EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

20 April 2016
EMA/MB/602884/2015 Adopted
Corporate Governance

Internal Control Standards and underlying framework

Strengthening control effectiveness

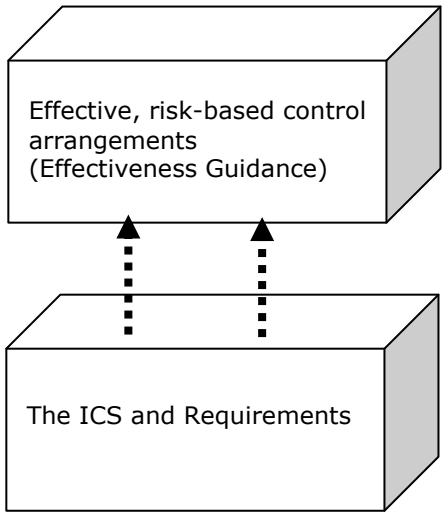
Adopted on 2 October 2015

30 Churchill Place ● Canary Wharf ● London E14 5EU ● United Kingdom
Telephone +44 (0)20 3660 6000 **Facsimile** +44 (0)20
Send a question via our website www.ema.europa.eu/contact

1. The internal control framework

The internal control framework consists of three closely interlinked components:

- the Internal Control Standards for effective management themselves;
- the "Requirements";
- Internal Control Effectiveness assessment whereby services judge the effectiveness of their internal control systems in practice. Optional guidance to help them in this respect is provided.



- The "Effectiveness Guidance" (which is optional) can help management determine whether the internal control arrangements are sufficiently adapted to the service's activities and risks and whether they work as intended in practice.

- The Internal Control Standards for effective management (ICS) and Requirements constitute the foundation of the internal control framework. They provide basic principles and minimum requirements.

In addition to the above and taking account of the overall obligation to comply with the Requirements, the framework will allow services flexibility in determining the standards on which further emphasis on effectiveness is necessary.

1.1. The Internal Control Standards for effective management

The Standards are structured around six "building blocks" (Annex 1):

1. Mission and Values;
2. Human Resources;
3. Planning and Risk Management Processes;
4. Operations and Control Activities;
5. Information and Financial Reporting, and
6. Evaluation and Audit.

Basic risk management principles (adapting controls to risks identified) apply to all Internal Control Standards for effective management, and the flexible approach and guidance outlined below can help to focus on standards representing higher risks. Moreover, the Standard 6 (risk management process) refers specifically to the process in place for identifying risks in the annual planning phase, in conformity with the principles laid down in the Agency's Risk Management Manual.

The Standards are accompanied by two assessment tools, the "Requirements" and "Effectiveness Guidance", which are detailed in the following sections.

1.2. The Requirements

The Requirements (Annex 2) specify the minimum features of internal control systems and processes.

1.3. Internal Control Effectiveness

1.3.1. Flexibility of approach

The Agency must put in place monitoring measures to show their internal control systems are effective. The approach recognises that certain Standards may be more important for certain activities and that their importance may change over time.

1.3.2. Optional Internal Control Effectiveness Guidance

The effectiveness of the internal control system as a whole can be measured through pertinent indicators. However, because the Standards are interdependent, it is hardly possible to quantify the effective implementation of each individual Standard through generic indicators. Nonetheless, this latter can be judged on a variety of bases (for example, process reviews, management supervision and ad-hoc verification, surveys and interviews, management self-assessments, audit reports, stakeholder feedback).

1.4. Reporting obligations

The Executive Director provides assurance in the Annual Activity Reports on the operation of the internal control systems.

2. Support for increasing understanding and ownership

To increase understanding and ownership of the internal control framework by all staff, and move towards strengthening internal control effectiveness in the Division and supporting the Executive Director's annual statement of assurance, the following accompanying actions are essential:

- *Top management support*: Top management decides the Standards to be prioritised for the strengthening of internal control effectiveness and define the internal responsibilities, taking into account their organisation and risk environment. Strong top management commitment to internal control, including the allocation of sufficient time and resources for raising awareness and developing internal control skills, will be vital to the further integration of the Standards in the working environment.
- *Effective communication*: Communication and presentations will be organised to inform and raise awareness of staff at all levels.
- *High quality training*: Administration will launch a training programme on internal control for managers and for staff.
- *Support from the Corporate Governance Department*: Corporate Governance will facilitate the sharing of good practices and experience between services. Effectiveness guidance and communication actions will be updated on the basis of experience and feedback reported by divisions. Assistance will be provided to the divisions through the different steps of the Planning and Programming cycle, notably the Annual Work Programme and the Annual Activity Report.

3. Conclusion

More needs to be done to ensure controls are working effectively in practice. In particular, further efforts are needed to ensure that all staff are aware of their responsibilities as regards internal control. The internal controls framework and their supporting guidance will facilitate this. The flexibility incorporated into the approach will also allow services to tailor the provisions to their own specific environments.

The following control standards should be read in conjunction with Agency's IQM system description (the 'Quality Policy').

Annex 1

The Internal Control Standards for Effective Management

Mission and Values

1. **Mission:** The EMA's raison d'être is clearly defined in an up-to-date and concise mission statement developed from the perspective of the relevant legislation and the EMA's stakeholders and partners.
2. **Ethical and Organisational Values:** Management and staff are aware of and share appropriate ethical and organisational values and uphold these through their own behaviour and decision-making.

Human Resources

3. **Staff Allocation and Mobility:** The allocation and recruitment of staff is based on the EMA's objectives and priorities. Management promote and plan staff mobility so as to strike the right balance between continuity and renewal.
4. **Staff Evaluation and Development:** Staff performance is evaluated against individual annual objectives, which fit with the EMA's overall objectives. Adequate measures are taken to develop the skills necessary to achieve the objectives.

Planning and Risk Management Processes

5. Objectives and Performance Indicators: The EMA's objectives are clearly defined and updated when necessary. These are formulated in a way that makes it possible to monitor their achievement. Key performance indicators are established to help management evaluate and report on progress made in relation to their objectives.
6. Risk Management Process: A risk management process that is in line with applicable provisions and guidelines is integrated into the annual activity planning.

Operations and Control Activities

7. Operational Structure: The EMA's operational structure supports effective decision-making by suitable delegation of powers. Risks associated with the EMA's sensitive functions are managed through mitigating controls and by specific ex-post controls and/or focused audit every two years. Adequate IT governance structures are in place.
8. Processes and Procedures: The EMA's processes and procedures used for the implementation and control of its activities are effective and efficient, adequately documented and compliant with applicable provisions. They include arrangements to ensure segregation of duties and to track and give prior approval to control overrides or deviations from policies and procedures.
9. Management Supervision: Management supervision is performed to ensure that the implementation of activities is running efficiently and effectively while complying with applicable provisions.

10. Business Continuity: Adequate measures are in place to ensure continuity of service in case of "business-as-usual" interruption. Business Continuity Plans are in place to ensure that the EMA is able to continue operating to the extent possible whatever the nature of a major disruption.

11. Document Management: Appropriate processes and procedures are in place to ensure that the EMA's document management is secure, efficient (in particular as regards retrieving appropriate information) and complies with applicable legislation.

Information and Financial Reporting

12. Information and Communication: Internal communication enables management and staff to fulfil their responsibilities effectively and efficiently, including in the domain of internal control. The EMA has an external communication strategy to ensure that its external communication is effective, coherent and in line with its key political messages. IT systems used and/or managed by the EMA are adequately protected against threats to their confidentiality and integrity.

13. Accounting and Financial Reporting: Adequate procedures and controls are in place to ensure that accounting data and related information used for preparing the organisation's annual accounts and financial reports are accurate, complete and timely.

Evaluation and Audit

14. Evaluation of Activities: Evaluations of expenditure programmes are performed to assess the results, impacts and needs that these activities aim to achieve and satisfy.

15. Assessment of Internal Control Systems: Management assess the effectiveness of the EMA's key internal control systems, including the processes carried out by implementing bodies, at least once a year.

16. Internal Audit Capability: The EMA has an Internal Audit Capability (IAC), which provides independent, objective assurance and consulting services designed to add value and improve the operations of the EMA.

Annex 2

Full set of Internal Control Standards for effective management, requirements and optional effectiveness guidance

(One "Fiche" per standard)

ICS 1. Mission: The Agency's *raison d'être* is clearly defined in up-to-date and concise mission statements developed from the perspective of the relevant legislation and the Agency's stakeholders and partners.

Requirements

- The EMA has an up-to-date mission statement that applies to all divisions across the Agency;
- The mission statement has been explained to staff and is readily accessible.

Main references:

- the EMA Mission Statement EMEA/MB/224100/2007
- All staff trained via introduction training for all new staff and other persons

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Is the Agency's mission statement up-to-date and sufficiently instructive? An effective mission statement is a concise statement developed from the perspective of the Agency's stakeholders and partners. It should answer two basic questions: Why do we exist? How do we fit within the broader architecture of the European medicines network?
- Are staff aware of the Agency mission statement?
- Would it be appropriate to involve selected staff/stakeholders to update the mission statement (e.g. in parallel with the Agency Road Map)?

ICS 2. Ethical and Organisational Values: Management and staff are aware of and share appropriate ethical and organisational values and uphold these through their own behaviour and decision-making.

Requirements

- The EMA has procedures in place - including updates and yearly reminders - to ensure that all staff is aware of relevant ethical and organisational values, in particular ethical conduct, avoidance of conflicts of interest, fraud prevention and reporting of irregularities. These procedures include the yearly reminder for the Code of Conduct as well as the review of sensitive functions.

  Main references:

  - the Staff Regulations (particularly Titles II -Art.22- and VI)
  - the EMA Financial Regulation, Art 53 (2) and Art 54 (5)
  - the Code of Conduct EMA/385894/2012
  - Decision on Rules relating to Article 11, 11a and 13 of the Staff Regulations concerning the handling of declared interests of staff members of the EMA and candidates before recruitment, EMA/622828/2013(revised)
  - Decision on rules concerning the handling of declared interests of national experts on secondment, trainees, interims and visiting experts of the European Medicines Agency, EMA/453783/2014
  - Best practice guide for staff leaving the Agency, EMA/70197/2013
  - Decision of the Management Board, European Medicines Agency on the adoption of implementing rules for outside activities and assignments, EMA/712718/2013
  - EMA Equal Opportunities Policy and Action Programme 2344 30.09.2006
  - EMA Sexual Harassment and Bullying Guideline EMEA/fn-2610 19.09.01
  - EMA guidelines on whistleblowing EMA/182359/2014
  - the EMA OLAF Agreement EMEA/D/15007/99
  - Communication on Professional Integrity, EMA/511563/2010 of 7 September 2010
  - Policy 0042 Protecting the dignity of the person and preventing any form of psychological or sexual harassment (1 May 2015, EMA/338797/2012)
  - EMA values, statements and behaviours, EMA/121858/2014
  - Anti-Fraud Strategy EMA/591051/2014

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Would EMA specific ethical guidance be meaningful? For example, although the rules relating to "conflict of interests" apply to all persons in the EMA, a division/department with significant procurement activities may want to emphasise this aspect. Dealing with insider information and preventing l fraud are other topics that certain divisions/departments may want to stress.
- Is the ethical guidance concise and user-friendly? The way the code of conduct/guidance is written will affect its effectiveness. Studies show that the most effective codes of conduct are those that are short and concise, focus on a few main messages and utilise a straightforward vocabulary.
- Are staff sufficiently aware of the different requirements and provisions concerning ethics and integrity (via training of newcomers, regular information, etc.)? Staff awareness of the need to fight fraud and other irregularities at all levels of the organisation can, for example, be analysed and enhanced through surveys and/or training and e-learning courses.
- Is enough done to facilitate the practical application of the code of conduct and other ethical guidance? For example, creating easily accessible and secure channels for staff to confidentially report alleged wrongdoings (including through the development of a template report) could make the code of conduct more effective in this domain.
- Do results of the supervisory activities, audit reports, reported deviations or other relevant sources suggest that there could be ethical issues or problems in the EMA/Division? Have adequate measures been taken to address these issues?

ICS 3. Staff Allocation and Mobility: The allocation and recruitment of staff is based on the EMA's objectives and priorities. Management promote and plan staff mobility so as to strike the right balance between continuity and renewal.

Requirements

- Whenever necessary - at least once a year - management aligns the organisational structures and staff allocations with priorities and workload.
- Staff job descriptions are consistent with relevant mission statements.
- The EMA has a policy to promote, implement and monitor mobility (e.g. publication of vacant posts) in order to ensure that the right person is in the right job at the right time and, where feasible, to create career opportunities.
- Necessary support is defined and delivered to new staff to facilitate their integration in the team.

Main references:

- Implementing Rules regarding Training for EMA Staff EMA/MB/12729/2010, 10.12.2009
- Equal opportunities' legislation: Treaty, Art 1 of Staff Regulations, Charter of Fundamental Rights
- EMA Planning & Reporting Schedule including EMA Work Programme, Environmental Scan , Annual (Activity) Report,
- Internal transfer and mobility rules, EMEA/31498/436 of 14 November 2003
- European Medicines Agency Decision of 30 June 2015 laying down general implementing provisions on the procedure governing the engagement and use of temporary staff under Article 2(f) of the Conditions of Employment of Other Servants of the European Union, EMA/329753/2015
- Internal vacancy announcements and selection procedures, external selection procedures
- Policy on Updating of Job Summaries and Job Descriptions (Policy/0017 EMA/352357/2005)
- Multiannual programming document

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are adequate arrangements in place to ensure effective staff planning and allocation? Do management have sufficient and relevant information about priorities and staff workloads as well as required and available skills?
- Are there any issues or problems related to staff recruitment and allocation that significantly affect the EMA's/ Division's/Department's performance? Could a modification of current recruitment and allocation procedures, to the extent possible at EMA level, address these? How?

- Are sufficient measures taken to ensure flexible and dynamic organisation, for example via targeted and intensive training programmes, re-organisation or other measures?
- Is staff turnover sufficiently monitored and analysed? Establishing EMA-specific ratios for "excessive" and "insufficient" staff turnover may be useful. Are the root causes of any abnormal staff turnover sufficiently analysed and addressed?
- In the event of "excessive" staff turnover, is appropriate action taken to retain staff with the required skills? Similarly, where there is "insufficient" staff turnover, is appropriate action taken to promote and facilitate staff mobility within the EMA or externally? Have these measures been successful? If not, why?
- Is the interest of the service taken into account when planning for the mobility of middle management or total replacement of the management team and/or critical staff? Is the possible loss of knowledge adequately managed?

ICS 4. Staff Evaluation and Development: Staff performance is evaluated against individual annual objectives, which fit with the EMA's overall objectives. Adequate measures are taken to develop the skills necessary to achieve the objectives.

Requirements

- In the context of the annual appraisal exercise discussions are held individually with all staff to establish their annual objectives, which fit with the EMA/Division/Department's objectives.
- Staff performance is evaluated in accordance with objectives set in agreement with management.
- A global average of 10 working days per staff member is devoted to learning and development activities.
- A Training Profile is completed annually by each temporary or contract agent to whom Art. 24a of the Staff Regulations applies by analogy, discussed with and approved by the line manager. The Training Record, recording all training activities undertaken by the staff member, is kept up to date.
- Management ensure that every staff member attends at least the training courses of a compulsory nature as defined in the Training Profile.

Main references:

- Information note – Staff Appraisals, EMA/554421/2014
- Policy on Updating of Job Summaries and Job Descriptions (Policy/0017 EMA/352357/2005)
- Generic Job Description in WORD/templates
- Appraisal template for annual report available in the intranet
- Provisions of Article 43 of the Staff Regulations and Article 15 and 87(1) of CEOS
- Implementing Rules regarding Training for EMA Staff EMA/MB/12729/2010, 10.12.2009
- Annual training report with mid-year training report
- Individual training record
- Management and Leadership Profile, EMA113760/2015

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are staff's objectives (as noted in the PER) meaningful, sufficiently challenging and accepted by the persons concerned? Are they kept up to date during the year?

- Are staff evaluations based on the achievement of pertinent and up-to-date annual objectives? Using generic or outdated objectives increases the risk of subjective and biased evaluations and can negatively impact on staff motivation.
- Are sufficient measures taken to analyse and develop the EMA's skills and to plan for future HR needs and skill requirements? An effective staff development plan should take into account not only individual training requests but also the collective skills and competences needed to meet the EMA/Division/Department's objectives. Performing an analysis to detect significant gaps between required and available skills and competences in the entity can be an effective means of improving staff development.
- Are pertinent training statistics available? An analysis of the EMA/Division/Department's training statistics may indicate whether the entity's training activities should be re-focused. On the basis of this, is there evidence that staff are taking the necessary courses in order to build their skills?

ICS 5. Objectives and Performance Indicators: The EMA's objectives are clearly defined and updated when necessary. These are formulated in a way that makes it possible to monitor their achievement. Key performance indicators are established to help management evaluate and report on progress made in relation to their objectives.

Requirements

- The EMA establishes road maps that document its medium-term vision and strategic objectives and are the basis for defining multi-annual activities
- Multi-annual work programmes implement road maps and set out milestones for the actions that need to be taken before the budget appropriations can be implemented for the whole period of the activity.
- The EMA's Annual Work Programme (WP) is derived from the multi-annual work programme and is developed in accordance with applicable guidance and on the basis of a dialogue between top managers, middle managers and staff in order to ensure it is understood and owned.
- The WP clearly sets out how the planned activities at each management level will contribute to the achievement of objectives set, taking into account the allocated resources and the risk identified.
- To the extent possible, the WP objectives are established in line with the SMART criteria, i.e. they are Specific, Measurable or verifiable, discussed and Accepted, Realistic and Timed.
- Whenever necessary, the objectives are updated to take account of significant changes in activities and priorities.
- In the WP, there is at least one performance indicator per objective, both at policy area and at operational activity level, to monitor and report on achievements. To the extent possible, the performance indicators are established according to the RACER criteria, i.e. they are Relevant, discussed and Accepted, Credible, Easy and Robust.
- Reporting structures are in place to alert management when indicators show that the achievement of the objectives is at risk.

  Main references:

  - EU Medicines Agencies Network Strategy to 2020, EMA/MB/151414/2015
  - EU guidelines for the single programming document, EMA/441152/2015
  - Multi annual work programme and Annual (Activity) Report
  - Template for consolidated annual activity report, EMA/441956/2015
  - Management Manual on Intranet
  - Timelines for planning and reporting activities
  - Annual Environmental analysis

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Is the concept of "management by objectives" (i.e. building the EMA's activities around WP objectives at different management levels) sufficiently understood, discussed and accepted by management and staff? Does this concept work in practice? If not, why?
- Does the process of objective-setting ensure a high degree of understanding and ownership? Are the EMA/Division/Department's WP objectives known to staff and meaningful?
- Is there a need for resources redeployment or (re)prioritisation of the objectives?
- Are the EMA/Division/Department's performance indicators meaningful, i.e. do they actually support and facilitate the management and monitoring of the EMA's activities?
- Are the performance indicators focused on the EMA/Division/Department's key activities and risks? Too many or too detailed indicators may be confusing and ineffective.
- In case performance cannot be quantified, are meaningful qualitative performance indicators established?

ICS 6. Risk Management Process: A risk management process that is in line with applicable provisions and guidelines is integrated into the annual activity planning.

Requirements

- A risk management exercise at EMA level is conducted at least once a year as part of the management review and whenever management considers it necessary (typically in the event of major modifications to the EMA's activities occurring during the year). Risk management is performed in line with applicable provisions and guidelines.
- 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.
- Risks considered "critical" from an overall EMA perspective are reported and followed-up in the management review and Annual Activity Report.

Main references:

- Integrated Quality Management System (Policy 0001) EMEA/MB/355781/2007Rev.1
- Agency-wide Risk Manual EMA/558279/2015
- Risk Register EMA/159414/2011
- Timelines for planning and reporting
- Anti-Fraud Strategy EMA/591051/2014

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Is the risk management concept sufficiently understood by management and staff? Surveys can be used to identify issues in this domain.
- Is risk management adequately integrated into the processes and procedures used for the planning, implementation and control of the EMA's activities? Is risk management regularly considered in division/department meetings?
- Is the EMA's risk management process user-friendly and pragmatic or is it considered a "bureaucratic burden"?
- Are EMA managers aware of the Health & Safety policies and the risks to staff?

ICS 7. Operational Structure: The EMA's operational structure supports effective decision-making by suitable delegation of powers. Risks associated with the EMA's sensitive functions are managed through mitigating controls and by specific ex-post controls and/or focused audit every two years. Adequate IT governance structures are in place

Requirements

- 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.
- All delegated and sub-delegated authorising officers have received and acknowledged the Charters and specific delegation instruments.
- As regards financial transactions, delegation of powers (including both "passed for payment" and "certified correct") is defined, assigned and communicated in writing.
- The EMA's sensitive functions are clearly defined, recorded and kept up to date. For each sensitive function:
- A risk assessment is carried out and relevant mitigating controls are established;
- The standard IT governance policy of the EMA is applied, and in particular:
  - The EMA has defined the appropriate organisation for management of the information systems it owns, generally in the form of an IT Steering Committee.
  - An annual 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 EMA 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 EMA project management and development methods, and take security into account from the very first stage.

Main references:

- EMA Organisational Charts
- Guidance on ex post controls, EMA/474929/2014
- Guidelines on sensitive functions EMA/486191/2013
- Security Policy 0076 EMA/530488/2014
- Delegations decision of powers of personnel matters as last amended.
- Decisions on delegation of powers of budget implementation of the Executive Director as last amended.
- Register of Executive Decisions
- EU Telematics Strategy 2014-2016 EMA/289808/2014
- EU Telematics Strategy and Implementation Roadmap 2015-2017 EMA/532765/2015

- The joint EU Telematics governance model EMA/139062/2014
- IT Infrastructure Library (ITIL) EMEA/130900/2007 & EMEA/33875/2006
- Charter of tasks and responsibilities of the Executive Director as authorising officer EMA/MB/56129/2015
- Charter of tasks and responsibilities of authorising officers by delegation EMA/235295/2015
- Decision of the Executive Director on agreement of budget allocations for programmes and projects
- EMA internal notice on programme and project roles and responsibilities: guiding principles for application of programme and project governance
- EMA internal notice on project-related selection and acquisition of commercial off-the-shelf IT solutions: guiding principles in relation to programmes and projects
- Project gated procedure (http://emeaplus/EMEAPlus_WebsiteNew/Projects/html/Step0.html)

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are there any organisational issues or problems that negatively impact on the EMA's/Division's performance or control environment? In what way? Could a reorganization of the EMA/Division improve the situation? How?
- Are the nature and scope of delegated functions and powers clear to all persons concerned?
- Are the risks associated with the delegated functions and powers sufficiently analysed?
- Where sensitive functions have been removed and allocated to a different member of staff, is management satisfied that the risks involved have been effectively mitigated?
- Where additional mitigating controls have been put in place, is management satisfied that these controls are effective and that the risks involved have been reduced to an acceptable level (considering impact and likelihood of the risk)?
- Do results of the supervisory activities, audit reports or other relevant sources suggest that there could be failings or issues associated with the EMA's sensitive functions?
- Is the number of sensitive functions that require mandatory staff mobility reasonable? The cost of excessive mandatory staff mobility (negative impact on operations) may outweigh the benefits (reduced risk of conflict of interest and fraud).
- Are all IT/IS (Information Technology/Information Systems) projects and their specific risks clearly identified and managed according to the relevant guidance?
- Regarding IT Governance and IS Development, does the IT Steering Committee adequately represent all relevant stakeholders? If the EMA owns Information Systems which are used by other organisations, are there appropriate governance arrangements in place to ensure all stakeholders' interests are considered?

- If the EMA owns Information Systems or if it wishes to develop one, have possible synergies among the EMA's Information Systems been explored and exploited, to the maximum extent possible? Are the systems interoperable to a satisfactory level? Are there duplicated investments in similar systems within the EMA or elsewhere which merit attention?

ICS 8. Processes and Procedures: The EMA's processes and procedures used for the implementation and control of its activities are effective and efficient, adequately documented and compliant with applicable provisions. They include arrangements to ensure segregation of duties and to track and give prior approval to control overrides or deviations from policies and procedures.

Requirements

- The main operational and financial processes and procedures and IT systems are adequately documented.
- The processes and procedures ensure appropriate segregation of duties (including for nonfinancial activities).
- The processes and procedures comply with applicable provisions, in particular the Financial Regulation (e.g. ex-ante and ex-post verifications) and the EMA policies.
- 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.

  Main references:

  - EMA Financial Regulation - Art 44 to 49; Implementing rules - Art. 21 to 27
  - Integrated Quality Management System (Policy 0001)
  - Quality Management Manual
  - Executive Decision on financial circuits
  - Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  - Decision on the adoption of implementing rules relating to the protection of individuals with regard to the processing of personal and free movement of such data (EMEA/253592/2007)
  - Decision on modification of the Implementing Rules relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data (EMA/455223/2011)
  - Report on exceptions
  - Procedure for requesting exceptions and recording of non-compliance events (SOP/EMA/0044)
  - Guidance on ex post controls EMA/474929/2014
  - Ex post control annual plan
  - Annual report on ex-post controls
  - Data protection Register established under Article 25 of Regulation (EC) 45/2001
  - Charter of tasks and responsibilities of Verifying officer and verifying assistants EMA/96380/2015

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are the main processes and procedures used for the implementation and control of the EMA's/Division's activities documented in a user-friendly fashion? Are they readily accessible? Are they kept up to date?
- Are arrangements in place to ensure data protection is applied to manual processes?
- Have management performed a risk assessment of their main processes and procedures, when appropriate and for example in case of major modifications (if not already covered through the risk management exercise - see ICS 6)? Accordingly, have the most vulnerable parts of the processes and procedures been identified and appropriate mitigating controls been implemented?
- Are the process controls in place adequately designed? Is it clear: (1) Who performs the control?; (2) How the control is being performed (methodology, sample size, etc.)?; (3) What information is required to perform the control?; (4) How frequently the control operates?; (5) What criteria are used to define the level of significance of "anomalies" identified (i.e. what type of issues detected by the controls should be considered significant; what type of error should be considered minor)?
- Are audit logs and corresponding alerts for actions considered risky foreseen for all critical information systems?
- Are the respective roles and responsibilities in the control chain clear to all parties involved? Is information about the control activities and results adequately and effectively shared between all parties involved?
- Are audit logs and corresponding alerts for actions considered risky foreseen for all critical information systems?

ICS 9. Management Supervision: Management supervision is performed to ensure that the implementation of activities is running efficiently and effectively while complying with applicable provisions.

Requirements

- Management at all levels supervise the activities they are responsible for and keep track of main issues identified. Management supervision covers both legality and regularity aspects and operational performance (i.e. achievement of WP objectives).
- The supervision of activities involving potentially critical risks is adequately documented.
- Management monitors the implementation of accepted ECA/IAS/IAC audit recommendations and related action plans.
- At least twice a year and at any time deemed appropriate, the Heads of Division inform the Executive Director of any potentially significant issues related to internal control and audit investigations as well as material budgetary and financial issues that might have an impact on the sound management of appropriations or which could hamper the attainment of the objectives set.

  Main references:

  - Annual report on ex-post controls
  - Guidance on ex post controls EMA/474929/2014
  - Ex post control annual plan
  - Charter of tasks and responsibilities of the Executive Director as authorising officer EMA/MB/56129/2015
  - Charter of tasks and responsibilities of authorising officers by delegation EMA/235295/2015
  - Executive Decision on financial circuits
  - Annual Report on Implementations of Audit Recommendations
  - Quarterly deviations report
  - Mid-Year Report
  - Annual Activity Report
  - Annual Report
  - Risk Register EMA/159414/2011

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are the supervisory activities sufficiently focused on high-risk areas? The following situations would typically warrant an increased level of supervision: - Complex operations; - Transactions of high monetary value; - Low control consciousness among staff; - Lack of experienced or skilled personnel; - Reorganisation or significant modification of operating activities; New or revamped IT systems; - Potential conflicts of interest or influence from external parties; - Activities of a politically sensitive nature; - Activities impacting significantly on the working conditions of staff (health, safety, security).
- Is there systematic follow-up of significant issues identified through the supervisory activities?
- If implementing bodies are responsible for carrying out actions (e.g. Member States or agencies), has appropriate supervision or follow-up been established by the responsible EMA service?
- Is the supervision of operational performance based on the EMA's WP objectives and related performance indicators? Are these objectives and indicators useful in practice? If not, why?
- Do management have satisfactory evidence that key controls in place are operating as intended in practice (for example via the results of supervisory activities, audits, investigations and other relevant sources of information)?
- Are all reported internal control weaknesses properly analysed and addressed where necessary?
- Depending on the nature of the work performed, the documentation of supervision can, for example, be constituted of minutes of meetings, notes explaining key decisions, signature of authorising officer in IT systems, or documents explaining the scope, methods, results and conclusions of the supervisory activities.

ICS 10. Business Continuity: Adequate measures are in place to ensure continuity of service in case of "business-as-usual" interruption. Business Continuity Plans are in place to ensure that the EMA is able to continue operating to the extent possible whatever the nature of a major disruption.

Requirements

- Adequate measures, including handover files and deputising arrangements for relevant operational activities and financial transactions, are in place to ensure continuity of service during "business-as-usual" interruptions (such as sick leave, staff mobility, migration to new IT systems, incidents, etc.).
- Business Continuity plans (BCPs) and business impact analyses (BIAs) cover the crisis response and recovery arrangements with respect to major disruptions (such as pandemic diseases, terrorist attacks, natural disasters, etc.). They identify the functions, services and infrastructure which need to be restored within certain time-limits and the resources necessary for this purpose (key staff, buildings, IT, documents and other). Procedures are established for the review and validation of Business continuity documentation. Reviews are at least annual, through the existing risk management process.
- Electronic and hardcopy versions of BC documentation are stored in secure and accessible locations, which are known to relevant staff.
- Contingency and backup plans for information systems are established, maintained, documented and tested as determined by operational, business continuity and security needs.

Main references:

- EMA Business Continuity Management Plan (BCMP) EMA/569486/2008
- EMA Pandemic Influenza Crisis Management Plan - EMEA/214301/2006
- Executive Decision on financial procedures in the Business Continuity Situation EMA/560484/2010
- BCP micro site: http://emeaplus/BCP/html/default.html
- Division and Department-specific plans: https://docs.eudra.org/webtop/drl/objectId/0b0142b2815627d5
- Business Impact Analyses: https://docs.eudra.org/webtop/drl/objectId/0b0142b28246287b
- Hand over file SOP/EMA/0127

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Continuity of Service (Business-As-Usual): Are the EMA's procedures to ensure continuity of service (handover arrangements, backup procedures, etc.) sufficiently known, readily accessible (in particular to new staff) and applied in practice?

- Business Continuity Plan: Are management and relevant staff sufficiently aware and appropriately trained regarding the BCP? Do they know what to do in the immediate response to major disruption in order to minimise the risks to staff and assets? Is the BCP easily understandable and readily accessible to those who need it when they need it?
- Business Continuity Plan: Are priorities and key risks – including IT risks – clearly defined and sufficiently highlighted in the BCP? Short and concise messages and instructions are usually more effective than long and detailed explanations, particularly in a stressful situation.
- Business Continuity Plan: Is the BCP – including relevant IT elements – sufficiently tested? Conducting periodic testing and practice drills are important means of determining whether the continuity plan works effectively in practice.
- Business Continuity Plan: Are results of testing activities sufficiently analysed and documented, necessary improvements identified and BCP updated accordingly?

ICS 11. Document Management: Appropriate processes and procedures are in place to ensure that the EMA's document management is secure, efficient (in particular as regards retrieving appropriate information) and complies with applicable legislation.

Requirements

- Document management systems and related procedures comply with relevant compulsory security measures, provisions on document management and rules on protection of personal data.
- In particular, every document that fulfils the conditions laid down in the implementing rules needs to be registered, filed in at least one official file (each file being attached to a heading of the Filing Plan), and preserved by appropriate use of the EMA's registration and filing systems, mainly EDMS.

  Main references:

  - /Records Management Policy EMA/590678/2007, reviewed on 10/07/2014
  - EC decision 2002/47/EC, ECSC, Euratom of 23.1.2002 concerning "Provisions on document management" and its Implementing rules on Registration SEC(2003) 349/1, Filing SEC(2003) 349/2 and Preservation SEC(2005) 1419
  - EC Decision 2004/563/EC, Euratom of 7.7.2004 concerning "Provisions on electronic and digitised documents" and its implementing rules SEC(2005) 1578
  - EC Implementing Rules 'Registration and Keeping Registers of the Institution's Documents' SEC(2003)349/1
  - EC Implementing Rules 'Filing and the Management of the Institution's Files' SEC(2003)349/2
  - EC Implementing Rules 'Preservation of the Institution's Files' SEC(2007)734
  - Guidelines for the registration of e-mails SEC(2006)353
  - EC Decision 2001/844/EC, ECSC, Euratom of 29.11.2001 concerning "EC provisions on security"
  - Model Requirement for the Management of Electronic Records (Moreq)

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are documents adequately protected against destruction, theft, fire, etc.?
- Are the procedures for registration sufficiently known? Are they applied in practice?
- Are the procedures for filing sufficiently known?
- In general, is the time spent on finding documents reasonable?
- Are applicable rules (EMA and EMA-specific) regarding handling of sensitive documents sufficiently known and applied in practice?

- Are adequate measures taken to ensure the readability of documents?
- Are management and staff sufficiently aware of applicable retention periods for documents? Are retention periods respected in practice? Any document in whatever medium (paper, fax, e-mail, electronic) received or formally drawn up by an EMA division in the course of its activities:
  - if it is likely to require action, follow-up or a reply from the EMA or one of more of its departments or involves the responsibility of the EMA or one or more of its departments;
  - if it contains important information which is not short-lived.

ICS 12. Information and Communication: Internal communication enables management and staff to fulfil their responsibilities effectively and efficiently, including in the domain of internal control. The EMA has an external communication strategy to ensure that its external communication is effective, coherent and in line with EMA's key messages. IT systems used and/or managed by the EMA (where the EMA is the system owner) are adequately protected against threats to their confidentiality and integrity.

Requirements

- Internal and external communications comply with relevant copyright provisions.
- Management tools are developed for the EMA's main activities and thereafter, if appropriate, at the level of the divisions. These include concise management information necessary to oversee the entity's activities and evolution, for example: performance indicators, financial information, legality and regularity error rates, project deadlines, audit findings and HR indicators, or other relevant management information.
- Arrangements in line with the EMA'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 divisions– that concern their work assignments and environment.
- All personnel are encouraged to communicate potential internal control weaknesses, if judged significant or systemic, to the appropriate management level. Contact person(s) is/are assigned to facilitate and coordinate such reporting.
- EMA has a documented strategy for external communication (outside the EMA), including clearly defined target audiences, messages and action plans.
- Arrangements are in place to systematically collect feedback from stakeholders and monitor public opinion to inform and adapt communication strategies.
- The Agency has a robust process for communication planning, which is embedded in the Agency's overall business planning.
- Documented approval processes ensure that for external communication materials are aligned and consistent with the EMA's key messages.
- Established cross-Agency process and procedures are in place to guarantee that product-related information is produced and published consistently at certain defined moments for all medicines evaluated by EMA.
- A system for quality control of the information produced by EMA is in place and is applied systematically to key information prior to its publication.
- Arrangements are in place to coordinate key messages within the European medicines regulatory network.
- The standard EMA Information Security Policy is applied. In particular, the EMA 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.

- 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.

  Main references:

  - Corporate Communication Strategy 2012-2015 (EMA/394375/2012)
  - Annual communication plan 2015 (EMA/96787/2015)
  - Press and media manual (EMA/693706/2014)
  - SOPs e.g. for public health communication (SOP/H/3347)
  - Communications focal points for improved communications planning (EMA/16582/2015)
  - Early Notification System and related SOP (SOP/H/3346)
  - SOP/H/3347 Preparation of 'lines-to-take'
  - WIN/H/3210 Sending of lines to take and safety-related information to the European Union regulatory network and international partners
  - Quality Control Strategy for product-related information (EMA/233963/2014)
  - Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  - Regulation (EC) No 1367/2006 on the application of the provisions of the Aarhus Convention on Access [...]
  - PROPOSAL for a Regulation (EC) regarding public access to European Parliament, Council and Commission documents COM(2008)229 final - 2008/0090 (COD)
  - Data Protection microsite
  - EMA online roadmap: 2012-2017 (EMA/330469/2012)
  - Annual EMA Staff Engagement Survey
  - EMA external and internal website
  - Internal corporate relations framework 2014-2016 EMA/257704/2014 Roles and Responsibilities in the Development, Operation and Maintenance of Information Systems at the EMA EMEA/592842/2007

  EUDRA Information Security Policy TSC/11/2005/004 – EMEA/176914/2005

  Security Policy 0076 EMA/530488/2014

  - Work instructions: Publishing content on www.ema.europa.eu (WIN/EMA/0099)
  - How to publish content on the EMA website
  - WCMS editorial guide (EMA/584692/2012)
  - Editorial style guide (EMA/560894/2012)

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Is the information provided in the EMA's/Division's performance indicators pertinent and useful for the management of these activities? Where possible, is there a clear link to the WP objectives? Are the performance indicators used by management and staff in practice? If not, why? Possible HR indicators are detailed in the annual staff policy plan: staff turnover, workforce evolution, number of training days per person, forecasting of departures
- Have the current arrangements used for internal communication been analysed? Are arrangements in place to ensure that management and staff are informed of other divisions' and departments' decisions/projects/initiatives that may affect their responsibilities and tasks?
- Are there any recent examples where flaws in inter and intra-division communication have caused problems or impacted on the EMA's performance? Have the underlying causes been analysed? Have measures been taken to prevent similar communication issues in the future?
- Have the current procedures and methods used for external communication been analysed to identify their strengths and weaknesses, including cost-benefit aspects?
- What is done in practice to seek and analyse feedback from target audiences regarding communication impact? Is the information obtained reliable and pertinent? Is relevant feedback escalated to the appropriate level and used to adapt ongoing communication strategies?
- What is done to align EMA's external communication activities with the EMA's key messages? Have there been examples where external messages were inconsistent with agreed Agency priorities and messages.
- Are all staff concerned sufficiently aware of the EMA Information Security Policy? Is IT Security a regular topic at management meetings? Are objectives for Information Security established and monitored? Do results of the regular supervision of IT systems, audit findings or information from other sources suggest that there may be IT-security-related issues? Are these issues escalated to and discussed at the appropriate management level?
- Is feedback from IT users regarding system performance collected and analysed, given that systematic collection and analysis of comments and suggestions from IT users (through surveys or channels for ad-hoc feedback) can be a good way of detecting effectiveness and efficiency issues? Are statistics on system down-time, server capacity and other performance indicators regularly analysed? Are system performance issues reported to the appropriate management level?
- Does the EMA have effective procedures in place concerning data retention periods, data backup, data access and archiving? Can management demonstrate that these procedures are applied in practice? Do the results of supervisory activities, "stakeholder complaints", audit findings or information from other sources suggest any weaknesses in the field of data management, e.g. data quality issues, missing or untimely data, etc.?

ICS 13. Accounting and Financial Reporting: Adequate procedures and controls are in place to ensure that accounting data and related information used for preparing the organisation's annual accounts and financial reports are accurate, complete and timely.

Requirements

- The Executive Director and each delegated Authorising Officer have responsibility for ensuring the reliability and completeness of the accounting information under his/her control necessary to the Accounting Officer for the production of accounts which give a true image of the EMA's assets and of budgetary implementation.
- The EMA's accounting procedures and controls are adequately documented.
- Financial and management information produced by the EMA, including financial information provided in the Annual Activity Report, is in conformity with applicable accounting rules and the Accountant's instructions.

Main references:

- EMA Financial Regulation - Art. 50 (3) Implementing rules – Art. 28 to 37
- Charter of tasks and responsibilities of the Executive Director as authorising officer EMA/MB/56129/2015
- Charter of tasks and responsibilities of the agency's accounting officer EMA/MB/655670/2015
- Charter of tasks and responsibilities of authorising officers by delegation EMA/235295/2015
- Charter of tasks and responsibilities of the verifying officer and verifying assistant EMA/96380/2015
- Charter of tasks and responsibilities of the operational and financial initiating agents EMA/408104/2015
- Executive Decision on financial circuits EMA/tbc/2015
- Budget Monitoring reports (4times per year)
- Regular Accounts Reports

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Does the EMA have the necessary skills and experience in the accounting and financial fields?
- Are accounting data quality controls pertinent and sufficiently documented? Such controls may, for example, include analyses of general accounts, analysis of ageing balances of outstanding invoices, outstanding pre-financing, separation of duties, reviews of reports, sample testing, review of account reconciliations, checks of IT system interfaces, etc. Is management satisfied that these controls work as intended in practice?

- Have the guidelines proposed by the European Commission’s Accounting Officer on the accounting quality project been put in place?

ICS 14. Evaluation of Activities: Evaluations of expenditure programmes are performed to assess the results, impacts and needs that these activities aim to achieve and satisfy.

Requirements

- 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.

Main references:

- Advisory Committee on Procurement and Contracts (ACPC) EMA/162846/2014
- Project gated procedure (http://emeaplus/EMEAPlus_WebsiteNew/Projects/html/Step0.html)
- Agency evaluation report (European Commission)
- EMA internal notice on project-related ex post and ex ante evaluations: guiding principles in relation to programmes and projects

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Are evaluation activities appropriately organised and resourced to meet their purposes?
- Are evaluation activities planned in a transparent and consistent way so that relevant evaluation results are available in due time for operational and strategic decision-making and reporting needs?
- Does the evaluation design provide clear and specific objectives, and appropriate methods and means for managing the evaluation process and its results?
- Do evaluation activities provide reliable, robust and complete results? Are the evaluation reports used by management in practice, i.e. do they have a real impact on the EMA's decision-making or the policy prepared by the EMA? If not, why?
- Are evaluation results communicated in such a way that they ensure maximum use of the results and that they meet the needs of decision-makers and stakeholders?

ICS 15. Assessment of Internal Control Systems: Management assess the effectiveness of the EMA's key internal control systems, including the processes carried out by implementing bodies, at least once a year.

Requirements

- Management assess the effectiveness of the EMA's key internal control systems, at least annually. Such self-assessments can, for example, be based on staff surveys or interviews combined with management reviews of supervisory reports, results of evaluation and ex-ante/ex-post verifications, audit recommendations and other sources that provide relevant information about the EMA's internal control effectiveness.
- On an annual basis – as part of the Annual Activity Report – the Executive Director signs a statement, to the best of his/her knowledge, on the accuracy and exhaustiveness of the information on management and internal control systems provided in the Annual Activity Report.

Main reference:

- Template for the consolidated Annual Activity Report, EMA/441956/2015
- Annual Review of Internal Control Standards
- Internal Audit Capability annual report
- Internal Audit Service annual report
- European Court of Auditors annual report
- Annual Activity Report
- BEMA Report

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Do managers and staff who participate in self-assessments of the EMA's internal control systems have a sufficient understanding of internal control and risk management? If not, what is done to avoid misinterpretations or misunderstandings that could affect the results and conclusions of the exercise?
- Is the self-assessment well organised, pragmatic and value-adding (or is it regarded as a "bureaucratic burden")? Is it sufficiently sponsored by senior management?
- Is the self-assessment focused on the EMA's main activities and risks? A too wide or too detailed scope may reduce its effectiveness.

Are self-assessment results sufficiently supported, for example via references to other relevant sources?

ICS 16. Internal Audit Capability: The EMA has an Internal Audit Capability (IAC), which provides independent, objective assurance and consulting services designed to add value and improve the operations of the EMA.

Requirements

- The role and responsibilities of the EMA's Internal Audit Capability (IAC) are formally defined in the Internal Audit Charter of the Audit Capability.
- External assessments of the audit activities and annual self-assessments are performed as required by the IIA Standards.
- The annual risk-based audit work plan is part of a multi-annual strategic plan coordinated with the IAS and it is approved by the Management Board.
- The Executive Director and Management Board ensure that the IAC is independent of the activities they audit.
- The Executive Director and Management Board ensure that the IAC has sufficient and adequate resources to perform the audit work plan.
- The IAC reports to the Management Board and Executive Director on findings and recommendations. It also reports on the status of corrective action implementations for the open recommendations.

Main reference:

- EMA Financial Regulation - Art 84
- Code of Ethics of EMA's IAA (doc. ref.: EMA/409140/2009)
- Internal Audit charter (doc. ref.: EMA/ 145450/2014
- Internal Audit Manual (doc. ref.: EMA/585484/2010)
- Auditors' assurance map prepared yearly.
- Audit Strategy
- Annual Audit Plan (approved yearly by the MB)
- Risk assessment methodology, 'MARCI' (doc. ref.: EMEA/583074/2009)
- Internal Assessment Report EMA/301261/2015

Tips for assessing control effectiveness

Reminder: When assessing control effectiveness, two fundamental questions should be asked:

(1) Considering the EMA's specific activities and risks, are the current control arrangements sufficient?

(2) Do the control arrangements work as intended in practice?

Set out below are some questions management may want to consider when assessing control effectiveness with regard to this particular ICS:

- Does the IAC apply, when appropriate for the EMA organisation, internationally recognized audit standards, such as the standards issued by the Institute of Internal Auditors (IIA) or equivalent? In

particular, are there any situations that could threaten the IAC's organisational independence? Are the auditors sufficiently aware of the principles of integrity, objectivity, confidentiality and competency, and do they apply them in all of their dealings?

Annex 3

Optional Assessment Template

One purpose of the revision of the internal control framework is to increase flexibility. Indeed, all ICS may not be equally important to the EMA - or Divisions and Departments - at all times. Thus, depending on each service's activities, priorities, main risks, control environment and other considerations, management will select those Standards on which further emphasis on effectiveness is perceived as necessary.

The template below – which is optional – may help management at all levels identify the ICS that are most relevant to them, i.e. the domains of internal control that need most effort and resources.

ATTENTION! The reasons for "high relevance" proposed in the table are indicative and not exhaustive.

Internal Control Standard for Effective Management	Relevance	Typical reasons for High relevance
1. Mission: The EMA's *raison d'être is* clearly defined in up-to-date and concise mission statements developed from the perspective of the relevant legislation and the EMA's stakeholders and partners.	High? Normal?	Significant modifications to the entity's overall goals, strategy or working methods Low awareness of the entity's mission and goals
2. Ethical and Organisational Values: Management and staff are aware of and share appropriate ethical and organisational values and uphold these through their own behaviour and decision-making.	High? Normal?	Activities exposed to conflict of interests, fraud, misuse of insider information or other ethical issues Concern regarding awareness of ethical provisions or ethical behaviour Recent concrete evidence of failure in this area
3. Staff Allocation and Mobility: The allocation and recruitment of staff is based on the EMA's objectives and priorities. Management promote and plan staff mobility so as to strike the right balance between continuity and renewal.	High? Normal?	Frequent changes of the entity's priorities and tasks (need for flexibility) Signs of rigidity - opposition to changes Recruitment or staff allocation issues, which negatively affect the entity's performance Need for enhanced staff planning and allocation tools High staff turnover affecting the entity's performance Signs of staff not being satisfied with job content or prospects Need for new ideas and working methods (renewal of staff profiles needed)

4. Staff Evaluation and Development: Staff performance is evaluated against individual annual objectives, which fit with the EMA's overall objectives. Adequate measures are taken to develop the skills necessary to achieve the objectives.	High? Normal?	Need to improve staff performance Significant staff complaints regarding annual objectives or evaluations Need to develop or retain competences and skills Current training activities are not sufficiently in line with the entity's activities and objectives
5. Objectives and Performance Indicators: The EMA's objectives are clearly defined and updated when necessary. These are formulated in a way that makes it possible to monitor their achievement. Key performance indicators are established to help management evaluate and report on progress made in relation to their objectives.	High? Normal?	Significant modifications to EMA's strategy, goals or objectives Current objectives not sufficiently clear, accepted or understood Current indicators not sufficiently pertinent Current objectives / indicators not used as a management tool in practice (for various reasons) Key new activities for which indicators/ reporting need to be created
6. Risk Management Process: A risk management process that is in line with applicable provisions and guidelines is integrated into the annual activity planning.	High? Normal?	New or significantly modified activities Major reorganisation of EMA/Divisions/Departments Current risk assessment process is cumbersome or not effective Risk management is not truly integrated into the regular management processes Low awareness of risk management concept

7. Operational Structure: The EMA's operational structure supports effective decision-making by suitable delegation of powers. Risks associated with the EMA's sensitive functions are managed through mitigating controls and by specific ex-post controls and/or focused audit every two years. Adequate IT governance structures are in place.	High? Normal?	Significant reorganisation of Divisions/Departments Current organisation not optimal and may hamper the entity's performance Risk assessment of delegated powers needs to be improved High number of sensitive functions Sensitive functions not sufficiently analysed Uncertainties whether mitigating controls work as intended in practice (sensitive functions) Significant responsibilities in the domains of Information System development, maintenance or security. The activity of the EMA relies heavily on IT systems. IT systems need to be modified frequently to adapt to changing needs The activity of the EMA requires a large amount of IT investment or development
8. Processes and Procedures: The EMA's processes and procedures used for the implementation and control of its activities are effective and efficient, adequately documented and compliant with applicable provisions. They include arrangements to ensure segregation of duties and to track and give prior approval to control overrides or deviations from policies and procedures.	High? Normal?	Complex activities (operational aspects) Complex activities (legal and regulatory aspects) Activities involving third parties (e.g. MS agencies) Activities representing significant legal/regulatory and financial risks Current processes and procedures are unnecessarily cumbersome and could be made more effective The documentation on processes and procedures is outdated, not user-friendly or not easily accessible The risk analysis of the entity's processes and procedures needs to be improved

9. Management Supervision: Management supervision is performed to ensure that the implementation of activities is running efficiently and effectively while complying with applicable provisions.	High? Normal?	Complex activities or procedures Politically sensitive activities Transactions of high monetary value Poor segregation of duties Low control consciousness Lack of experienced or skilled personnel Reorganisation or significant modification of operating activities Uncertainties whether the processes and procedures work as intended in practice New or revamped IT systems High risk of conflicts of interest Supervisory skills and techniques insufficient High reliance on external parties (contractors, national agencies or auditors)
10. Business Continuity: Adequate measures are in place to ensure continuity of service in case of "business-as-usual" interruption. Business Continuity Plans are in place to ensure that the EMA is able to continue operating to the extent possible whatever the nature of a major disruption.	High? Normal?	Interruption of the entity's activities, even for short periods, may have significant consequences (stakeholder complaints, negative press, security issues, etc.) The entity's core activities strongly depend on IT systems Frequent issues or problems due to insufficient handover arrangements, backup procedures, high staff turnover, etc.
11. Document Management: Appropriate processes and procedures are in place to ensure that the EMA's document management is secure, efficient (in particular as regards retrieving appropriate information) and complies with applicable legislation.	High? Normal?	The volume of documents produced, received or managed by the entity is high The EMA's activity entails a significant amount of document handling The entity manages sensitive documents

12. Information and Communication: Internal communication enables management and staff to fulfil their responsibilities effectively and efficiently, including in the domain of internal control. The EMA has an external communication strategy to ensure that its external communication is effective, coherent and in line with the EMA's key political messages. IT systems used and/or managed by the EMA (where the EMA is the system owner) are adequately protected against threats to their confidentiality and integrity.	High? Normal?	*Internal communication* Complex activities where high-quality information is key High level of delegation Geographically dispersed activities Current management tools do not provide pertinent or sufficient management information Sharing of management information with staff should be improved Effects are expected on motivation, commitment and team spirit. Issues indicating that management and staff are not sufficiently aware of their responsibilities in the domain of internal control *External communication* Frequent communications with external world/ activity of the EMA affect external parties Reactions from external partners or stakeholders suggest that external communication should be improved Management has no precise idea of how its stakeholders appreciate the services provided *Information system security* Significant responsibilities in the domains of Information System security/ management of sensitive data/significant or frequent issues that could impact on information security. There are frequent or significant Information System issues impacting on the entity's performance
13. Accounting and Financial Reporting: Adequate procedures and controls are in place to ensure that accounting data and related information used for preparing the organisation's annual accounts and financial reports are accurate, complete and timely.	High? Normal?	High volume/value or complexity of financial transactions High dependence on manual controls Complex or new accounting systems Uncertainties regarding the reliability and integrity of the entity's accounting data and information Lack of required accounting and financial reporting skills

14. Evaluation of Activities: Evaluations of expenditure programmes are performed to assess the results, impacts and needs that these activities aim to achieve and satisfy.	High? Normal?	The risk of adverse publicity (press) is high if policy achievements are unsatisfactory There are concerns regarding the evaluation function's resources, skills or experience Evaluation reports produced usually have little or no impact on management decisions (for various reasons)
15. Assessment of Internal Control Systems: Management assess the effectiveness of the EMA's key internal control systems, including the processes carried out by implementing bodies, at least once a year.	High? Normal?	Complex activities or activities involving significant risks Uncertainties regarding the quality of internal control systems Signs of insufficient internal control (high error rates, complaints) Uncertainties regarding the adequacy of the self-assessment process and reliability and pertinence of self-assessment results
16. Internal Audit Capability: The EMA has an Internal Audit Capability (IAC), which provides independent, objective assurance and consulting services designed to add value and improve the operations of the EMA.	High? Normal?	Current IAC activities do not add sufficient value Concern regarding IAC's resources, skills or experience There are situations that could threaten IAC's independence and objectivity, such as conflict of interests, inappropriate reporting lines, incompatible involvement in activities they audit, etc.