



Protection level **LIMITED BASIC**

Releasable to Management Board

Decision No 2019-042 of 19.03.2019 the Management Board of the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter 'eu-LISA')

Subject: Adoption of the revised internal control framework for eu-LISA

THE MANAGEMENT BOARD OF EU-LISA,

Having regard to Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT systems in the Area of Freedom, Security and Justice (eu-LISA) and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EC) No 1077/2011¹;

Having regard to Regulation (EU, Euratom) 2018/1046² 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 referred to as "Financial Regulation");

Having regard to Management Board Decision No 2014-007 adopting the Financial Regulation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereinafter referred to as "Financial Regulation of eu-LISA), and in particular Articles 5, 30, 44 (2) and 47(1) (b) thereof;

Having regard to Management Board Decision No 2014-059 adopted on 15 June 2014 which provides the eu-LISA with minimum Internal Control Standards based on equivalent standards laid down by the European Commission for its own department.

Having regard to the Communication of the Commission on the Revision of the Internal Control Framework, adopted on 19 April 2017 by the European Commission³,

¹ OJ L 295, 21.11.2018, p. 99–137

² OJ L 193, 30.7.2018, p. 1–222

³ C(2017) 2373 final.

Protection level **LIMITED BASIC**

Releasable to Management Board

Whereas:

- 1) In accordance with Article 5 of the Financial Regulation of eu-LISA, the budget of the Agency shall be established and implemented in accordance with *inter alia* the principle of sound financial management which requires effective and efficient internal control, and transparency.
- 2) In accordance with Article 30 of the Financial Regulation of eu-LISA, “Internal control of budget implementation”, effective internal control shall be based on best international practices and shall be efficient.
- 3) In accordance with Article 44 of the Financial Regulation of eu-LISA on the powers and duties of the Authorising Officer, the Executive Director in her or his capacity as Authorising Officer, shall, in accordance with the minimum standards adopted by the Management Board, on the basis of equivalent standards laid down by the European Commission for its own departments, and, having due regard to the risks associated with the management environment and the nature of the action financed, put in place the organizational structure and the internal control systems suited to the performance of the duties of Authorising Officer. The establishment of such structure and systems shall be supported by a comprehensive risk analysis, which takes into account their cost effectiveness and performance considerations. The Authorising Officer may establish within his or her departments an expertise and advice function to help him or her control the risks involved in his or her activities.
- 4) In line with Article 44 of the Financial Regulation of eu-LISA and the Communication of the Commission on the revision of the Internal Control Framework⁴, the Management Board shall:
 - a) Adopt the internal control principles and characteristics set out in Chapter II of the Communication of the Commission on the Revision of the Internal Control Framework. These shall constitute the minimum standards referred to in Article 44.2 of the Financial Regulation of eu-LISA.
 - b) Instruct the Executive Director of eu-LISA to implement the internal control principles and characteristics in 2019 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 Consolidated Annual Activity report for 2019.
 - c) Task eu-LISA’s Executive Director and Authorising Officer(s) by delegation with taking appropriate action to define the baselines for each internal control

⁴ C(2017) 2373 of 19 April 2017

principle by the end of 2019, taking into account their specificities and risks, and to improve the awareness and understanding of them by all staff, in particular through training, information and support activities.

- 5) In accordance with Article 47 of the Financial regulation of eu-LISA, the Executive Director shall report to the Management Board on the performance of his/her duties in a form of a consolidated annual activity report ('CAAR'), which shall contain in particular:
- a) Information on management and internal control systems, and
 - b) A declaration by the Executive Director stating whether he/she has reasonable assurance that the information contained in the report presents a true and fair view, the resources assigned have been used for their intended purpose and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The CAAR shall indicate the results of the operations by reference to the objectives set, the risks associated with the operations, the use made of the resources provided and the efficiency and effectiveness of the internal control systems, including an overall assessment of the costs and benefits of controls.

HAS DECIDED AS FOLLOWS:

Article 1

1. The revised eu-LISA Internal Control Framework, as set out in the Annex to this Decision, is hereby adopted. The internal control principles and characteristics set out therein shall constitute the minimum standards referred to in Article 44.2 of the Financial Regulation of eu-LISA.
2. The Executive Director in his or her capacity as Authorising Officer, is fully responsible for the implementation of eu-LISA's internal controls. The Executive Director is hereby tasked to implement the internal control principles and characteristics and to put in place an organizational structure and internal control system that is in accordance with the principles and characteristics adopted by the Management Board as listed in Annex 1 to this Decision.
3. To this end, the Management Board tasks the Executive Director to appoint a Manager in charge of risk management and internal control to support her/him with the setting up, monitoring, implementation, assessment and reporting the Internal Control Framework.
4. The Executive Director, in collaboration with the Manager in charge of risk management and Authorising Officers by delegation, is mandated to take the

appropriate actions to define as soon as possible Internal Control Monitoring Criteria (including performance indicators and the baselines) for each internal control principle and characteristic. In this process the Executive Director shall make sure that eu-LISA specificities, change environment and risks are taken into account, and shall improve the awareness and understanding of the internal control system by all staff, in particular through training, dissemination of best practices, information and support activities to ensure a consistent and effective implementation and assessment of the eu-LISA internal control system across the Agency.

5. The Executive Director shall put in place appropriate working arrangements and communication channels to communicate in timely manner to the Management Board on internal control deficiencies and significant risks.
6. The Executive Director is hereby mandated to conduct an overall assessment of the efficiency of eu-LISA Internal Control Framework annually. The first such annual assessment shall take place in the context of the Consolidated Annual Activity Report 2019. This assessment shall be based on the methodology defined in Annex 2.

Article 2

All Annexes form an integral part of this Decision.

Article 3

This Decision repeals and replaces Management Board Decision No 2014-059 of 15 June 2014 adopting the Minimum Internal Control Standards based on the standards laid down by the Commission for its own Departments.

Article 4

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

Done in Tallinn, on 19.03.2019

For the Management Board of eu-LISA

Zsolt Szolnoki
Chairperson

ANNEX 1

The components, principles and characteristics of eu-LISA Internal Control Framework

1. Context and definitions

Internal control applies to all activities, irrespective of whether they are financial or non-financial. It is a process that helps an organisation to achieve its objectives and sustain operational and financial performance, respecting rules and regulations. It supports sound decision making, taking into account risks to the achievement of objectives and reducing them to acceptable levels through cost-effective controls.

The internal control framework of eu-LISA is designed to provide reasonable assurance regarding the achievement of the five objectives set in Article 30 of eu-LISA Financial Regulation⁵: "(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, and (5) adequate management of the risks relating to the legality and regularity of the underlying transactions, taking into account the multiannual character of programmes as well as the nature of the payments concerned".

This framework supplements the eu-LISA Financial Regulation and other applicable rules and regulations⁶ with a view to align eu-LISA standards to the highest international standards. The framework implemented by the Commission⁷ served as a base for defining principles and their characteristics.

eu-LISA will pursue the exchange of best practice between agencies in the context of the Agencies' Network, notably in the framework of the subnetwork on performance development (PDN).

The new Internal Control Framework consists of five internal control components and 17 principles based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2013 Internal Control-Integrated Framework⁸.

The internal control **components** are the control environment, risk assessment, control activities, information and communication and monitoring activities. They are the building blocks that underpin the framework's structure and support the agency in its efforts to achieve its objectives. The five components are interrelated and must be present and effective at all levels of the organisation for internal control over operations to be considered effective.

⁵ Financial Regulation of eu-LISA adopted by the Management Board on 07.02.2014 (ref.2014-007).

⁶ Notably Staff Regulations and MB Decisions on its implementing rules, Decisions of the Executive Director of eu-LISA, eu-LISA Quality Management System and Quality Policy, eu-LISA anti-fraud strategy, the strategic planning and programming cycle, etc.

⁷ European Commission, Communication to the Commission from Commissioner Oettinger, Revision of the Internal Control Framework, 19 April 2017, C(2017) 2373 final.

⁸ The full text of the Internal Control-Integrated Framework is available at www.coso.org.

In order to facilitate the implementation of the internal control framework and management’s assessment of whether each component is present and functioning and whether the components function well together, each component consists of several **principles**. Working with these principles helps provide reasonable assurance that the organisation’s objectives are met. The principles specify the actions required for internal control to be effective.

The framework also identifies the **characteristics** of each principle. These characteristics are defined in such a way as to take into account the specific governance arrangements in the Agency. There is no requirement for the Agency to assess whether each individual characteristic is in place. The characteristics are defined to assist management in implementing internal control procedures and in assessing whether the principles are present and functioning. Management is expected to have persuasive evidence to support their assessment.

This framework is a basis for reflection, assessment and action across the agency. Its implementation should not be perceived as a bureaucratic requirement. It is a pragmatic exercise in which common sense should be the guiding principle. To ensure a consistent and effective assessment of the internal control system in the agency, the Executive Director, together with management support shall disseminate best practices throughout the organisation regularly.

2. The components, principles and characteristics of eu-LISA Internal Control Framework

CONTROL ENVIRONMENT	<ol style="list-style-type: none"> 1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
----------------------------	---

The control environment is the set of standards of conduct, processes, and structures that provide the basis for carrying out internal control across an organisation. The Management Board (MB), Executive Director and management set the tone at the top for the importance of internal control, including expected standards of conduct.

Principle 1 - eu-LISA demonstrates commitment to integrity and ethical values.
<p><u>Characteristics:</u></p> <ul style="list-style-type: none"> - Tone at the top. <i>The Management Board, Executive Director and all management levels respect integrity and ethical values in their instructions, actions and behaviour.</i> - Standards of conduct. <i>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.</i>

- **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.

Principle 2 - The Management Board (MB) demonstrates independence from management and exercises oversight of the development and performance of internal control.

Characteristics:

- **The Management Board** oversees the Agency's governance, risk management and internal control practices and takes overall political responsibility for management carried out by the Executive Director. This happens through the use of appropriate working arrangements and communication channels between the MB, and managers of the Agency.

- **The Executive Director** oversees the internal control systems and oversees the development of and performance of internal control. The Executive Director is supported in this task by the Manager in charge of risk management and internal control.

- **In his or her capacity as Authorising Officer**, the 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 template enclosed).

- **If appointed in their capacity as Authorising Officer by Delegation**, each head of department and unit reports to the Executive Director on the use of resources assigned to them, so that the Executive Director can build his assurance.

- **The manager in charge of risk management and internal control** plays a key role by coordinating the preparation of the Executive Director's Consolidated Annual Activity Report. In this context, s/he signs a declaration taking responsibility for the completeness and reliability of management reporting. This declaration covers both the state of internal control in the Agency and the robustness of reporting on operational performance. However, responsibility for achieving operational objectives remains with the relevant department and unit (see template enclosed).

Principle 3- Management establishes, with Management Board's oversight, 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 management modes, expenditure types, delivery mechanisms and entities in charge of budget implementation to support the achievement of policy, operational and control objectives.

- **Authorities and responsibilities.** *The Management Board and 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 Agency.*
- **Reporting lines.** *The Executive Director designs and evaluates reporting lines within departments and with entrusted entities to enable the execution of authority, fulfilment of responsibilities, and flow of information.*

Principle 4- eu-LISA demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives

Characteristics:

- **Competence framework.** *The Agency defines 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 Agency provides the training and coaching needed to attract, develop, and retain a sufficient number of competent staff.*
- **Mobility.** *The Agency recognizes mobility of staff so as to strike the right balance between continuity and renewal.*
- **Succession planning** and deputising arrangements for operational activities, human resources activities and financial transactions are in place to ensure continuity of operations.

Principle 5- eu-LISA holds individuals 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.*

RISK ASSESSMENT	6. Specifies suitable objectives 7. Identifies and analyses risk 8. Assesses fraud risk 9. Identifies and analyses significant change
------------------------	--

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.

Principle 6- eu-LISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Characteristics:

- **Mission.** *The Agency, departments 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 Agency's responsibilities under the establishing regulation and the objectives set in the legal base.*

- **Objectives are set at every level.** *The Agency'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 top to the various levels of the organisation, and are communicated and understood by management and staff.*

- **Objectives are set for the most significant activities.** *Objectives⁹ and indicators¹⁰ cover the Agency's most significant activities contributing to the delivery priorities relating to the core business, as well as operational management.*

- **Objectives form the basis for committing resources.** *Management 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 the Agency.*

- **Non-financial reporting objectives.** *Non-financial reporting provides management with accurate and complete information needed to manage the organisation at Agency, 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.*

⁹ Objectives must be SMART (specific, measurable, achievable, relevant and time-framed).

¹⁰ Indicators must be RACER (relevant, accepted, credible, easy to monitor and robust).

- *Monitoring. Setting objectives and performance indicators make it possible to monitor progress towards their achievement.*

Principle 7- eu-LISA identifies risks to the achievement of its objectives across the organisation and analyses risks as a basis for determining how the risks should be managed

Characteristics:

- **Risk identification.** *The Agency identifies and assesses risks at the various organisational levels (Agency, department, unit, programme, project) and those related to entrusted entities, analysing internal and external factors. Management and staff are involved in the process at the appropriate level.*

- **Risk assessment.** *The Agency 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.

Principle 8- eu-LISA 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 Agency sets up and implements measures to counter fraud and any illegal activities affecting the financial interests of the EU. It 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.*

Principle 9- eu-LISA identifies and assesses changes that could significantly impact the internal control system.

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.*

CONTROL ACTIVITIES	10. Selects and develops control activities 11. Selects and develops general control over technology 12. Deploys through policies and procedures
---------------------------	---

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.

Principle 10- eu-LISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels
<p><u>Characteristics:</u></p> <ul style="list-style-type: none"> - 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 or 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 the Agency is able to continue working to the extent possible in case of a major disruption. Business continuity plans must include coordinated and agreed disaster recovery plans for time-sensitive supporting infrastructure (e.g. IT systems) without prejudice to the legal obligation of the Management Board under Article 19(1)z) of the establishing Regulation to adopt security rules including business continuity and disaster recovery plans concerning the large-scale IT systems it operates.
Principle 11- eu-LISA selects and develops general control activities over technology to support the achievement of objectives
<p><u>Characteristics:</u></p> <ul style="list-style-type: none"> - 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 Agency

selects and develops control activities over the acquisition, development and maintenance of technology and related infrastructure.

*- **Security of IT systems.** The Agency applies appropriate controls to ensure the security of the IT systems of which they are the system owners without prejudice to the legal obligation under Article 19(1)z) of the establishing Regulation for the Management Board to adopt the necessary security measures concerning the large-scale IT systems it operates. It does so in accordance with the IT security governance principles, in particular as regards data protection, professional secrecy, availability, confidentiality and integrity.*

Principle 12- eu-LISA deploys control activities through corporate 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 expenditure programmes and projects are performed in accordance with Agency's policies and procedures.*

INFORMATION AND COMMUNICATION	13. Uses relevant information 14. Communicates internally 15. Communicates externally
--------------------------------------	--

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 Agency'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.

Principle 13- eu-LISA obtains or generates and uses relevant quality information to support the functioning of internal control

Characteristics:

-Information and document management. The Agency 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.

Principle 14- eu-LISA internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

Characteristics:

- **Internal communication.** The Agency 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 hotlines, are in place at Agency level to ensure information flow when normal channels are ineffective, without prejudice to the legal obligation under Article 19(1) of the establishing Regulation for the Management Board to adopt detailed internal rules and procedures for the protection of whistleblowers, including appropriate channels of communication for reporting misconduct.

Principle 15- eu-LISA communicates with external parties about matters affecting the functioning of internal control

Characteristics:

- **External communication.** Without prejudice to the specific rules laid down in the Memorandum of Understanding between the Commission and the Agency on external communication, the Agency ensures that their external communication is consistent, relevant to the audience being targeted, and cost-effective. The Agency establishes clear responsibilities to align communication activities with the Agency' priorities and narrative of the institution.

- **Communication on internal control.** The Agency communicates with its external stakeholders 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.

MONITORING ACTIVITIES	16. Conducts ongoing and/or separate assessments 17. Assesses and communicates deficiencies
------------------------------	--

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.

Principle 16- eu-LISA selects, develops, and performs ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning
<p><u>Characteristics:</u></p> <ul style="list-style-type: none">- Continuous and specific assessments. The Agency 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 Agency 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 Annex 2.- 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 (at least once a year). The Agency varies the scope and frequency of specific assessments depending on the identified risks. Specific assessments are performed periodically to provide objective feedback.
Principle 17- eu-LISA assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including management and the Management Board, as appropriate
<p><u>Characteristics:</u></p> <ul style="list-style-type: none">- Deficiencies. <i>With the support of the manager 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 Agency. Deficiencies are communicated to management and to the departments/units responsible for taking corrective action. They are reported in the Annual Activity Reports and to the Management Board, as appropriate.</i> <p><i>The term 'internal control deficiency' means a shortcoming in a component or components and relevant principle(s) that reduces the likelihood of the Agency 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</i></p>

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.*

ANNEX 2 - General principles for the assessment of internal control

A system of internal control allows management to stay focused on the Agency's pursuit of their operational and financial objectives. In addition, the Financial Regulation 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 Agency must carry out continuous and specific assessments to ascertain whether the internal control systems and their components are present and functioning. The Agency must carry out an overall assessment of the presence and functioning of all internal control components at least once per year.

Before assessing its internal control system, the Executive Director, with the collaboration of the Manager in charge of risk management and internal control and Authorising Officers by delegation must set the Agency' own baseline for each principle, as best adapted to its specificities and risks. This should be done by an Executive Director decision. The adaptation of baselines by the Executive Director must nevertheless observe the mandatory provisions defined at Agency level and particularly those of the Financial Regulation and Staff Regulations. 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.

Protection level **LIMITED BASIC**
Releasable to Management Board

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.

To ensure the consistent and effective assessment of the internal control system in the Agency, the Manager in charge of risk management and internal control and Authorising Officers by delegation, as relevant, will regularly share best practices. In this context, the Manager in charge of risk management and internal control will exchange views on the setting of baselines for the different principles and on designing proper implementing tools with the input of those Authorising Officers by delegation most qualified and experienced in particular areas.

16
Protection level **LIMITED BASIC**
Releasable to Management Board

Templates

Executive Director's Declaration of Assurance

I, the undersigned,

Executive Director of European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA),

In my capacity as Authorising Officer,

Declare that the information contained in this report gives a true and fair view¹¹.

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 audits of the Internal Audit Service of the European Commission, the audits of the Internal Audit Capability of eu-LISA – *delete this if not applicable*, and the audits of the European Court of Auditors) for years prior to the year of this declaration.

I confirm that I am not aware of anything not reported here which could harm the interests of the Agency or its stakeholders.

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

Place date

(signature)

[Name of the Executive Director]

¹¹ True and fair in this context means a reliable, complete and correct view on the state of affairs in the Agency.

Statement of the Manager in charge of risk management and internal control

I, the undersigned,

Manager in charge of risk management and internal control within European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA),

In my capacity as Manager in charge of risk management and internal control, I declare that in accordance with eu-LISA Internal Control Framework, I have reported my advice and recommendations on the overall state of internal control in the Agency to the Executive Director.

I hereby certify that the information provided on the internal control system in the present Annual Activity Report and in its annexes is, to the best of my knowledge, accurate, reliable and complete.

Place date

(signature)
[Name of jobholder]