system consisting of five Internal Control Components and 17 Internal Control Principles. Its aim is to ensure robust internal controls with the necessary flexibility to adapt to specific characteristics and circumstances of the ECCC.

**Components**: the components are the building blocks that underpin the structure of the framework. They are interrelated and must be present and functioning at all levels of ECCC for internal control to be considered effective.

**Principles**: Each component consists of several principles. Working with these principles helps to provide reasonable assurance that ECCC's objectives have been met. The principles specify the actions required for the internal control to be effective.

**Characteristics of each principle**: The characteristics are based on the characteristics of the Commission's Internal Control Framework, but have been defined in such way as to take into account the specific Governance arrangements and the specific situation of ECCC. There is no requirement for the ECCC to assess whether each individual characteristic is in place. The characteristics have been defined to assist management in implementing internal control procedures and in assessing whether the principles are present and functioning.

Characteristics of each principle have been included to help to define the principles.

[1] C(2017) 2373 final

# Design of the Internal Control Framework

| Internal Control Components | Internal Control Principles |
|---|---|
| CONTROL ENVIRONMENT | 1. The ECCC demonstrates commitment to integrity and ethical values |
| | 2. ECCC Management exercises oversight responsibility of the development and performance of internal control |
| | 3. ECCC Management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives |
| | 4. The ECCC demonstrates commitment to attract, develop and retain competent individuals in alignment with objectives |
| | 5. The ECCC holds individuals accountable for their internal control responsibilities in the pursuit of objectives |
| RISK ASSESSMENT | 6. The ECCC specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives |
| | 7. The ECCC identify risks to the achievement of its objectives across the organisation and analyse risks as a basis for determining how the risks should be managed |
| | 8. The ECCC considers the potential for fraud in assessing risks to the achievement of objectives |
| | 9. The ECCC Identifies and analyses change that could significantly impact the internal control system |
| CONTROL ACTIVITIES | 10. The ECCC selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels |
| | 11. The ECCC selects and develops general control over technology to support the achievement of objectives |
| | 12. The ECCC deploys control activities through policies that establish what is expected and in procedures that put policies into action |
| INFORMATION AND COMMUNICATION | 13. The ECCC obtains or generates and uses relevant quality information to support the functioning of internal control |
| | 14. The ECCC communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control |
| | 15. The ECCC communicates with external parties about matters affecting the functioning of internal control |
| MONITORING ACTIVITIES | 16. The ECCC selects,,develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning |
| | 17. The ECCC assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management, as appropriate |

# Components and Principles

**1.** First Component: Control Environment

The Control Environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ECCC. The ECCC Management sets the tone at the top with respect to the importance of the internal control, including expected standards of conduct.

**1.1 Principle 1**: The ECCC demonstrates commitment to integrity and ethical values

Characteristics:

- Tone at the top: The Executive Director and all management levels respect integrity and ethical

values in their instructions, actions and behaviour.

- Standards of conducts: The ECCC's expectations on integrity and ethical values are set out in standards of conduct and understood at all levels of the organisation, as well as by entrusted bodies, outsourced service providers and beneficiaries.
- Alignment with standards: Processes are in place to assess whether individuals and departments are aligned with the ECCC's expected standards of conduct and to address deviations in a timely manner.

**1.2 Principle 2**: ECCC's Management exercises oversight responsibility of the development and performance of internal control.

Characteristics:

- The ECCC's Executive Director oversees the development and performance of internal control. She/he is supported in this task by the Internal Control Coordinator.
- In his/her capacity as Authorising Officer, ECCC's Executive Director provides a Declaration of Assurance on the appropriate allocation of resources and their use for their intended purpose and in accordance with the principles of sound financial management, as well as on the adequacy of the control procedures in place (see Appendix 2).
- The Internal Control Coordinator, in charge of risk management and internal control, plays a key role by coordinating the preparation of the ECCC Annual Activity Report. In this context, he/she signs a declaration taking responsibility for the completeness and reliability of management reporting (Appendix 3). This declaration covers both the state of internal control in the ECCC and the robustness of reporting on operational performance. However, responsibility for achieving operational objectives remains with the relevant operational unit.
- Each Head of unit oversees the internal control systems within their unit. Each Head of unit oversees the development and performance of internal control and is supported in this task by designated staff in charge of risk management and internal control.
- Assurance cascading process. To reinforce the assurance cascading process, each manager signs a declaration of assurance in which he/she reports on the use of his/her respective budgetary powers and related use of resources. This cascading declaration includes information both on the state of internal controls in his/her area of responsibility and the soundness of reporting on operational performance.

**1.3 Principle 3**: ECCC's Management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Characteristics:

- Management structures are comprehensive. The design and implementation of management and supervision structures cover all policies, programmes and activities. In particular, for spending programmes, they cover all expenditure types, delivery mechanism to support the achievement of policy, operational and control objectives.
- Authorities and responsibilities. The Executive Director, as appropriate, delegate authority and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the ECCC.
- Reporting lines. The Executive Director designs and evaluates reporting lines within departments to enable the execution of authority, fulfilment of responsibilities, and flow of information.
-

**1.4 Principle 4**: The ECCC demonstrates commitment to attract, develop and retain competent individuals in alignment with objectives

Characteristics:

- Competence framework. The Executive Director defines the competences necessary to support the achievement of objectives and regularly evaluate them across the ECCC, taking action to address shortcomings where necessary.
- Professional development. The Executive Director and Head of Units provide the training and coaching needed to attract, develop, and retain a sufficient number of competent staff.
- Mobility: The Executive Director and Head of Units promote and plan staff mobility so as to strike the right balance between continuity and renewal.
- Succession planning and deputising arrangements for operational activities and financial transactions are in place to ensure continuity of operations.

**1.5 Principle 5**: The ECCC holds individuals accountable for their internal control responsibilities in the pursuit of objectives

Characteristics:

- Enforcing accountability. The ECCC defines clear roles and responsibilities and holds individuals and entrusted entities accountable for the performance of internal control responsibilities across the organisation and for the implementation of corrective action as necessary.
- Staff appraisal. Staff efficiency, abilities and conduct in the service are assessed annually against expected standards of conduct and set objectives. Cases of underperformance are appropriately addressed.
- Staff promotion. Promotion is decided after consideration of the comparative merits of eligible staff taking into account, in particular, their appraisal reports.

## 2. Second Component: Risk Assessment

Risk assessment is a dynamic and iterative process for identifying and assessing risks which could affect the achievement of objectives, and for determining how such risks should be managed.

**2.1 Principle 6**: The ECCC specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

Characteristics:

- Mission. The ECCC and units have up-to-date mission statements that are aligned across all hierarchical levels, down to the tasks and objectives assigned to individual staff members. Mission statements are aligned with the body's responsibilities set in the legal base.
- Objectives are set at every level. ECCC's objectives are clearly set and updated when necessary (e.g. significant changes in priorities, activities and/or the organigram). They are consistently filtered down from the level of the Executive Director to the various levels of the organisation, and are communicated and understood by management and staff.
- Objectives are set for the most significant activities. Objectives[2] and indicators[3] cover the ECCC's most significant activities that contribute to the delivery of the ECCC's priorities or other priorities relating to the core business, as well as operational management. Setting objectives and performance indicators make it possible to monitor progress towards their achievement.
- Objectives form the basis for committing resources. The Executive Director uses the objectives set as a basis for allocating available resources as needed to achieve policy, operational and financial performance goals.

[2] Objectives must be SMART (specific, measurable, achievable, relevant and time-framed).
[3] Indicators must be RACER (relevant, accepted, credible, easy to monitor and robust).

- Financial reporting objectives. Financial reporting objectives are consistent with the accounting principles applicable in the ECCC.
- Non-financial reporting objectives. Non-financial reporting provides management with accurate and complete information needed to manage the organisation at Executive Director and unit level.
- Risk tolerance and materiality. When setting objectives, management defines the acceptable levels of variation relative to their achievement (tolerance for risk) as well as the appropriate level of materiality for reporting purposes, taking into account cost-effectiveness.
- Monitoring. Setting objectives and performance indicators make it possible to monitor progress towards their achievement.

**2.2 Principle 7**: The ECCC identifies risks to the achievement of its objectives across the organisation and analyse risks as a basis for determining how the risks should be managed

Characteristics:

- Risk identification. The ECCC identifies and assesses risks at the various organisational levels analysing internal and external factors. Management and staff are involved in the process at the appropriate level.
- Risk assessment. The ECCC estimates the significance of the risks identified and determines how to respond to significant risks considering how each one should be managed and whether to accept, avoid, reduce or share the risk. The intensity of mitigating controls is proportional to the significance of the risk.
- Risk identification and risk assessment are integrated into the annual activity planning and are regularly monitored.

**2.3 Principle 8**: The ECCC considers the potential for fraud in assessing risks to the achievement of objectives

Characteristics:

- Risk of fraud. The risk identification and assessment procedures (see principle 7) consider possible incentives, pressures, opportunities and attitudes which may lead to any type of fraud, notably fraudulent reporting, loss of assets, disclosure of sensitive information and corruption.
- Anti-fraud strategy. The ECCC sets up and implements measures to counter fraud and any illegal activities affecting the financial interests of the EU and of the ECCC. The ECCC does this by putting in place a sound anti-fraud strategy to improve the prevention, detection and conditions for investigating fraud, and to set out reparation and deterrence measures, with proportionate and dissuasive sanctions.

**2.4 Principle 9**: The ECCC identifies and analyses changes that could significantly impact the internal control system

Characteristic:

- Assess changes. The risk identification process considers changes in the internal and external environment, in policies and operational priorities, as well as in management's attitude towards the internal control system.

## 3. Third Component: Control Activities

Control activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.

**3.1 Principle 10**: The ECCC selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels

Characteristics:

- Control activities are performed to mitigate the identified risks and are cost-effective. They are tailored to the specific activities and risks of each unit and their intensity is proportional to the underlying risks.
- Control activities are integrated in a control strategy. The control strategy includes a variety of checks, including supervision arrangements, and where appropriate, should include a balance of approaches to mitigate risks, considering manual and automated controls, and preventive and detective controls.
- Segregation of duties. When putting in place control measures, management considers whether duties are correctly divided between staff members to reduce risks of error and inappropriate or fraudulent actions.
- Business continuity plans based on a business impact analysis following corporate guidance are in place, up-to-date and used by trained staff to ensure that ECCC is able to continue working to the extent possible in case of a major disruption. Where necessary, business continuity plans must include coordinated and agreed disaster recovery plans for time-sensitive supporting infrastructure (e.g. IT systems).

**3.2 Principle 11**: The ECCC selects and develops general control over technology to support the achievement of objectives

Characteristics:

- Control over technology. In order to ensure that technology used in business processes, including automated controls, is reliable, and taking into account the overall corporate processes, the ECCC management selects and develops control activities over the acquisition, development and maintenance of technology and related infrastructure.
- Security of IT systems. The ECCC applies appropriate controls to ensure the security of the IT systems of which they are the system owners. They do so in accordance with the IT security governance principles, in particular as regards data protection, professional secrecy, availability, confidentiality and integrity.

**3.3 Principle 12**: The ECCC deploys control activities through policies that establish what is expected and in procedures that put policies into action

Characteristics:

- Appropriate control procedures ensure that objectives are achieved. The control procedures assign responsibility for control activities to the department or individual responsible for the risk in question. The staff member(s) put in charge perform the control activities in a timely manner and with due diligence, taking corrective action where needed. Management periodically reassesses the control procedures to ensure that they remain relevant.
- Exception reporting is one of the management tools used to draw conclusions about the effectiveness of internal control and/or the changes needed in the internal control system. A system is in place to ensure that all instances of overriding controls or deviations from established processes and procedures are documented in exception reports. All instances must be justified and approved before action is taken, and logged centrally.
- The impact assessment and evaluation of the ECCC's activities are performed in accordance with the guiding principles of the Commission's better regulation guidelines.

## 4. Fourth Component: Information and Communication

Information is necessary for the organisation to carry out internal control and to support the achievement of objectives. There is external and internal communication. External

communication provides the public and stakeholders with information on the ECCC's policy objectives and actions.

Internal communication provides staff with the information it needs to achieve its objectives and to carry out day-to-day controls.

**4.1 Principle 13**: The ECCC obtains or generates and uses relevant quality information to support the functioning of internal control

Characteristic:

- Information and document management. The ECCC identifies the information required to support the functioning of the internal control system and the achievement of its objectives.Information systems process relevant data, captured from both internal and external sources, to obtain the required and expected quality information, in compliance with applicable security, document management and data protection rules. This information is produced in a timely manner, and is reliable, current, accurate, complete, accessible, protected, verifiable, filed and preserved. It is shared within the organisation in line with prevailing guidelines.

**4.2 Principle 14**: ECCC communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

Characteristics:

- Internal communication. The ECCC communicates internally about their objectives, challenges, actions taken and results achieved, including but not limited to the objectives and responsibilities of internal control.
- Separate communication lines, such as whistleblowing arrangements, are in place at the ECCC level to ensure information flow when normal channels are ineffective.

**4.3 Principle 15**: The ECCC communicates with external parties about matters affecting the functioning of internal control

Characteristics:

- External communication. The ECCC ensures that their external communication is consistent, relevant to the audience being targeted, and cost-effective. The ECCC establishes clear responsibilities to align ECCC's communication activities with the priorities and narrative of the body.
- Communication on internal control. The ECCC communicates with external parties on the functioning of the components of internal control. Relevant and timely information is communicated externally, taking into account the timing, audience, and nature of the communication, as well as legal, regulatory, and fiduciary requirements.

## 5. Fifth Component: Monitoring Activities

Continuous and specific assessments are used to ascertain whether each of the five components of internal control is present and functioning. Continuous assessments, built into business processes at different levels of the organisation, provide timely information on any deficiencies. Findings are assessed and deficiencies are communicated and corrected in a timely manner, with serious matters reported as appropriate.

**5.1 Principle 16:** The ECCC selects, develops and performs ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning

Characteristics:

- Continuous and specific assessments. The ECCC continuously monitors the performance of the internal control system with tools that make it possible to identify internal control deficiencies, register and assess the results of controls, and control deviations and exceptions. In addition,

when necessary, the ECCC carries out specific assessments, taking into account changes in the control environment. Ongoing assessments are built into business processes and adjusted to changing conditions. Both kinds of assessment must be based on the general principles set out in Appendix 1.

- Sufficient knowledge and information. Staff performing ongoing or separate assessments has sufficient knowledge and information to do this, specifically on the scope and completeness of the results of controls, control deviations and exceptions.
- Risk-based and periodical assessments. The ECCC varies the scope and frequency of specific assessments depending on the identified risks. Specific assessments are performed periodically to provide objective feedback.

**5.2 Principle 17:** The ECCC assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management, as appropriate

Characteristics:

- Deficiencies. With the support of the Internal Control Coordinator in charge of risk management and internal control, the Executive Director considers the results of the assessments of how the internal control system is functioning within the ECCC.
- Deficiencies are communicated to management and to the units responsible for taking corrective action. They are reported in the Annual Activity Reports and to the Governing Board, as appropriate. The term 'internal control deficiency' means a shortcoming in a component or components and relevant principle(s) that reduces the likelihood of the ECCC achieving its objectives. There is a major deficiency in the internal control system if management determines that a component and one or more relevant principles are not present or functioning or that components are not working together. When a major deficiency exists, the Executive Director cannot conclude that it has met the requirements of an effective system of internal control. To classify the severity of internal control deficiencies, management has to use judgment based on relevant criteria contained in regulations, rules or external standards.
- Remedial action. Corrective action is taken in a timely manner by the staff member(s) in charge of the processes concerned, under the supervision of their management. With the support of the Internal Control Coordinator, the Executive Director monitors and takes responsibility for the timely implementation of corrective action.

## Appendix 1 — General principles for the assessment of internal control

A system of internal control allows management to stay focused on the ECCC pursuit of its operational and financial objectives. In addition, the ECCC Financial Rules requires that the budget must be implemented in compliance with effective and efficient internal control.

The Executive Director must be able to demonstrate not only that he/she has put controls in place but also that these controls take account of the risks involved and that they work as intended.

Internal control principle 16 states that the ECCC must carry out continuous and specific assessments to ascertain whether the internal control systems and their components are present and functioning. They must carry out an overall assessment of the presence and functioning of all internal control components at least once per year.

Even though the principles and their characteristics are straightforward, their implementation in practice, and therefore the assessment of their implementation, can vary from one EU body to another.

Therefore, before assessing its internal control system, the ECCC must set its own baseline for each principle, as best adapted to its specificities and risks. These baselines are a starting point for effective internal control, from which regular monitoring and specific assessments can be implemented.

The baselines should be expressed in terms of relevant and pertinent indicators. Where possible, these indicators should be quantitative.

Since the principles are interdependent, sometimes it is impossible to fully quantify the effective implementation of each individual principle other than through generic qualitative indicators. Nonetheless, effective implementation can be assessed based on a variety of sources of evidence (e.g. process reviews, register of exceptions, reporting of internal control weaknesses, management supervision and ad-hoc verification, surveys and interviews, management self-assessments, audit reports, stakeholder feedback). The baselines may be adapted in subsequent years in order to make sure monitoring activities remain appropriate and up-to-date.

The assessment of whether the internal control system reduces the risk of not achieving an objective to an acceptable level should follow these logical steps, leading to the identification of internal control deficiencies:

- establishment of a baseline for each principle;
- assessment at principle and at component level;
- overall assessment.

## Appendix 2 — Declaration of Assurance of the Authorising Officer

*I, the undersigned, Executive Director of the European Cybersecurity Competence Centre (ECCC)*

*In my capacity as authorising officer*

*Declare that the information contained in this report gives a true and fair view*[4]*.*

*State that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.*

*This reasonable assurance is based on my own judgement and on the information at my disposal, such as the results of the self-assessment, ex-post controls, [the work of the Internal Audit Service — delete this if not applicable] [and the lessons learnt from the reports of the Court of Auditors — delete this if not applicable] for years prior to the year of this declaration.*

*Confirm that I am not aware of anything not reported here which could harm the interests of the ECCC.*

*[However the following reservations should be noted: … … …] (delete this sentence if not applicable)*

*Place ……....., date ……*
*…… (signature)*
*[Name of the AOD]*

[4] True and fair in this context means a reliable, complete and correct view on the state of affairs in the EU body.

## Appendix 3 — Statement of the manager in charge of risk management and internal control

**a) If the manager in charge of risk management and internal control takes responsibility for the completeness and reliability of all management reporting, the declaration should read**:

*'I declare that in accordance with the internal control framework adopted by the Governing Board of ECCC, I have reported my advice and recommendations on the overall state of internal control in the EU body to the Executive Director.*

*I hereby certify that the information provided in the present Annual Activity Report and in its annexes is, to the best of my knowledge, accurate and complete.'*

**b) If responsibility for the completeness and reliability of management reporting is split between two people, the text of the declarations should be amended as follows:**

For the manager in charge of risk management and internal control:

*'I declare that in accordance with the* internal *control framework adopted by the Governing Board of ECCC I have reported my advice and recommendations on the overall state of internal control in the EU body to the Executive Director.*

*I hereby certify that the information provided in Section […] of the present Annual Activity Report and in its annexes is, to the best of my knowledge, accurate and complete.'*

For the manager taking responsibility for the completeness and reliability of management reporting on results and on the achievement of objectives:

*'I hereby certify that the information provided in Section […] of the present Annual Activity Report and in its annexes is, to the best of my knowledge, accurate and complete.'*