# Criteria Catalogue for the Assessment of the Internal Audit System

Annex 1 from DIIR Revisionsstandard No. 3

Version 1.0, published 24.6.2018

DIIR Deutsches Institut für Interne Revision e.V.

# Preamble

This publication is a translation of Annex 1 of DIIR Revisionsstandard No. 3 "Review of Internal Audit Systems (Quality Assessments)" published in April 2017.

In doing so, we are responding to a widespread wish of our internationally active members, who want to communicate to their non-German-speaking colleagues the criteria by which the effectiveness of an internal audit activity in Germany can be assessed.

# Content

# Criteria Catalogue for the Assessment of the Internal Audit System

The following catalogue of criteria is a tool regarded by IDW and DIIR as appropriate for conducting an IRS audit in accordance with this auditing standard in order to ensure uniform audit quality. The list of criteria is aligned to the requirements resulting from the mandatory elements of the International Professional Practices Framework (IPPF) of Internal Auditing. Further requirements may result from the other agreed examination criteria, so that the list of criteria may have to be extended accordingly.

The criteria catalogue is designed in such a way that a general application is possible in different size classes, industries and organisational structures. This means that both public and private sector characteristics of corporate governance can be taken into account.

# Fundamentals

## I. Organization, integration into the company and Responsibilities

1. There is an official written, appropriate regulation (audit charter, internal audit guideline or similar) (**minimum standard 1**).

2. The regulation has been approved and published by the board. It is regularly checked for topicality and adequacy, also with regard to the corporate culture.

3. The main tasks of the internal audit activity are the auditing of the adequacy and effectiveness of the internal control system, the management and monitoring processes and the effectiveness of the risk management system. This also includes assessing the effectiveness of measures to prevent and detect fraud.

4. The areas of activity of the internal audit activity are based on the objectives of the company/organisation and include all activities of the company/organisation and, where applicable, activities outsourced to third parties (unrestricted right of audit).

5. Neutrality, independence from other functions and unlimited right to information are guaranteed (**minimum standard 2**).

6. The employees of the internal audit activity do not assume any responsibility in operations and do not audit any activities that they are biased in.

7. The internal audit activity is included in the distribution of key company information.

8. The internal audit activity has an audit manual with the following key contents: Procedures and/or methods for audit planning, preparation, performance, follow-up, reporting, documentation, access to and archiving of audit results.

9. The employees know the internal audit manual. It is reviewed on a regular basis for topicality and adequacy. Compliance is continuously monitored.

10. Differentiation from other governance functions is ensured. The internal audit activity is established as the third line of defense ("Three Lines of Defense Model") as a central element of good corporate governance.

11. The value system of the internal audit activity is established and aligned in accordance with the Code of Ethics and the Core Principles of the IPPF.

## II. Budget/Resources

12. The internal audit activity has adequate quantitative and qualitative staffing (**minimum standard 3).**

13. The personnel cost budget corresponds to the tasks and requirements of the internal audit activity and is suitable for recruiting and retaining qualified staff.

14. The IT equipment for the administrative processes (e.g. audit planning, audit control) is sensible and adequate.

15. The IT equipment for the operational processes of conducting an audit (e.g. analysis software, audit documentation and follow-up process) is sensible and adequate.

16. The other operating cost budget (e.g. travel expenses, education and training, external resources) corresponds to the tasks and requirements of the internal audit activity.

## III. Planning

17. The audit plan of the internal audit activity is prepared based on a standardised and risk-oriented planning process (**minimum standard 4**).

18. The audits for the planning period are systematically compiled at least once a year and presented to the board for approval.

19. Legal requirements, special requirements of the board, and proposals from within and outside the internal audit activity are taken into account in planning.

20. The audit objects (audit universe) are completely mapped during planning.

21. A standardized methodology exists for the systematical analysis of the risk potential of the audit objects.

22. Regular checks are established to ensure that the scope and the assessment of the audit objects are current and complete.

23. The authorities to amend the risk assessment method and audit objects are determined.

24. Unscheduled audits that become necessary on short notice are taken into consideration appropriately.

25. Subsequent changes/adjustments to the audit plan, e.g. the cancellation or addition of audits, are documented in a traceable manner. These changes are communicated to the responsible management board to an appropriate extent.

## Performance

### IV. Preparation

26. The audit plan is the basis for developing timeframes and prioritisation of the audit objects. Resources and responsibilities are allocated in a traceable manner.

27. The audit object is being analysed, information is obtained and audit methods are determined.

28. Prior to starting the audit, milestones and the anticipated audit duration are determined.

29. In general, audits are announced to the auditee with sufficient advanced notice. Deviations from this procedure are plausible and adequate in individual cases (e.g. audits of fraudulent acts).

30. A kick-off meeting with the department to be audited is part of the audit process (possible also via telephone or video conference).

31. The objectives and scope of the audit are defined and documented.

32. The work program is approved by internal audit management or by an appointed person.

### V. Audit

33. The audit is conducted in accordance with the approved work program.

34. Legal stipulations and internal company regulations are assessed during the audit to determine if they have been implemented and adhered to (compliance).

35. Aspects such as efficiency, profitability, corporate objectives, security, risk appetite, and effectiveness of controls in place to prevent and discover fraudulent acts are audited.

36. Measures/recommendations are provided for any negative audit findings.

37. If necessary, the audit results are reconciled with the audited department and the person responsible for the audit.

38. Major deviations between the audit steps and the work program are documented and approved.

39. The type and scope of the audit activities and results are documented in a standardised, proper and orderly manner (**minimum standard 5**).

40. A standardised rating of the audit results (system for all types of audits and audit objects) is implemented.

41. The audit results can be clearly derived from the working papers and therefore are traceable for knowledgeable third parties within an adequate period of time.

42. The methods and checklists used are systematic, up-to-date and adequate.

43. A closing meeting with the auditee, if necessary, is conducted in a timely manner. Any changes to the audit results are reconciled and documented.

44. In the closing meeting, adequate measures are agreed with implementation dates and clear responsibilities. Agreement or differences in opinion are documented with regard to the audit results.

45. If a closing meeting is waived, another traceable and documented form for reconciliation of the audit results is ensured.

## VI. Reporting

46. The report is comprised of the following components:

    Assignment and implementation (audit objective and scope) including definition of topics (what?), audit team (who?), audit period (when?), audit location (where?), audit reason (why?), type of audit (how?)

    Management Summary

    Detailed report incl. findings, risks, measures/recommendations with implementation dates (action plan), responsibilities and rating, if applicable

47. The form of the audit reports is standardised.

48. Preliminary audit results, e.g. in the form of draft reports, are presented to the management of the audited unit in good time prior to the closing meeting.

49. In case of disagreement, it is possible for the auditee to include a comment in the report explaining the differences in opinion.

50. The finalisation and distribution of the report including the list of measures takes place in a timely manner.

51. Prior to distribution the audit report is approved by the Chief Audit Executive or a person authorised.

52. A standard distribution list is established and used for the regular distribution of audit reports.

53. An audit report or memorandum is available for each completed audit.

54. The reports or a summary of the reports (e.g. in annual reports) are distributed to the executive board.

## VII. Post-audit activities

55. The Chief Audit Executive or a responsible person conducts feedback meetings with the audit team.

56. Based on the feedback meetings, potential for improvement is derived to further develop the internal audit activity (e.g. risk assessment, audit methods and processes, as well as resource planning).

57. Any insights gained during the audits are made available to the employees of the internal audit activity (knowledge management).

58. Retention methods and timeframes for audit reports and working papers are defined and adhered to.

## VIII. Follow-up

59. The implementation of measures documented in the report is monitored by the internal audit activity through an effective follow-up process (**minimum standard 6**).

60. Deadline extensions for the implementation of measures are justified and documented.

61. Notification regarding measures which were – without justification – not implemented is provided to the management board on a regular basis.

62. On-site audits are conducted as a supplemental instrument to the follow-up process.

## Employees

### IX. Selection

63. A personnel planning process exists in the internal audit activity, which considers factors such as average fluctuation, retirement, training level, professional experience and foreign language qualifications, or similar.

64. Job or functional descriptions are available for all employees within the internal audit activity.

65. The selection of personnel takes place on the basis of the job or functional descriptions.

66. The employee's professional experience and qualification is suitable to ensure fulfilment of the internal audit activity's tasks.

67. If the necessary professional experience and qualification is not available to fulfil the audit assignment/advisory assignment, the internal audit activity does engage competent third parties.

### X. Development/Advanced Training

68. The functional and audit-related staff qualification is ensured through regular internal or external training measures.

69. The further development of social skills and management qualifications is ensured through targeted internal or external measures.

70. Obtaining audit-related qualifications (e.g. Interner Revisor[DIIR], CIA, CISA, and CFE) is promoted.

71. Annual reviews and target-setting take place on a regular basis with each staff member, and include aspects such as audit tasks, strengths-weaknesses analysis, assessment of personal development and training measures.

72. The internal audit personnel also itself ensures that they develop their skills and qualifications further.

## XI. Management of the internal audit activity

73. The Chief Audit Executive is qualified in accordance with the requirements of the position.

74. The internal audit activity is accepted and highly regarded by the management board.

75. The Chief Audit Executive has developed quality standards that are documented in the internal audit manual. They are the basis on which quality checks are conducted.

76. The Chief Audit Executive must develop and maintain a quality assurance and improvement program, which covers all areas of the internal audit activity.

77. The activities of the internal audit activity, current developments and the main risks are reported periodically to the management board and the audit committee (or comparable bodies).

78. The Chief Audit Executive ensures the implementation of the principles defined in the audit manual through process-integrated measures of quality management.

79. The Chief Audit Executive or a representative appointed by him/her conducts feedback meetings with the audited departments and audit report recipients on a regular basis.

80. Laws, publications with legislative character, as well as national standards for professional practice of internal audit of the DIIR and the mandatory elements of the IIA's IPPF are complied with. Deviations from the standards are communicated adequately.

81. The Chief Audit Executive ensures a regular exchange of information with external third parties, such as the company's external auditor.

82. The Chief Audit Executive ensures a regular exchange of information with internal departments and functions, such as compliance, risk management, security and data privacy.

# Glossary for using the Criteria Catalogue

**Working papers**

Comprise the information and documents received during an audit, the analyses conducted and the resulting conclusions.

**Work program**

Document in which the procedural steps to be conducted during an audit are listed. The audit objectives are also formulated in the work program.

**Follow-up**

Process in which the internal audit activity determines whether the actions taken by management as a result of the reported audit findings were executed appropriately, effectively and timely.

**Governance function**

In addition to internal auditing, compliance and risk management, the governance function also includes other guideline functions such as purchasing, human resources and security.

**Management board**

”Management board“ is synonymous with the executive board of a joint-stock corporation, managing directors of a limited liability company, the executive board of a cooperative, management of an administrative authority, management of a corporate entity, the board of directors of a registered association.

**Prüfer für Interne Revisionssysteme[DIIR]**

A person who has the qualification in accordance with IIA standard 1312 to assess internal audit activities and evaluating whether and to what extent the professional requirements of the DIIR/IIA are fulfilled.

**Audit plan (audit program)**

Comprises several audits in a specific time period (e.g. annual audit program).

**Quality assessment**

Description of the audit practice for reviewing activities, working and control frameworks of an internal audit activity by assessors. It involves a quality review by external assessors regarding the quality and compliance with and observance of prescribed and generally accepted standards.

**Quality management**

Program for quality assurance and improvement, which comprises all aspects of audit activities and the continuous monitoring of their effectiveness. The purpose of quality management is to sufficiently ensure that the activities of the internal audit activity correspond to the set objectives.

**Regular**

This is basically regarded as one year, e.g. for the revision period of the internal audit manual.

**Regulation**

The regulation (”rules of procedure“, ”internal audit guideline“ or similar) of the internal audit activity is an official written document which defines the tasks, authorities and responsibility of the internal audit activity. The regulation must (a) define the position of the internal audit activity within the company, (b) secure access to the records, to the workforce and to the assets that are relevant for the fulfilment of audit and advisory assignments and (c) define the scope of the internal audit activity’s activities. In opposite to the audit manual, the regulation regarding the internal audit activity in the company is determined (external presentation).

**Internal audit manual**

The manual summarises the definitions applicable for an internal audit activity regarding the tasks, objectives (vision), structure, and organisational procedures (for the internal audit activity personnel).

**Risk-oriented planning process**

Forms the basis for risk-oriented and targeted audit planning and is based on the systematic analysis of all business processes and corporate entities, under specific consideration of e.g. economic, operational or other corporate risks.

**Corporate culture**

Cultural value patterns within a company or organisation, consisting, among other things, of a mission statement, value system and incentive system.

**Mandatory Elements of the International Professional Practices Framework (IPPF)**

The mandatory elements of the IPPF are:

- Core principles for the professional practice of internal auditing
- Definition of internal auditing
- Code of ethics
- International standards for the professional practice of internal auditing (Standards)

Compliance with the principles set out in the mandatory guidelines is necessary and indispensable for the professional practice of internal auditing. Mandatory guidelines are developed in accordance with an established due diligence process that provides for a defined period of public consultation for stakeholder submissions.

DIIR – Deutsches Institut für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main

Veröffentlicht am 24. Juni 2018 auf www.diir.de

Version 1.0