Brussels, 5.8.2009
COM(2009) 419 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Annual Report to the Discharge Authority on internal audits carried out in 2008

(Article 86(4) of the Financial Regulation)

{SEC(2009) 1102}

EN **EN**

TABLE OF CONTENTS

## 1.	INTRODUCTION

This report informs the Discharge Authority about the work carried out by the Commission's Internal Audit Service (IAS), in accordance with Article 86(4) of the Financial Regulation (FR). It is based on the report of the IAS according to Article 86(3) of the FR on key audit findings and, in accordance with professional standards, on significant risk exposures and control issues and corporate governance issues.

This report is based on IAS audit and consulting reports finalised in 2008[1]. It concerns audit and consulting work related to Commission DGs and Services and executive agencies only. It does not cover the IAS work on other agencies or bodies.

The Commission's reactions to the findings and conclusions of the Internal Auditor are covered in the synthesis report on the annual activity reports of the Directors-General. In this synthesis report, adopted at the same time, the Commission takes a position on the cross-cutting issues raised by the Internal Auditor, the European Court of Auditors and the Discharge Authority, or identified by the Audit Progress Committee and by the Director-General for Budget in his overview report.

## 2.	WORKING ENVIRONMENT AND AUDIT PLAN

### 2.1.	Working environment

The revised Internal Control Standards came into force at the beginning of 2008. DGs were asked to select the standards they wish to give priority with a view to demonstrating effectiveness. At the request of several DGs, DG BUDG issued guidelines on assessing the effectiveness of the internal control systems in order to help the Directors-General perform this exercise.

A review of the current Commission risk management, which has been in place for three years and two months, was carried out by DG BUDG.

Amendments were made (by SG and DG BUDG) to the standing instructions for preparation of the annual activity reports, in particular relating to the functioning and effective implementation of the internal control standards and to reporting reputational events.

In March 2008 the Commission decided on a series of measures to be taken in relation to ethics, including a broad discussion in all DGs of the draft statement of principles of professional ethics and appointment of an ethics correspondent in every DG.

The IAS continued to enjoy the full support of the College, and the Audit Progress Committee (APC), which enabled it to remain independent and objective in performance of its tasks.

---

[1]	Some reports drafted in 2008, but finalised at the beginning of 2009, have also been included in this report.

2.2. Developments in the internal audit process

The external quality assessment of the IAS was completed in July 2008, certifying that the IAS's audit activity within the Commission generally complies with the Institute of Internal Auditors' (IIA) Standards and Code of Ethics. Action taken following this certification included a reflection on a more detailed definition of the audit universe, quantitative assessment of the audit coverage, intensified planning and risk assessment in favour of a single audit approach and establishment of an audit report users' group that developed a revised internal audit reporting template.

In addition, in order to free resources for additional audits and increase coverage, a new follow-up strategy is now focusing on a more risk-based approach targeting only high-risk areas and concentrating on implementing recommendations classified as "critical" or "very important".

A fully fledged vocational training programme for internal auditors was elaborated in cooperation between the IAS, Auditnet and DG ADMIN. This programme allows all internal auditors in the Commission to develop the required skills over a period of two or three years, in line with the IIA's Professional Practices Framework, so that they become well prepared to pass the certification tests organised by the IIA.

2.3. Implementation of the IAS audit plan

The IAS Strategic Audit Plan for 2007-2009, drawn up in close cooperation with the IACs, was updated.

In all, 89% of the 2008 work programme was implemented, including 100% of the "C1" engagements (those identified in the audit plan endorsed by the APC as having to be finalised by the end of 2008): 93 reports (36 audit reports, 51 follow-up reports, 2 reviews, 1 consultancy report and 3 management letters) were completed in 2008[2]. Executive summaries of these can be found in the Annex, together with details of the rates of acceptance and, where available, of implementation of the recommendations.

DG	Engagement	Issue date (2008 unless stated otherwise)
List of completed IAS reports		
Administrative and other support systems		
ESTAT	Follow-up on local IT management*	26.2
EPSO	Facilitated self-assessment of a proposed organigramme	9.4
ECFIN	Implementation of selected internal control standards in DG ECFIN*	11.4

---

[2] Some reports drafted in 2008, but finalised at the beginning of 2009 have also been included in this report.

OPOCE	Procurement*	7.5
OIL	Evaluation of targeted internal control standards	19.5
ECFIN	Follow-up on local IT management in DG ECFIN*	27.6
PMO	Missions	11.7
BUDG, LS, AIDCO, EAC, INFSO, EACEA	Recoveries	7.10
DIGIT	Corporate data network infrastructure and services	17.10
SCIC	Follow-up on financial management and procurement	3.12
ADMIN	Monitoring of security managed by ADMIN-DS	11.12
LS	Local IT	11.12
ADMIN, OIB, INFSO, RTD, SG, TRADE	Ethics in the Commission	12.12
DGT	Follow-up on demand management	17.12
BUDG	Management letter on ethics in the Commission	19.12
SG, BUDG, ADMIN, DIGIT	Management letter on IT procurement and service delivery in the Commission	19.12
PMO	Follow-up on regularity of financial management and implementation of financial circuits	22.12
ADMIN, AGRI, AIDCO, BUDG, COMM, COMP, DEV, EAC, ECFIN, ECHO, ELARG, EMPL, ENV, ESTAT, INFSO, JLS, JRC, LS, MARE, MARKT, OLAF, OPOCE, REGIO, RELEX, RTD, SANCO, SG, TAXUD, TRADE	Follow-up on IAS validation of self-assessment of the Internal Audit Capability	Various dates
OLAF	Anti-fraud information system (AFIS)	21.1.2009
OIB	Follow-up on evaluation of targeted internal control standards	22.1.2009
OIB	Follow-up on management of procurement contracts	23.1.2009
Internal policies		
PHEA	Public Health Executive Agency	24.1
INFSO	Management of research information systems	31.3
SANCO	Follow-up on the effectiveness and efficiency of the SPP/ABM cycle	1.4
TREN	Follow-up on the effectiveness and efficiency of the SPP/ABM cycle	11.4

EACI	Follow-up on the EACI	18.4
RTD	Management of research information systems	22.4
EAC	Second follow-up on the in-depth audit	25.4
RTD, INFSO, TREN, ENTR, DIGIT	Management letter on inter-DG FP7 IT governance	26.5
COMP	Follow-up on the effectiveness and efficiency of the SPP/ABM cycle and activity-based management	29.5
MARKT	Follow-up on local IT management process	17.6
ENV	CITL management in DG ENV*	10.7
JLS	Follow-up on IT management	14.7
JLS	Grants under shared management of the European Refugee Fund	4.11
COMP	Recovery of fines	13.11
JLS	IT procurement	17.11
INFSO	Follow-up on *ex-post* controls (2006)	8.12
EACEA	Grant management, awarding and contracting	11.12
RTD	Follow-up on *ex-post* controls (2006) and financial circuits and financial management (2007)	11.12
TREN-TEN-T	Audit of the TREN-TEN-T Executive Agency	16.12
SANCO	Follow-up on large IT systems	21.1.2009
SANCO	Grant management in the food safety, animal health and welfare and plant health activity	30.1.2009
Structural measures		
REGIO	Review on financial corrections and recoveries in the Structural Funds area	14.11
EMPL	Review on financial corrections and recoveries in the Structural Funds area	14.11
REGIO	Internal control system for managing the new Structural Funds programming period – Phase I	19.11
EMPL	Internal control system for managing the new Structural Funds programming period – Phase I	19.11
REGIO	Follow-up on financial corrections in the Cohesion Fund (2006)	12.12
External policies		
AIDCO	Second follow-up on the in-depth audit	20.6
AIDCO	Financial management procedures of Directorate C related to its devolved delegations**	30.6

AIDCO	Financial management of regional projects	18.7
ELARG	Follow-up on *ex-post* control activities	18.7
ELARG	Readiness assessment/phasing-in of delegations in the Balkans	17.12
AIDCO	Financial management of main programmes in Directorate B	22.12
AIDCO, ECHO	Follow-up on FAFA implementation	22.1.2009
RELEX	Follow-up on *ex-post* control activities	23.1.2009

* Joint audit/follow-up with the Internal Audit Capability (IAC) of the DG concerned.

** Audit carried out by the IAC of DG AIDCO in cooperation with the IAS.

2.4. Acceptance of recommendations and views of auditees and stakeholders

In 2008 the rate of acceptance of audit recommendations by auditees was 99.4%.

Commission and executive agency audits				
Recommendations	**Accepted**	**Rejected**	**%**	**Total**
Critical	0	0	0	**0**
Very important	150	2	46	**152**
Important	160	0	49	**160**
Desirable	15	0	5	**15**
%	99.4	0.6		
Total	**325**	**2**		**327**

Feedback from auditees on the scope and conduct of the audits yielded an average result of 1.74 on a scale from 1 (highest) to 4 (lowest) compared with 1.86 for 2007 and 1.95 for 2006. A fresh stakeholder survey at the beginning of 2009 found that 90.8% thought that the IAS had a clear audit strategy, 83.1% that audits were performed with honesty, objectivity and fairness and 61.5% that the IAS recommendations were readily useful, while, overall, 86.2% considered that the IAS's work contributes to the quality of management and control systems in the Commission.

3. MAIN FINDINGS AND RECOMMENDATIONS

Ethics

An audit on the Commission's ethics framework in two horizontal and four operational DGs came to the conclusion that the ethics framework is reasonably solid and complete and that

the DGs audited had recently taken or were currently taking a number of additional measures to raise awareness of or improve the ethics framework.

The audit found that there was a need for further clarification of the existing rules, including on gifts, hospitality and reporting conflicts of interest, backed up by guidance from central DGs and more intense monitoring of implementation.

Awareness on the part of all staff of their obligations, both now and after employment with the Commission, and communication to staff about enforcement measures is constantly being improved.

Procurement and grant management

The series of audits on IT procurement and service delivery was completed with an audit in one operational DG and a management letter on IT procurement and service delivery.

Improvements in this area have been concentrating on strengthening central management to provide support and guidance, closer coordination at Commission level to ensure that priorities are set optimally and that best value for money is obtained and greater involvement of senior DG management in developing and monitoring implementation of sourcing strategies.

In addition to the IT procurement reports, two follow-up audits and three new audits addressed procurement and/or grant management processes. Issues identified in these audits included the concentration on a limited number of contractors (as in IT procurement) that could be reduced by a formal outsourcing strategy. There was a lack of a consolidated procurement manual, of a comprehensive management information system and of an integrated all-encompassing strategy for auditing funds and a need for improved terms of reference and technical specifications, for more adequate monitoring of and reporting on contracts and for better workload management.

Executive agencies

As the number of executive agencies continues to increase, the related control and audit issues are coming increasingly into the limelight.

In 2008, four audits of executive agencies were completed, relating to the internal control system, grant management, awarding and contracting, the administrative budget or recoveries[3]. While the overall results were fairly positive, the findings were mainly influenced by the fact that the protracted start-up phase of the agencies had resulted in non-compliance with either the Financial Regulation for executive agencies (i.e. with the "four-eyes" principle) or with the legal base (composition of the Steering Committee, publication of budgets and meeting international accounting standards), non-transfer of fixed assets from the "parent" DG to its executive agency or a need to streamline and harmonise the procedures of the parent DG.

---

[3]   See the section on recovery.

IT issues

The extensive audit work related to IT issues (other than procurement) was continued with one management letter, six audit reports and five follow-up reports.

Five follow-up reports on local IT management were completed. In three cases the corresponding action plans were almost fully implemented. However, in one case almost half the measures in the action plan were delayed and in another one third of the recommendations were still being implemented.

Two new reports covered management of research information systems. One of them came to the conclusion that, due in particular to the lack of harmonised business processes, there was no reasonable assurance regarding the processes audited. Common risks included delays in projects, possible unavailability of systems, inoperability of different IT modules and security issues such as insufficient protection of IT assets and lack of controls to safeguard the logical and physical security of IT assets. These two audits also led to more systemic considerations that are being taken into account by the relevant DGs with a view to extending the role of the joint IT Project Steering Committee in order to oversee all common and shared IT systems and projects in the research family and to developing an IT systems architecture ensuring business process coherence and IT interoperability.

The corporate data network is one of the seven corporate IT services identified as critical for the entire Commission in the context of business continuity plans. While reasonable assurance could be given on operation of the corporate data network, improvements are needed in management of the network (by strengthening the management of network configuration changes and providing an exhaustive list of services offered to users) and the logical security arrangements (*inter alia*, by adopting central security standards and guidelines to ensure system security and a continuous service). The audit identified governance issues in the information systems security framework which were resulting in significant delays in drawing up the implementing rules and in actual implementation of certain security measures. To address this issue, the audit particularly recommended further clarification of the roles of ADMIN/DS and DIGIT regarding IT security and close, structured cooperation between ADMIN/DS and DIGIT on development of IT security standards, drawing on the available expertise.

Recoveries and financial correction

An audit engagement in two horizontal and four operational DGs addressed management of the recovery of sums unduly paid under centralised management[4]. Recommendations were made on every phase of the recovery process: better monitoring tools are needed in several operational DGs to provide more detailed and up-to-date information to detect unduly paid amounts; more systematic issuing and follow-up of revenue forecasts are needed in order to ensure that all recovery orders are issued, together with close monitoring of deadlines for issuing pre-information letters and recovery orders; and delays in the recovery processes should be shortened, with more systematic monitoring. One specific issue was identified in an executive agency audited in this context: as executive agencies have their own legal personality and therefore their own legal units, the Commission is not responsible when a recovery order is issued by an agency or a decision supporting it is disputed by the contractor.

---

[4]   The audit also covered the recovery of conditionally reimbursable loans (related to the MEDIA projects).

In some cases, there is a risk of ineffective recovery of unduly paid funds. In the absence of legal restrictions, this risk will be mitigated by the conclusion of a service-level agreement between executive agencies and the Commission's Legal Service, defining the conditions under which the latter would provide legal support to the agencies in the recovery process.

Two reviews addressed financial correction and recoveries in the Structural Funds. Significant efforts have been made by the Structural Funds DGs to deliver the actions set out in the action plan by the deadlines required and the IAS recognised the complexity of the financial correction processes both at Commission level and in relation to the reporting by Member States. Issues for consideration were included in the reports regarding the need for a harmonised approach to the point in time when revenue forecasts are accounted for and the procedure for quarterly reporting on financial corrections to DG BUDG. Overviews on all potential financial corrections in the pipeline and on the timeliness of audits feeding into the financial correction process will considerably increase the Commission's monitoring capacity.

An audit on recovery of fines revealed no significant weaknesses in the effectiveness of the recovery process.

PMO (*financial management and financial circuits*)

A follow-up audit of financial circuits and financial management in PMO came to the conclusion that the recommendations had not been adequately and effectively implemented. This was partly due to the difficulties encountered with implementation of the new IT system for management of careers, rights and salaries (SYSPER2, IRIS and NAP). There was still a need to ensure the quality (accuracy and completeness) of personal data, the interoperability of the systems involved and that all necessary documents related to individuals are maintained in a single global information system. Other open recommendations relate to the need to tighten operational and *ex-post* controls and management of personnel files and for an updated table of sub-delegated responsibilities, documenting procedures and checklists and updated job descriptions.

For management of payment of mission expenses, the audit recommended improving the system of *ex-ante* controls, with a view to reducing the number of errors, and stepping up training for payment officers in order to avoid incorrect or multiple reimbursement. PMO management established an action plan to address all these issues.

Security

An IAS audit on security monitoring in the Commission, as managed by the Security Directorate in DG ADMIN, made a number of recommendations concerning, *inter alia*, the need to improve the regulatory framework and bilateral arrangements, definition of the roles and responsibilities of local security officers, the security authorisation process, systematic reporting on the state of play with security in the Commission as a whole and security rules for protection of sensitive non-classified information. The results of this audit will be included in a management review of security policy within the Commission.

External policies

The follow-up reports on external policies revealed that the Commission should pay particular attention to implementation of past recommendations in this area[5].

The follow-up audit of the Financial and Administrative Framework Agreement (FAFA) confirmed that major achievements had made it possible to close five of the eight recommendations. However, there were some delays in implementation, in particular of the outstanding recommendation to agree on further means of securing assurance from the UN.

Three new audits[6] on external policy were completed, two of which were accompanied by a partially unsatisfactory audit opinion. In the case of the audit on the management of regional projects, this was due to significant observations relating to the SADC (Southern African Development Community) Secretariat, combined with the situation of the EC Delegation in Botswana. Other issues raised were the acute shortage of staff, the long project inception phase, the lack of streamlined EDF (European Development Fund) and SADC procedures, the limited integration between national and regional components and, more generally, the monitoring mechanisms to be strengthened for joint management relating to ACP regional organisations. In the case of the audit on financial management of the Latin American programme, the part found unsatisfactory in the audit opinion – contested by the auditee – related to shortcomings identified under decentralised management in Latin American Delegations: insufficient *ex-ante* assessment of compliance with the Financial Regulation and other weaknesses which significantly limit the assurance expected from key control layers (e.g. insufficient project and portfolio monitoring and low quality of mandatory project audits).

Follow-up

Despite the new, more risk-based, follow-up strategy, a substantial part of the audit work still related to follow-ups. One major activity was the follow-up of the 2007 external quality review of Internal Audit Capabilities (IACs). The result was generally positive, with a very large majority of IACs (26 out of 29) still to complete or partially implement no more than two recommendations.

The remaining follow-up audits found eleven cases (concerning AIDCO, EAC, ECFIN, ELARG, OIB, PMO, RELEX, RTD and SANCO) in which more than one recommendation had not yet been implemented. In five of these cases (concerning OIB, PMO, AIDCO/ECHO and ELARG) the progress made with implementation was clearly insufficient, with more than half of the recommendations not yet implemented.

A more detailed progress report is sent to the APC twice a year. The latest found that 29% of the recommendations (two out of the three critical and 41 out of 147 very important recommendations) were overdue by more than six months (compared with 25% a year ago – seven out of 14 critical and 37 out of 138 very important recommendations).

---

[5]   In the case of the second follow-up of the in-depth audit of DG AIDCO, six out of 22 recommendations were more than one year past the original target date and in the case of the follow-up on *ex-post* controls in DG ELARG ten out of 15 recommendations were still being implemented and two had been turned into a new recommendation.

[6]   One of which was carried out by the IAC of DG AIDCO in cooperation with the IAS.

4. CONCLUSIONS

On the basis of the Commission audits and reviews finalised in 2008 and other related work the following conclusions can be drawn:

Conclusion 1: Further progress made, but more improvements needed

In the course of its audits, reviews and consultancy work, the IAS saw further improvements in the Commission's internal control systems. Six critical recommendations had been issued in 2007, but none in 2008. The number of unsatisfactory or partly unsatisfactory opinions in new audit reports dropped from six in 2007 to four in 2008. However, further improvements are still needed:

For instance several aspects of financial management can still be improved:

– Significant progress was made concerning the completeness and consistency of the Commission's recovery/financial corrections statistics. For example, DG REGIO and DG EMPL, in collaboration with DG BUDG, have undertaken to produce an overall table on financial corrections (already made or in the process of being made): this will enhance considerably the audit trail of multi-annual controls in shared management. However, in areas of centralised management a backlog of recovery orders is to be noted. Hence, internal recovery procedures need be simplified and shortened.

– Whether it is appropriate to apply the 2% materiality limit of error across the board to both standard financial transactions and certain particularly complex or highly sensitive projects needs to be reassessed. The proposed concept of "tolerable risk of error" – if and when endorsed by Council and Parliament – would be more appropriate and should improve in the future the achievable level of reasonable assurance of financial management in certain areas.

– Attention was drawn to the need for solid monitoring of procurement procedures, especially if major parts of outsourced activities are attributed to a limited number of bidders, exposing the Commission to risks of market concentration.

With regard to Security, considerable progress has been made and follow-up audits confirmed that the difficulties encountered in ensuring that relevant Commission delegations were properly equipped for handling EU classified information have now been resolved. The findings of the audits have also helped the general review of the Commission's security policy, which took place in 2008.

Ethics standards require continuous attention, and throughout the year initiatives at DG and central level have been launched to further strengthen the Commission ethics framework and raise staff awareness. The IAS has not yet provided an audit opinion on the Commission's Ethics framework, but will follow a schedule of actions until the end of 2010.

Timely implementation by the Commission services of critical and very important recommendations is an ongoing challenge. The Audit Progress Committee, assisted by the IAS, holds DGs to account in implementing their own Action Plans. It issues reminders, addressed to portfolio Commissioners, which are generally effective, improving follow-up and facilitating the reassessment of residual risks.

Conclusion 2: IT

The extensive audit work on IT issues showed that an effective and efficient IT environment is important for the successful implementation of the Commission's policies. Greater efforts to follow up past recommendations, an integrated systems approach with a view to gaining an overview of all IT developments at all times and the need for comprehensive security arrangements to guarantee, *inter alia*, business continuity seem more and more important. Better management of projects and service providers are also key success factors.

Conclusion 3: Strong Embedded Audit Culture

The second external quality review of the IAS demonstrated that the service fully complies with the "International Standards for the Professional Practice of Internal Auditing". The IAS is an integrated and accepted driver of positive change in the Commission, covering jointly with the Internal Audit Capabilities all identified risks with the strategic audit plan 2007-2009.

While the IAS audit plan focuses to a large extent on financial management, it also covers areas such as governance (e.g. ethics), IT, security and operations (e.g. implementation of EC law). As reported here, the IAS's audit work helps to draw attention to risks and areas for improving control of risks: it is therefore important that control of non-financial risks should continue to receive attention throughout the Commission.