

DECISION 34/2014/GB

OF THE GOVERNING BOARD OF THE EUROPEAN POLICE COLLEGE

ADOPTING THE EUROPEAN POLICE COLLEGE'S
POLICY ON IDENTIFICATION AND MANAGEMENT OF SENSITIVE FUNCTIONS

Adopted by the Governing Board
on 12 November 2014

THE GOVERNING BOARD,

Having regard to Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL)¹;

Having regard to Decision 01/2014/GB of the Governing Board of the European Police College (CEPOL) adopting the Financial Regulation and repealing decision 28/2011/GB;

Having regard to Decision 08/2011/GB of the Governing Board of the European Police College (CEPOL) adopting the European Police College's Internal Control Standards and repealing decision 36/2007/GB;

Having regard to the Internal Audit Service Report on HR Management recommending that the Agency should identify sensitive functions, as defined in the Commission's Guidance on sensitive functions -SEC(2008)77.

Whereas:

Internal Control Standards 7 'Operational structure' requires that the risks associated with sensitive functions are managed through mitigating controls and ultimately staff mobility.

Internal Audit Service Report on HR Management recommends that CEPOL should identify sensitive functions, as defined in the Commission's Guidance on sensitive functions - SEC(2008)77.

HAS DECIDED AS FOLLOWS:

Article 1

To adopt the European Police College's Policy on identification and management of sensitive functions.

Article 2

This decision shall enter into force on the day of adoption by the Governing Board. Any update during the course of the implementation of the Policy which does not affect relevant or sensitive parts of its content, can be decided by the Director who will inform the Governing Board accordingly.

Done in Rome, 12 November 2014

For the Governing Board

*Rossanna Farina
Chair of the Governing Board*

¹ OJ L 256, 1.10.2005, p. 63. Decision as amended by Regulation (EU) No 543/2014 (OJ L 163, 29.5.2014, p. 5)

Policy on identification and management of sensitive functions	Document number:	PO.INCO.005-1
	Approval date:	12/11/2014

DOCUMENT CONTROL SHEET

Process area Agency Support Processes
Main process Internal Control
Main process owner Director

TABLE OF CONTENT

Reference	Title	Pages (from-to)
Cover	Cover Page	1
DCS	Document Control Sheet	2
Content	1. Background	4
	2. Definition	4
	3. Criteria for defining sensitive posts (Identification)	4-5
	4. Defining the preventing measures and mitigating controls in order to reduce the risk	5
	5. Managing sensitive posts	5-6
	6. Conclusions	6

Abbreviations

CEPOL	European Police College
ICS	Internal Control Standards
AO(D)	Authorizing Officer (by Delegation)
AIPN	Autorité Investie du Pouvoir de Nomination (Appointing Authority)

Definitions

Sensitive functions Those functions where a member of staff executing an activity, has a degree of autonomy and/or decisional power sufficient to permit them, should they wish so, to misuse these powers for personal gain (financial or otherwise)²

Sensitive information³ Information whose unauthorised disclosure might undermine the private or public Interests protected by the legislation in force.

Confidentiality⁴ The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

LOG OF ISSUES

Issue	Issue date	Change description
001	28/10/2014	First issue

² EC Guidance on sensitive functions

³ ³(based on the Commission Decision of 23 January 2002 amending its Rules of Procedure – Annex Provisions on Document Management and REGULATION (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; BS ISO 15489-1:2001)

Policy on identification and management of sensitive functions

Document number:

PO.INCO.005-1

Approval date:

12/11/2014

1. Background

The overall purpose for defining sensitive functions is to prevent fraud and corruption within the EU institutions and bodies. In addition to safeguards provided by the management systems, IT-tools and internal controls, certain sensitive functions can be subject to rotation if the related residual risks are not properly mitigated or reduced to an acceptable level.

In general, sensitive functions are those where a member of staff executing an activity, has a degree of autonomy and/or decisional power sufficient to permit them, should they wish so, to misuse these powers for personal gain.

Internal Control Standard 7 'Operational structure'⁵ requires that risks associated with sensitive functions shall be managed through mitigating controls and by specific ex-post controls and/or focused audit every two years and ultimately staff mobility.

The management of sensitive posts is an ongoing process and part of the annual reporting of the Agency.

2. Definition

In general, a job can be characterized as being sensitive:

- a) by the nature of the activity itself. This could be the case for all activities where a high degree of personal judgment for taking decisions with financial implications is involved, e.g. staff members taking decisions in the area of procurement or contracts, or in areas where there is a relatively high degree of freedom to act and/or where supervision levels might be low.
- b) by the context in which the activity is carried out. This could apply to functions where staff members might be subject to pressure to disclose sensitive information and where disclosure might harm the interest of the Agency or its customers.

A sensitive post is defined as a post that had been analysed against criteria contributing to the sensitivity of a post, preventing measures, the associated risk of a post and the mitigating measures in place. Where the preventing and mitigating measures did not sufficiently reduce the residual risk level, the function is considered as sensitive and additional management processes (control processes), such as rotation are needed.

3. Criteria for defining sensitive posts (Identification)

The following criteria contributing to the sensitivity of a post shall be assessed:

- decision-making capacity (binding the agency by signature (AO, AOD, AIPN), approvals)
- capacity to influence decisions (capacity to collect, present and link, factual elements that support any decision making process)
- recurrent contacts with third parties outside the Agency (suppliers, private sector...)
- regular access to and/or manipulation of sensitive information (which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organisation owning it. Also called sensitive asset.)
- high level of specialised expertise (expertise that is available in the Agency in a monopolistic manner and can thus not be challenged internally)

⁵ Decision 10/2014/GB of the Governing Board adopting the European Police College's internal control standards and amending the Decision 08/2011/GB

Policy on identification and management of sensitive functions

Document number:

PO.INCO.005-1

Approval date:

12/11/2014

For these and any other criteria used, risks should be evaluated in relation to the field of activity and the context of the post.

Fields of activity which may be sensitive are:

- *Procurement and financial matters*: budgetary and financial management, budget execution, contract management, accounting issues
- *Recruitment and staff management*: activities with human resource implications, e.g. recruitment, personnel policy
- *Programme management*: managing programmes and projects from the programming stage to implementation and up to evaluation stage
- *Security considerations*: the security level associated with the activity concerned, confidentiality of activities, access to sensitive information/ secure offices, etc.
- *Managing physical goods and safeguarding of assets*
- *Legal framework*: jobs involving decisions linked to procedures defined by Community legislation (infringements etc.)
- *Negotiations and representation of the Agency*: activities on behalf of the Agency where the staff member has a wide margin of manoeuvre.

4. Defining the preventing measures and mitigating controls in order to reduce the risk

In the process of defining the sensitive functions at the Agency, the preventing measures and mitigating controls that can reduce the risks are assessed.

The measures and controls shall be cost effective and feasible. Measures and controls to the potential sensitivity of a job can take a number of forms related to the specificities of the Agency's tasks, including proper segregation of duties, collective approval process, panel of experts, procedures, etc. but might also include strong supervision arrangements and the implementation of the Code of Conduct for the staff of the Agency.

Any supervision and/or control procedures should be evaluated regularly for their adequacy and effectiveness in order to monitor the residual risk properly.

5. Managing sensitive posts

Being a small sized agency, with a staff Establishment Plan of 37 TA/CA posts and given the nature of staff (temporary and contractual staff engaged for a fixed period) CEPOL managed the risks associated with the sensitive functions primarily through preventing measures and mitigating controls and not through compulsory staff mobility.

In 2012 the Governing Board adopted implementing rules allowing a second renewal of TA/CA contract for an indefinite period of time; therefore there is ground that CEPOL may apply in the future rotation of tasks as a management tool. Therefore, as a supplementary measure to the mitigating controls – if residual risk could be significant – mandatory mobility can be applied, as a general rule, after 5-7 years.

The posts concerned by this task rotation principle should be flagged in the job description as 'sensitive post'. Before taking up a sensitive post, the job holder will be informed by the HR Office that the post is sensitive and that he/she will be required to change jobs at the end of the benchmark period.

Policy on identification and management of sensitive functions

Document number:

PO.INCO.005-1

Approval date:

12/11/2014

The Director may explicitly decide (and formally document) to postpone the implementation of the task rotation principle, in cases where:

- no alternative staff member with an equivalent level of expertise is available, or
- the status of one or more ongoing projects requires the continuity of the staff allocation.

In such cases the mitigating controls have to be reinforced.

Sensitive functions will be assessed as part of CEPOL's risk assessment process which is implemented on yearly basis. The criteria contributing to the sensitivity of a post as well as the ever-changing context in which the activities are carried out shall be given consideration. The identified risks associated with sensitive functions shall be included in the Risk Register and managed through mitigating actions/controls and the posts concerned shall be flagged in the job description as 'sensitive post'.

The identification and management of sensitive functions shall follow the steps described in Appendix 1.

6. Conclusions

CEPOL has reviewed its posts and the criteria contributing to the sensitivity of a post, together with the initial analysis of sensitive functions. The objective was to identify the preventing measures already in place for each post subject for evaluation and to review and update the mitigating controls.

The following functions have been identified as being sensitive by nature, considering the factors contributing to the sensitivity of the function:

- Authorizing Officer and Appointing Authority (Director) and Authorizing Officers by Delegation (Deputy Director, Head of Corporate Services, Head of Finance) - decision-making capacity
- Procurement Officer - recurrent contacts with third parties outside the Agency (suppliers, private sector)
- HR Officer and HR interim staff - regular access to confidential information
- IT Officer and IT interim staff - regular access to confidential information, high-level of specialised expertise

Based on the assessment made, taking into account the agency context, the control environment and procedures in place, it is considered that the preventing and mitigating measures sufficiently reduce the residual risk level, therefore these functions have not been flagged as sensitive in the job descriptions.

Nevertheless CEPOL has to remain vigilant and enhance the controls and procedures in place in order to promote the highest level of integrity of CEPOL staff.

CEPOL Anti-fraud Strategy includes specific actions with regard to raising and maintaining staff awareness on ethics and integrity, to be implemented on regular basis.

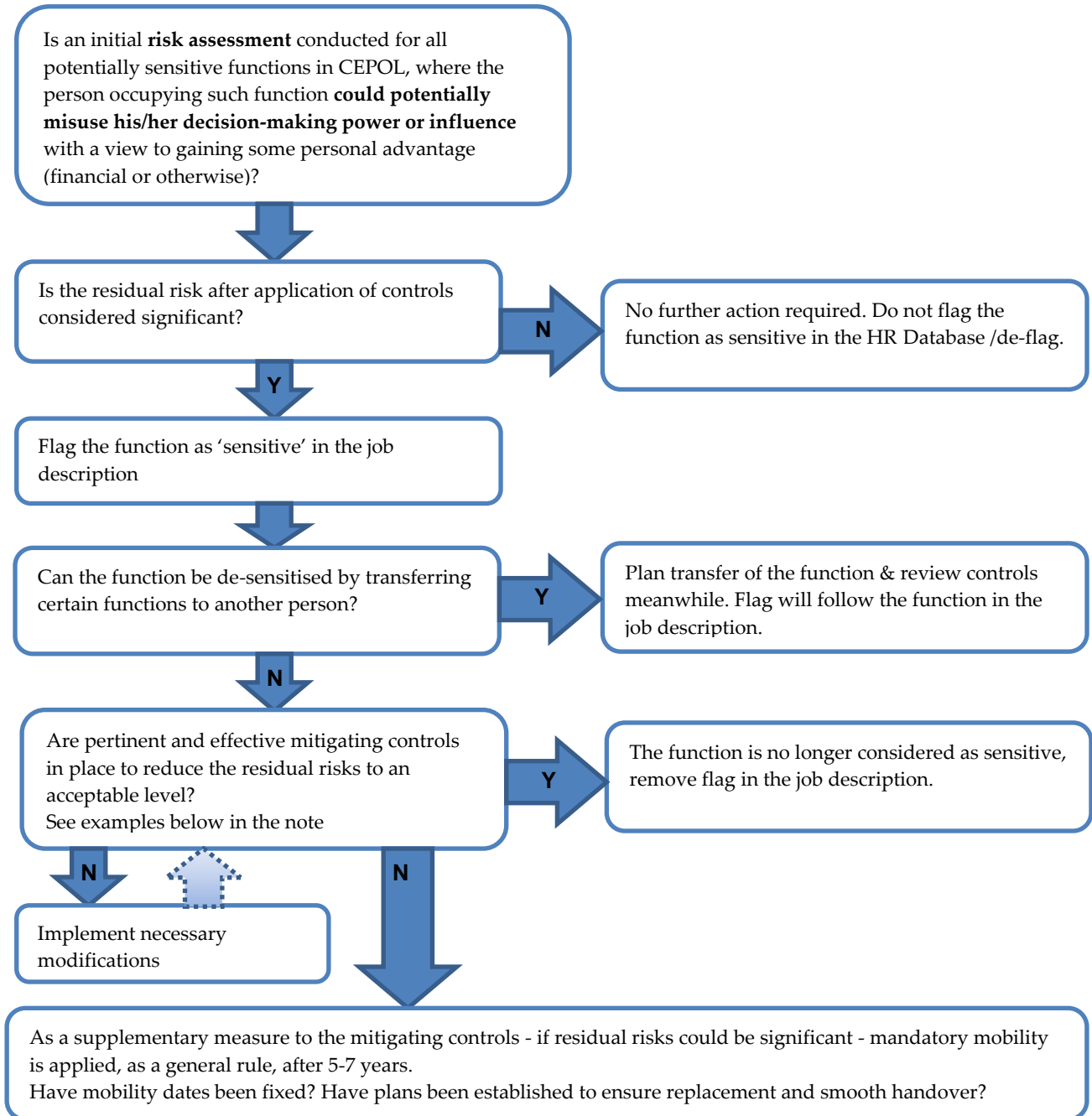
Policy on identification and management of sensitive functions

Document number:
Approval date:

PO.INCO.005-1
12/11/2014

Appendix 1 - Sensitive function flowchart

This flowchart shall be used for the identification and management of sensitive functions



Note – Examples of mitigating controls

- Four-eye principle (segregation of duties)
- Management supervision (e.g. supervisor checks a sample of transactions, files, etc.)