

ΕΒΡΟΠΕΪΣΚΑ ΣΜΕΤΗΑ ΠΑΛΑΤΑ
TRIBUNAL DE CUENTAS EUROPEO
EVROPSKÝ ÚČETNÍ DVŮR
DEN EUROPÆISKE REVISIONSRET
EUROPÄISCHER RECHNUNGSHOF
EUROOPA KONTROLLIKODA
ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
EUROPEAN COURT OF AUDITORS
COUR DES COMPTES EUROPÉENNE
CÚIRT INIÚCHÓIRÍ NA HEORPA



CORTE DEI CONTI EUROPEA
EIROPAS REVĪZIJAS PALĀTA
EUROPOS AUDITO RŪMAI

EURÓPAI SZÁMVEVŐSZÉK
IL-QORTI EWROPEA TAL-AWDITURI
EUROPESE REKENKAMER
EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
TRIBUNAL DE CONTAS EUROPEU
CURTEA DE CONTURI EUROPEANĂ
EURÓPSKY DVOR AUDÍTOROV
EVROPSKO RAČUNSKO SODIŠČE
EUROOPAN TILINTARKASTUSTUOMIOISTUIN
EUROPEISKA REVISIONSRÄTTEN

Report on the annual accounts
of the European Network and Information Security Agency
for the financial year 2011

together with the Agency's replies

INTRODUCTION

1. The European Network and Information Security Agency (hereinafter "the Agency"), which is located in Heraklion, was created by Regulation (EC) No 460/2004 of the European Parliament and of the Council¹, amended by Regulation (EC) No 1007/2008 of the European Parliament and of the Council² and by Regulation (EC) No 580/2011³. 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 (where relevant) 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, the Court has audited the annual accounts⁵ of the Agency, which comprise the "financial statements"⁶ and the "reports on the

¹ OJ L 77, 13.3.2004, p. 1.

² OJ L 293, 31.10.2008, p. 1.

³ OJ L 165, 24.6.2011, p. 3.

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

⁵ These accounts are accompanied by a report on the budgetary and financial management during the year which gives further information on budget implementation and management.

⁶ The financial statements include the balance sheet and the economic outturn account, the cash-flow table, the statement of changes in net assets and a summary of the significant accounting policies and other explanatory notes.

implementation of the budget”⁷ for the financial year ended 31 December 2011, and the legality and regularity of the transactions underlying those accounts.

The Management’s responsibility

4. As authorising officer, the Director implements the revenue and expenditure of the budget in accordance with the financial rules of the Agency, under his own responsibility and within the limits of the authorised appropriations⁸. The Director is responsible for putting in place⁹ the organisational structure and the internal management and control systems and procedures relevant for drawing up final accounts¹⁰ that are free from material misstatement, whether due to fraud or error, and for ensuring that the transactions underlying those accounts are legal and regular.

The Auditor’s responsibility

5. The Court’s responsibility is to provide, on the basis of its audit, the European Parliament and the Council¹¹ with a statement of assurance as to the reliability of the annual accounts of the Agency and the legality and regularity of the transactions underlying them.

6. The Court conducted its audit in accordance with the IFAC International Standards on Auditing and Codes of Ethics and the INTOSAI International

⁷ The budget implementation reports comprise the budget outturn account and its annex.

⁸ Article 33 of Commission Regulation (EC, Euratom) No 2343/2002 (OJ L 357, 31.12.2002, p. 72).

⁹ Article 38 of Regulation (EC, Euratom) No 2343/2002.

¹⁰ The rules concerning the presentation of the accounts and accounting by the Agencies are laid down in Chapters 1 and 2 of Title VII of Regulation (EC, Euratom) No 2343/2002 as last amended by Regulation (EC, Euratom) No 652/2008 (OJ L 181, 10.7.2008, p. 23) and are integrated as such in the Financial Regulation of the Institute.

¹¹ Article 185(2) of Council Regulation (EC, Euratom) No 1605/2002.

Standards of Supreme Audit Institutions. These standards require that the Court plans and performs the audit to obtain reasonable assurance as to whether the annual accounts of the Agency are free of material misstatement and the transactions underlying them are legal and regular.

7. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the accounts and the legality and regularity of the transactions underlying them. The procedures are selected based on the auditor's judgment, including an assessment of the risks of material misstatement of the accounts and of material non-compliance of the underlying transactions with the requirement of the legal framework of the European Union, whether due to fraud or error. In assessing those risks, the auditor considers internal controls relevant to the preparation and fair presentation of the accounts and supervisory and control systems implemented to ensure legality and regularity of underlying transactions, in order to design audit procedures that are appropriate in the circumstances. An audit also includes evaluating the appropriateness of accounting policies used and reasonableness of accounting estimates made, as well as evaluating the overall presentation of the accounts.

8. The Court considers that the audit evidence obtained is sufficient and appropriate to provide a basis for the opinions set out below.

Opinion on the reliability of the accounts

9. In the Court's opinion, the Agency's Annual Accounts¹² present fairly, in all material respects, its financial position as of 31 December 2011 and the results of its operations and its cash flows for the year then ended, in accordance with

¹² The Final Annual Accounts were drawn up on 25 June 2012 and received by the Court on 2 July 2012. The Final Annual Accounts, consolidated with those of the Commission, are published in the Official Journal of the European Union by 15 November of the following year. These can be found on the following website <http://eca.europa.eu> or <http://www.enisa.europa.eu/>.

the provisions of its Financial Regulation and the accounting rules adopted by the Commission's accounting officer¹³.

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

10. In the Court's opinion, the transactions underlying the annual accounts of the Agency for the financial year ended 31 December 2011 are legal and regular in all material respects.

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

COMMENTS ON BUDGETARY AND FINANCIAL MANAGEMENT

12. As in 2010, the Agency's budget amounted to 8,1 million euro. Budget implementation improved as compared with the previous year. However, total appropriations carried over to 2012 amount to 1,1 million euro. For Title II (administrative expenditure) 0,2 million euro (34 %) and for Title III (operational expenditure) 0,8 million euro (33 %) of appropriations were carried forward. This high level of carry over is at odds with the budgetary principle of annuality.

COMMENTS ON KEY CONTROLS OF THE AGENCY'S SUPERVISORY AND CONTROL SYSTEMS

13. The Court identified the need to improve the documentation of fixed assets. Purchases of fixed assets are recorded at invoice and not at item level. When several new assets are covered by one single invoice, there is only one entry for all the purchased assets and the total amount.

¹³ The accounting rules adopted by the Commission's accounting officer are derived from International Public Sector Accounting Standards (IPSAS) issued by the International Federation of Accountants or, in their absence, International Accounting Standards (IAS)/International Financial Reporting Standards (IFRS) issued by the International Accounting Standards Board.

OTHER COMMENTS

14. The Agency needs to improve the transparency of recruitment procedures. No adequate measures were taken to address the lack of transparency reported by the Court in 2010. The thresholds candidates had to meet in order to be invited to interview, the questions for written tests and interviews and their weightings were not prepared before the examination of the applications. Threshold scores for being put on a list of suitable candidates were not established before the examination of applications.

This Report was adopted by Chamber IV, headed by Dr Louis GALEA, Member of the Court of Auditors, in Luxembourg at its meeting of 11 September 2012.

For the Court of Auditors

Vítor Manuel da SILVA CALDEIRA
President

European Network and Information Security Agency (Heraklion)**Competences and activities**

<p>Areas of Union competence deriving from the Treaty</p> <p>(Article 114)</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>(Regulation (EC) No 460/2004 of the Parliament and the Council)</p>	<p>Objectives</p> <ol style="list-style-type: none"> 1. The Agency enhances the capability of the Union, the Member States and the business Union to prevent, address and respond to network and information security problems. 2. The Agency provides assistance and delivers advice to the Commission and the Member States on issues related to network and information security falling within its competencies. 3. The Agency develops a high level of expertise and uses this expertise to stimulate broad cooperation between actors from the public and private sectors. 4. The Agency assists the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security. <p>Tasks</p> <p>The Agency:</p> <ol style="list-style-type: none"> (a) collects information on current and emerging risks that could produce an impact on electronic communications networks, (b) provides the European Parliament, the Commission and European bodies or competent national bodies with advice and assistance, (c) enhances cooperation between actors in its field, (d) facilitates cooperation on common methodologies to address network and information security issues, (e) contributes to awareness-raising on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including methods of alerting users and seeking synergy in public and private sector initiatives, (f) assists the Commission and the Member States in their dialogue with industry, (g) tracks the development of standards for products and services on network and information security, (h) advises the Commission on research in the area of network and information security and the use of risk prevention technologies, (i) promotes risk assessment activities on prevention management solutions, (j) contributes to cooperation with third countries and international organisations, (k) expresses independently its own conclusions, orientations and gives advice on matters within its scope and objectives.
<p>Governance</p>	<p>Management Board</p> <p>One representative from each Member State, three representatives appointed by the Commission, as well as three representatives, proposed by the Commission and appointed by the Council, without the right to vote, each of whom represents one of the following groups:</p> <ol style="list-style-type: none"> (a) information and communication technologies industry; (b) consumer groups; (c) academic experts in network and information security. <p>Permanent Stakeholders Group</p> <ul style="list-style-type: none"> – 30 high-level experts representing the relevant stakeholders, such as the information and communication technologies (ICT) industry, ICT user organisations and academic experts in network and information security. – Following an open call, the Members are selected by the Executive Director, who after informing the Management Board of his decision, appoints the selected applicants <i>ad personam</i> for a term of office of 2,5 years. <p>Executive Director</p> <p>Appointed by the Management Board, from a list of candidates proposed by the European Commission and following a hearing in the European Parliament, for a term of five years.</p> <p>External audit</p> <p>European Court of Auditors.</p>

	<p>Internal audit Internal Audit Service of the European Commission.</p> <p>Discharge authority European Parliament on a recommendation from the Council.</p>
<p>Resources made available to the Agency in 2011 (2010)</p>	<p>Final Budget 8,1 million euro (8,1 million euro) of which the Union subsidy is 100% (100%)</p> <p>Staff at 31 December 2011 44 (44) posts foreseen in the establishment plan, of which occupied: 41 (40). Other posts occupied: 13 (11) Contract Agents, 4 (2) Seconded National Experts. Total staff: 58 (53), undertaking the following tasks: operational: 40 (34) administrative: 18 (19)</p>
<p>Products and services in 2011 (2010)</p>	<p>WS¹⁴: the Agency as facilitator for improving cooperation The principal goal of the first Work Stream was to support the European Commission and the Member States in building on current cooperation schemes to intensify the exchange of information and cooperation between Member States. This includes providing data and opinions to the Commission in order to assist them in drafting new regulation as well as the identification and promotion of good practice in support of such legislation. This work fed into and takes into account the discussions at the European Forum for Member States (EFMS) and the European Public Private Partnership for Resilience (EP3R). The problems to be solved have been described in other documents, notably the European Commission's Communications on Security (COM 2006 251), the CIIP (COM 2009 149), which highlighted the importance of network and information security and resilience for the creation of a single European Information Space, and the Digital Agenda. As interdependencies become complex, a disruption in one infrastructure can easily propagate across boundaries (geographical and jurisdictional) as well as into other infrastructures and have a European-wide impact. The global nature of telecommunication business requires a common approach to deal with issues such as resilience and security of public communication networks. Number of deliverables: 13</p> <p>WS2 – Improving Pan-European CIIP¹⁵ & Resilience The objective of work stream 2 is to assist Member States in implementing secure and resilient ICT systems and to increase the level of protection of critical information infrastructures and services in Europe. This Work Stream is closely aligned with the CIIP Action Plan described in the Commission's communication of March 2009 and of March 2011. Much of this work also directly supports objectives laid down in the Internal Security Strategy document as well as the Digital Agenda. Work packages in the area of CIIP are, for the most part, a natural continuation of work carried out as part of the work programme of 2010. More specifically, the objectives of this work stream are: <ul style="list-style-type: none"> – To enhance the operational capabilities of Member States by helping relevant stakeholders to increase their level of efficiency and effectiveness – To support and promote exercises on a pan-European level – To identify and address the information security challenges in CIIP – To identify and address information security issues in ICT and Interconnected Networks – To support to the EU-U.S. Working Group on Cyber-security and Cyber-crime established in the context of the EU-U.S. summit of 20 November 2010. Number of deliverables: 16</p> <p>WS3 : the Agency as promoter of privacy & trust WS3 comprised of four work packages (WPK): <ul style="list-style-type: none"> – Understanding and analysing economic incentives and barriers to information security. – Ensuring that privacy, identity and trust are correctly integrated into new services. – Supporting the implementation of article 4 of the ePrivacy Directive (2002/58/EC). – Promoting the establishment of a European Cyber Security month. The first WPK analysed the economic barriers and incentives for improving information security at the pan-European level. The Agency analysed economic drivers and barriers in legal, policy, technical and educational areas and identified potential improvements. The second WPK examined how privacy, identity and trust are integrated into new services, proposing recommendations for improvements. The goal was to assess and evaluate current developments in protecting the privacy of individuals and in enhancing the level of trust in network services. The third WPK covered the support that the Agency provided for the implementation of Article 4 of the ePrivacy Directive. This was a continuation of the collaboration with Art.29, the EDPS as well the European Commission (DGs JUST and INFOS) and aimed at investigating how to practically implement at EU level the provisions of Article 4.</p>

¹⁴ WS: Work stream

¹⁵ CIIP: Critical Information Infrastructure Protection

	Finally, the Agency collaborated with Member States on the organisation of a European Cybersecurity month. Number of deliverables: 5
--	---

Source: Information supplied by the Agency.

THE AGENCY'S REPLY

12. As stated by the Court, budget implementation improved in 2011. In order to further reduce the carry overs, the Agency started its procurement planning for 2012 and managed to launch respective procurement procedures related to activities provided for in the Work Programme 2012 in the last quarter of 2011. This practice should show results at the end of 2012.

13. The Agency has streamlined its asset management with the introduction of ABAC Assets, the asset management module introduced by the Commission and used by Institutions and Agencies. The said tool, that is fully deployed and used in 2012, provides for unique identification of all assets registered, therefore the comment of the Court is fully addressed.

14. The Agency has adopted relevant guidelines on the recruitment of staff on 2 March 2012, which fully address the comment of the Court. These guidelines are handed out to the members of the Selection Boards as soon as they are appointed by the Executive Director.