DECISION OF THE MANAGEMENT BOARD
of 14 October 2010

on Internal Control Standards for Effective Management

THE MANAGEMENT BOARD OF ENISA,

Having regard to Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, that has been amended by Regulation (EC) No. 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No. 460/2004 establishing the European Network and Information Security Agency as regards its duration, and in particular Article 6(6) thereof,

Having regard to the referred to in art. 38(4) of the Agency's Financial Regulation.

Having regard to the Management Board Decision of 10 October 2007 on Minimum standards

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.

These Internal Control Standards are drafted on the basis of equivalent standards laid down by the Commission for its own departments, and having due regard to the risks associated with the management environment and the nature of the action financed.

The Management Board adopts the Internal Control Standards of the Agency.

HAS DECIDED AS FOLLOWS:

Article 1

The Internal Control Standards annexed hereto are hereby adopted. They correspond to the minimum standards referred to in art. 38(4) of the ENISA Financial Regulation. These Internal Control Standards regard the organisational structure and internal management and

control systems and procedures suited to the performance of the duties of the Authorising Officer.

These Internal Control Standards are amended from time to time in line with updates laid out by the European Commission with regard to its own internal control requirements.

Article 2

This Decision enters into force on the day of its adoption by the Management Board and replaces the Management Board Decision of 10 October 2007, on Minimum standards, which is hereby repealed.

Done at Athens on 14 October 2010

For the ENISA Management Board

Prof. Dr. Reinhard Posch,
Chairman of the Management Board

Signature Value	jflmJLuHBOnFMZCX6rHmWWd28k0rrfctjiIvN8RGAqAbz6/XB/1EhiYTewl/6oBGMGBmJ7GbBKViQMIDa7fOsQ==
Signatory	Dr. Reinhard Posch
Date/Time-UTC	2010-10-14T12:00:48Z
Issuer-Certificate	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Serial-No.	448413
Method	urn:pdfsigfilter:bka.gv.at:text:v1.2.0
Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:sha1
Verification	https://www.signaturpruefung.gv.at/en/

Annex I

THE REVISED INTERNAL CONTROL STANDARDS FOR EFFECTIVE MANAGEMENT

Mission and Values

1. Mission: The Agency's *raison d'être* is clearly defined in up-to-date and concise mission statements developed from the perspective of the Agency customers.

2. Ethical and Organisational Values: Management and staff are aware of and share appropriate ethical and organisational values and uphold these through their own behaviour and decision-making.

Human Resources

3. Staff Allocation and Mobility: The allocation and recruitment of staff is based on the Agency's objectives and priorities. Management promote and plan staff mobility so as to strike the right balance between continuity and renewal.

4. Staff Evaluation and Development: Staff performance is evaluated against individual annual objectives, which fit with the Agency's overall objectives. Adequate measures are taken to develop the skills necessary to achieve the objectives.

Planning and Risk Management Processes

5. Objectives and Performance Indicators: The Agency's objectives are clearly defined and updated when necessary. These are formulated in a way that makes it possible to monitor their achievement. Key performance indicators are established to help management evaluate and report on progress made in relation to their objectives.

6. Risk Management Process: A risk management process that is in line with applicable provisions and guidelines is integrated into the annual activity planning.

Operations and Control Activities

7. Operational Structure: The Agency's operational structure supports effective decision-making by suitable delegation of powers. Risks associated with the Agency's sensitive functions are managed through mitigating controls and ultimately staff mobility. Adequate IT governance structures are in place.

8. Processes and Procedures: The Agency's processes and procedures used for the implementation and control of its activities are effective and efficient, adequately documented and compliant with applicable provisions. They include arrangements to ensure segregation of duties and to track and give prior approval to control overrides or deviations from policies and procedures.

9. Management Supervision: Management supervision is performed to ensure that the implementation of activities is running efficiently and effectively while complying with applicable provisions.

10. Business Continuity: Adequate measures are in place to ensure continuity of service in case of "business-as-usual" interruption. Business Continuity Plans are in place to ensure that the Agency is able to continue operating to the extent possible whatever the nature of a major disruption.

11. Document Management: Appropriate processes and procedures are in place to ensure that the Agency's document management is secure, efficient (in particular as regards retrieving appropriate information) and complies with applicable legislation.

Information and Financial Reporting

12. Information and Communication: Internal communication enables management and staff to fulfil their responsibilities effectively and efficiently, including in the domain of internal control. Where appropriate, the Agency has an external communication strategy to ensure that its external communication is effective, coherent and in line with the Commission's key political messages. IT systems used and/or managed by the Agency (where the Agency is the system owner) are adequately protected against threats to their confidentiality and integrity.

13. Accounting and Financial Reporting: Adequate procedures and controls are in place to ensure that accounting data and related information used for preparing the organisation's annual accounts and financial reports are accurate, complete and timely.

Evaluation and Audit

14. Evaluation of Activities: Evaluations of expenditure programmes, legislation and other non-spending activities are performed to assess the results, impacts and needs that these activities aim to achieve and satisfy.

15. Assessment of Internal Control Systems: Management assess the effectiveness of the Agency's key internal control systems, including the processes carried out by implementing bodies, at least once a year.

16. Internal Audit Capability: The Agency has an Internal Audit Capability (IAC), which provides independent, objective assurance and consulting services designed to add value and improve the operations of the Agency.