**DECISION No MB/2019/12
of the Management Board of
the European Union Agency for Cybersecurity**

**on the Internal Control Framework
for effective management applicable to the
European Union Agency for Cybersecurity**

The MANAGEMENT BOARD,

Having regard to the Regulation (EU,Euratom) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and repealing Regulation (EU) No 526/2013[1];

Having regard to the decision No MB/2019/8 of the Management Board of ENISA the European Union Agency for Cybersecurity on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018, and in particular Article 30;

Whereas:

The Authorising Officer of the Agency puts in place the organisational structure and the internal management and control systems and procedures suited to the performance of his duties, including where appropriate ex post verifications.

The Internal Control Framework as implemented by the Commission was revised on 19 April 2017. The Internal Control Framework moves away from a purely compliance-based to a principle-based system. The new Internal Control Framework consists of five internal control components and 17 principles.

The Internal Control Framework is designed to provide reasonable assurance regarding the achievement of five objectives set in Article 30 of the ENISA Financial Regulation: (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.

In particular, the Executive Director signs a declaration of assurance in the Annual Activity Report that provides 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.

ENISA's Internal Control Framework will supersede the provisions on ENISA's Internal Control Standards adopted by ENISA Management Board on 14 October 2010.

---

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563265599312&uri=CELEX:32019R0881

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

1. 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 ENISA Financial Regulation.

2. ENISA Executive Director shall implement the revised Internal Control Framework as from the adoption date and to conduct an overall assessment of the presence and functioning of all internal control components at least once a year and for the first time at the latest in the context of the Annual Activity Report 2019.

Article 2

1. This Decision shall enter into force on the date of its adoption.
2. The entry into force of this Decision repeals Decision of the Management Board on Internal Control Standards of 14 October 2010.

Done at Athens on 21 November 2019.

On behalf of the Management Board,

[signed]

Mr. Jean-Baptiste Demaison

Chair of the Management Board of ENISA

**Annex
to the MB Decision of the Management Board of
the European Union Agency for Cybersecurity**

**on the Internal Control Framework
for effective management applicable to the
European Union Agency for Cybersecurity**

Scope

ENISA Internal Control Framework is based on the framework of the European Commission which was revised in 2017 with a view to align the Commission standards to the international standards set by the COSO framework.

The aim of the Commission was to move from a compliance-based system to a principle-based system and to ensure a more robust Internal Control Framework through consistent assessment, while providing the necessary flexibility to enable the framework to be adapted to fit the specific characteristics and circumstances of the Commission[2] .

In order to keep up with these recent changes in the international best practices and following the Commission's revision in 2017, it is appropriate for ENISA to update its internal control framework. The revised framework consists of 5 Internal Control Components and 17 Internal Control Principles.

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

Principles: Each components consists of several principles. Working with these principles helps to provide reasonable assurance that ENISA'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 those of the Commission, but have been defined in such way as to take into account the specific Governance arrangements and the specific situation of ENISA. There is no requirement for ENISA to assess whether each individual characteristic is in place. The characteristics have been defined to assist management in implementting 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.

---

[2] EC Communication: Revision of the Internal Control Framework: C(2017)2373 of 17/04/2017

Design of the Internal Control Framework

Internal Control Components	Internal Control Principles
CONTROL ENVIRONMENT	1. ENISA demonstrate commitment to integrity and ethical values
	2. ENISA Management exercises oversight responsibility of the development and performance of internal control
	3. ENISA's Management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives
	4. ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignement with objectives
	5. ENISA holds accountable for their internal control responsibilities in the pursuit of objectives
RISK ASSESSMENT	6. ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives
	7. ENISA 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. ENISA considers the potential for fraud in assessing risks to the achievement of objectives
	9. Identifies and analyses significant change
CONTROL ACTIVITIES	10. ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable level
	11. ENISA selects and develops general control over technology to support the achievement of objectives
	12. ENISA deploys control activities through policies that establish what is expected and in procedures that put policies into action through policies and procedures
INFORMATION AND COMMUNICATION	13. ENISA obtains or generates and uses relevant quality information to support the functioning of internal control
	14. ENISA communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control
	15. ENISA communicates with external parties about matters affecting the functioning of internal control
MONITORING ACTIVITIES	16. ENISA selects,develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning
	17. ENISA 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 ENISA. The Management Team set the tone at the top with respect to the importance of the internal control, including expected standards of conduct.

1.1 Principle 1: ENISA 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 Agency'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 Agency's expected standards of conduct and to address deviations in a timely manner.

1.2 Principle 2: ENISA's Management exercises oversight responsibility of development and performance of internal control

Characteristics:

- In his/her capacity as Authorising Officer, ENISA's 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.
The Internal Control Coordinator in charge of risk management and internal control plays a key role by coordinating the preparation of the Annual Activity Report. In this context, he signs a declaration taking responsibility for the completeness and reliability of management reporting.
- Each Head of Department oversees the internal control systems within their department. Each Head of Department 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: ENISA'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 to support the achievement of operational and control objectives.

- Authorities and responsibilities. The Executive Director, as appropriate, delegates authority and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the Agency.
- Reporting lines. The Agency designs and evaluate reporting lines within departments to enable the execution of authority, fulfilment of responsibilities, and flow of information.

1.4 Principle 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives

Characteristics:

- Competence framework. The Executive Director, Head of Departments and Head of Units define the competences necessary to support the achievement of objectives and regularly evaluate them across the Agency, taking action to address shortcomings where necessary.
- Professional development. The Executive Director, Head of Departments 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, Head of Departments and Head of Units promote and plan staff mobility so as to strike the right balance between continuity and renewal.

1.5 Principle 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives

Characteristics:

- Enforcing accountability. The Agency 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: ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

Characteristics:

- Mission. ENISA and its departments 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 ENISA's responsibilities set in the legal base.
- Objectives are set at every level. ENISA'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 Director to the various levels of the organisation, and are communicated and understood by management and staff.

- Indicators measure the achievement of ENISA's activities. Objectives and indicators cover ENISA's most significant activities that contribute to the delivery of ENISA'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. ENISA uses the objectives set as a basis for allocating available resources as needed to achieve policy, operational and financial performance goals.
- Financial reporting objectives. Financial reporting objectives are consistent with the accounting principles applicable in ENISA.
- Non-financial reporting objectives. Non-financial reporting provides management with accurate and complete information needed to manage the organisation at Executive Director, Department 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.

2.2 Principle 7: ENISA 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. ENISA 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. ENISA 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: ENISA 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. ENISA sets up and implements measures to counter fraud and any illegal activities affecting the financial interests of the EU.ENISA 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.

No |

2.4 Principle 9: ENISA Identifies and analyses significant change

Characteristics:

- 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: ENISA 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 Department 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 ENISA 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: ENISA 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, ENISA management selects and develop control activities over the acquisition, development and maintenance of technology and related infrastructure.
- Security of IT systems. ENISA 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.

EUROPEAN UNION AGENCY FOR CYBERSECURITY
www.enisa.europa.eu

8

3.3 Principle 12: ENISA 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 ENISA'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 ENISA'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: ENISA obtains or generates and uses relevant quality information to support the functioning of internal control

Characteristics:

- Information and document management. ENISA 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

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

Characteristics:

- Internal communication. ENISA and the management communicate 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 Agency level to ensure information flow when normal channels are ineffective.

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

Characterstics:

- External communication. All managers ensure that their external communication is consistent, relevant to the audience being targeted, and cost-effective. ENISA establishes clear responsibilities to align ENISA's communication activities with the priorities and narrative of the institution.
- Communication on internal control. ENISA 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: ENISA selects, develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning

Characterstics:

- Continuous and specific assessments. ENISA 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, ENISA 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 qualitative and quantitative assessment criteria to be measured through clearly defined indicators.
- 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. ENISA 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: ENISA assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management as appropriate

Characterstics:

- Deficiencies. With the support of the designated staff member in charge of risk management and internal control, ENISA considers the results of the assessments of how the internal control system is functioning within ENISA.
  Deficiencies are communicated to management and to the departments responsible for taking corrective action. They are reported in the Annual Activity Reports and to the responsible

Member of the Management 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 ENISA 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 manager in charge of risk management and internal control, the Executive Director monitors and takes responsibility for the timely implementation of corrective action.

6. KPIs for Internal Control Assessment

The proposed KPIs (Annex 1) will be used in order to assess the functioning of the Internal Control. These KPIs could be modified or changed at any time based on the evolution of the Agency. When modifications or changes are foreseen, the Annex 1 will be submitted to the Management Board for approval.

Annex 1: KPIs per components and principles
FIRST COMPONENT : Control Environment - Principle 1 Indicators

PRINCIPLE 1: ENISA demonstrate commitment to integrity and ethical values (Tone at the top - Standards of conduct - Alignment with standards)	
Indicator #	1
Indicator	Training/Workshop on ethics has been organized in the reporting year
Source of data/evidence	ENISA's Intranet announcement and invitations sent to all Staff. Training/workshop are mandatory
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	HR report on training/workshop attendances

PRINCIPLE 1: ENISA demonstrate commitment to integrity and ethical values (Tone at the top - Standards of conduct - Alignment with standards)	
Indicator #	2
Indicator	Management encourages staff to follow ethics training and mandatory "refresh" training
Source of data/evidence	ENISA's Intranet announcement and invitations sent to all Staff. Training/workshop are mandatory
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	HR announcement and invitations sent to staff

PRINCIPLE 1: ENISA demonstrate commitment to integrity and ethical values (Tone at the top - Standards of conduct - Alignment with standards)

Indicator #	3
Indicator	Percentage of staff members who followed the training/workshop on ethics
Source of data/evidence	HR report on training/workshop attendances
Baseline Value	95%
Target Value (after assessment)	xx%
Indicator Owner	Human Resources
Method measuring indicator	HR report on training/workshop attendances

PRINCIPLE 1: ENISA demonstrate commitment to integrity and ethical values (Tone at the top - Standards of conduct - Alignment with standards)

Indicator #	4
Indicator	Management communicated to/discussed with staff the Annual Report of the IDOC
Source of data/evidence	Publication of IDOC reports on ENISA's Intranet
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Publication of IDOC reports on ENISA's Intranet

FIRST COMPONENT : Control Environment - Principle 2 Indicators

PRINCIPLE 2: ENISA Management exercises oversight responsibility of the development and performance of internal control	
Indicator #	5
Indicator	ENISA's Consolidated Annual Activity Report (CAAR) includes the Declaration of Assurance of the Executive Director as an Annex
Source of data/evidence	ENISA's Consolidated Annual Activity Report (CAAR)
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director
Method measuring indicator	Publication of CAAR including the declaration of Assurance of the Executive Director

PRINCIPLE 2: ENISA Management exercises oversight responsibility of the development and performance of internal control	
Indicator #	6
Indicator	The delegated Authorising Officers sign a cascading declaration of assurance covering their areas
Source of data/evidence	Cascading declaration of assurance in which he/she reports on the use of his/her respective budgetary powers and related use of resources
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director ; Authorising Officer's by Delegation
Method measuring indicator	Signed declarations

FIRST COMPONENT : Control Environment - Principle 3 Indicators

PRINCIPLE 3: ENISA's Management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives	
Indicator #	7
Indicator	Organisational chart is adopted and updated
Source of data/evidence	ENISA's Intranet publication
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	ENISA's Intranet publication

PRINCIPLE 3: ENISA's Management establishes structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives	
Indicator #	8
Indicator	Delegation of authority is documented respecting the segregation of duties
Source of data/evidence	ENISA's Intranet publication
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources ; Finance and Procurement
Method measuring indicator	Signed declarations

FIRST COMPONENT : Control Environment - Principle 4 Indicators

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	9
Indicator	Wide dissemination and awareness of ENISA's vacancy notices is ensured
Source of data/evidence	Vacancy notices on ENISA webpage; mailing list to ENISA staff dissemination plan; social networks
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	ENISA's website publication; email sent and social networks

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	10
Indicator	Percentage of staff turnover
Source of data/evidence	HR statistics
Baseline Value	< 15%
Target Value (after assessment)	xx%
Indicator Owner	Human Resources
Method measuring indicator	Human Resources statistics

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	11
Indicator	The process of Staff appraisal includes a dialogue where staff members receive feedback on how to improve their performance and identify training needs
Source of data/evidence	Career Development Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	Career Development Reports

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	12
Indicator	Number of days of unused holidays. Unused leave that exceeds the 12 days of leave that can be transferred to year n+1
Source of data/evidence	Leama
Baseline Value	12 days
Target Value (after assessment)	xx days
Indicator Owner	Human Resources
Method measuring indicator	Leama Reports

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	13
Indicator	Allocation for general trainings and specific trainings are forecasted
Source of data/evidence	L&D policy and Budget allocation
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	L&D policy and Budget execution

PRINCIPLE 4: ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with objectives	
Indicator #	14
Indicator	Internal mobility opportunities
Source of data/evidence	Internal vacancies publication and mobility
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	Communication to ENISA's staff on Internal Vacancies and Mobility Decisions

FIRST COMPONENT : Control Environment - Principle 5 Indicators

PRINCIPLE 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives	
Indicator #	15
Indicator	Annual objectives reviewed in the course of the year as needed and related to ENISA SPD
Source of data/evidence	Mid-term review per unit
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Departments and Units
Method measuring indicator	Mid-term review per unit completed

PRINCIPLE 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives	
Indicator #	16
Indicator	Job description are revised when needed
Source of data/evidence	Revised job description
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	Job description are revised

PRINCIPLE 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives	
Indicator #	17
Indicator	Staff appraisal exercise is done within the time frame set by HR (as per Implementing rules of Staff Regulation)
Source of data/evidence	Career Development Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	Career Development Reports

PRINCIPLE 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives	
Indicator #	18
Indicator	Staff promotion yearly exercise
Source of data/evidence	Staff promoted every year
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	HR data - publication on Intranet

SECOND COMPONENT : Risk Assessment
Principle 6 Indicators

PRINCIPLE 6: ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	
Indicator #	19
Indicator	Mission statements have been reviewed at Agency, Department and Unit level; endorsed or formally approved by stakeholders
Source of data/evidence	SPD adopted by ENISA and its Management Board
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Adoption of SPD

PRINCIPLE 6: ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	
Indicator #	20
Indicator	Objectives of the Agency are clearly defined
Source of data/evidence	SPD adopted by ENISA and its Management Board
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Adoption of SPD

PRINCIPLE 6: ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	
Indicator #	21
Indicator	Rate of budget implementation
Source of data/evidence	Budgetary reports; Budget Committee reports; Executive Director's reports
Baseline Value	95%
Target Value (after assessment)	xx%
Indicator Owner	Finance and Procurement Unit
Method measuring indicator	Budgetary reports; Budget Committee reports; Executive Director's reports

PRINCIPLE 6: ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	
Indicator #	22
Indicator	Rate of Budget Outturn
Source of data/evidence	Budgetary reports; Budget Committee reports; Executive Director's reports
Baseline Value	95%
Target Value (after assessment)	xx%
Indicator Owner	Finance and Procurement Unit
Method measuring indicator	Budgetary reports; Budget Committee reports; Executive Director's reports

SECOND COMPONENT : Risk Assessment
Principle 7 Indicators

PRINCIPLE 7: ENISA 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.	
Indicator #	23
Indicator	Risks have been identified
Source of data/evidence	Risk Register
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk Register updated

PRINCIPLE 7: ENISA 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.	
Indicator #	24
Indicator	Risks have been assessed
Source of data/evidence	Risk identification and assessment
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk identification and assessment updated

PRINCIPLE 7: ENISA 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.	
Indicator #	25
Indicator	Risks have been regularly monitored
Source of data/evidence	Action plan for mitigation measure
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Action plan for mitigation measure updated

SECOND COMPONENT : Risk Assessment
Principle 8 Indicators

PRINCIPLE 8: ENISA considers the potential for fraud in assessing risks to the achievement of objectives	
Indicator #	26
Indicator	Anti-Fraud strategy updated
Source of data/evidence	Action plan for mitigation measure
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Anti-Fraud strategy updated and adopted

PRINCIPLE 8: ENISA considers the potential for fraud in assessing risks to the achievement of objectives	
Indicator #	27
Indicator	Fraud risks have been inserted in risk register
Source of data/evidence	Risk register
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk Register updated

PRINCIPLE 8: ENISA considers the potential for fraud in assessing risks to the achievement of objectives	
Indicator #	28
Indicator	The Agency provides a training on preventing fraud yearly
Source of data/evidence	Training on fraud prevention
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	HR report on training/workshop attendances

SECOND COMPONENT : Risk Assessment
Principle 9 Indicators

PRINCIPLE 9: Identifies and analyses significant change	
Indicator #	29
Indicator	Constant update of the Risk Register
Source of data/evidence	Risk Register
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk Register updated

THIRD COMPONENT : Control Activities
Principle 10 Indicators

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	30
Indicator	Results of control and performance indicators are monitored as to ensure achieving related objectives. These controls are happening twice a year (mid-term review and end of year report)
Source of data/evidence	Mid-term review and Annual Activity Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Mid-term review and Annual Activity Report

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	31
Indicator	The assessment of the functioning of the internal control principles has been used as activity supervision tool and mid-term review
Source of data/evidence	Mid-term review
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Mid-term review

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	32
Indicator	Percentage Ex Ante financial verification
Source of data/evidence	ABAC and BO
Baseline Value	100%
Target Value (after assessment)	xx%
Indicator Owner	Finance and Procurement Unit
Method measuring indicator	ABAC and BO

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	33
Indicator	Ex Post control Financial transactions
Source of data/evidence	Ex Post Control Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Ex Post Control Report

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	34
Indicator	ABAC access rights are reviewed once a year
Source of data/evidence	ABAC Security Report and ABAC neutral Verification
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	ABAC Security Report and ABAC neutral Verification

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	35
Indicator	4 eyes principle has been ensured in all financial and non-financial workflows (design of financial circuits and operational workflows)
Source of data/evidence	ABAC and Paperless Application
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	ABAC and Paperless Application

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	36
Indicator	Business continuity arrangements identified in ENISA. BCP is reviewed/tested regularly (at least once a year)
Source of data/evidence	BCP report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Corporate Services
Method measuring indicator	BCP report

PRINCIPLE 10: ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	
Indicator #	37
Indicator	A map of critical and sensitive positions exists
Source of data/evidence	Sensitive positions map
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Human Resources
Method measuring indicator	Sensitive positions map

THIRD COMPONENT : Control Activities
Principle 11 Indicators

PRINCIPLE 11: ENISA selects and develops general control over technology to support the achievement of objectives	
Indicator #	38
Indicator	Existence of IT strategy, IT security strategy
Source of data/evidence	IT strategy, IT security strategy; ITAC
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Corporate Services
Method measuring indicator	Updated IT strategy, IT security strategy

PRINCIPLE 11: ENISA selects and develops general control over technology to support the achievement of objectives	
Indicator #	39
Indicator	Existence of IT Risk Assessment
Source of data/evidence	IT Risk Assessment; ITAC
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Corporate Services
Method measuring indicator	IT Risk Assessment

PRINCIPLE 11: ENISA selects and develops general control over technology to support the achievement of objectives	
Indicator #	40
Indicator	Complete recording of number of security breaches/incidents and properly addressed
Source of data/evidence	Recording of number of security breaches/incidents
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Corporate Services
Method measuring indicator	Recording of number of security breaches/incidents

THIRD COMPONENT : Control Activities
Principle 12 Indicators

PRINCIPLE 12: ENISA deploys control activities through policies that establish what is expected and in procedures that put policies into action	
Indicator #	41
Indicator	Recommendations stemming from the IAS performance audits are addressed
Source of data/evidence	Team Mate and IAS reports
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Team Mate and IAS reports

PRINCIPLE 12: ENISA deploys control activities through policies that establish what is expected and in procedures that put policies into action	
Indicator #	42
Indicator	Existence of a register of Exceptions
Source of data/evidence	Register of Exceptions
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Register of Exceptions

PRINCIPLE 12: ENISA deploys control activities through policies that establish what is expected and in procedures that put policies into action	
Indicator #	43
Indicator	Procedure for exception reporting exists and is widely communicated within the Agency
Source of data/evidence	Paperless Application
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Register of Exceptions

PRINCIPLE 12: ENISA deploys control activities through policies that establish what is expected and in procedures that put policies into action	
Indicator #	44
Indicator	External evaluation of the Agency are done yearly (as per ENISA Financial Regulation Art 29; 32; 48)
Source of data/evidence	External Evaluation Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	External Evaluation Report

FOURTH COMPONENT : Information and Communication
Principle 13 Indicators

PRINCIPLE 13: ENISA obtains or generates and uses relevant quality information to support the functioning of internal control	
Indicator #	45
Indicator	Existence of a centralised external communication incoming/outgoing
Source of data/evidence	Intranet
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Resources Department
Method measuring indicator	Intranet

PRINCIPLE 13: ENISA obtains or generates and uses relevant quality information to support the functioning of internal control	
Indicator #	46
Indicator	Existence of ENISA internal communications platform
Source of data/evidence	Intranet
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Communication
Method measuring indicator	Intranet

PRINCIPLE 13: ENISA obtains or generates and uses relevant quality information to support the functioning of internal control	
Indicator #	47
Indicator	Percentage of documents requested by IAS/CoA retrievable
Source of data/evidence	Intranet
Baseline Value	100 %
Target Value (after assessment)	xx%
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Intranet

No |

FOURTH COMPONENT : Information and Communication
Principle 14 Indicators

PRINCIPLE 14: ENISA communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	
Indicator #	48
Indicator	ENISA and the management communicate internally about their objectives, challenges, actions taken and results achieved
Source of data/evidence	Intranet
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Core Operation Department
Method measuring indicator	Intranet

PRINCIPLE 14: ENISA communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	
Indicator #	49
Indicator	Separate communication lines, such as whistleblowing arrangements, are in place at Agency level to ensure information flow when normal channels are ineffective
Source of data/evidence	Anti-Fraud strategy describes all channels existing
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Anti-Fraud strategy

PRINCIPLE 14: ENISA communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	
Indicator #	50
Indicator	Weekly staff meetings providing information on Agency's objectives and deliverables
Source of data/evidence	Intranet
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Intranet

PRINCIPLE 14: ENISA communicates information internally, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	
Indicator #	51
Indicator	Mid-term review providing information on Agency's objectives, challenges and lessons learned
Source of data/evidence	Mid-term reviews
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director; Departments and Units
Method measuring indicator	Mid-term reviews

FOURTH COMPONENT : Information and Communication Principle 15 Indicators

PRINCIPLE 15: ENISA communicates with external parties about matters affecting the functioning of internal control	
Indicator #	52
Indicator	ENISA press coverage
Source of data/evidence	press releases
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Core Operation Department
Method measuring indicator	Intranet; press releases

PRINCIPLE 15: ENISA communicates with external parties about matters affecting the functioning of internal control	
Indicator #	53
Indicator	ENISA has an up to date Communication Strategy in place
Source of data/evidence	Crisis Communication Strategy
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Corporate Services
Method measuring indicator	Crisis Communication Strategy

PRINCIPLE 15: ENISA communicates with external parties about matters affecting the functioning of internal control	
Indicator #	54
Indicator	ENISA has the CAAR where all internal controls are reported
Source of data/evidence	Consolidated Annual Activity Report
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Executive Director ; Departments and Units
Method measuring indicator	ED; Departments and Units

FIFHT COMPONENT : Monitoring Activities
Principle 16 Indicators

PRINCIPLE 16: ENISA selects, develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning	
Indicator #	55
Indicator	Timely follow up of recommendations and risks identified in ex-ante and ex-post controls and evaluations
Source of data/evidence	Risk register and action plan; Ex Post control and evaluations
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk register and action plan; Ex Post control and evaluations

PRINCIPLE 16: ENISA selects, develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning	
Indicator #	56
Indicator	ICC informs twice a year on the performance/functioning of the internal control, outcome of the risk management exercise and exceptions
Source of data/evidence	Risk register; action plan and register of exceptions
Baseline Value	Yes
Target Value (after assessment)	Yes/No
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Risk register; action plan and register of exceptions

FIFHT COMPONENT : Monitoring Activities
Principle 17 Indicators

PRINCIPLE 17: ENISA assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management as appropriate	
Indicator #	57
Indicator	Rate of accepted audit recommendations implemented within agreed deadlines
Source of data/evidence	Audit reports and TeamMate
Baseline Value	100%
Target Value (after assessment)	xx%
Indicator Owner	Internal Control Coordinator
Method measuring indicator	Audit reports and TeamMate