



EUROPEAN
COURT
OF AUDITORS

Report on the annual accounts
of the European Union Agency for Network and Information Security
for the financial year 2014
together with the Agency's reply

INTRODUCTION

1. The European Union Agency for Network and Information Security (hereinafter “the Agency”, aka “ENISA”), which is located in Athens and Heraklion¹, was created by Regulation (EC) No 460/2004 of the European Parliament and of the Council² which, following different amendments was superseded by Regulation (EU) No 526/2013³. The Agency's main task is to enhance the Union’s capability to prevent and respond to network and information security problems by building on national and Union efforts⁴.

INFORMATION IN SUPPORT OF THE STATEMENT OF ASSURANCE

2. The audit approach taken by the Court comprises analytical audit procedures, direct testing of transactions and an assessment of key controls of the Agency's supervisory and control systems. This is supplemented by evidence provided by the work of other auditors and an analysis of management representations.

STATEMENT OF ASSURANCE

3. Pursuant to the provisions of Article 287 of the Treaty on the Functioning of the European Union (TFEU), the Court has audited:

- (a) the annual accounts of the Agency, which comprise the financial statements⁵ and the reports on the implementation of the budget⁶ for the financial year ended 31 December 2014, and

¹ The Agency’s operational staff were relocated to Athens in March 2013. Its administrative staff remain in Heraklion.

² OJ L 77, 13.3.2004, p. 1.

³ OJ L 165, 18.6.2013, p. 41.

⁴ ***Annex II*** summarises the Agency's competences and activities. It is presented for information purposes.

⁵ These include the balance sheet and the statement of financial performance, the cash flow table, the statement of changes in net assets and a summary of the significant accounting policies and other explanatory notes.

⁶ These comprise the budgetary outturn account and the annex to the budgetary outturn account.

- (b) the legality and regularity of the transactions underlying those accounts.

The management's responsibility

4. The management is responsible for the preparation and fair presentation of the annual accounts of the Agency and the legality and regularity of the underlying transactions⁷:

- (a) The management's responsibilities in respect of the Agency's annual accounts include designing, implementing and maintaining an internal control system relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies on the basis of the accounting rules adopted by the Commission's accounting officer⁸; making accounting estimates that are reasonable in the circumstances. The Executive Director approves the annual accounts of the Agency after its accounting officer has prepared them on the basis of all available information and established a note to accompany the accounts in which he declares, inter alia, that he has reasonable assurance that they present a true and fair view of the financial position of the Agency in all material respects.
- (b) The management's responsibilities in respect of the legality and regularity of the underlying transactions and compliance with the principle of sound financial management consist of designing, implementing and maintaining an effective and efficient internal control system comprising adequate supervision and appropriate measures to prevent irregularities and fraud and, if necessary, legal proceedings to recover funds wrongly paid or used.

The auditor's responsibility

5. The Court's responsibility is, on the basis of its audit, to provide the European Parliament and the Council⁹ with a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions. The Court conducts its audit in accordance with the

⁷ Articles 39 and 50 of Commission Delegated Regulation (EU) No 1271/2013 (OJ L 328, 7.12.2013, p. 42).

⁸ The accounting rules adopted by the Commission's accounting officer are derived from the International Public Sector Accounting Standards (IPSAS) issued by the International Federation of Accountants or, where relevant, the International Accounting Standards (IAS)/International Financial Reporting Standards (IFRS) issued by the International Accounting Standards Board.

⁹ Article 107 of Regulation (EU) No 1271/2013.

IFAC International Standards on Auditing and Codes of Ethics and the INTOSAI International Standards of Supreme Audit Institutions. These standards require the Court to plan and perform the audit to obtain reasonable assurance as to whether the annual accounts of the Agency are free from material misstatement and the transactions underlying them are legal and regular.

6. The audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the accounts and the legality and regularity of the underlying transactions. The procedures selected depend on the auditor's judgement, which is based on an assessment of the risks of material misstatement of the accounts and material non-compliance by the underlying transactions with the requirements in the legal framework of the European Union, whether due to fraud or error. In assessing these risks, the auditor considers any internal controls relevant to the preparation and fair presentation of the accounts, as well as the supervisory and control systems that are implemented to ensure the legality and regularity of underlying transactions, and designs audit procedures that are appropriate in the circumstances. The audit also entails evaluating the appropriateness of accounting policies, the reasonableness of accounting estimates and the overall presentation of the accounts. In preparing this report and Statement of Assurance, the Court considered the audit work of the independent external auditor performed on the Agency's accounts as stipulated in Article 208(4) of the EU Financial Regulation¹⁰.

7. The Court considers that the audit evidence obtained is sufficient and appropriate to provide a basis for its statement of assurance.

Opinion on the reliability of the accounts

8. In the Court's opinion, the Agency's annual accounts present fairly, in all material respects, its financial position as at 31 December 2014 and the results of its operations and its cash flows for the year then ended, in accordance with the provisions of its Financial Regulation and the accounting rules adopted by the Commission's accounting officer.

Opinion on the legality and regularity of the transactions underlying the accounts

9. In the Court's opinion, the transactions underlying the annual accounts for the year ended 31 December 2014 are legal and regular in all material respects.

¹⁰ Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 298, 26.10.2012, p. 1).

10. The comments which follow do not call the Court's opinions into question.

COMMENTS ON BUDGETARY MANAGEMENT

11. The overall level of committed appropriations was high at 100 % (94 % in 2013). In total, committed appropriations carried over to 2015 amount to 1,3 million euro, i.e. 15 % of total appropriations (2013: 1,2 million euro, i.e. 13,5 %). Commitment appropriations carried over are high for title II (administrative expenditure) at 0,6 million euro, i.e. 49 % (2013: 0,8 million euro, i.e. 59 %). These were linked to investments in IT infrastructure ordered as planned near the year-end for the Agency's two offices.

FOLLOW-UP OF PREVIOUS YEARS' COMMENTS

12. An overview of the corrective actions taken in response to the Court's comments from the previous years is provided in **Annex I**.

This Report was adopted by Chamber IV, headed by Mr Milan Martin CVIKL, Member of the Court of Auditors, in Luxembourg at its meeting of 8 September 2015.

For the Court of Auditors

Vítor Manuel da SILVA CALDEIRA

President

Follow-up of previous years' comments

Year	Court's comment	Status of corrective action (Completed / Ongoing / Outstanding / N/A)
2012	Whereas the Financial Regulation and the corresponding Implementing Rules provide for a physical inventory of fixed assets at least every three years, the Agency has not carried out a comprehensive physical inventory since 2009.	Ongoing
2013	The overall level of committed appropriations was 94 %, which is explained mainly by the fact that additional funds requested from the Commission to finance the refurbishment of the new office in Athens were only approved in November 2013. In this context, an amount of 0,5 million euro that was not yet committed at year-end was carried over following a Management Board decision.	N/A
2013	In total, non-committed and committed appropriations carried over to 2014 amounted to 1,2 million euro (or 13,5 % of total appropriations). This mainly concerned title II (administrative expenditure) with 0,8 million euro or 59 % of title II appropriations. This high level is explained by the 0,5 million euro carry-over referred to in paragraph 11 and an additional 0,3 million euro carried over in order to finance furniture and networking equipment for the Athens office which was ordered towards the year-end.	N/A
2013	Operational staff of ENISA were relocated to Athens in 2013 while administrative staff remain in Heraklion. It is likely that the administrative costs could be reduced if all staff were centralised in one location.	N/A

Year	Court's comment	Status of corrective action (Completed / Ongoing / Outstanding / N/A)
2013	According to the lease agreement between the Greek authorities, the Agency and the landlord, rent for the offices in Athens is paid by the Greek authorities. This rent is constantly paid with a delay of several months which is a business continuity and financial risk to the Agency: its operations would be affected, and its investments in office fitting and refurbishment would be lost, if the landlord were to cancel the lease agreement because of these delays in payment.	Completed

Annex II**European Union Agency for Network and Information Security****(Athens and Heraklion)****Competences and activities**

<p>Areas of Union competence deriving from the Treaty</p> <p><i>(Article 114 of the Treaty on the Functioning of the European Union)</i></p>	<p>The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.</p> <p>The Internal Market responsibility is a shared competence between the Union and the Member States (Article 4(2)(a) TFEU).</p>
<p>Competences of the Agency</p> <p><i>(Regulation (EU) No 526/2013 of the European Parliament and of the Council)</i></p>	<p>Objectives</p> <ol style="list-style-type: none"> 1. The Agency shall develop and maintain a high level of expertise. 2. The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security. 3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market. 4. The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. 5. The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors. <p>Tasks</p> <ol style="list-style-type: none"> 1. The Agency shall perform the following tasks: <ol style="list-style-type: none"> (a) support the development of Union policy and law, by: <ol style="list-style-type: none"> (i) assisting and advising on all matters relating to Union network and information security policy and law; (ii) providing preparatory work, advice and analyses relating to the development and update of Union network and information security policy and law; (iii) analysing publicly available network and information security

strategies and promoting their publication;

(b) support capability building by:

- (i) supporting Member States, at their request, in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, and providing them with the necessary knowledge;
- (ii) promoting and facilitating voluntary cooperation among the Member States and between the Union institutions, bodies, offices and agencies and the Member States in their efforts to prevent, detect and respond to network and information security problems and incidents where these have an impact across borders;
- (iii) assisting the Union institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, in particular by supporting the operation of a Computer Emergency Response Team (CERT) for them;
- (iv) supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;
- (v) supporting the organisation and running of Union network and information security exercises, and, at their request, advising Member States on national exercises;
- (vi) assisting the Union institutions, bodies, offices and agencies and the Member States in their efforts to collect, analyse and, in line with Member States' security requirements, disseminate relevant network and information security data; and on the basis of information provided by the Union institutions, bodies, offices and agencies and the Member States in accordance with provisions of Union law and national provisions in compliance with Union law, maintaining the awareness, on the part of the Union institutions, bodies, offices and agencies as well as the Member States of the latest state of network and information security in the Union for their benefit;
- (vii) supporting the development of a Union early warning mechanism that is complementary to Member States' mechanisms;
- (viii) offering network and information security training for relevant public bodies, where appropriate in cooperation with stakeholders;

(c) support voluntary cooperation among competent public bodies, and between stakeholders, including universities and research centres in

the Union, and support awareness raising, inter alia, by:

- (i) promoting cooperation between national and governmental CERTs or Computer Security Incident Response Teams (CSIRTs), including the CERT for the Union institutions, bodies, offices and agencies;
- (ii) promoting the development and sharing of best practices with the aim of attaining an advanced level of network and information security;
- (iii) facilitating dialogue and efforts to develop and exchange best practices;
- (iv) promoting best practices in information sharing and awareness raising;
- (v) supporting the Union institutions, bodies, offices and agencies and, at their request, the Member States and their relevant bodies in organising awareness raising, including at the level of individual users, and other outreach activities to increase network and information security and its visibility by providing best practices and guidelines;

(d) support research and development and standardisation, by:

- (i) facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services;
- (ii) advising the Union and the Member States on research needs in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

(e) cooperate with Union institutions, bodies, offices and agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern, including by:

- (i) exchanging know-how and best practices;
- (ii) providing advice on relevant network and information security aspects in order to develop synergies;

(f) contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues, including by:

- (i) being engaged, where appropriate, as an observer and in the organisation of international exercises, and analysing and reporting on the outcome of such exercises;
 - (ii) facilitating exchange of best practices of relevant organisations;
-

	<p>(iii) providing the Union institutions with expertise.</p> <p>2. Union institutions, bodies, offices and agencies and Member State bodies may request advice from the Agency in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services.</p> <p>3. The Agency shall carry out tasks conferred on it by legal acts of the Union.</p> <p>4. The Agency shall express independently its own conclusions, guidance and advice on matters within the scope and objectives of this Regulation.</p>
<p>Governance</p>	<p>Management Board</p> <p>The Management Board is composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives have voting rights. Each member of the Management Board has an alternate to represent the member in his/her absence.</p> <p>Members of the Management Board and their alternates are appointed in light of their knowledge of the Agency's tasks and objectives, taking into account the managerial, administrative and budgetary skills relevant to fulfil the tasks of a member of the Management Board.</p> <p>The term of office of members of the Management Board and of their alternates is four years. That term is renewable.</p> <p>Permanent Stakeholders Group</p> <p>The Management Board, acting on a proposal by the Executive Director, sets up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security, and representatives of national regulatory authorities notified under Directive 2002/21/EC as well as of law enforcement and privacy protection authorities. The term of office of the Permanent Stakeholders' Group's members is two-and-a-half years.</p> <p>The Permanent Stakeholders' Group advises the Agency in respect of the performance of its activities. In particular, it advises the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme.</p> <p>Executive Director</p> <p>The Executive Director is appointed by the Management Board, from a list of candidates proposed by the Commission, following an open and transparent selection procedure, for a term of five years which is renewable.</p> <p>Executive Board</p> <p>The Executive Board is made up of five members appointed from among the members of the Management Board and includes the Chairperson of the Management Board, who may also chair the Executive Board, and one of the</p>

	<p>representatives of the Commission.</p> <p>External audit</p> <p>European Court of Auditors.</p> <p>Internal audit</p> <p>Internal Audit Service of the European Commission.</p> <p>Discharge authority</p> <p>European Parliament on a recommendation from the Council.</p>
<p>Resources made available to the Agency in 2014 (2013)</p>	<p>Final Budget</p> <p>9,7 million euro (9,7 million euro) of which the Union subsidy is 94 % (93 %).</p> <p>Staff at 31 December 2014</p> <p>48 (47) posts in the establishment plan, of which occupied: 46 (43).</p> <p>Other posts occupied: 14 (13) contract staff, two (three) Seconded National Experts.</p> <p>Total staff: 62 (59), undertaking the following tasks:</p> <p>operational: 44 (42)</p> <p>administrative: 18 (17)</p>
<p>Products and services in 2014 (2013)</p>	<p>The core activities of ENISA for 2014 have been grouped into three work streams (WSs).</p> <p>WS¹ - Support EU Policy Building</p> <p>During 2014, ENISA provided support for the policy marking process. This was achieved by making available to policy makers consolidated information on the emerging threat landscape and by formulating key messages to the Member States on how to ensure that their policies and capabilities are aligned with EU objectives taking into account lessons learned within the different Member States. These results relied on the unification of available information sources under a common context and at the same time required the collaboration and involvement of important stakeholders in the areas of threat assessment, risk mitigation and policy definition.</p> <p>The following objectives and results were achieved.</p> <ul style="list-style-type: none"> • Identification of technological evolution, risks and challenges: identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors). • Contribution to EU policy initiatives: supporting policy initiatives by providing security perspective and recommending security measures and security and data protection best practices. • Support for the EU in education, research & standardisation: fostering collaboration and cooperation to improve the uptake of security standards and of security research; promoting NIS in education at all levels.

Number of deliverables: 10 (7)

WS2 – Support Capacity Building

A number of activities aimed at supporting ENISA's key stakeholders in developing new operational and policy capabilities to address the various challenges in cybersecurity and to extend existing capabilities were carried out during 2014.

EU Member States and private sector companies have different maturity levels in respect of their capabilities to address cyber-attacks and disruptions. ENISA's activities carried out within this work stream were aimed at raising the level of security across Member States and the private sector by collecting and disseminating good practice for public and private sectors and for the European citizen in general.

The objectives and consequently results of this Work Stream were to:

- Support Member States' capacity building: assisting MSs in the development and harmonization of National Cyber Security Strategies (NCSS), PPPs as well as security methodologies and training materials in the area of CERTs.
- Support private sector capacity building: developing best practice guides, guidelines, minimum security recommendations or harmonization guidelines in different areas of NIS (i.e. NIS and procurement, certification of smart grids, ICS SCADA, ISP providers, Cloud computing).
- Raising the level of preparedness of EU citizens: providing technical guidance, dissemination materials and supporting EU Cyber Security Month.

Number of deliverables: 16 (16)

WS3 - Support Cooperation

Cooperation is a necessary prerequisite for enhancing and strengthening NIS in the European single market and for building the NIS capacities of Member States, EU institutions and third countries.

In 2014, ENISA continued its work in this area by building on existing collaboration in relevant communities developed since the creation of the agency. ENISA supported cooperation by continuing to build trust, bridging the gap between the products and services offered in the market and their needs, and continuously updating the information provided to those implementing NIS policy. Another means to support cooperation covered in 2014 addressed the development of tools to facilitate and improve the international communication and interchange of security-relevant information within communities sharing the same interest in different Member States.

The objectives and results of this Work Stream were:

- Crisis cooperation exercises: organizing Cyber Europe 2014: exercise plan, exercise carried out and report on cyber crisis cooperation.
 - Implementation of EU legislation: preparation of technical guidelines and security measures following analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents.
 - Regular cooperation among NIS communities: updating and enhancing the
-

	<p>operational capabilities of Member States' institutions by helping the CERT community to increase its level of efficiency and effectiveness.</p> <p>Number of deliverables: 9 (15)</p> <p><i>Note: Some deliverables of 2014 have more than one outcome/publication – i.e. the work of WP 3.2 D1 resulted in 6 publications.</i></p>
--	---

¹ WS: Work stream.

Source: Annex supplied by the Agency.

THE AGENCY'S REPLY

11. A significant building project related to the refurbishment of the office in Athens was completed in late December 2014. The time of completion of the main works was such that additional or complementary investments in infrastructure, mainly in Athens building, needed to be contracted for at the end of the year 2014. Subsequently, the delivery of such complementary investments was planned in the first months of 2015 and thus the high rate of carry overs was observed.