Decision of the Management Board 20/2021/MB

ON REPLACING AND REPEALING DECISION 34/2014/GB
ADOPTING THE CEPOL’S POLICY ON IDENTIFICATION AND MANAGEMENT OF SENSITIVE FUNCTIONS

Adopted by the Management Board

on 23 November 2021
THE MANAGEMENT BOARD,


Having regard to Management Board Decision 13/2019/MB on the CEPOL Financial Regulation and repealing decision 01/2014/GB of 22 May 2019,

Having regard to Management Board Decision 26/2018/MB on adopting the revised CEPOL internal control framework.

Whereas:

(1) Internal Control Framework, principle 10 requires that sensitive positions are identified in order to mitigate the risks associated with specific duties and/or responsibilities.

(2) The policy on identification and management of sensitive functions as latest adopted by decision 34/2014/GB became outdated due to obsolete terminology and legal references used.

HAS ADOPTED THIS DECISION:

Article 1

The renewed CEPOL’s Policy on identification and management of sensitive functions, as set out in the Annex to this decision, is hereby adopted.

Article 2

Decision 34/2014/GB is hereby repealed and replaced by the present Decision.

This Decision shall take effect on the day following that of its adoption.

Done at Lisbon, on 29 November 2021

For the Management Board

<< Signature on file >>

........................................

Mr José Leitão
Chair of the Management Board

ANNEX: CEPOL’s Policy on identification and management of sensitive functions
ANNEX

DOCUMENT CONTROL SHEET

Process area  Agency Management Processes
Main process  Internal Control
Main process owner  Executive Director

TABLE OF CONTENT

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

Abbreviations

CEPOL European Union Agency for Law Enforcement Training
ICF Internal Control Framework
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)\(^1\)

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

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

LOG OF ISSUES

<table>
<thead>
<tr>
<th>Issue</th>
<th>Issue date</th>
<th>Change description</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>28/10/2014</td>
<td>First issue</td>
</tr>
<tr>
<td>002</td>
<td>24/11/2021</td>
<td>Second issue – to update the legal references and obsolete terminology</td>
</tr>
</tbody>
</table>

\(^1\) EC Guidance on sensitive functions
1. Background

Internal Control Framework, Principle 10 requires that sensitive positions are identified in order to mitigate the risks associated with specific duties and/or responsibilities.

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.

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).

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
- **Selection/Invitation of Short Term Experts (STEs)**: repeated use of the same STEs from the staff member’s personal network
- **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 Good Administrative Behaviour\(^2\) 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 an Establishment Plan of 33 TA posts; 20 additional CA posts/CA posts and 3 SNEs, and approximately 40 posts for externally funded projects and given the nature of staff (a large majority of staff engaged for a fixed period), CEPOL manages the risks associated with 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. Mobility can also be applied in case of middle management staff, as provided in the Management Board Decision 11/2019/MB on implementing rules on middle management staff.

---

\(^2\) 26-2019-DIR
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. It is however to be noted that CEPOL has limited number of staff that remained in post after being granted indefinite contract, since staff fluctuation continued to remain high for the latest 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.

The Executive 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, in order 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 delegated by the MB (Executive Director) and Authorizing Officers by Delegation (Head of Operations, Head of Corporate Services, Head of Finance, Procurement and Travel) - 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.
Appendix 1 - Sensitive function flowchart

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

Is an initial risk assessment conducted for all potentially sensitive functions in CEPOL, where the person occupying such function could potentially misuse his/her decision-making power or influence with a view to gaining some personal advantage (financial or otherwise)?

- Y
  - Is the residual risk after application of controls considered significant?
    - Y
      - Flag the function as ‘sensitive’ in the job description
    - N
      - No further action required. Do not flag the function as sensitive in the HR Database / de-flag.

- N
  - Can the function be de-sensitised by transferring certain functions to another person?
    - Y
      - Plan transfer of the function & review controls meanwhile. Flag will follow the function in the job description.
    - N
      - Are pertinent and effective mitigating controls in place to reduce the residual risks to an acceptable level?
        - Y
          - The function is no longer considered as sensitive, remove flag in the job description.
        - N
          - Implement necessary modifications

As a supplementary measure to the mitigating controls - if residual risks could be significant - mandatory mobility is applied, as a general rule, after 5-7 years. Have mobility dates been fixed? Have plans been established to ensure replacement and smooth handover?

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