DIIR Audit Standard No. 4

Auditing Projects by Internal Audit

First published in August 2008 and
extensively revised in September 2019
(Version 3.0)

DIIR
Deutsches Institut für
Interne Revision e.V.

Contents

1 Preamble

1 Projects are of great importance as a strategic success factor for the future sustainability of companies. Changes in globally aligned markets and shorter technology lifecycles must be appropriately addressed in a timely manner through adjustments to business processes, organization, and IT systems within the company. The rapid or agile introduction of an innovative process or system may become a decisive competitive advantage in the market.

2 Often, project results do not meet planning and stakeholder expectations. Many projects miss their goals, in many cases due to a low degree of project management maturity, unrealistic assumptions in the business case or insufficient technical requirements.

3 The resulting risks require internal audit to take projects into scope. This standard is intended to provide an overview of possible procedures for internal audit when considering projects.

4 In addition, the standard addresses the interlinking of project topics with aspects of the audit process. Due to the generic consideration of the project control instruments, the standard can be adopted for projects using classical methods, e.g. the waterfall model, as well as for agile projects.

2 Addressees, Scope and Binding Nature of the Standard

5 This standard is primarily aimed at both management and employees of internal audit departments. In addition, it supports boards in fulfilling their due diligence and monitoring obligations through the defined requirements for auditing project management systems. The audit content set out provides other project stakeholders in the organization with an overview of requirements for an adequate and effective project management system.

6 This standard is detailed by audit guidance, e.g. in the DIIR publication series.

7 An audit of the project management system requires basic knowledge of project management itself.

8 This audit standard was developed and approved by the DIIR - Deutsches Institut für Interne Revision e.V. through a careful procedure. It supplements the International Professional Practice Framework (IPPF) as a local guideline.[1] The use of this auditing standard is strongly recommended for internal auditors in Germany.

[1] DIIR/IIA (2019), "Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017" - Version 7.

3 Legal Basis

9 Cross-industry, there is no legal basis from which direct or indirect requirements for the audit can be derived on how projects, programs, portfolios or other components of project management systems are to be handled.

10 For certain industries, there are basic requirements that have to be taken into account and operationalized by individual internal audit departments. For example, there are “Mindestanforderungen an das Risikomanagement” (MaRisk) set by “Bundesanstalt für Finanzdienstleistungsaufsicht” (BaFin), which also formulate general requirements for audits and, in particular, for involvement in projects. Furthermore, there are guidelines that influence individual phases of project management, e.g. within the framework of publicly funded projects.

4 Definitions of Terms

11 This standard uses the following definitions. A variety of standards and other publications use these terms in a similar manner, however these can often be narrower or broader. Depending on the context, each organization must individually define which activities fall under the following definitions.

12 *Business Case*

The business case (business plan) is the key document for the justification and goal of a project. The goal should always follow the strategy set by the company or department (or the customer, if applicable) and the business case should also ensure that the investment and use of resources are economically sound.

13 *Project*

A project is an initiative which is generally characterised by the uniqueness of its overarching conditions, such as target, time-, financial-, personnel- and other constraints, differentiation from other projects and project-specific organization.[2] This involves a temporary organizational and operational structure, including a particular management environment, and the goal of fulfilling a specific business case (business plan).

14 *Program*

A program comprises several projects under uniform management that serve a common business case and which require higher-level control. In a program, the content and goals of the associated projects are developed, program wide decisions are made and the implementation of individual projects is controlled. A program is treated as a large project from an auditing point of view, taking into account special features such as interdependencies and synergies between projects. Therefore, the following chapters do not distinguish between programs and projects.

15 *Portfolio*

A portfolio is the entirety of all programs and/or projects in an organization, several organizations or a specific organizational unit. They have different business cases and are not under uniform management.

[2] DIN 69901 of the “Deutsches Institut für Normung e.V.“

16 *Project Management System*

A project management system is the organizational and operational structure defined by the management of the organization for implementing portfolio- and project management. This involves the coordination of the organizational units, procedures and processes in the creation, prioritization and implementation of projects.

17 In practice, the organizational structures defined above do not often exist in a pure sense. Occasionally, they are linked to line organizations. Regardless of the terminology used in the company, all structures in the organization that correspond to the project definition set out in this standard should be included in the audit analysis by the internal audit department.

5 Mandate of Internal Audit for Dealing with Projects

18 The cross-industry requirement to deal with project management in-house as an internal audit department is based on the International Standards of Internal Audit Professional Practice, including Planning Standard 2010: "[…] The chief audit executive must review and adjust the [audit] plan, as necessary, in response to changes in the organization’s business, risks, operations, programs, systems, and controls." Since such changes are often driven by projects, these should regularly be subject to audit activities.

6 Review of the Elements of a Project Management System

19 The review of the project management system can be illustrated in figure 1 with regard to the audit objectives, the audit areas and the scope of the audit:

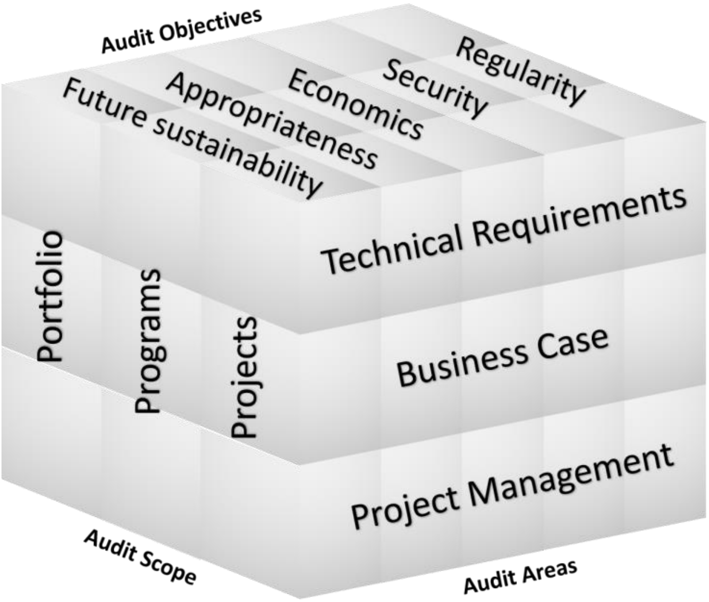

Fig. 1: Perspectives of the Project Review in the Project Cube

20 The contents of a project review can thus be determined from the three dimensions of the project cube by focusing on audit objective, audit scope and audit area, e.g.

a. Audit objective: Economics

b. Audit scope: Project A

c. Audit area: Business case

A combination of several audit objectives/scopes/areas is possible.

6.1 Audit Objectives

21 Essentially, audit objectives can be divided into regularity, security, economics and appropriateness (including future sustainability).

22 Projects can be reviewed for compliance with legal, regulatory, and corporate policies, as well as for effectiveness and efficiency. It is irrelevant which frameworks and methodologies (e.g. classic waterfall or agile scrum) are being used.

23 Regularity is the assurance of compliance with internal and external company requirements. Actual deviations from the requirements are determined here.

24 Security includes the adequacy of regulations and precautions to protect assets and data and, where applicable, internal and external security measures. The internal control system (ICS) is evaluated for appropriateness and effectiveness with regard to the level of protection to be achieved.

25 Economics means to ensure the efficiency of all operating and business processes, taking regulatory requirements into account.

26 Appropriateness is the suitability of the business processes, as well as the ICS with regard to their support in achieving the company's goals. This also includes future sustainability through the viable implementation of the company´s strategy.

27 The audit objectives for a project review should be adapted to the risks and contents of the respective audit areas.

6.2 Audit Areas

28 Project management, the business case as well as the technical requirements and their implementation can be the subject of a risk-based project review.

29 The audit should relate to the organization, framework conditions, targets, strategic objectives, plans, controls and project management processes as well as the results of the projects. The statutory regulations, internal company guidelines and specifications, as well as the best practice standards for the project

management frameworks, e.g. PMBOK[3], PRINCE2[4], or ICB[5], can be used as a benchmark for evaluation.

30 Projects follow a life cycle that can be divided into five project phases from an auditing perspective. The audit areas of a project contains additional areas, so-called audit fields. The audit areas and audit fields can be displayed as rows of a matrix and the project phases as columns. Within the respective audit fields, certain auditable objects (cells of the matrix) can be expected in the respective project phases. Altogether, audit areas, project phases and auditable objects form the matrix of the "Project Audit Universe". The structure of the "Project Audit Universe" is based on the project management processes of the PMBOK, but it has been modified for auditing purposes. An exemplary list of the audit fields in the form of the matrix above can be found in the appendix (see Appendix 12.1: Overview of the audit areas and audit fields in classical projects).

Recommendation

31 Due to the strong interdependencies of the auditable objects in the audit areas, it is advisable to carry out a complete evaluation of all project deliverables in an audit area that can be tested at this point in time in a project phase. However, exclusing auditable objects may be necessary or even mandatory due to certain circumstances. These circumstances may include, for example, experience from previous reviews, special features of the type and content of the project assignment or the size and complexity of the project.

32 Taking into account the specific characteristics and circumstances of the project under review and in order to make the best use of any limited resources, it is appropriate to focus the audit acitivites according to risk-based priorities, to review them on an ongoing basis and, where appropriate, to adjust them.

[3] Project Management Institute (2017): A guide to the project management body of knowledge (PMBOK guide) - 6. Edition.

[4] AXELOS (2018): Managing Successful Projects with PRINCE2® 2017 Edition, The Stationery Office Verlag.

[5] GPM (2017): Individual Competence Baseline for Project Management, Program Management, Portfolio Management - Version 4.0, GPM Deutsche Gesellschaft für Projektmanagement e.V., Nuremberg.

6.3 Review of Technical Requirements

33 The review of technical requirements involves the auditor's assessment of the technical specifications of the project and their implementation within the framework of the project work. Technical requirements include technical core requirements (e.g. IT requirements) and non-technical requirements.

Recommendation

34 A review of the technical requirements determines whether the specification of the technical requirements and their subsequent implementation is appropriate with regard to the approved business case and whether it meets the legal, regulatory or company-specific requirements. The subject of the review of the technical requirements therefore constitutes the intermediate and final results of the technical project work, taking the respective project phase into account.

35 Often, an assessment of the achievement of targets at the end of a project takes place too late, as counter-control measures are hardly or no longer possible at this point. Inconsistent or poorly practiced project management increases the risk of project failure.

6.4 Assessment of the Business Case

36 The business case assessment is the investigation of the processes for creating the business case of a project or the assessment of the business case itself.

Recommendation

37 The assessment of the business case should include whether the justification and objectives of the project are based on appropriate analysis processes and calculations, as well as on sufficiently well-founded assumptions.

38 The design of an assessment of the business case should be defined in connection with the project-specific mandate of Internal Audit in order to avoid a conflict of independence or an overlap with other divisions or third parties.

39 The business case's audit may include its creation, review and approval, as well as the actual documentation of the case itself, and, if necessary, its update and use. The audit fields and auditable objects of the Business Case assessment are shown in Appendix 12.1.

40 In the event of changes (e.g. to assumptions) in the business case, there are dependencies on adjacent processes. It should be reviewed whether the associated value-added analyses or profitability analyses are updated during the course of the project so that adjacent activities can be carried out in a consistent manner, e.g. set of project priorities based on resource bottlenecks.

6.5 Review of Project Management

6.5.1 Classic Project Management Models

41 In course of the project management review the organization, processes and products of project and portfolio management will be audited.

Recommendation

42 Project management is reviewed to determine whether project or portfolio management is suitable for controlling project activities in such a way that the project goals can be achieved in terms of time, budget and quality. In the event of a vulnerability, appropriate recommendations for improvement should be made.

43 Furthermore, the organization, plans, specifications, controls and operational measures of project management or portfolio management units are reviewed with regard to their effectiveness and efficiency, as well as their regularity in the effectiveness of defined controls.

44 All project management reviews should be based on a uniform "Project Audit Universe" in matrix form (see Appendix 12.1 or 12.2). If you use another Project Audit Universe, for example due to the consideration of company specifications or the application of a uniform project management standard in the company in accordance with another, recognized project management framework (e.g. PRINCE2, ICB or PMBOK), it is also recommended to use an audit universe in matrix form.

45 The following audit fields may be considered in connection with the review of project management:

46 **Project Organization:** In order to ensure successful project work, a cross-cutting process and organizational framework must be defined. All stakeholder groups (project management, project team, stakeholders, project contractor, etc.) must be taken into account.

47 **Integration Management:** The aim of integration management is to ensure the adequate and holistic coordination of all project activities, including the involved parties.

48 **Content and Scope Management:** The objective of content and scope management is to operationalize the approved project order in the form of detailed planning and to define the output/project products based on the business case or preliminary study. Based on this, a comprehensible change management system must be implemented.

49 **Schedule Management:** The aim of schedule management is to determine the completion dates for the output/project products. The completion dates are communicated and monitored. Appropriate escalation processes should be implemented in the event of missed deadlines.

50 **Cost Management:** The aim of cost management is to estimate the project costs completely, realistically and comprehensibly and to monitor their development throughout the course of the project.

51 **Quality and Test Management**: The aim of quality management is to define and monitor quality criteria for the output/project products.
The goal of test management is to define and monitor all measures of the test activities. These include the method, the organization, the planning, the execution and documentation of the test.

52 **Resource Management:** The goal of resource management is to plan and provide the necessary human resources and other physical resources (e.g. infrastructure, materials).

53 **Communications Management:** The aim of communication management is to control the communication channels within a project and to the outside world.

54 **Project Reporting:** The aim of project reporting is to provide recipient-oriented status reporting (e.g. a steering committee, stakeholder meeting) and to report regularly on the current state of the project. This enables targeted project decisions.

55 **Risk Management:** The aim of risk management is to identify, evaluate and mitigate all risk factors that endanger the achievement of the project objectives throughout the course of the project.

56 **Procurement Management:** The aim of procurement management is to control all procurement processes in the project (e.g. procurement of work materials, external employees and external services).

57 **Stakeholder Management:** The objective of stakeholder management is to identify and analyze all persons (internal and external), groups or organizations

that influence the project and to involve their needs appropriately and efficiently in project planning and execution.

58 The project life cycle, i.e. the status of the project in the project phase in which the audit takes place, should be taken into account appropriately in each audit. Since the project is constantly evolving, there are recurring but also additional review elements (cumulative review approach) as the project progresses.

59 Reporting on the audit results: The evaluation of the audit results must always take into account the respective project phase.

60 The selection of the audit fields for a specific audit should be risk-oriented.

6.5.2 Agile Process Models

61 The importance of agile methods is steadily increasing, especially in software development projects. As a result, in the future auditors will encounter more agile methods in projects. The following special features arise in comparison to classic project reviews.

Agile Management of Projects

62 The agile management of projects is carried out with special roles, techniques, artifacts, etc., which represent potentially auditable objects during an review. On the basis of the audit´s mandate, the auditor should identify appropriate audit items and perform appropriate audit procedures. An example of the identification of Scrum audit objects[6] using the Project Audit Universe according to this standard is shown in Appendix 12.2.

The Soft Factors

63 Experience from many agile projects shows that it is not important to be dogmatic about the wording of values and principles (in the sense of agile) but rather it is about finding a new orientation and mindset regarding the organization, management and execution of the work as a whole. With regards to agility, the situational dimension and self-responsibility are emphasized much more strongly than the formal follow-up of methodological elements.[7]

[6] As an example of an agile process model.

[7] The Agile Manifesto of Kent Beck et al. from 2001 (http://www.agilemanifesto.org/). The Agile Manifesto describes in its original version 4 values and 12 principles derived from them that describe the "new type" of agile software development.

64 For the audit, this means that the auditor has understood the agile values and incorporates this view into the auditing procedures. The benefits of using agile methods must be questioned if agile values are not embedded in the project or in the project environment (client, management, etc.).

Integrating agile Methodologies into the Enterprise

65 Even with agile projects, not all project or project management risks can be solved in the project alone. Existing or lacking company-wide requirements for the use of tools, processes and methods influence company projects.

66 Therefore, the audit procedures must also be related to the project environment. As part of this, you can review whether

- the interfaces to other projects and the line organization,
- the specifications or defined processes,
- the templates, IT support and other tools

are suitable to adequately support the success of the project. From a sufficient spread of agile methods in the company, company-wide, uniform guidelines are required to ensure compatibility between agile projects and to achieve synergies by avoiding a duplication of efforts. The auditor can be the driving force here in order to achieve a structured introduction of agile methods, including anchoring in the internal company guidelines. Documented internal guidelines and uniform tools and processes for agile methods not only help to meet auditing requirements but also to support the quality and success of agile projects.

Summary for Reviewing Agile Process Models

67 Thus, it can be concluded that an auditor should have gained an understanding of agile project management, agile values and the integration of agile procedures in the company before reviewing an agile project. The auditor should not apply the standards of classical project management to the audit but should take into account the opportunities and ideas of agile methods. This also applies to the Project Audit Universe for agile projects, which may include other audit objects, such as possible audit areas and fields (see Appendix 12.2).

6.6 Audit Objects

68 Any element of a project management system can be an audit object. From an auditing point of view, the review of the audit objects portfolio, program and project can be distinguished in descending order, as shown in Figure 2.

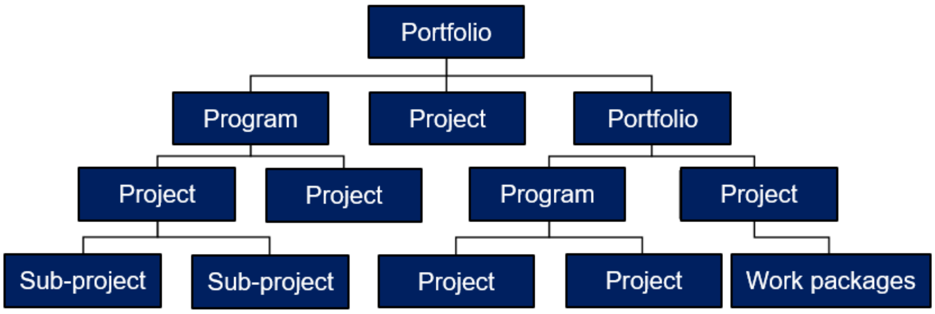

Fig. 2: Possible Audit Objects in the Project Management System

69 In the following, suggestions are given for the review of portfolios and on projects and programs in consolidated form, as already explained in the definitions of terms (see Chapter 4).

6.6.1 Review of Portfolios

70 Portfolio management involves management/controlling of portfolios, as well as the alignment, planning and management of programs/projects that are geared towards a company's strategic objectives and operational needs. Portfolio management is less concerned with the management of individual programs/projects but more with the management between programs/projects and with the organizational structure necessary to do so. The following processes are the subject of portfolio management reviews:

- Process definition and governance
- Strategy compliance
- Benefit forecasts
- Prioritization/Assessment
- Portfolio optimization
- Portfolio analysis (scoring model)
- Capacity analysis
- Portfolio reporting
- Benefit realization
- Risk management

Recommendation

71 From an audit perspective, it is advisable to assess portfolio management based on the respective organizations, as well as procedures for generation, priorization or methodological support for the successful implementation of several programs or projects in a company or an independently managed business division.

6.6.2 Review of Programs (or Projects)

72 Since a series of similar or coherent projects or a project of large size, long duration and high complexity can be divided into individual projects with a limited content, programs and projects have many similarities from an auditing point of view. It is therefore advisable to combine these into a higher-level organizational system, a program. The similarities can be shown on the basis of the following (common) objects for programs / projects, which accordingly enable similar audit approaches:

- (Program/project) steering committee
- (Program/project) management
- (Program/project) office

73 In addition, further organizational levels, such as program management or the establishment of a program company, which will be dissolved after the business objective has been reached, may also be present in programs. A transformation manager who accompanies major changes that are brought about by programs can also be present as a regular instance for larger projects.

Recommendation

74 Due to the many overlaps between programs/projects, it is advisable to review the levels of consideration of the program integration in a vertical perspective (cooperation of the program with the individual projects) and in a horizontal perspective (cooperation/integration of the projects with one another) in a risk-related manner.

75 The auditor’s approach to the management of required specifications and controls necessary for a functional process-based interaction of the audit objects portfolio, program and project should be considered in the following chapter.

7 Review a Project Management Office

76 For a final assessment of all relevant project management risks, it is necessary to consider the underlying organizational framework. Such a framework is usually defined by a Project Management Office (PMO). This can be handled by different departments or, for example, by a central PMO. In the following, the term PMO is used, even though these tasks can be organized decentrally in many organizations.

77 The tasks and skills of a PMO can include the following topics:

- Creation and further development of regulations and methods
- Control of compliance with corporate regulations
- Provision and administration of appropriate tools for project and portfolio management
- Coordination/preparation of committee meetings
- Coordination of portfolio planning
- Data quality management (specifications for project master data)
- Controlling the projects incl. analyses (e.g. milestone trend analyses, value contribution, management of project/portfolio budgets).

78 The need for audit procedures to ensure that the above-mentioned tasks are handled properly is determined by taking into account the three-lines-of-defense model (see Figure 3).

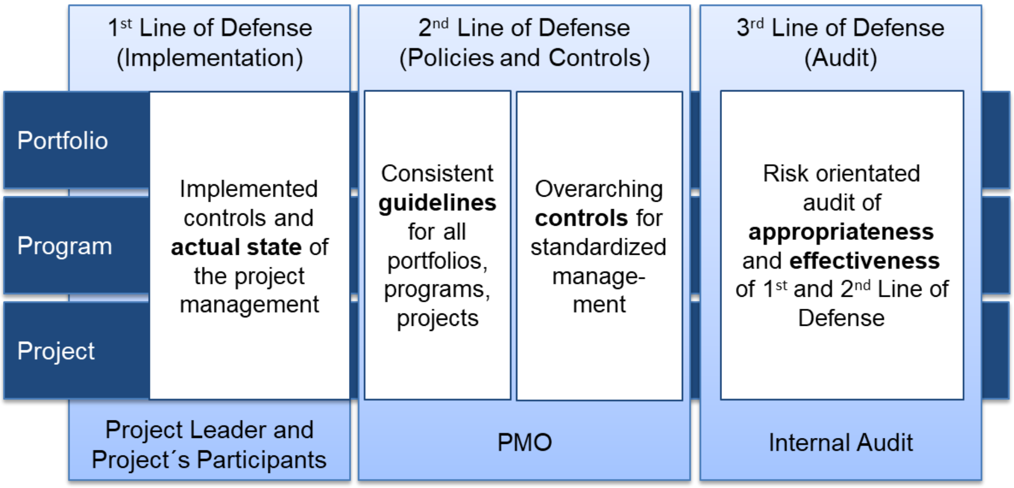
1st Line of Defense (Implementation)
2nd Line of Defense (Policies and Controls)
3rd Line of Defense (Audit)
Portfolio
Program
Project
Implemented controls and actual state of the project management
Consistent guidelines for all portfolios, programs, projects
Overarching controls for standardized manage-ment
Risk orientated audit of appropriateness and effectiveness of 1st and 2nd Line of Defense
Project Leader and Project´s Participants
PMO
Internal Audit

Figure 3: Three Lines of Defense in Project Management

79 The PMO is understood to be a function of the 2nd line within this model which performs important control functions.

Recommendation

80 A consistent application of the three-lines-of-defense model must be taken into account in the audit planning and it should be based on the requirements and control results of the second line.

8 Accompaniment of Projects

81 The trigger for the accompaniment of a project by internal audit may be a request from management or project management. It may also be due to a detection of special risks arising from project goals or activities through the assessment and the fulfillment of regulatory requirements[8].

82 These different triggers lead to different types of accompaniment - from reviewing project document, to reviewing project management and project content, to secondment of auditors in the projects. In practice, project accompaniment is often perceived as a mixture of project reviews, project advice and other audit activities, which only have in common that they are carried out alongside the course of the project.

83 However, for the purpose of this standard, the following more narrow interpretation of project accompaniment is recommended, which allows a distinction to be made between auditing and consulting:

84 The aim of the project accompaniment is to gain information in order to enable internal audit to act dynamically due to particular risk situations, especially if a non-functional ICS is suspected in the project. This dynamic action may be, for example, the triggering of ad hoc reviews or the consideration of project topics in follow-up planning. The distinction from a project review should take into account that a final assessment is not the aim of the accompaniment. The focus is on information acquisition. Even the suspicion of a possible vulnerability may be sufficient to trigger further activities. In contrast to the audit engagements, outputs from project accompaniment are often only used within internal audit and, if necessary, within the project.

85 Furthermore, the role of internal audit within the scope of project accompaniment must be clarified and documented appropriately. This includes maintaining independence. This means that internal audit makes its technical and substantive contribution to the project but the representative of internal audit in the project does not have decision-making authority in the project.

[8] The MaRisk require in BT 2.1 Tz. 2 the accompaniment of essential projects.

86 The formal framework applicable to audits should also apply to accompaniment in an adapted form. This may mean, for example, the use of accompanying engagements (including audit objectives, scope, etc.) and accompaniment announcements.

Forms of project support

87 Depending on the accompanying engagement, the accompanying auditor can obtain information in different intensities .Possible forms of project accompaniments are shown in Figure 4.

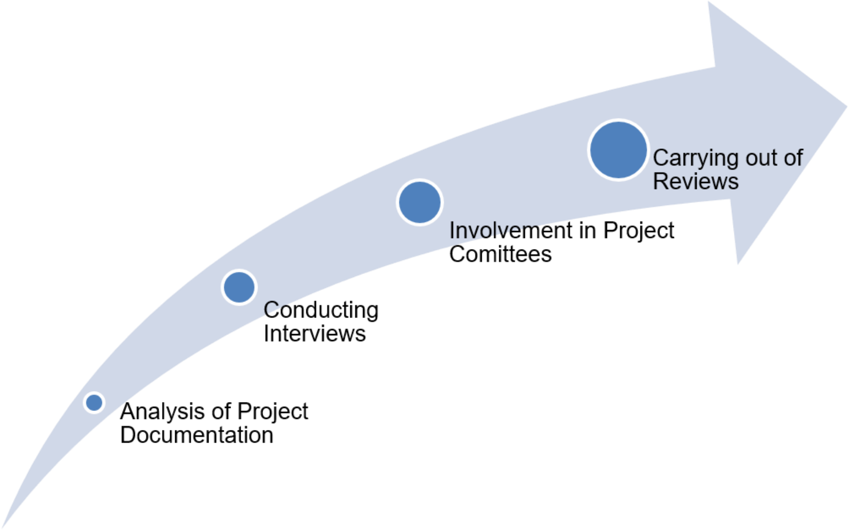
Carrying out of Reviews
Involvement in Project Comittees
Conducting Interviews
Analysis of Project Documentation

Fig. 4: Forms of Project Accompaniments

88 The evaluation of the project documents (project order, risk overviews, project reporting etc.) is one of the central activities of internal audit within the framework of project accompaniment. Ideally, internal audit has read access to electronically created project documentation ("project drive").

89 The interview is a valuable tool to answer questions from the evaluation of the project documents or to clarify further questions.

90 Another possibility for accompaniment is the participation of internal audit in meetings of project committees (e.g. steering committees, stakeholder meetings). When attending a project meeting for the first time, the internal audit employee must ensure that the other participants understand his role not entitled to vote.

91 The analysis of individual project management processes within the scope of internal audit reviews can also be useful in project accompaniment. An internal audit review can provide a good basis for further involvement, especially at the

beginning of accompaniment and, in particular, on the subjects of risk management, quality and test management and project reporting.

Reporting

92 Reporting should generally be adapted to the role of internal audit in project accompaniment. It has proven useful to provide internal audit management with (short) interim reports on the scope and results of the activities as soon as the audit engagment has been carried out. However, other forms of reporting are also possible, for example with the involvement of project management.

9 Consulting Services for Projects

96 In line with the international standards for the professional practice of internal auditing, consulting services for projects can be provided at the explicit request of a customer.

97 As part of these advisory services, the internal auditor must maintain his objectivity and therefore must not assume any decision-making or management responsibility.[9]

[9] DIIR/IIA (2019), "Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017" - Version 7 - 1130.A3, p. 30.

10 Consideration of Projects in Audit Planning

10.1 Consideration of Projects in the annual Audit Planning of Internal Audit

98 The annual audit planning of internal audit also affects a company's project portfolio. The aim is to schedule the reviews of the project portfolio in terms of time, subject matter and personnel.

99 At the time of the annual audit planning, there is often no detailed project information for projects to be started available. In this case, detailed risk-oriented annual or multi-annual planning of the audit of individual projects is not possible due to the insufficient data basis. In this instance, a capacity buffer for the review of projects can be determined and taken into account as part of the annual audit planning.

100 A generalized determination of the effort for the review of projects can be made on the basis of general portfolio information (e.g. portfolio budget, number of projects, number of person-days). A multi-year analysis also allows information on the development of the portfolio and the development of the capacity buffer for the review of projects to be taken into account .

101 If internal audit has an organizational unit responsible for the reviewi of projects, the corresponding personnel capacity can also be an influencing factor for determining the capacity buffer.

102 If it can be seen in the course of the preparation of the annual audit planning that the personnel capacities of the internal audit function, intended for the audit of projects is not sufficient, this should be taken into account in the personnel planning and, if necessary, the commissioning of external service providers for project reviews should be considered.

103 Project reviews usually require expertise in different disciplines. It may therefore be useful to have a project review carried out by audit teams with different audit competencies. If the required audit skills are not available at the time of the audit, this must be taken into account in the context of personnel planning and, if necessary, the commissioning of external service providers for project reviews should be considered.

10.2 Risk-oriented Selection of Projects to be audited or accompanied

104 The internal audit should deal with the individual project at the latest with approval of the project start or when all the information required for this is available. For reasons of traceability, it is advisable to record projects in the internal audit’s audit universe.

105 It is recommended to identify the projects that are of particular importance to the company from a risk perspective. For this purpose, internal audit should document and establish a risk assessment methodology.

106 The risk assessment methodology should be company and industry specific. In the event that there is the need to deviate from the result of the risk assessment in justified individual cases, this should be decided and documented by the management of internal audit.

107 The following questions can be taken into account in the context of a risk assessment methodology:

- Is the project implementing content that is triggered by internal or external guidelines?
- Should the projects enable the achievement of financial and corporate policy objectives? Are the measures to be implemented in the project in line with the corporate strategy?
- Will the project implement content that is likely to be subject to third-party audit engagements?
- Does the project have an external impact?
- What is the complexity of the project´s structure and object?
    - Number of stakeholders who influence or actively involved in the project (including commissioning organizational units, service providers, customers),
    - Number and complexity of affected IT systems and
    - Organization of the project in subprojects.
- What interdependencies must be observed?
    - Availability and dependency of internal and external employees (especially know-how carriers),
    - Delivery of results from other projects, interdependencies between projects and binding deadlines.

108 The risk assessment for a project should be completed upon starting the project and updated as t the need arises. A risk assessment should be possible based on the information described in the project documentation. If necessary, this can be repeated at a frequency to be defined.

109 The regular validation of the risk assessment methodology ensures the effectiveness and efficiency of the auditing process.

11 Projects in the Reporting of Internal Audit

110 The reporting of internal audit in relation to projects corresponds to the reporting on other audit activities of internal audit. This includes

- Audit report
- Quarterly report
- Annual report

111 Responsibilities and escalation instances may differ from the line organization with regard to projects. Internal audit must take this into account when selecting the addressees.

112 The reporting of the results of project reviews or reviews of the project management system is usually in the same format as standard audit engagements. Different formats are, however, possible.

113 If project reviews are carried out, the results should be communicated to those, responsible for the project. Reporting to other bodies should be considered, taking into account the materiality of the findings.

114 Any anomalies or risks identified in the context of project accompaniment should be communicated to the project managers in a timely manner. In the case of material findings, reporting to other bodies should also be considered. In addition, regular reporting of the results of the project accompaniment may take place. In the financial industry in particular, it may still be useful to prepare interim reports for long-term project accompaniment (e.g. audit activities going beyond the turn of the year) so as not to jeopardize the timeliness required by MaRisk.

115 Audit practice shows that in the case of project audits, findings may not be under control of a project and therefore responsibility lies outside the project.

116 Internal audit’s activities relating to projects are to be presented in the annual and quarterly reports.

117 In all reporting formats, it must be ensured that, analogously to other audit activities by internal audit, working papers are documented to an appropriate extent and in a comprehensible manner to prove one's own findings or observations.

12 Appendix

12.1 Overview of the Audit Areas and Audit Fields in classical Projects

The following audit areas and audit fields can be examined when considering projects over the different project phases.

Project Phases **Audit Areas/-Fields**	Project Phase I Initialization	Project Phase II Planning	Project Phase III Implementation	Project Phase IV Closure	Project Phase V Review
I. Audit Area: Project Management					
1. Project Organization	Project contractor, environment analysis with regard to acting parties	Plan, project organization, project manager Governance	Project organization, project roles	Project organization, project roles	Resolution of project organization
2. Integration Management	Project mandate, Preliminary project assignment, Open items list	Project Plan, Project structure, Project management plan, edited Open items list	Project management meetings, steering committee meetings, documented decisions, open items management	Handover of open items to line organization	Ideas for follow-up projects
3. Content and Scope Management		Change management plan, change request form	Change requests, updated project plan	Handover of project results to line organization	
4. Schedule Management		Milestone plan, activity and sequence planning, resources and work packages, critical path	Scheduling, measures to fulfil milestone plans, updated milestone plans		
5. Cost Management		Cost plan	Cost/benefit comparison (target/actual, forecast)	Final presentation	Cost/benefit-reviewed calculation, deviation analyses

Project Phases **Audit Areas/-Fields**	Project Phase I Initialization	Project Phase II Planning	Project Phase III Implementation	Project Phase IV Closure	Project Phase V Review
6. Quality and Test Management	Definition/designation of quality requirements	Quality plan	Quality inspection reports, releases, ongoing lessons learned analyses	Quality inspection reports, releases	Lessons learned
7. Resource Management	Skill definitions	Personnel requirements plan, project team list	Recruiting, -controlling, internal/external employee list	Resolution of project team	
8. Communications Management		Meeting list, communication plan, project documentation	Project management meetings, protocols, workshops, project results documentation	Knowledge transfer (transition to line organization)	Lessons learned
9. Project Reporting		Templates for reports, KPIs of the project	Project progress reports	Final report	
10. Risk Management	Initial risk list (incl. evaluation)	Risk Management Plan, Risk List Update, Setup Issues Management	Risk measures, updated risk list, issues management		
11. Procurement Management	Initial purchase requisitions	Purchase plan, Quotes	Contracts, statements, contract fulfillment	Closing invoices	
12. Stakeholder Management	Initial stakeholder overview	Stakeholder overview, -analysis, stakeholder action plan	Stakeholder actions, updated stakeholder portfolio		

Project Phases **Audit Areas/-Fields**	Project Phase I Initialization	Project Phase II Planning	Project Phase III Implementation	Project Phase IV Closure	Project Phase V Review
II. Audit Area: Business Case					
Business Case	Strategic factors and organization of the project in the context of the company Project objectives, benefits and -scope (Possible) Project sponsor Assessment of feasibility including project restrictions and assumptions Value analyses	Business case, calculations, e.g. Cost comparison calculation, profit comparison calculation (break-even analysis), profitability calculation (ROI), amortization calculation, capital value method, internal interest base method Market analyses and benchmarks Possible schedule and potential bottlenecks Indicator approvals, budget releases	Additions to the business case Changes in assumptions	Review of benefit collection	
III. Audit Area: Technical Requirements					
Technical Requirements	Definition of scope	Results of the project teams, e.g. actual analyses, plans, drafts	Output from the project teams such as specialist-/rough-/IT concepts, prototypes, test plans/-concepts, roll-out plans, test cases	Final outputs from the project teams	Outputs from the project teams after transition to line organization

The matrix only shows a minimum breakdown. Further subdivisions as well as other subjects of assessment are conceivable. In particular, the specific determination of the subject matter of the audit depends on the individual project content and course as well as on the respective individual assessment. Note that the audit fields are not free from overlaps.

12.2 Overview of the Audit Areas and Audit Fields in agile Projects

The audit subjects in classical project management cannot be transferred directly to agile methods. For this reason, the following table provides an overview of the "Scrum audit objects" as an example for agile methods for the audit fields defined in the DIIR audit standard – audit of projects.

Audit Areas and Project Phases (Team Level)	Project Phase I Finding	Project Phase II Planning	Project Phase III Implementation	Project Phase IV Conclusion
I. Project Management Audit Area				
Project Organization	Product Owner, Scrum Master	Product Owner, Development Team (7+-2), Scrum Master, Collocation	Product Owner, Development Team (7+-2), Scrum Master, Collocation	Product Owner, Development Team (7+-2), Scrum Master
Integration Management	Product Vision	Product Backlog	Product Backlog, Sprint Backlog, Product Backlog Refinement (Grooming), Impediment Backlog	Product Backlog
Content and Scope Management	Product Vision	(Ordered) Product Backlog, Product Backlog Refinement (Grooming)	Product Backlog, Sprint Backlog, Product Backlog Refinement (Grooming)	
Time Management	Defined Sprint Length/Sprint Calendars	Release Planning, Task Breakdown, Planning Poker	Sprint Burndown, Release Burndown	
Project Reporting	Initial Product Backlog Workshop, Product Vision	Sprint Planning (1+2), Product Backlog Refinement	Sprint Burndown, Release Burndown, Sprint Review	Sprint Review, Sprint Retrospective
Risk Management		Internal Risks are handled via Daily Scrums, ordered Product Backlog, Definition of Ready (DoR)	Internal Risks are handled via Daily Scrums, ordered Product Backlog, Definition of Ready (DoR), Impediment Backlog	Sprint Review, Sprint Retrospective

12.3 List of Figures

13 Authors

Developed by the DIIR working group Project Audit

DIIR – Deutsches Institut für Interne Revision e.V. Theodor-Heuss-Allee 108

60486 Frankfurt am Main

Published September 2019 on www.diir.de

Version: 3.0

(Translation into English published May 2020 on www.diir.de)