

Quality Assessment

QA

Certification



Guideline for Conducting a Quality Assessment (QA)

Addendum to DIIR Standard Number 3
("Quality Management")
Second revised Edition, September 2007

Table of Contents

	Page
Introduction	4
A Assessment Process	4
B Requirements for Accredited Assessors	5
C Evaluation Process	5
D Quality Criteria	6
 BASICS	
I. Organization, Position within the Company and Responsibilities	7
II. Budget	8
III. Planning	8
 AUDIT PROCESS	
IV. Preparation	9
V. Execution	10
VI. Reporting	11
VII. Post Audit Work	12
VIII. Follow-up	13
 STAFF	
IX. Selection	13
X. Development/Training	14
XI. Management of the Internal Audit Function	14
 Attachment:	
Glossary	16
 Appendix 1:	
1.1 Confidentiality Statement	17
1.2 Privacy Statement According to Paragraph 5 of the German Federal Data Protection Act	18
 Appendix 2:	
Management Representation Letter	19
 Appendix 3:	
QA Certificate for Certified Companies – Sample	20
 Appendix 4:	
QA Certificate for Certified Assessors	21

Introduction

Given a changing environment in areas such as corporate governance, the quality of internal audit is of utmost importance to an organization. Therefore, a codified process has been developed to assess the quality of any internal audit department. This guideline further specifies the requirements of DIIR Standard Number 3 ("Quality Management") with regard to these quality assessments. It refers to the audit activities of members of DIIR – Deutsches Institut für Interne Revision e.V. For German financial services companies, the minimum risk management requirements (MaRisk) for internal audit as published by the Federal Financial Supervisory Authority (BaFin) apply.

A Assessment Process

A.1 Assessment Types¹

A quality assessment can be conducted

- by a third party or
- as a self assessment with independent validation. In this case, the results of the self assessment are validated by a third party with identical qualifications as described in section B.

A.2 Commissioning of a Third Party

- The DIIR provides a list of accredited assessors upon request.
- No further involvement of the DIIR in the individual assessment takes place.
- The drafting of the contract is performed by the parties without assistance of the DIIR.
- A confidentiality statement and a privacy statement based on paragraph five of the German Federal Data Protection Act should be signed (see appendix for sample statements).
- When commissioning a third party, it is important to ensure that the audit team collectively meets all necessary requirements:
 - Experience in all areas of internal audit (leadership, management, auditing, and quality management).

¹Here it is important that the two companies do not audit each other within a period of five years.

- Personal qualifications
- Professional requirements according to the audit function being assessed (industry knowledge, IT, finance and accounting, etc.)
- That at least the head of the audit team is accredited as described in section B
- That every assessor is independent and has documented experience in internal audit.

A.3 QA Preparation

- Prior to the QA, the audited unit should become familiar with the assessment process and requirements using this guideline.
- The initiator should make all necessary documents and information available to the contracted assessors, ideally prior to the start of the assessment.
- The initiator should ensure that office space, any necessary hardware and access to any relevant IT systems are available prior to the assessment. Additionally, the required contact persons (e.g. staff members, customers, colleagues) should be informed.
- The contracted assessor on his part should provide documents (questionnaires, tools, templates), ask for necessary information and also arrange meetings prior to the assessment.
- Planning and execution of the assessment should occur in a standardized and risk oriented manner (in accordance with the requirements for assessments by internal audit).

A.4 QA Execution

- During the assessment itself, all levels of the audit department being assessed should be interviewed. Additionally, interviews should be conducted with at least one member of the company's executive management, executives from areas audited by the internal audit department and external auditors and, if applicable also representatives of the audit committee.
- Processes, methods and documents are to be assessed based on this guideline according to the quality criteria requirements.
- Samples from multiple years should be utilized (at a minimum from the current and the previous year).
- As part of quality assessments the implementation of measures identified in previous assessments should be audited.

A.5 QA Reporting

- The recipient of the report is the initiator of the QA. The following minimum requirements apply to the report:
 - Description of the organizational structure of the internal audit department reviewed and its position within the company (among other things, its organizational and process independence).
 - Description of the audit strategy, the audit program, as well as the risk analysis.
 - Significant findings, especially identified deficiencies and measures to eliminate them, including responsibilities and deadlines for implementation.
 - Documentation that deficiencies identified in previous QAs have been eliminated.
 - Concluding remarks regarding the appropriateness and effectiveness of the internal audit department during the assessment period.

Upon request by the initiator, a certificate can be issued by the accredited assessor (see appendix 3 for an example).

B Requirements for Accredited Assessors

The requirements for the accreditation of assessors are:

- Successful participation in a specific seminar offered by the DIIR (QA Seminar).
- Evidence of management experience with written confirmation from the assessor's employer specifying management experience.
- Evidence of at least three years work experience in internal audit; written confirmation from the assessor's employer.

If these requirements are met, the assessor receives a certificate from the DIIR and is listed as an accredited assessor in the DIIR registry.

Individuals possessing a QA certificate from the IIA can be registered with DIIR by presentation of this certificate and successful completion of the DIIR QA Seminar.

Participation in at least one of the annual information exchange sessions offered by the DIIR is required to maintain the listing with the DIIR.

C Evaluation Process

The evaluation of quality criteria is based on a 0–3 scale as follows:

- 3 = satisfactory/all requirements fulfilled
- 2 = room for improvement
- 1 = significant improvement needed
- 0 = unsatisfactory
- n.a. = not applicable

Rating Approach

- The respective rating for the quality criteria is entered into the rating column.
- The points are added and consolidated for the respective observation area (the eleven observation areas correspond to the eleven points highlighted in the table of contents). The rating for each observation area is determined by the percentage of target achievement for a particular area.

Target Achievement	Points	Rating
> 90 %	28–30	satisfactory/ all requirements fulfilled
75 % – 90 %	23–27	room for improvement
50 % – < 75 %	15–22	significant improvement needed
< 50 %	< 15	unsatisfactory

Example: For the observation area **Organization, Position within the Company and Responsibilities**, a maximum of 30 points is possible (= 10 questions with a maximum of 3 points each). The rating is based on the following scale according to the total number of points achieved.

D Quality Criteria

The quality criteria represent specific characteristics of the requirements for an efficient and effective internal audit function. Furthermore, they serve as the basis for assessments of internal audit departments, both self assessments by department management and assessments by third parties, whether by internal sources or by external quality control bodies. All of the following quality criteria are valid for audit activities and, where applicable, for consulting activities.

In evaluating the effectiveness of internal audit, the adherence to certain minimum standards is considered essential. Thus, the non-adherence to any one of the defined criteria results principally in a rating of "unsatisfactory".

If a certain criterion is not in place at the time of the audit but will be implemented within a reasonable timeframe determined in advance by the assessor, it should be taken into account in the overall assessment and evidence should be shown to the assessor after the established timeframe has elapsed. If the evidence of implementation is not provided, then the assessor should report this to the review initiator as "unsatisfactory".

The minimum standards are:

1. An official written "charter" exists (see I.1).
2. Impartiality, independence from other functions, as well as the unrestricted ability to conduct audits and consulting projects are ensured (see I.5).
3. The audit plan is created based on a risk-oriented and standardized planning process (see III.13).
4. Type and scope of audit activities and results are documented consistently, appropriately and properly (see V.37).
5. The implementation of measures documented in the report is effectively monitored by internal audit using an established follow-up process (see VIII.61).

BASICS**I. Organization, Position within the Company and Responsibilities**

- | | |
|---|--|
| 1. An official written charter exists (see Glossary). | |
| 2. The charter was approved by executive management (see Glossary) and communicated within the company. The timeliness and appropriateness of the charter is evaluated on a regular basis. | |
| 3. The key tasks of internal audit are the evaluation of the appropriateness and effectiveness of internal control systems, the effectiveness of the risk management system, as well as the evaluation of the effectiveness of measures to prevent and detect fraudulent actions. | |
| 4. Internal audit covers all activities of the company. | |
| 5. Impartiality, independence from other functions, as well as the unrestricted ability to conduct audits and consulting projects are ensured. | |
| 6. Internal audit staff hold no operational responsibilities and do not audit any activities where they are biased. | |
| 7. The internal audit department is included in the distribution lists for relevant company information. | |
| 8. Internal audit has an audit manual containing information on the following subjects: Guidelines for program planning, audit preparation, audit execution, post audit work, reporting, documentation and archiving of audit results, and methods. | |
| 9. Internal audit staff is familiar with (and/or have been made aware of) the contents of the audit manual. Adherence to the manual is monitored continuously. | |
| 10. The audit manual is regularly reviewed with respect to timeliness and appropriateness. | |

II. Budget

11. The budget for labour costs is adequately determined to meet internal audit's requirements and tasks.

12. The material costs budget (e.g. IT equipment, travel expenses, training costs) adequately reflects the work requirements.

III. Planning

13. The audit plan is created based on a risk-oriented and standardized planning process.

14. The audits of a particular planning period are systematically compiled at least on an annual basis and presented to executive management for approval.

15. Legal requirements, special requests by executive management and suggestions from internal audit and other areas are included in the planning process.

16. Potential risks of audit objects are analyzed systematically based on a consistent method.

17. All audit objects (Audit Universe) are taken into account within the planning process.

18. The scope and rating of audit objects are reviewed on a regular basis (at least once a year) to ensure that they are complete and up-to-date.

19. Authorities for modifying risk evaluation methods or audit objects are defined.

20. The resources for necessary unplanned audits occurring on short notice are adequately included in capacity planning.

Rating/Comments

21. Subsequent changes to the audit plan, such as the cancellation or addition of audits, are comprehensible and communicated adequately to the responsible members of executive management.

22. The IT tools utilized are reasonable and appropriate.

AUDIT PROCESS

IV. Preparation

23. Based on the audit plan, the timeframe and the sequence of the audit objects are developed and resources and responsibilities are assigned.

24. The audit object is analyzed. Information is obtained and audit methods are defined.

25. Prior to the audit, milestones are defined and the estimated duration of the audit is determined.

26. The audit is generally announced to the organization/department being reviewed. Deviations from this practice are reasonable and appropriate (e.g. when auditing fraudulent actions).

27. A kick-off meeting with the auditee is part of the audit preparation (also via phone or video conference).

28. The objectives of the audit are basically defined.

29. The work program is approved by the head of internal audit or an appointed responsible person.

30. The actual audit process corresponds to the audit process defined in the audit manual.

V. Execution

31. The audits are generally conducted according to the work program.

32. The implementation of legal regulations and internal corporate guidelines and policies are evaluated in the audits (compliance assured).

33. Aspects such as efficiency, profitability, corporate objectives, security, risk impact, and effectiveness of measures to prevent and detect fraudulent acts are audited as well.

34. Measures or recommendations are provided for negative audit findings.

35. Audit results are agreed between the auditee and the audit team, as appropriate.

36. The audit steps are reconciled continuously with the work program.

37. Type and scope of audit activities and results are documented consistently, appropriately and properly.

38. Attention is paid to a consistent rating of audit results (systematic approach for all audit types and objects).

39. Audit results are clearly derivable from the working papers and traceable by competent third parties within an appropriate time.

40. The methods and check lists utilized are systematic, up-to-date and appropriate.

	Rating/Comments
41. The IT tools utilized are reasonable and appropriate.	<input type="text"/>
42. A closing meeting is conducted with the audited department in a timely manner (as appropriate). Audit results are agreed upon and documented.	<input type="text"/>
43. Appropriate measures, including deadlines for implementation and clear responsibilities, are agreed upon in the closing meeting. Concordance and/or disagreement with audit findings are confirmed.	<input type="text"/>
44. If no closing meeting takes place, an alternative and reasonable approach for reconciling audit findings is chosen and documented.	<input type="text"/>

VI. Reporting

45. The report consists of an executive summary and a detailed report. Deviations from this structure are plausible and appropriate in individual cases.	<input type="text"/>
46. The reports include statements on: <ul style="list-style-type: none"> • Audit objectives and scope • Audit process • Audit object • Measures and recommendations with deadlines for implementation, responsibilities and, if so, ratings. 	<input type="text"/>
47. The report format is standardized.	<input type="text"/>
48. Preliminary audit findings, e.g. in the form of a draft report, are presented to the management of the audited organization/department in a timely manner prior to the closing meeting.	<input type="text"/>

	Rating/Comments
49. In the case of major dissensions, a statement from the auditee should be included in the report or, at a minimum, a reference should be made to the disagreement.	<input type="text"/>
50. Reporting and distribution of the audit report and the action plan should occur in a timely manner.	<input type="text"/>
51. The audit report is approved before final distribution.	<input type="text"/>
52. The distribution list is defined according to the general regulations.	<input type="text"/>
53. The head of internal audit determines access to and distribution of audit-related documents.	<input type="text"/>
54. An audit report or a memo is available for every completed audit.	<input type="text"/>
55. The IT tools utilized are reasonable and appropriate.	<input type="text"/>
56. The reports or the summary of reports (e.g. annual report) are provided to the executive management.	<input type="text"/>

VII. Post Audit Work

57. Feedback discussions/project reviews are conducted and documented by the head of internal audit, or an appointed individual, with the entire audit team (and if applicable with quality management) within reasonable time after completion of the audit. (These project assessments can be supplemented with customer surveys.)	<input type="text"/>
58. Based on feedback discussions, changes and adjustments to risk ratings, audit methods and processes and resource planning will be made as necessary.	<input type="text"/>

Rating/Comments

59. General interesting information obtained during an audit is made available to all (knowledge management).

60. Retention policies and periods for audit reports and working paper documents are adhered to.

VIII. Follow-up

61. The implementation of measures documented in the report is effectively monitored by internal audit using an established follow-up process.

62. Deadline postponements for the implementation of measures are justified and documented.

63. Executive management is informed if measures are not implemented and no acceptable reason for the lack of implementation exists.

64. Criteria should be defined to determine the condition on which and when (at the latest) a follow-up audit has to be performed.

STAFF

IX. Selection

65. A staff planning process suitable to the size of the internal audit department exists and takes into account such determining factors as average fluctuation, retirement, level of education, language skills, etc.

66. Job and task descriptions exist for internal audit staff.

67. Employee selection is based on profiles suitable for internal audit including professional, personal, verbal and foreign language skills as well as work experience. If certain qualifications necessary for carrying out the audit or consulting assignment are not available in the team, the expertise of third parties will be utilized.

68. The mixture of the internal audit staff regarding skills and professional experience warrants the fulfillment of the audit tasks.

X. Development / Training

69. Continuous professional and personal training of staff is assured by regular:

- internal measures (e.g. internal audit department training, other trainings offered within the company)
- external measures (e.g. attendance of professional trainings not offered within the company).

70. Further development of social and leadership skills is supported by defined measures.

71. The employee's objectives and target agreements should include training, e.g. advanced training for the CIA (Certified Internal Auditor) certificate.

72. Annual target agreements are established and performance discussions are conducted with each employee and take into account influencing factors such as audit assignments, analysis of strengths and weaknesses, level of potential, employee development goals and training measures.

73. Internal audit staff is responsible for ensuring that they keep their knowledge and qualifications up-to-date.

XI. Management of the Internal Audit Function

74. The head of internal audit possesses the qualifications necessary for that position.

75. Internal audit is highly accepted by executive management.

76. The head of internal audit has established quality standards, which are documented in the audit manual and which are used to conduct quality checks.

77. Internal audit utilizes a process to monitor and evaluate the overall effectiveness of quality assurance programs. These programs include continuous evaluation of internal audit assignments and periodic self assessments.

Rating/Comments

78. Internal audit activities, new developments and significant risks are reported periodically to executive management.

79. The head of internal audit ensures the implementation of principles defined in the audit manual among others via integrated quality management processes.

80. Laws and other legal regulations as well as IIA-/DIIR-Standards are adhered to. Deviations from these standards are adequately communicated.

81. The head of internal audit should meet regularly with the company's external auditor.

Attachment:

Glossary

Accreditation: Describes the DIIR admission procedure for assessors qualified to perform quality assessments.

Assessor: For the purpose of this guideline an assessor conducts quality assessments (Quality Assessor).

Audit Manual: Intended to summarize current information with respect to defined activities, structure and procedural and organizational guidelines/rules within the internal audit department (presentation for internal audit staff).

Audit Plan: Encompasses a number of audits occurring in a particular timeframe (e.g. Annual Audit Plan).

Certification: Certification is a process to prove compliance with specific standards. In general, a certificate is issued after certification (see Appendices 3 and 4).

Charter: The charter ("Rules & Regulations", "Audit Guideline" etc.) is an official written document defining the assignment, authority and responsibility of internal audit. The guideline must (a) define the position of internal audit within the company, (b) ensure access to records, staff members and assets necessary for the completion of audit and consulting assignments and (c) define the scope of internal audit activities. In comparison to the audit manual, the guideline is intended to characterize the role of internal audit in the company (external presentation).

Executive Management: "Executive Management" is synonymous with the board of management of a corporation (public or private) or limited liability company, the board of an association or administrative agency or the board of a club.

Follow-up: The process by which internal audit determines whether the measures implemented by management in response to the reported audit findings are adequate, effective and in due time.

On a regular basis: Generally understood as annually, e.g. the timeframe for updating the audit manual (see 1.10).

Quality Assessment: Audit term used to describe the review of an audit department's activities, methods of operation and established controls by an auditor. It is a matter of quality control by external assessors evaluating the quality and the adherence to required and broadly accepted standards.

Quality Management: Quality assurance and improvement program which encompasses all aspects of audit work and supports continuous monitoring of their effectiveness. The goal of quality management is to ensure that internal audit work is compliant with agreed objectives.

Risk Management System: A comprehensive system of rules/regulations covering all corporate activities that provides a systematic and permanent approach based on a defined risk strategy.

Risk-oriented Planning Process: Serves as the basis for audit program planning (one-year and/or multiple year planning) and is based on systematic analysis of all business processes and company divisions taking into account risks and opportunities.

Working papers: contain the information obtained during the audit, the analyses conducted and the resulting conclusions.

Work program: a document in which the process steps to be carried out during the audit are listed. The work program also contains the audit objectives.

Appendix 1

1.1 Confidentiality Statement

1. _____ commits to strict confidentiality of all information (verbal, written or other) received from _____ or associated companies according to § 15 Aktiengesetz in the context with this assignment (later summarized under the term "information"). This information will not be provided in full or in part to third parties.

Additionally, _____ ensures the protection of data according to data protection laws and by exercising due professional care.

_____ will use information exclusively for the intended purpose and not for his/her own or third party purposes. This obligation exists already before signing the contract and persists unchanged after the contract is finished.

2. The confidentiality agreement does not include information for which _____ can prove that:

- It was already known at the time this statement was established,
- It was obtained from a third party, who obtained the information legally and is authorized to share it, prior to or after completion of this agreement,
- At the time the information was obtained it was generally available or state of the art and its availability was not caused by _____,
- Disclosure of the information is a result of a legal or judicial obligation or
- It was officially excluded from this agreement in written form by _____.

3. The same confidentiality commitment applies to the commissioning area and to the contractor with respect to all confidential information and documents received as part of the cooperation with the contractor.

Agreement _____:

Location, Date

Signature

Appendix 1

1.2 Privacy Statement According to Paragraph 5 of the German Federal Data Protection Act

Dear Mr./Mrs.,

Due to your assignment in conjunction with the Quality Assurance Review of _____ conducted by the audit team from _____, the above requirements with respect to data confidentiality apply to you.

According to paragraph 5 of the German Federal Data Protection Act, you are obliged to ensure data confidentiality. Unauthorized collection, storage, or use of data relating to individuals and accessible to you during your assignment is prohibited.

By signing you confirm that you have read this agreement and fully understand your obligations to ensure data confidentiality and privacy.

Location, Date

Signature

Appendix 2

Management Representation Letter

Company: _____

Audit Department Manager _____

Quality Assurance Review for the business year _____

In context with the Quality Assurance Review conducted by the audit team from

_____, I, as the head of internal audit at

_____, declare the following

A. Explanations and Supporting Documentation

I have provided the explanations and supporting documents requested completely and to the best of my knowledge.

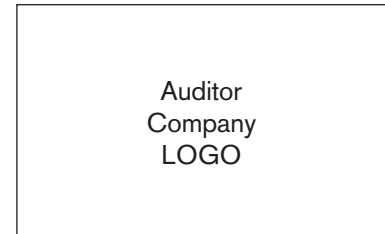
B. Additions and Comments

Location, Date

Signature

Appendix 3

QA Certificate for Certified Companies – Sample



This certificate signifies that the internal audit department of

«Company Name»

fulfills the audit standard Number 3 “Quality Management in Internal Audit” as recommended
by DIIR – Deutsches Institut für Interne Revision e.V.

This quality assessment was conducted from
<<Start Date>> through <<End Date>>

The certification is valid for <<x>> years after signing.

Quality Assessor

Appendix 4

QA Certificate for Certified Assessors – Example



This certificate signifies that

«Name»

has successfully completed the training course “Quality Assessment”
provided to the Assessor/Validator on «course_date»
necessary to achieve

Accreditation in Quality Assessment/Validation

As established by The Institute of Internal Auditors

Tutor

DIIR

**Deutsches Institut für
Interne Revision e.V.**

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 713769-0
Fax (069) 713769-69
www.diir.de
info@diir.de