Brussels 27th March 2014
BUDG D3/CVL/ICUpdate/IC-Req-Simplif-v-after
ICCs & 2nd review.doc

Simplified & Reduced Internal Control Requirements

Contents

1: Mission .................................................................................................................................1
2: Ethical and Organisational Values.....................................................................................1
3: Staff Allocation and Mobility ...........................................................................................1
4: Staff Appraisal and Development .....................................................................................1
5: Objectives and Performance Indicators..........................................................................1
6: Risk Management Process ...............................................................................................1
7: Operational Structure .......................................................................................................2
8: Processes and Procedures ...............................................................................................2
9: Management Supervision ...............................................................................................2
10: Business Continuity .........................................................................................................2
11: Document Management .................................................................................................3
12: Information and Communication ....................................................................................3
13: Accounting and Financial Reporting ..............................................................................3
14: Evaluation of Activities ..................................................................................................4
15: Assessment of Internal Control Systems .......................................................................4
16: Internal Audit Capability ...............................................................................................4

Total Requirements from 61 to 35
1: **Mission**

1. The DG, Directorates and Units have up-to-date mission statements which are linked across all hierarchical levels and made known to staff.

2: **Ethical and Organisational Values**

2. The Director General ensures that his/her staff are aware of relevant ethical and organisational values and the associated rules and procedures. In particular staff are made aware of the necessity to avoid conflicts of interest and the procedure to manage such situations should they arise, the rules regarding whistleblowing and the procedure to report fraud and irregularities. A solid and targeted antifraud strategy is organised at DG level.

3: **Staff Allocation and Mobility**

3. Whenever necessary, management aligns the organisational structures and staff allocations with priorities and workload.

4. The DG promotes, implements and monitors mobility in order to ensure that the right person is in the right job at the right time and, where feasible, to create career opportunities.

4: **Staff Appraisal and Development**

5. Staff performance is appraised according to rules and instructions set by the Commission. As part of the appraisal dialogue and report, the learning and development needs of staff are discussed and recorded. Managers support staff in developing knowledge and competencies useful for their job and career.

6. Learning and development needs are defined on the basis of the policy goals of the DG and the staff profiles needed to reach those goals. The definition of needs respects the strategy, guidelines and instructions issued by the central services.

5: **Objectives and Performance Indicators**

7. The DG’s objectives are set out in accordance with applicable guidance in such a way as to ensure that they are understood and owned by management and staff. Whenever necessary, objectives are updated to take account of significant changes in activities and priorities.

8. The DG’s Management Plan clearly sets out how planned actions and deliverables will contribute to the achievement of objectives set, taking into account the allocated resources and the risk identified.

9. The DG monitors the attainment of its objectives throughout the year using performance indicators and adequate reporting tools. The DG reports on its achievements, expected results and impact, and if relevant, on its contribution to Commission-wide priorities, in the Annual Activity Report. The DG adheres to corporate reporting requirements.

6: **Risk Management Process**

10. A risk assessment exercise is conducted at least once a year as part of the MP process and whenever management considers it necessary (typically in the event of major modifications to the DG’s activities occurring during the year). Risk management is performed in line with applicable provisions and guidelines.

11. Risk management action plans are realistic and take into account cost/benefit aspects in order to avoid disproportionate control measures. Processes are in place to ensure that actions are implemented according to plan and continue to be relevant.
7 Operational Structure

12. Delegation of authority is clearly defined, assigned and communicated in writing, conforms to legislative requirements and is appropriate to the importance of decisions to be taken and risks involved.

13. The DG’s sensitive functions are identified through risk assessments. They are recorded and kept up to date. Measures are in place to ensure that risks are mitigated and that staff do not perform a sensitive function for more than the time limits prescribed in relevant decisions.

14. The standard IT governance policy of the Commission is applied, and in particular:
   - The DG has defined the appropriate organisation for management of the information systems it owns, generally in the form of an IT Steering Committee.
   - An annual ‘schéma directeur’ (IT masterplan), covering all information systems developments (regardless of budget source) for a period of three years, has been produced.
   - Each information system owned by the DG possesses a clearly identified business owner and is overseen by a steering committee.
   - All new information systems projects are approved on the basis of a vision document.
   - All new information systems are developed using the standard Commission project management and development methods, and take security into account from the very first stage.

8 Processes and Procedures

15. The DG’s main processes and procedures are adequately documented, particularly those associated with critical risks. They ensure segregation of duties and comply with applicable provisions.

16. A method is in place to ensure that all instances of overriding of controls or deviations from established processes and procedures are documented in exception reports, justified, duly approved before action is taken and logged centrally. Exception report is one of the management tools used to conclude on effectiveness of internal control and/or changes needed to internal control system.

9 Management Supervision

17. Management supervise the activities they are responsible for. They keep track of main issues and ensure the follow-up of accepted audit and other recommendations e.g. linked to interval evaluations and reviews. Management supervision covers both legality and regularity aspects and operational performance and includes supervision of external bodies entrusted with the budget implementation tasks.

18. At least twice a year and at any time deemed appropriate, the Director-General informs the responsible Commissioner of any potentially significant issues related to internal control and audit and OLAF investigations as well as material budgetary and financial issues that might have an impact on his/her position in the College or on the sound management of appropriations or which could hamper the attainment of the objectives set.

10 Business Continuity

19. Adequate measures - including handover files and deputising arrangements for relevant operational activities and financial transactions - are in place to ensure the continuity of all service during “business-as-usual” interruptions (such as sick leave, staff mobility, migration to new IT systems, incidents, etc.).

20. The DG has developed, following in-depth Business Impact Analysis (BIA) and using SG template and guidance, a Business Continuity Plan (BCP) that is well maintained, exercised
and revised regularly, at least once a year. The BIA, BCP and other relevant documentation are safeguarded and easily accessible to the relevant staff that should be appropriately trained.

21. Contingency and backup plans for information systems are established, maintained, documented and tested in the context of Disaster Recovery Planning (DRP) and security needs.

11 Document Management

22. Document management procedures and related systems comply with relevant compulsory security measures, provisions on document management and rules on protection of personal data;

23. Every document that fulfils the conditions laid down in the implementing rules needs to be registered, filed in at least one official file and preserved during the period established by the document management rules. To do so, the DG uses systems which respect the above rules, mainly HERMES-ARES-NOMCOM.

12 Information and Communication

24. Arrangements, in line with the Commission’s Internal Communication and Staff Engagement Strategy, are in place to ensure that management and staff are appropriately informed of decisions, projects or initiatives – including those in other DGs – that concern their work assignments and environment. There are processes in place for the voice of staff to be heard.

25. Each DG has a communication strategy which shall contribute to corporate communication. Staff, management and the Cabinet are consulted in devising the strategy, which must use the corporate communication themes as reference points. These corporate themes shall also be conveyed wherever possible in DGs’ communication of portfolio policy issues to their stakeholders. The Communication Steering Board is informed and its advice is sought for all corporate communication strategies and actions. Coordination is sought with other DGs.

26. Communication actions respect legal and regulatory requirements (including copyright laws) and are in line with the instructions and guidelines of central services.

27. The standard Information Systems Security Policy of the Commission is applied. In particular, each DG has adopted and implements an IT Security Plan based on an inventory of the security requirements and a risk analysis of the IT systems under their responsibility, and applies at least the relevant control measures of the corporate IS Security Policy.

28. The IT systems support adequate data management, including database administration and data quality assurance. Data management systems and related procedures comply with relevant Information Systems Policy, compulsory security measures and rules on protection of personal data.

13: Accounting and Financial Reporting

29. Each Authorising Officer ensures that the financial and accounting information submitted to management, to the central services and to the Accounting Officer for the production of accounts and management reports (including the AAR) is reliable and complete.

30. The DG nominates an Accounting Correspondent (AC) to help ensure the respect of rules, instructions and quality of financial information submitted to the Commission central accounting and reporting systems
14: Evaluation of Activities

31. Evaluations are performed in accordance with the guiding principles of the Commission’s evaluation standards. Corresponding evaluation baseline requirements are applied for retrospective evaluations (interim, final and ex-post) while prospective evaluations (ex-ante and impact assessments) follow the relevant specific guidelines.

15: Assessment of Internal Control Systems

32. Management assesses the effectiveness and efficiency of the DG’s internal control system at least annually. The results of the review should be presented in the Annual Activity Report. Both the review and relative reporting must be carried out in accordance with applicable guidance.

33. Management facilitates communication and reporting of internal control weaknesses. Internal Control Coordinator coordinates such reporting and ensures the use of information to reinforce the effectiveness of controls as needed.

16: Internal Audit Capability

34. The DG has an Internal Audit Capability (IAC), which adheres to internationally accepted internal audit standards and practices (IPPF) and coordinates its work with IAS. It reports directly to the Director General and provides independent, objective assurance and consulting services designed to add value and improve the effectiveness of risk management, control, and governance processes of the DG;

35. The Director General ensures that the IAC is independent of the activities they audit, and that it has sufficient and adequate resources to perform the audit work plan.