The Role(s) of the Auditor in Projects: Proactive Project Auditing
Sam C.J. Huibers
Published online: 16 May 2013.

To cite this article: Sam C.J. Huibers (2013): The Role(s) of the Auditor in Projects: Proactive Project Auditing, EDPACS: The EDP Audit, Control, and Security Newsletter, 47:5, 1-14
To link to this article: http://dx.doi.org/10.1080/07366981.2013.786940

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
THE ROLE(S) OF THE AUDITOR IN PROJECTS: PROACTIVE PROJECT AUDITING

SAM C.J. HUIBERS

Abstract. In the era of dynamically changing environments, globalization and increasing legislation companies need to re-visit their strategy on a continuous basis. Consequently this requires the redesign of the organization, processes, and systems, all of which are often executed through (large) projects. With increasing demands from management on the internal audit profession, the question is raised of how the auditor’s role can be redefined, as it shifts from the more traditional assurance role to being involved as a proactive partner in projects, without losing its independent position. Potentially the advisory and participative roles might conflict with the assurance role of the auditor. However, if for this reason the auditor’s role is restricted to the compliance aspect only, the added value of the auditor may be substantially reduced. This article is based on research aiming to provide a practical relevance to audit profession and industry. It describes the different types of roles that can be fulfilled by the auditor, taking into consideration the shift from the traditional assurance role toward more proactive roles in projects: advisory and participative roles without jeopardizing the auditor’s position.

ROLE(S) OF THE AUDITOR IN PROJECTS

In order to gain more insight into the potential roles that the auditor can play in projects I have divided these roles into three groups:

1. assurance roles,
2. consulting roles, and
3. participative roles.

Next, I have used a position paper from the Institute of Internal Auditors (2004, 2009) to categorize the different types of roles that the auditor can play in projects (see Figure 1):

- The core roles of internal audit: traditional assurance roles such as project reviews.
- Legitimate roles with safeguards: consulting and participative project roles that can be performed by the internal auditor if certain preconditions are met.
- Roles that should not be undertaken by internal audit such as the management of project-related risks.
An important remark to be made is that the roles I further describe in the next paragraph are generic and can be applied to the audit profession in general. In this article I have added additional examples that can be applicable to the daily practice of IT auditors who are involved in project audits.

**Assurance, Consulting, and Participative Roles in Projects**

I have summarized the roles that can be fulfilled by the auditor described in Figure 1 and Table 1. Note that this is not a restricted list but I have categorized the roles in groups in order to gain more
<table>
<thead>
<tr>
<th>Type of role</th>
<th>Project roles</th>
<th>Description</th>
<th>Example specific to the IT auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurance</td>
<td>Quality Assurance (QA)— Program/project reviews</td>
<td>4 levels</td>
<td>Give an opinion on the project design; the governance, management, the project process and milestones including the risks associated with the design and implementation of an application.</td>
</tr>
<tr>
<td></td>
<td>Quality Assurance— deliverables</td>
<td>Review focusing on the quality of the products (deliverables).</td>
<td>Review the authorization strategy and roles or assess the system design documents.</td>
</tr>
<tr>
<td></td>
<td>Post-implementation audit</td>
<td>Provide an opinion about the quality of the internal control system embedded in the operational processes.</td>
<td>Review the effectiveness of the authorizations half a year after go-live.</td>
</tr>
<tr>
<td>Consultative roles</td>
<td>Quality Assurance— advisor to program/project management</td>
<td>Advise the project management on project management and risk assessment methodology.</td>
<td>Advise how to structure the project and include milestones such as approval of the business blue print, translation into a technical design, development, testing and training.</td>
</tr>
<tr>
<td></td>
<td>Advisor (content)</td>
<td>Act in an advisory capacity in a narrow sense, answering questions and expressing particular views but no direct involvement in realization.</td>
<td>Advise on the design of a control framework to come to a good balance in application controls and procedures.</td>
</tr>
<tr>
<td></td>
<td>Sounding board—objective observer</td>
<td>Raise questions to reflect.</td>
<td>Sound boarding role and raise questions to reflect how change management aspects will be addressed. For instance, ask how relevant users will be involved early on in the project.</td>
</tr>
<tr>
<td></td>
<td>Coach/trainer</td>
<td>Advise in designing learning experiences or acts as coach.</td>
<td>Facilitate a project risk workshop or advise in the setup of a training program.</td>
</tr>
<tr>
<td>Participative roles</td>
<td>Proactive expert role</td>
<td>Own specific knowledge in the area of internal control systems and IT security and proactively participates in a project to define alternatives, provide recommendations and solutions.</td>
<td>Suggest alternative solutions to improve the system security and provide recommendations how to implement these.</td>
</tr>
<tr>
<td></td>
<td>Project/process coordinator</td>
<td>Coordinate project activities.</td>
<td>Coordinate the setup of so-called business control frameworks and provide templates in a business process redesign project.</td>
</tr>
<tr>
<td></td>
<td>Documentation controls</td>
<td>Support in documentation of controls.</td>
<td>Support in documentation of system and end user controls.</td>
</tr>
<tr>
<td></td>
<td>Proactive QA partner—facilitator role</td>
<td>QA partner that not only identifies risks but also translates them into real business issues and makes recommendations.</td>
<td>Identification of risks associated with the introduction of a new system and provide recommendations to improve the user acceptance.</td>
</tr>
</tbody>
</table>
insight into the potential roles that the auditor can play in projects: assurance, consulting and participative roles.

In the next paragraphs I would like to highlight some points that can be of relevance when considering the auditors’ role in a project: programs versus projects, the internal versus the external auditor and the role of the auditor during different phases of the project.

Programs

An individual project can be part of a larger program. The program is the “umbrella” under which individual projects have been grouped in order to contribute to an identical objective. The OGC² points out that the quality assurance and overall compliance of the program—focusing inwardly on the internal consistency of the program structure; and outwardly on its coherence with infrastructure, interfaces with other projects and corporate standards—is the primary responsibility of the program manager. The program manager will define the governance structure and make sure that appropriate assurance roles are appointed. It is the responsibility of the project manager to coordinate with the staff assigned to the assurance roles to ensure the overall integrity and coherent structure of the project.

Since quality assurance is relevant at both levels and the way projects are grouped and structured depends on the organization and situation, the roles I describe in this article are both applicable for programs and projects.

Role of internal and external auditors in projects

Various variables can be important when deciding if one or more external parties will be involved in a project such as experience, knowledge, independent position, and available resources.

However, the starting point is that an external auditor can fulfill the same role in projects as the internal auditor. The external auditor can be the public accountant of the organisation or a different third party accounting and advisory firm.

When different roles are assigned to various parties it is important to avoid overlapping roles and inefficiencies. The following considerations might, among others, be taken into consideration:

- Knowledge of the business: the internal auditor is assumed to know the organization better than the external auditor does.
- Share best practices: on the other hand, the external auditor can share best practices and experiences gained at projects with other customers.
- Knowledge of the system/process: the external auditor can give an opinion on the design of a system/process using experiences gained at other clients as a reference.
- Sponsor: the project manager can ask the internal auditor to facilitate a risk analysis. The (supervisory) Board could ask the external auditor to advise and provide recommendations.

The aforementioned examples can influence the decision when assigning roles in a project. Please note that in some cases the combination of the involvement of the internal and external auditor may also very well result into synergies.
The role of the auditor during the different phases of a project

The role of the auditor might differ per phase of the project. In the project literature, project phases are described with several levels of detail that can vary depending on the nature of the project. However, on a highly generic level, three levels can be distinguished as a common denominator to all projects:

- project preparation/start,
- project execution, and
- project close.

In Appendix 1, I have provided examples of how the role can differ per phase of the project. I have used the PRINCE2 project methodology as a reference. PRINCE (an abbreviation of Projects in Controlled Environments) was developed by the OGC in 1989 as the standard approach to IT projects. Over time the method has been enriched to become a generic, best practice project management framework covering a wide variety of disciplines and activities for all kinds of projects outside the IT and public sectors. Today PRINCE2 has been widely adopted by both public and private organizations as the de facto standard for project management and has a demonstrable track record.

**Safeguards (Preconditions) for Consulting and Participative Roles**

The assurance role is the traditional role of the auditor (core role). The consulting and participative roles are typically roles that can be fulfilled by the auditor but only when certain safeguards (i.e., preconditions) are put in place. The safeguards are preconditions necessary if the auditor is to extend his role beyond the traditional assurance role:

- It should be clear that management remains responsible for project risks and determining the risk appetite.
- The nature of internal audit’s responsibilities should be documented in the audit charter and approved by the Audit Committee.
- The auditor should not manage any of the project risks and mitigate those on behalf of the management.
- The auditor should provide advice and support to the management’s decision making, as opposed to taking management decisions themselves or implementing solutions on behalf of management.
- The auditor should avoid any impairment of independence and objectivity in fact or appearance. The auditor should not audit activities in which he or she has been involved in the previous year. Segregation of duties should be applied and/or tasks be transferred to other governance departments or outsourced.
- Any work beyond assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

The most important precondition, both for roles with safeguards and the roles that should not be undertaken, is that the auditor must refrain from any managerial accountability in all project areas, from initially setting the project risk appetite to the final embedding of deliverables in the standing organization.

"THE AUDITOR MUST REFRAIN FROM ANY MANAGERIAL ACCOUNTABILITY IN ALL PROJECT AREAS, FROM INITIALLY SETTING THE PROJECT RISK APPETITE TO THE FINAL EMBEDDING OF DELIVERABLES IN THE STANDING ORGANIZATION."
areas, from initially setting the project risk appetite to the final embedding of deliverables in the standing organization.

A final remark I would like to make here is that the exact boundaries of the extent to which the auditor can fulfill a consulting and participative role without risking any infringement of independence cannot always be carved in stone. Since the context, objectives, and tasks to be performed might differ from project to project there will always be an individual judgment to be made. As pointed out by Mautz and Sharaf in their book *The Philosophy of Auditing* first published in 1961, the responsibility of making a judgment in order to maintain independence in different situations must rest in the first place with the individual audit practitioner and he must constantly be aware of his professional responsibility in all kinds of situations.

**Role(s) Not to be Undertaken by the Auditor**

It is the primary responsibility of the project manager to manage project risks. The auditor can assist in making risks transparent but it is up to the business management to determine the risk appetite and define and implement mitigation actions. In addition, the embedding of project deliverables into the standing organization is a line management responsibility. If the auditor takes on these roles it has crossed the line and therefore cannot provide sufficient safeguards to ensure independence and objectivity (see Table 2).

**GUIDANCE AND CONDITIONS PROVIDED IN A FRAMEWORK**

I have compiled a framework that describes the guidance and conditions that enable the internal auditor to fulfill potentially conflicting roles in projects. Each quadrant represents a different perspective: (I) guidance from the Institute of Internal Auditors (IIA), (II) the structure of the internal audit department, (III) interchangeable roles with other governance departments, and (IV) project governance and de facto project management frameworks. Every quadrant entails two levels, which are described in detail:

1. the organizational level describing guidance that is applicable in a broad company-wide context and,
2. guidance at the individual program/project level.

<table>
<thead>
<tr>
<th>Table 2 Roles Not to be Undertaken by the Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of roles not to be undertaken by the internal auditor</td>
</tr>
<tr>
<td>- Setting the project risk appetite.</td>
</tr>
<tr>
<td>- Imposing the project management process.</td>
</tr>
<tr>
<td>- Managing risks identified in quality assurance.</td>
</tr>
<tr>
<td>- Taking managerial decisions regarding the proposed solutions.</td>
</tr>
<tr>
<td>- Implementing solutions on behalf of the management.</td>
</tr>
<tr>
<td>- Being accountable for project deliverables</td>
</tr>
<tr>
<td>- Being accountable for project budget and/or progress against milestones.</td>
</tr>
<tr>
<td>- Being accountable for embedding project deliverables in the organization.</td>
</tr>
</tbody>
</table>
Below I will describe the key elements of each quadrant. For a full description of all quadrants I refer to the original thesis (Huibers, 2008).

**Quadrant I—Guidance of the IIA**

The first quadrant provides guidance from the Institute of Internal Auditors (IIA). At the organizational level the purpose, authority, and nature of activities should be clearly defined in the audit charter and approved by the board. At the program/project level every single assignment beyond the scope of assurance activities should follow the IIA standards starting with a clear understanding about objectives, scope, and activities being established with the client in line with the nature of the activities in the Audit Charter.

**Quadrant II—Audit Department**

Within the audit department a segregation of duties can avoid jeopardizing independence by fulfilling conflicting roles. This can be realized on several levels depending on the size of the departments and the number of activities of internal audit: a division of the audit department into consulting/facilitating and assurance-related activities, dividing tasks between existing internal audit sub-
departments based on specialization (IT audit, financial audit) or by applying a segregation of duties at the project level. In the latter case the auditor should not audit activities in which he has been involved in the previous year.

Quadrant III—Other Governance Departments

In quadrant III the increasing prominence of risk management and control awareness in organizations gives new possibilities. The emergence of different governance departments such as Risk Management, Compliance, and Internal Control, creates a safeguard to avoid potentially conflicting roles by dividing different roles between these separate departments. Assigning different roles across the so-called lines of defense is a way to ensure the internal auditor’s independence at both the organizational (organization-wide) and program/project level. The “lines of defense model” within an organization can be a starting point for dividing roles:

1. First line of defense—management: business and project management have the primary responsibility to monitor and control the operations.
2. Second line of defense—supporting functions: the management is supported by the staff departments in their monitoring responsibility, for example Internal Control, Risk Management, Compliance, and Quality Assurance.
3. Third line of defense—Internal Audit: provide additional assurance on top of the activities of the first and second line of defense. Different types of audit might be applicable and can operate in an integrated way: for example, operational, IT, and financial audit.
4. Fourth line of defense—external audit: additional assurance to external parties (SAS-70, ISO audits for example).

In case potentially conflicting roles might arise, the activities can be split among departments:

1. general roles can be defined at organization level following the three lines of defense model,
2. (conflicting) roles can be divided between different governance/staff departments, and
3. (conflicting) roles might be divided between departments within the audit function (see previous paragraph)

The first step in effective cooperation is to define and agree with the executive management the roles and responsibilities in the organizational governance structure. Accordingly, at program/project level the different roles can be assigned to individuals of different governance departments to avoid potential conflicts in project roles. To give an illustrative example, Internal Control is involved in the design of controls in a process, whereas Internal Audit reviews the completeness of the control design.

An important remark to be made is that some factors might influence the extent to which activities will be divided between governance departments; for example, the business environment...
in which an organization is operating and the maturity of the organizational governance system.

Quadrant IV—Project Governance

The Office of Government Commerce (OGC) provides standards and guidance on best practices with respect to project management that have globally been adopted across industries (i.e., PRINCE2). The OGC de facto standard role description does not explicitly mention the role of internal audit but their guidance regarding quality assurance and advisory roles is mutually supportive of the IIA view.

The internal audit function can support the implementation of standard project and audit methodology. Often organizations adapt a general common used framework/methodology and tailor this to the needs of the organization. For instance, with respect to IT-driven projects, COBIT (Control Objectives for Information and Related Technology) is a framework created by ISACA and includes a section on program and project management. By supporting the definition and embedding of a standard project methodology a safeguard is created and this enables the project management to manage projects in a controlled way. The quality criteria for project gateways and deliverables can be made explicit and transparent and can serve as a reference model for project reviews.

At the organizational level the purpose of quality assurance is to provide an assurance that the project has adequate plans and measures, in line with the established project methodology, to ensure that the project processes are suitably controlled and are likely to result in products that meet explicit quality criteria. Audit can support the design of the quality assurance and standard audit project methodology in the organization, including clearly defined roles and responsibilities of both line management, internal audit and other governance functions. At project level audit can consult and facilitate the embedding of quality assurance in the project by assisting the project management with implementing the quality assurance system in an effective way. In this case advising means to make the audit reference framework explicit in advance in order to ensure that an adequate review is undertaken.

Steering committee

Finally, I have argued, supported by the insights of psychological and organizational theory (group decision-making processes) (Beach & Connolly, 2005; Janis, 1972), that the internal auditor should be extremely reluctant to participate in Steering Committee meetings even as a non-voting member.

If a decision is taken in the presence of the auditor, it might in hindsight be unclear what the role of the auditor in a particular decision had been. Even if he or she had not expressed an opinion, once the results turn out to be different from what was expected, it could always be used against the internal auditor that he or she “could or should have known” or had at least been part of the decision by being present in the meeting at which the decision was taken. Therefore it is important to document in writing what the relationship of the auditor is toward the Steering Committee. If the
internal auditor does participate in the meeting by expressing a second opinion it should be clear in the project charter that:

- The auditor acts completely independently and has no managerial responsibility whatsoever for the managerial decisions taken by the Project Board.
- There is no formal reporting line to the Project Board and Project Board chairman. In line with the Audit Charter and IIA Attribute Standards (2013) the internal auditor should report independently to the senior business management.
- Following good audit practices as described in the IIA Performance Standards (in particular IIA 2300–Performing the Engagement) the auditor should document advice and opinions given and maintain an audit trail based on retention requirements.

**CONCLUSION**

In this article I have described the different types of roles that can be fulfilled by the auditor, taking into consideration the shift from the traditional assurance role toward more proactive roles in projects. In order to gain more insight into the potential roles that the auditor can play in projects, I have divided these roles into three groups:

1. assurance roles,
2. consulting roles, and
3. participative roles.

Subsequently, I have categorized the different types of roles following a paper of the IIA:

1. The core roles: traditional assurance roles such as project reviews.
2. Legitimate roles with safeguards: consulting and participative project roles that can be performed by the internal auditor if certain preconditions are met.
3. Roles that should not be undertaken by internal audit such as the management of project-related risks.

The most important precondition, both for roles with safeguards and the roles that should not be undertaken, is that the auditor must refrain from any managerial accountability in all project areas, from initially setting the project risk appetite to the final embedding of deliverables in the standing organization. In order to guarantee unambiguous mutual understanding of the role of the auditor in projects it is of crucial importance to define, formalize, and communicate the agreed roles and responsibilities at all organizational levels.

To conclude, I have argued in this article, supported by the insights of psychological and organizational theory (group decision-making processes), that the internal auditor should be extremely reluctant to participate in Steering Committee meetings even as a non-voting member.

The aim of this article and my research is to provide a practical relevance to the internal audit profession and industry. The results have been confirmed and enriched by interviews with the Chief Audit Executives/Managers of large multinational organizations. The shared view is that the real added value of internal audit is its
involvement in the project from an early stage and its ability to act in a proactive way. This is not perceived to be in conflict with the independent position and objectivity of the auditor. On the contrary, one of the executives stated that: “one should see the opportunities for the internal audit discipline rather than focusing on the threats.”

Notes
1. In 2004 the Institute of Internal Auditors (IIA) published a position paper that elaborated on the roles of the internal audit function in Enterprise-wide Risk Management.
2. The Office of Government Commerce (OGC), an independent office of the U.K. government, provides standards and guidance on best practices with respect to project management such as PRINCE2 that have been globally adopted across industries.
3. In the IIA position paper of 2004 safeguards with respect to ERM have been described that I have adapted for project management.
5. COBIT 5, Chapter 5, Process reference guide contents, BAI01.01–14.

APPENDIX 1: THE ROLES OF THE AUDITOR DURING DIFFERENT PHASES OF THE PROJECT

<table>
<thead>
<tr>
<th>Generic project phases</th>
<th>PRINCE2—Process</th>
<th>PRINCE2—Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project preparation/ start</td>
<td>Project initiation</td>
<td>Plans, Management of Risk, Organization Business Case</td>
</tr>
<tr>
<td></td>
<td>Project start-up</td>
<td>Plans, Quality, Management of Risk, Business Case, Controls</td>
</tr>
<tr>
<td>Project execution</td>
<td>Controlling a stage</td>
<td>Controls, Change Control, Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Managing project delivery</td>
<td>Change Control, Plans, Controls</td>
</tr>
<tr>
<td></td>
<td>Managing stage boundaries</td>
<td>Plans, Business Case, Management of Risk, Controls, Organization</td>
</tr>
<tr>
<td>Project close</td>
<td>Closing a project</td>
<td>Controls, Configuration Management, Business Case</td>
</tr>
</tbody>
</table>
### Table A2 Examples Role(s) of the Auditor in Different Phases of the Project

<table>
<thead>
<tr>
<th>Generic project phases</th>
<th>PRINCE2 process</th>
<th>Component PRINCE2</th>
<th>Examples of the role of an auditor</th>
<th>Examples (with reference to the safeguards)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project preparation/ start</td>
<td>Project initiation</td>
<td>Plans, Management of Risk, Organization, Business Case</td>
<td>-QA assurance to program/project management</td>
<td>Review if project objectives are consistent with the overall values and goals of the organization.</td>
</tr>
<tr>
<td>Project start up</td>
<td>Plans, Quality, Risk Management, Business Case, Controls</td>
<td>-QA advise to project management</td>
<td>Advise in the setup and organization of the project management and quality assurance processes.</td>
<td></td>
</tr>
<tr>
<td>Project execution</td>
<td>Controlling a stage</td>
<td>Controls, Change Control, Configuration Management</td>
<td>-QA independent assurance</td>
<td>Milestone review of progress and quality of deliverables.</td>
</tr>
<tr>
<td>Managing project delivery</td>
<td>Change Control, Plans, Controls</td>
<td>-Advisor on content - Sounding board - Proactive expert role - Project/process coordinator - Documentation controls</td>
<td>Advise in setup of the security design of a process. Facilitate in the definition and documentation of process controls. Provide support in the coordination of defining controls.</td>
<td></td>
</tr>
<tr>
<td>Managing stage boundaries</td>
<td>Plans, Business Case, Management of Risk, Controls, Organization</td>
<td>-QA proactive support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project close</td>
<td>Closing a project</td>
<td>Controls, Configuration Management, Business Case</td>
<td>-QA assurance to program/project management</td>
<td>Project evaluation to generate lessons learned for future projects.</td>
</tr>
</tbody>
</table>

### REFERENCES


Websites Used
www.prince2.org.uk
http://www.cabinetoffice.gov.uk
 Archived OGC information:
http://webarchive.nationalarchives.gov.uk/20110822131357/
http://www.ogc.gov.uk/index.asp
www.theiia.org
www.isaca.org
COBIT 5: http://www.isaca.org/COBIT/Pages/default.aspx

FURTHER READINGS

Websites
www.gov.uk/government/organisations/cabinet-office
www.ipma.ch
www.pmi.org
www.theiia.org
www.icmci.org
www.iia.nl

For an extensive list of all references, please refer to the full version of the thesis: Huibers, Drs. EMIA RO, S.C.J., CRMA, The role (s) of the internal auditor in projects, Amsterdam Business School, Executive Master of Internal Auditing, University of Amsterdam, 2008. Published by Kluwer; http://financebase.kluwer.financielmanagement.nl/ and available for download at site of the IIA Netherlands; http://www.iia.nl/educatie/universiteiten/scripties. Thesis and various related articles based on an ongoing research are published by the IIA Netherlands and the professional bodies for registered IT auditors and certified accountants in the Netherlands (NBA and NOREA).
Drs. Sam C.J. Huibers, EMIA RO, CRMA, has vast experience in various international managerial business, audit, and advisory functions. He has led large international projects in the areas of finance, governance, internal control, and audit. He is currently employed by Heineken International and has a managerial position in the Global Audit Function. He holds an Executive Master of Internal Auditing degree and is a certified member of the IIA. He also holds a certification in Risk Management Assurance. He is a member of the Dutch IIA Professional Practice Committee and the Dutch Sounding Board on Risk Management. He's the owner of the LinkedIn Group: Project Auditing; join his discussion group to exchange views on this subject. He can be reached at his private email: sam.huibers@proactiveprojectauditing.info