AB Decision n° 26/2009
Date: 04.02.2009

DECISION n°26

of the Administrative Board of the European Railway Agency

adopting the Internal Audit Service Strategic Audit Plan 2009-2011 for the Agency

THE ERA ADMINISTRATIVE BOARD,

Having regard to Regulation (EC) No 881/2004 of the European Parliament and of the Council ([1]) establishing a European Railway Agency (hereinafter referred to as "the Agency") as amended by Regulation (EC) No 1335/2008[2] of the European Parliament and of the Council of 16 December 2008;

Having regard to the Internal Audit Standards adopted on 28.10.2008 by Decision n° 23 of the European Railway Agency Administrative Board adopting Internal control standards for the European Railway Agency;

Considering that the IAS Strategic Audit Plan 2009-2011 is based on the previous IAS Audit Plan 2008-2010 updated by a risk assessment conducted in 2008;

HAS ADOPTED the Agency's Internal Audit Service Strategic Plan for 2009-2011, as set out in Annex 1 of this decision.

Done at Valenciennes, 04.02.2009

For the Administrative Board

The Chairman

MICHAEL HARTING

Annex 1: ERA IAS Strategic Audit Plan 2009-2011

[1] OJ L 220, 21.6.2004, p. 3
[2] OJ L 354, 31.12.2008 p.51

EUROPEAN COMMISSION

INTERNAL AUDIT SERVICE

Limited distribution

European Railway Agency (ERA)

IAS Strategic Audit Plan for 2009 / 2011

Version: final

Date: 18 November 2008

Table of content

1. EXECUTIVE SUMMARY

This document contains the IAS audit strategy for the period 2009 / 2011 for the European Railway Agency (ERA). It outlines the areas in which the IAS will strive to carry out its work, the audit themes as well as the assumptions on which the work plan is based, including the definition of the "audit universe" and the assessment of risk.

The IAS' audit planning 2009 / 2011 will be coordinated with the work plan of the Internal Audit Capability (IAC) of ERA to avoid any potential overlap. As from 2009, the IAS will update its Risk Assessment annually and adjust its audit planning accordingly.

Audit work planned for 2009

Human Resources Management

According to EC Regulation No 881/2004 and its Annexes, the Agency's main task is to develop technical specifications in the areas of interoperability and safety targets, methods and requirements in the rail sector. Therefore ERA must rely on the expertise of qualified professionals. In this regard, the Agency's selection procedure is a challenging issue, enhanced by the specificity of its areas of competence and by the steadily increasing number of staff hired. In 2008, the Agency plans to carry out the first promotion exercise and launch the staff performance appraisal scheme. The Agency must also have mechanisms put in place in order to attract and retain competent staff.

The independence of staff can also be considered as an important risk factor for the Agency.

The IAS will carry out in 2009 an Audit on Human Resources to assess the effectiveness and efficiency of procedures on recruitment, training, appraisal and career development. It will also focus on the management of conflicts of interests.

IT Risk Assessment

The IAS plans to perform an IT Risk Assessment (based on common IAS Methodology) covering IT Tools and Infrastructure in 2009. This Risk Assessment will provide the Agency Management with an overview of the major IT risks. It will be a reference for future IT audits.

Follow-up

The IAS foresees to perform a Follow-up Audit of all its recommendations still open.

Update of the Risk Assessment

In the context of the preparation of its audit plan for 2010, the IAS will update its current Risk Assessment.

Prospective audit themes for 2010 / 2011

Planning/ Priority Management and Communication

The legal mandate of ERA is still under review. New tasks and responsibilities could be added to the portfolio. Besides, ERA is under the obligation to offer "on demand" opinions and evaluations to external stakeholders on topics linked to the Agency scope. These circumstances increase the importance of an extensive, correct and still flexible planning and a transparent method of priority setting.

In order to manage stakeholder expectations, an efficient way of communicating potentially changing priorities and achievement of objectives is crucial.

The IAS could:

- assess the effectiveness and efficiency of planning and priority setting processes and tools;
- analyse the communication tools and processes with regards to transparency, effectiveness and efficiency.

Document Management

As the Agency strongly focuses on coordination and reporting, document, management is one of the core capabilities needed in ERA. The Agency has developed a publicly accessible database on safety related documents. It also works on the development of an "Interoperability Documents Database".

The IAS could audit the effectiveness and efficiency of document management systems and processes and the efficient application of procedures.

Quality Management

ERA is working in the sensitive areas of safety, investigations, specifications and certifications where Quality Management of operations and output is of increasing importance. Therefore, Quality Management procedures and rules are all the more essential since ERA's mandate is changing and new tasks and responsibilities are added to the existing portfolio. Quality Management is a priority issue. It needs to be effective, efficient and anchored in the operational processes.

The IAS will assess in 2010 / 2011:

- the effectiveness and efficiency of existing processes and tools for Quality Management;
- the compliance of internal controls in operations.

Information Technology

ERA is highly dependent on the reliability of the IT Systems for collecting data and providing its prompt services, as well as system authority for the ERTMS (European Rail Traffic Management System). The Agency highly depends on external IT expertise and deals with complex IT systems.

Based on the results of the IT Risk Assessment planned to be conducted in 2009, a more detailed Audit on IT systems, security and Management could be carried out in 2010 / 2011.

Risk Management

EC regulations have steadily increased the importance of management assurance. One important aspect is the Management of risks, their identification and mitigation on a regular basis.

The IAS could carry out an audit on ERA Risk Management including aspects like the risk framework, the risk assessment processes, risk register and roles and responsibilities.

Stakeholder Management – Expectations management and communication

As described, the mandate of ERA is regularly under review. New tasks and responsibilities could be added to the portfolio. ERA might go through a transition phase in order to progressively adapt to its potentially new mandate and will set and implement new objectives.

As a result, the stakeholders' expectations may substantially change. The Agency should be prepared to demonstrate more than usual that objectives and priorities assigned are achieved. It should also put in place mechanisms to communicate on its new missions and 'raison d'être' to all relevant stakeholders.

The IAS could assess:

- ERA's knowledge about stakeholders and their expectations;
- The communications mechanisms put in place in order to know and manage stakeholders' expectations.

Timing for Annual Audit

The IAS intends to:

- carry out the new Audit in the 1st semester,
- perform the Follow-up Audit and the Risk Assessment update in the 2nd semester of the year.

2. FULL REPORT

2.1. Annual planning for audits

The following table summarises the audit work planned by the IAS for 2009 and the prospective audit themes for 2010 / 2011.

	2009	2010 / 2011
AUDITS	Human Resources Management	Planning/ Priority Management & Communication
		Document Management
		Quality Management
	IT Risk assessment	Information Technology
		Risk Management
		Stakeholder Management
FOLLOW-UP	Closure of old Follow-ups	2010: Human Resources Management
RISK ASSESSMENT	Update of Risk Assessment	Update of Risk Assessment

2.2. Context and process of the IAS Risk Assessment

The Financial Regulation[1] states that the Internal Audit Service (IAS) is the internal auditor of the European Railway Agency (ERA) and this provides the mandate of the IAS.

In line with the professional standards set by the Institute of Internal Auditors (IIA), the IAS "establishes risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals".

This document summarises the IAS audit strategy for the period 2009 / 2011 for ERA. As such, it outlines the areas in which the IAS will strive to carry out its work and the assumptions on which the work plan is based, including the definition of the audit universe and the assessment of risks. It also contains details of the audit themes resulting from the first full risk analysis on Agencies performed by the IAS.

This document describes:

- the basic principles of the audit planning the IAS will use;
- the underlying objectives and the methodology used to define both the "audit universe" and the Risk Assessment.

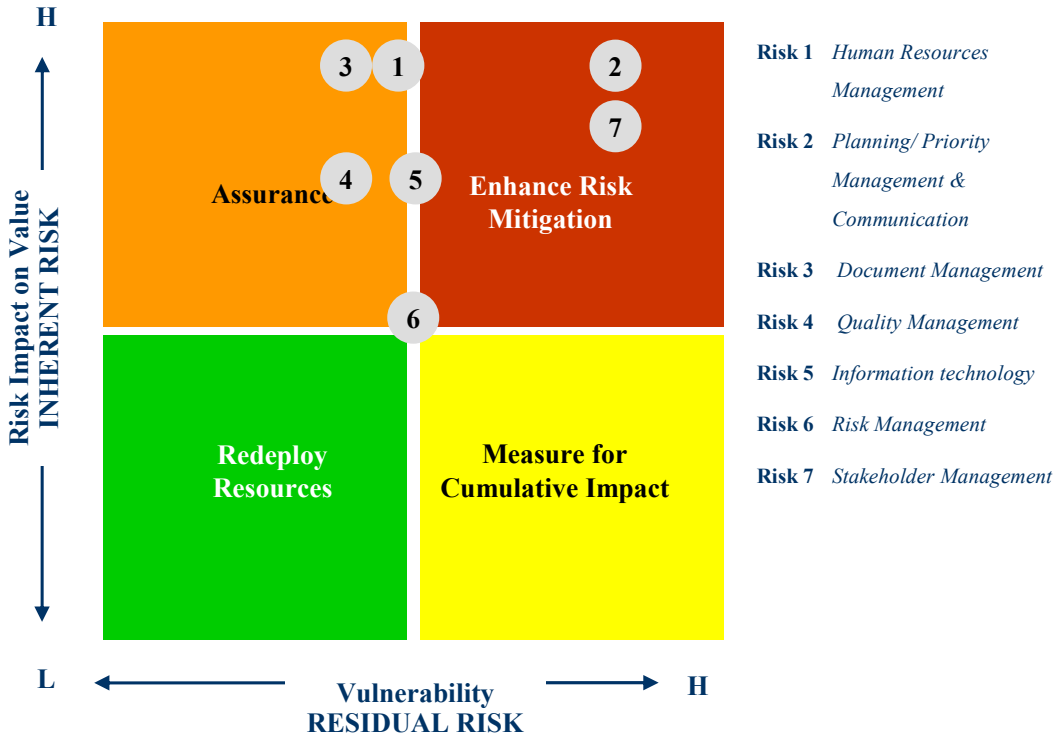
[1] Article 185 of General Financial Regulation.

The document then presents the results of the Risk Assessments and the planned timetable for the IAS audit work in ERA.

The basic internal audit planning principles are provided in annex 1.

2.3. Results of the Risk Assessment and audit themes for 2009 / 2011

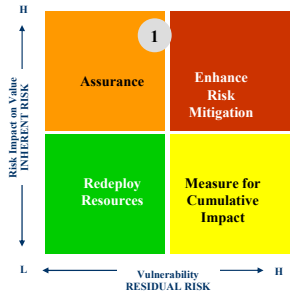
Using the planning methodology as described in annex 1, the IAS identified 7 major risks and constructed the ERA Risk Map Profile as shown thereafter:



The individual components of this Risk Map Profile are summarised in the tables below:

Risk 1 – Human Resources Management

Risk factor 1:	Difficulty of attracting and retain candidates with appropriate expertise
Risk factor 2:	High dependency on experts
Risk factor 3:	"Open-end" mandate requires quick reaction in terms of recruitment
Risk factor 4:	Compliance with Staff Regulations for HR processes
Risk factor 5:	Conflict of interest
Impact:	High
Vulnerability:	Medium



Audit theme 1:	**Effectiveness, efficiency and compliance of procedures on recruiting, training, appraisal and career development**
Planned in:	**2009**

Risk 2 – Planning/ Priority Management & Communication

Risk factor 1: Mandate under review leading to more responsibilities and tasks

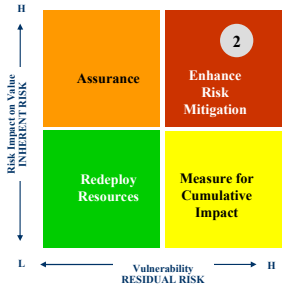
Risk factor 2: Non-achievement of objectives due to "on-demand" delivery of opinions and evaluations and change of priorities

Risk factor 3: Inadequate planning and priority setting

Risk factor 4: Insufficient management of stakeholders – Lack of Communication with them

Impact: High

Vulnerability: High



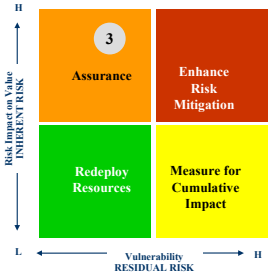
Audit theme 2: **Effectiveness and efficiency of planning and priority setting processes and tools.**

Analysis of the communication tools and processes with regards to transparency, effectiveness and efficiency

Planned in: **2010 / 2011**

Risk 3 – Document Management

Risk factor 1:	Assurance of knowledge management
Risk factor 2	Dependence on effective documentation as core process of the Agency
Risk factor 3:	Highly dependence on IT systems built externally
Impact:	High
Vulnerability:	Medium



Audit theme 3:	**Effectiveness and efficiency of document management systems and processes** **Efficient application of procedures**
Planned in:	**2010 / 2011**

Risk 4 – Quality Management

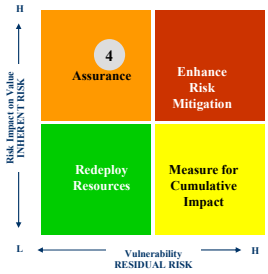
Risk factor 1: Sensitivity of operations of ERA (safety, certification, investigations)

Risk factor 2: Increased importance of Quality Management for existing portfolio due to the constantly changing mandate of the Agency

Risk factor 3: Risk of relying upon people instead of integrated Quality control procedures

Impact: High

Vulnerability: Medium



Audit theme 4 **Effectiveness and efficiency of existing processes and tools for Quality Management**
Compliance of internal controls in operations

Planned in: **2010 / 2011**

Risk 5 – Information Technology

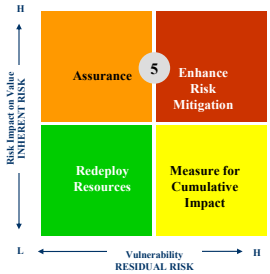
Risk factor 1: Dependence on IT systems for core operations

Risk factor 2 Complexity of IT applications

Risk factor 3: Reliance upon external IT knowledge

Impact: High

Vulnerability: Medium



Audit theme 5: **IT Risk Assessment (based on common IAS Methodology) covering IT Tools and Infrastructure in 2009.**

More detailed Audit on IT systems, security and management in 2010 / 2011 (based on the results of this IT Risk Assessment)

Planned in: **2009 and 2010 / 2011**

Risk 6 – Risk Management

Risk factor 1: Risk Management as integral part of management assurance

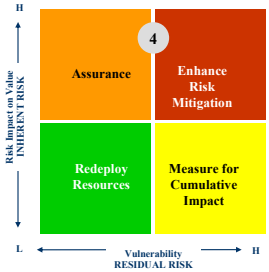
Risk factor 2 Proactive management of risks and potential risks

Risk factor 3: Tools for Risk Management in place and used effectively

Risk factor 4: Management involvement in Risk Management and mitigation

Impact: High

Vulnerability: Medium



Audit theme 6: **Risk Management: risk framework, Risk Assessment processes, risk register, roles and responsibilities**

Planned in: **2010 / 2011**

Risk 7 – Stakeholder Management

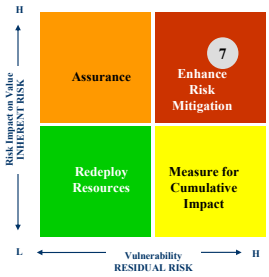
Risk factor 1: Potential change of mandate for ERA

Risk factor 2 Lack of proactive management of stakeholders' expectations

Risk factor 3: Effectiveness of communication with stakeholders

Impact:

Vulnerability:



Audit theme 7: **Knowledge about stakeholders, management of stakeholders' expectation, quality management of the external and internal communications mechanisms put in place in order to answer new objectives**

Planned in: **2010 / 2011**

2.4. Next steps

As the main addressees of audit reports are the Director and the Governing Board, it is necessary that this planning be endorsed by the Board of ERA. The annual review of the Risk Assessment will take into account the results of:

- the audits conducted by the IAS, the IAC and the ECA (together with the results of the discharge);
- the annual Risk Assessment carried out by the Agency.

This will allow the IAS to regularly submit the extended audit plan to the Director and the Board.

ANNEX 1 - BASIC INTERNAL AUDIT PLANNING PRINCIPLES

The audit strategy is based on: the Framework Financial Regulation (FFR), the IAS Charter and the IIA standards.

The FFR states: "*The internal auditor shall advise the Community Body on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management*"[2].

The IAS Charter states that in order to perform its mission properly, the IAS must act in accordance with generally recognised principles and international standards governing internal audit.

IIA standard 2010 requires that "*The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals*". IIA standard goes on to state: "*The internal audit activity should evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding:*

- *Reliability and integrity of financial and operational information*
- *Effectiveness and efficiency of operations*
- *Safeguarding of assets*
- *Compliance with laws, regulations, and contracts.*"

As the European Court of Auditors (ECA) focuses its activities on the first control objective mentioned above, the IAS will coordinate its audit activity with this institution to avoid overlap.

In line with the IIA Professional Framework, the IAS will cover Internal Control, Risk Management and Governance.

Risk based planning methodology: Definition of the audit universe and audit Risk Assessment.

The IAS's approach to the Strategic Plan contains three steps:

(1) Clearly define what constitutes the different auditable systems, processes, units and bodies which make up the Agency's overall audit universe ;

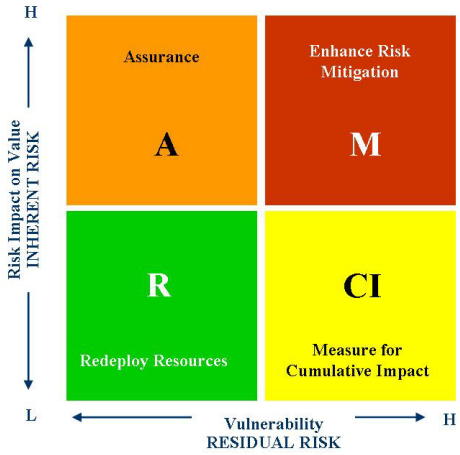
(2) Make an assessment of the risks associated to the auditable units ;

(3) Identify the audit themes flowing from the risks identified and validated with the Management.

[2] Article 72 of Framework Financial Regulation.

The IAS stressed on the 'value-added' of the planned audits when preparing the audit plan. The professional judgement of the auditor plays a critical role in determining where focus should be placed when auditing. In making this determination, the IAS will consider the impact (inherent risk) of a risk if a control breakdown occurs and the vulnerability (residual risk) of the controls in ERA. These two dimensions are shown in Figure 1: Framework Risk Profile.

Figure 1: Framework Risk Profile



Management's own Risk Assessment is a key element taken into account by auditors in their Risk Assessment. Although the IAS will carryout its own Risk Assessment the audit approach and focus is influenced by management's assessment of impact of risks and the vulnerability of its core processes. This is elaborated below.

Reassurance: When Management provide reasonable assurance (Fig. 1: "A" quadrant) that controls to prevent, detect, correct, a risk are both effective and efficient, the role of the Internal Audit Service is to provide reassurance that Management's reports can be relied upon. When Management can only provide "qualified" assurance — meaning that some controls are working while others are not — the IAS should audit the controls that are deemed to be effective and support improvement in other areas as required.

Enhance risk mitigation: When Management is unable to provide any assurance (Fig. 1: "M" quadrant) that controls are either effective or efficient, it should address risks requiring mitigation. In this situation, the added value might be limited if the Internal Audit Service work simply confirms the existence of risks already well known by Management. However, the Internal Audit Service could provide recommendations to help Management to develop and to design controls aimed at reducing exposure and track progress on remediation plans.

Redeploy Resources: For the processes leading to risk with low impact on value, and low vulnerability, the Internal Audit Service could test controls for effectiveness and develop recommendations helping Management to improve efficiency (Fig. 1: "R" quadrant).

Measure for Cumulative Impact: Finally, in case of low impact on value associated with a high vulnerability, the Internal Audit Service could assess cumulative impacts and frequency to determine whether these risks may in aggregation have a more significant impact (Fig. 1: "CI" quadrant).

Definition of audit universe and Risk Assessment

The definition of the audit universe involved mapping standard Agency processes. At an aggregate level, the audit universe of the Agency has been broken down into 22 processes. These processes were mapped to the possible risk types (see **Annex 2** for the standard template). They were then assessed for risk mainly through:

- an extended analysis of existing documents;
- interviews with key people in the organisation when possible.

ANNEX 2 - STANDARD TEMPLATE FOR ASSESSMENT OF AUDIT RISK AGAINST STANDARD AGENCY PROCESSES

Entity: ERA