GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Practice Guide

Auditing IT Projects

The Institute of Internal Auditors

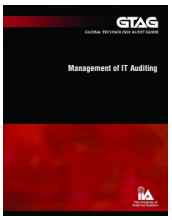
Global Technology Audit Guide (GTAG)

Written in straightforward business language to address a timely issue related to IT management, control, and security, the GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Information Technology Controls: Topics discussed include IT control concepts, the importance of IT controls, the organizational roles and responsibilities for ensuring effective IT controls, and risk analysis and monitoring techniques.

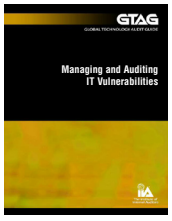
Change and Patch Management Controls: Describes sources of change and their likely impact on business objectives, as well as how change and patch management controls help manage IT risks and costs and what works and doesn't work in practice.

Continuous Auditing: Addresses the role of continuous auditing in today's internal audit environment; the relationship of continuous auditing, continuous monitoring, and continuous assurance; and the application and implementation of continuous auditing.



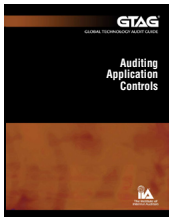
Management of IT Auditing: Discusses IT-related risks and defines the IT audit universe, as well as how to execute and manage the IT audit process.

Managing and Auditing Privacy Risks: Discusses global privacy principles and frameworks, privacy risk models and controls, the role of internal auditors, top 10 privacy questions to ask during the course of the audit, and more.



Managing and Auditing IT Vulnerabilities: Among other topics, discusses the vulnerability management life cycle, the scope of a vulnerability management audit, and metrics to measure vulnerability management practices.

Information Technology Outsourcing: Discusses how to choose the right IT outsourcing vendor and key outsourcing control considerations from the client's and service provider's operation.



Auditing Application Controls: Addresses the concept of application control and its relationship with general controls, as well as how to scope a risk-based application control review.

Identity and Access Management: Covers key concepts surrounding identity and access management (IAM), risks associated with IAM process, detailed guidance on how to audit IAM processes, and a sample checklist for auditors.

Business Continuity Management: Defines business continuity management (BCM), discusses business risk, and includes a detailed discussion of BCM program requirements.

Developing the IT Audit Plan: Provides step-by-step guidance on how to develop an IT audit plan, from understanding the business, defining the IT audit universe, and performing a risk assessment, to formalizing the IT audit plan.

For more information and resources regarding technology related audit guidance, visit www.theiia.org/technology.

Global Technology Audit Guide (GTAG®)12: Auditing IT Projects

Authors

Karine Wegrzynowicz, Lafarge SA

Steven Stein, Hewlett-Packard

March 2009

Table of Contents

Letter from The IIA's President

As is true for most internal auditors of my generation, I have witnessed technology's remarkable evolution from a ringside seat. When I was a young, newly minted internal auditor directly out of college in the 1970s, the most complex technology I regularly encountered was a 10-key calculator. Today, though, we live and work in quite a different world.

Thanks to unrelenting IT advancement since I entered the workforce, virtually everything we encounter now is embedded with technology. Regardless of the industry or enterprise, information technology is critical to maintaining a competitive edge, managing risks, and achieving business objectives; and organizations worldwide are allocating vast resources to vital IT projects.

Whether IT projects are developed inhouse or are co-sourced with third-party providers, they are fraught with challenges that must be considered carefully to ensure success. Less than desirable outcomes can result from such issues as poorly defined project scope and objectives, lack of senior manager support, insufficient user involvement, incorrect or inappropriate technology choices, or lack of knowledge about changing technologies. Insufficient attention to these and other IT challenges will result in wasted money and resources, loss of trust, and reputation damage — all of which are huge risks and none of which is acceptable.

Inherent in information technology is its cross-functionality. It must involve people and processes throughout an organization. And because of the internal auditors' unique perspective and positioning within their organization, their early involvement can help ensure positive results and the accompanying benefits. They can serve as a bridge between individual business units and the IT function, point out previously unidentified risks, and recommend controls for enhancing outcomes.

For all of these reasons, I am especially pleased with the release of The IIA's new GTAG: *Auditing IT Projects*. This timely guidance provides an overview of techniques for effectively engaging with project teams and management to assess the risks related to IT projects. This Practice Guide includes:

- How to outline a framework for assessing project-related risks.
- Key project management risks.
- How the internal audit activity can actively participate in the review of projects while maintaining independence.
- Five key components of IT projects for internal auditors to consider when building an audit approach.
- Top 10 reasons for project success.
- Types of project audits.
- A sample audit work program with a suggested list of questions for use in the IT project assessment.

The development of this Practice Guide truly was a team effort. We are grateful to The IIA's Advanced Technology Committee for selecting the topic and developing the guidance. We owe a great debt of gratitude to the two principal authors, Karine Wegrzynowicz, CIA, internal audit director at Lafarge SA, and Steve Stein, CIA, global IT audit manager at Hewlett-Packard, for contributing a great deal of time and effort to the project.

I encourage you to use this authoritative guidance to build your working knowledge on IT-related project management, for it surely will contribute to the success of your organization's future IT efforts.

Sincerely,

Richard F. Chambers

Richard F. Chambers, CIA
IIA President
Global Headquarters

1. Executive Summary

Organizations invest large amounts of capital to fund the implementation of new information systems, enter new markets, develop new products, and manage alliances and acquisitions. Project teams are often created to manage such efforts. These investments don't just bring about positive change to the organization, but also present a high degree of risk. As a result, the success or failure of these investments can be critical to the strategy of an organization, as well as have an impact on the organization's efficiency and reputation.

Many projects and investments are focused around information technology (IT). In the past, studies such as "The CHAOS Report," conducted by The Standish Group, indicate that for IT projects in particular, the failure rate can be as high as 50 percent[1]. Project failure often comes down to two key things: too much optimism from a people aspect, or technology failures from a systems perspective. Given the level of risk that projects face, it is essential for the internal audit department to be aware of the projects taking place in the organization and to determine at what stage it should be involved in order to provide guidance on the controls aspect of the project or an independent assessment of the achievement of desired results.

Internal auditing can contribute to the success of IT projects by assessing project-related risks. Auditors can focus on areas such as security and internal controls, and they can play a role in evaluating the overall project management. By helping project teams respond to risks, internal auditing can increase the project's chance of success. As discussed in *GTAG 8: Auditing Application Controls*, internal auditing can add value through both traditional assurance and consultative engagements.[2]

In a 2002 *Internal Auditor* article, Richard B. Lanza wrote: "To be successful, auditors must demonstrate to both senior management and project managers the value that an independent advisor can bring. Senior management can give auditors access to projects, but auditors can be more effective when the project managers buy into their involvement and give them greater access."[3]

The purpose of this GTAG is to provide the chief audit executive (CAE) and internal auditors with an overview of techniques for effectively engaging with project teams and project management offices (PMOs) to assess the risks related to IT projects. The field of project management is quite broad, and as such the purpose of this guide is to outline a framework for assessing project-related risks, provide examples of common project management risks, and discuss how the internal audit function can participate actively in the review of projects while maintaining its independence. The IIA's *International Standards for the Professional Practice of Internal Auditing* provide principle-focused guidance for performing these engagements.

Within the context of this GTAG we have chosen to focus on five key components of IT projects for which we recommend building an audit approach (see Figure 1):

1. Business and IT Alignment
2. Project Management
3. IT Solution Readiness
4. Organizational and Process Change Management
5. Post Implementation

Figure 1 shows that project management is the central concept that links all of these areas. When planning the project audit approach, the auditor should consider all five of these areas to ensure that all major risks are addressed.

This guide is not intended to be a complete project risk assessment or audit guidance; rather it provides an outline of key considerations for auditing IT projects. Auditing projects is an excellent opportunity for internal auditing to provide assurance on strategic risk. A number of studies have shown that internal auditing spends a large amount of time auditing operational risk, but not enough on strategic risk. Project audits can provide an opportunity to expand the risk focus.

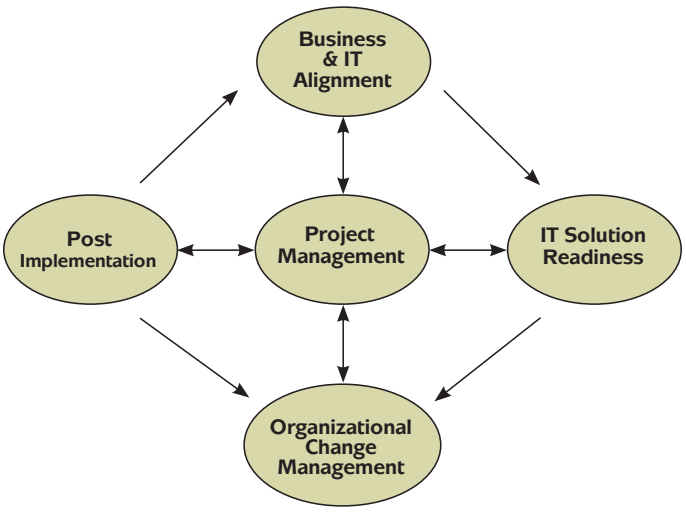


Figure 1: Five Key Focus Areas for Auditors

[1] The *CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*

[2] GTAG 8: Auditing Application Controls, *p. 5.*

[3] *"Technology Projects: The Riskiest Parts of the Business."* Internal Auditor, *May 15, 2002, Richard B. Lanza, CPA, PMP.*

2. Introduction

2.1 What Exactly Is an IT Project?

The term *IT Project* is a bit of a misnomer. In reality, most system implementation or maintenance projects are increasingly complex initiatives that involve or impact more than just the IT department and, as such, should be considered as a business project as well as an IT project. In the most general sense, a project is a unique set of activities with a discreet beginning and end, undertaken to achieve a particular purpose within defined constraints of schedule, scope, and resources. It is important to note that this GTAG is intended to focus on projects that include a technology-related solution; however the principles are very similar to other types of projects.

IT-related investments have been a major source of expenditure for organizations for many years. They tend to come in waves, and all organizations worldwide respond to them. Large IT projects easily can cost tens of millions of dollars. Major waves of IT system-related projects in the last 15 years include enterprise resource planning (ERP) systems, solving the Year 2000 problem, e-commerce/dot-com solutions, and customer relationship management (CRM) systems. Such projects could include building new infrastructure, new product development (commonly referred to as research and development, or R&D), and the implementation of new business processes or business transformations. In the evaluation of such projects, it is necessary to understand the key risks, and to develop a set of criteria to evaluate the project at various stages.

2.2 Understanding the Impact

Today, determination of a project's success extends beyond traditional on-time, on-budget metrics. Failed or challenged projects can have a significant impact on an organization, depending on the business need behind the project. A few examples of possible risks include:

- Disruption of service to customers.
- Loss of competitive advantage.
- Fines from failed regulatory compliance.
- Loss of revenue.
- Negative impact on reputation.
- Delays in deploying critical strategic initiatives, products, or processes.
- Loss of expected return-on-investment.
- Loss of critical business and IT personnel.
- Facility closure or damage.
- Loss of shareholders/investors.

Many researchers and consulting firms have performed studies reporting on the fact that IT projects are regularly challenged or fail — they are over budget, behind schedule, do not achieve objectives, or are cancelled. As a result, there is no shortage of ideas, articles, and white papers on the subject. Regardless of the interpretation of the data, there is overwhelming evidence that projects pose a significant challenge. Ultimately, management is accountable for ensuring that the project and benefit outcomes are achieved.

2.3 Examples of Failed IT Projects

Most large IT project failures will never be publicized because of the negative impact the disclosure would have on an organization's reputation and shareholders. However, the following are some examples of significant failures that have been reported.

- In August 2005, *CIO Magazine* reported that a large U.S. government agency had to scrap a US $170 million virtual case file management system development project due to schedule delays, cost overruns, and technical difficulties.[4]
- In 2004, one of the top telecommunications companies in the world experienced a project failure during a CRM system upgrade. The resulting problems cascaded across the IT environment and led to disruptions in wireless service to customers. The company lost many customers over the incident, and the revenue impact was estimated to be US $100 million. The stock price fell and before it could recover, the company was sold to a competitor for less than half of the original share price.[5]
- In 1999, one of the largest food manufacturers in the world suffered a significant ERP implementation failure, which resulted in two profit warnings in the last quarter of the year. The event led to significant product distribution problems during the critical holiday sales season. By year end, the stock price was down 27 percent, which was very poor considering a stock market boom was occurring at the time.[6]

2.4 Historical Statistics on IT Project Success and Failure

Statistics around IT project failures have been studied consistently and reported over the last two decades by numerous analysts and consultants, including the Gartner Group, Forrester Group, The Standish Group, and KPMG. There are far too many reports and statistics to discuss here, but

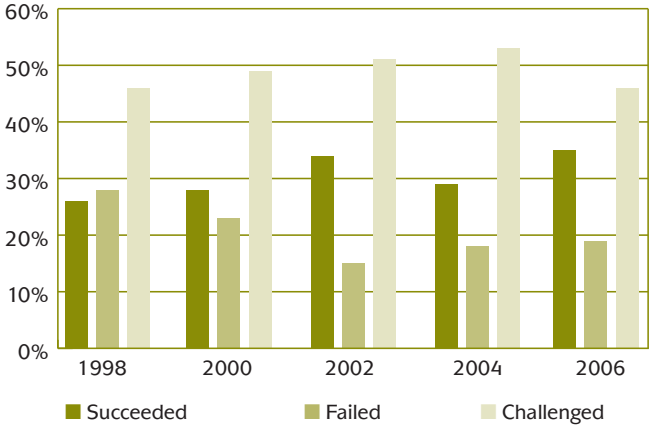
---

[4] *"Why the G Men Aren't IT Men," Allan Holmes, CIO Magazine Online, Aug. 15, 2005.*

[5,6] *20 Questions Directors Should Ask About IT Projects, 2007. Adapted with permission from the Canadian Institute of Chartered Accountants, Toronto, Canada. Any changes to the original material are the sole responsibility of the publisher and have not been reviewed or endorsed by the CICA.*

the CAE should be aware of the research to understand the inherent risks associated with IT projects. Auditors should investigate statistics and failures that relate to their specific organization and industry. Such statistics can be presented to management when discussing the need for project audits. The following are some examples of relevant research regarding project failures.

- The 2007 CHAOS Report from The Standish Group[7] provides summary results of its research studies from 1998 to 2006. The data shows that project success cannot be taken for granted. As of 2006, 65 percent of projects either failed or were challenged, meaning that they were unable to meet all or part of their objectives, cost, or schedule goals.



	1998	2000	2002	2004	2006
Succeeded	26%	28%	34%	29%	35%
Failed	28%	23%	15%	18%	19%
Challenged	46%	49%	51%	53%	46%

Table 1. CHAOS Research Study

- CA, Inc. sponsored an independent research group in the United Kingdom, Loudhouse, to survey 100 IT directors across the UK and Ireland. The study concluded that poor visibility into IT project status and a lack of management control over projects is costing UK companies a quarter of a billion pounds (US $350 million) each year. A third of all projects implemented each year end up over budget, with the typical over-spend between 10 percent and 20 percent of the original budget. The survey also highlighted the increased complexity of IT projects; it indicated a typical company runs 29 projects at any one time and has an average IT budget of between £1m and £5m[8] (US $1.4m and US $7.03m).
- KPMG's Global IT Project Management Survey, released in 2005, found that 49 percent of survey participants had experienced at least one project failure in the previous 12 months. Further, the report revealed that 59 percent of organizations either have no process or only an informal process in place to assess whether or not a project is on track to provide the intended benefit.[9]

These are just a few examples. While it is possible to debate the detailed accuracy of such statistics, the fact remains that the large number of project failures has been reported consistently.

2.5 Top 10 Factors for Project Success

To counter the failures many research groups provide ideas on steps to take to ensure that projects have the best chance for success. The Standish Group provides an annual report based on its research of why projects succeed. The following 10 rules for success come from the latest Standish annual project management report, "The CHAOS Report 2007."[10]

1. **User Involvement** – Business and IT users are involved with key consensus-building, decision-making, and information-gathering processes.
2. **Executive Support** – Key executives provide alignment with business strategy, as well as financial, emotional, and conflict resolution support.
3. **Clear Business Objectives** – Stakeholders understand the core value of the project and how it aligns with business strategy.
4. **Agile Optimization** – Project uses iterative development and optimization processes to avoid unnecessary features and ensure critical features are included.
5. **Emotional Maturity** – Project manager directs the emotions and actions of project stakeholders and avoids ambition, arrogance, ignorance, abstinence, and fraudulence.

[7] The *CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*

[8] *Over Budget IT Projects Cost UK Plc £256m Per Year, CA Inc., Sept. 12, 2007.*

[9] *Global IT Project Management Survey.* © 2005 KPMG International. KPMG International is a Swiss cooperative that serves as a coordinating entity for a network of independent firms operating under the KPMG name. KPMG International provides no services to clients. Each member firm of KPMG International is a legally distinct and separate entity and each describes itself as such. All rights reserved. Printed in Hong Kong. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative. August 2005.

[10] The *CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*

6. **Project Management Expertise** – Organization uses project managers who understand the basic skills and practices, such as certified Project Management Professional from the Project Management Institute (PMI) or the like.
7. **Financial Management** – Project manager is able to manage financial resources, account for project budget/costs, and demonstrate the value of the project.
8. **Skilled Resources** – Skilled project personnel are acquired, managed, retained, and controlled to move forward in the face of turnover and other personnel hurdles.
9. **Formal Methodology** – There is a predefined set of process-based techniques that provide a road map on when, how, and what events should occur in what order.
10. **Tools and Infrastructure** – The project infrastructure is built and managed with tools that enable management of tasks, resources, requirements, change, risks, vendors, user acceptance, and quality management.

2.6 Purpose and Benefits of Internal Audit Involvement

While all of the success factors outlined above are clearly the role of management, internal auditing can add considerable value by evaluating the effectiveness of risk management over both the IT and organizational aspects of IT-related projects. Internal auditing offers an independent approach to assessing whether an organization or function is achieving its stated objectives. Auditors analyze business processes or activities in a methodical way to highlight issues and recommend corrective actions. Given the IT-related project risks outlined above, internal auditing can bring the value of their experience and methodology to review projects in the early stages to also help increase the likelihood of success. Benefits of internal audit involvement may include:

- Providing independent ongoing advice throughout the project.
- Identifying key risks or issues early, which enables project teams to operate proactively to mitigate risks.

3. Five Key Focus Areas for Project Audits

Research has shown not only what some of the risks are, but also that early intervention is a key to success. As stated in the introduction, this GTAG focuses on five key areas of projects around which we recommend building an audit approach. The following five categories were chosen as the logical areas around which to focus based on a variety of research and the authors' past experience with using various project risk assessment methodologies.

1. Business and IT Alignment
2. Project Management
3. IT Solution Readiness
4. Organizational and Process Change Management
5. Post Implementation

The next sections provide considerations for each of the five key focus areas. (See Appendix F for a suggested list of audit questions and examples of specific risks and controls for each of these focus areas.)

3.1 Business and IT Alignment

Alignment simply means that the vision and objectives of both the business and IT are understood, are in harmony with each other, and that the project is in line with the strategy of the organization. Almost every project consists of interdependence among various levels and functions of an organization. This means that achieving and maintaining alignment is a significant challenge throughout the life of the project! Regular meetings with all stakeholders present and channels for an open flow of communication are critical, as are fully dedicated sponsors who provide the leadership, time, and energy that the project requires. Further to the sponsorship, the project team selection is equally crucial. A project team that is lacking the right experience, skill set, and willingness to support the project is a prevalent barrier to project success. There are many aspects associated with project alignment, and for many organizations these aspects are incorporated into the business case.

Assessing the Business Case

For any project to get started, management needs information to determine the viability of taking what sounds like a good idea forward. Preparation of the business case is a process that is followed by a dedicated team to provide the information necessary to facilitate a decision regarding whether to proceed with the project. The ultimate decision may be taken by the project steering committee, or may be taken at a higher level in the organization. Indeed, entire audit guides have been written on the subject of reviewing the business case. Therefore, for the purposes of this GTAG, we will focus on just a few of the common risk areas.

Key components of the business case should include:

- Benefits that are realistic, understood, and measurable.
- Environmental concerns such as the regulatory landscape, architectural compatibility, etc.
- Organizational considerations such as who should be involved from what functions.
- A clearly defined project scope.
- Project deliverables, in terms or process and functionality.
- Necessary resources, both in terms of cost and people.
- Analysis of the risks regarding the viability of partners or vendors.
- Measurement or likelihood of success.

In building the business case, it is essential to establish project sponsorship as well as project impact. At the earliest phase, project sponsors must understand the full impact of the project and to ensure all internal and external stakeholders are considered. The direct stakeholders include internal departments or functions that will use the new system, external customers or suppliers who may interact with it, and anyone else with a vested interest. It is important also to ensure that indirect stakeholders are consulted early, which could include finance, internal audit, IT security, legal, purchasing, or regulatory functions. Feedback should be received from all impacted groups — even those on which the impact may be minimal — to ensure all considerations are taken into account.

The business case should ensure that all available alternatives are considered. Typical factors include building the solution in-house or buying an external package; using internal resources versus outsourcing; and of course considering whether the project is in response to a regulatory requirement, or simply a business efficiency solution. In the analysis of alternatives, a strong business case enables management to make the most informed decision and to understand the trade-offs that must be considered. Lastly, the business case should assess the capacity of the organization to undertake the project, the priority level of the project, and whether the organization has the people with the right skill set to execute it.

3.2 Project Management

Understanding Project Management

As depicted in Figure 1, project management is central to the five focus areas. Project management, like internal auditing, is a profession with its own set of best practices, terminology, and standards. (Due to the wide availability and broad

scope of guidance on project management as a profession, the appendices of this GTAG were developed to provide a summary of project management reference material, best practices, and standards.) Auditors should be careful to ensure they fully understand the risks associated with project management. Even an auditor with a strong IT and business background may find many project management best practices unfamiliar. Internal auditors will have to invest time to study and better understand project management processes and terminology.

The following terminology is fundamental to project management:

- **Project Portfolio** – The collection of projects within an organization. Programs may include a number of projects. In order to plan, scope, and assess projects and programs, the auditors must understand the concepts of project management, project governance, and project management methodology within the context of their business and organization.
- **Project Management** – The discipline of organizing and managing resources (e.g. people and budget) so that the project is completed within defined scope, quality, time, and cost constraints.
- **Project Governance** – The overlap between projects and corporate governance, the governance of project management at the entity level. It ensures the organization undertakes the right projects, controls the project portfolio, establishes priorities, assigns authority to the correct level, and has appropriate decision-making processes in place. Good project management governance ties all of the areas illustrated in Figure 2 (on page 8) together and ensures that they have the support to operate effectively.
- **Project Management Methodologies** – Broad collections of integrated policies, standards, methodologies, life cycles, procedures, tools, techniques, stakeholders, and organizations that are used to guide the planning and execution of a project. The Standish Group points out that the methodology also includes what it calls "the other 90 percent of a project environment" (e.g., emotional attitudes, culture, stakeholder education, and nonprocess/procedure maturity of the organization).[11]

Auditors and Project Management Methodologies

Just like it is true that no two businesses are the same, it is also true that no two project management methodologies are the same. Every organization will use a different combination of methodologies, life cycles, best practices, tools, etc. For instance, large defense contractors may use a complex methodology such as earned value management (EVM) — a project management technique for measuring project progress in an objective way by combining scope, schedule, and cost[12] — in order to support large government contracts, while a small organization may use a simple project management software package or spreadsheet just to track the project tasks and status.

Before performing any project audits, the CAE and the internal audit team should first gain an understanding of the organization's project management methodology — also known as an ecosystem or life cycle. Additionally, they must understand the best practices, risks, and controls associated with both project management and systems development. Failure to understand this relationship could result in an internal auditor not scoping IT project audits to account for the full range of possible risks.

Figure 2 shows the components that might be included in a methodology and where key controls should reside. It also highlights the interdependence between levels and functions that exist, and to what level the audit may need to go to have a complete understanding of the project magnitude. The organization's project management methodology provides the context the auditor needs to perform the audit. The methodology offers a basis for helping the auditor during the planning and execution of audits to identify key project governance groups and key project management control points, and to determine the policies, standards, and best practices against which to audit.

Table 2, Project Methodology Components and Value to Auditor, highlights the major methodology components and their value to the auditor.

[11] *CHAOS Chronicles Online, v14.2.1, Glossary Definition of Ecosystem, The Standish Group, 2008.*

[12] *Practice Standard for Earned Value Management, Project Management Institute, March 2005.*

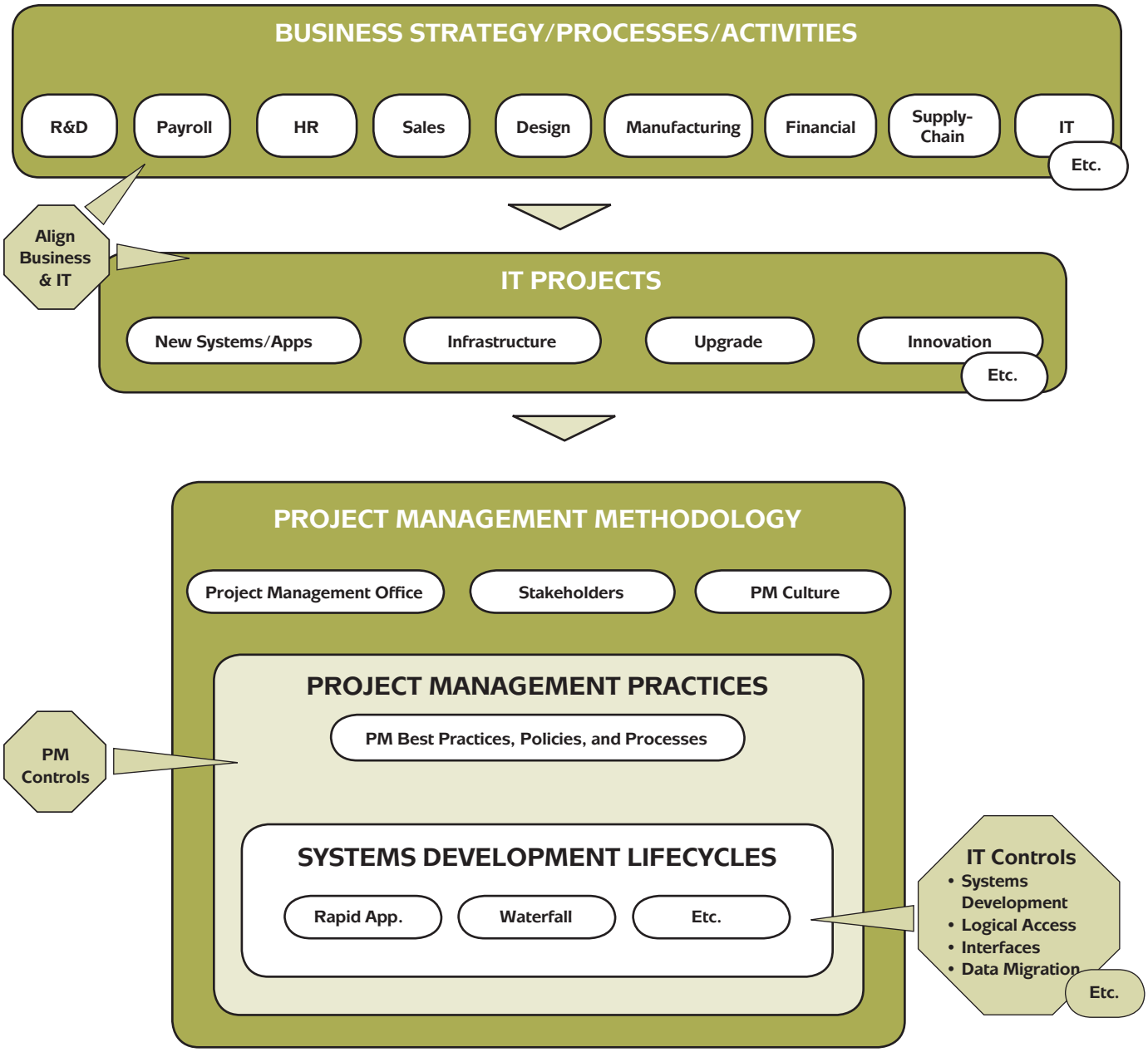


Figure 2. Project Management Methodology. Adapted and revised from *IT Control Objectives for Sarbanes-Oxley, Second Edition*, used with permission of the IT Governance Institute (ITGI) © 2006 ITGI. All rights reserved.

Methodology Component	Value to Auditors	Examples
Organizational		
Project Stakeholders	Provide auditors with multiple perspectives (business, IT, contractor, etc.) on the risks and issues associated with individual projects.	• Business Owner • IT Owner
Project Management Offices	Provide a centralized location to identify and review all project methodologies and associated deliverable requirements, which aids in annual audit planning and scoping, audit program development, etc.	• Strategic/Global • Single Project • Business Unit
Models and Methods		
Project Portfolio Management	Provides a centralized location to identify and review all projects, which aids in annual audit planning, audit prioritization, etc.	• Strategic/Global • Single Project
Project Management Maturity Models	Provides a "measuring stick" for planning project audits. Auditors can assess project methodologies and processes to identify gaps as a basis for improvement.	• The Portfolio, Program, and Project Management Maturity Model (P3M3) • Organizational Project Management Maturity Model (OPM3)
System Development Maturity Models	Provides a "measuring stick" for scoping and planning project audits. Auditors can assess project methodologies and processes to identify gaps for improvement.	• Capability Maturity Model Integration for Development (CMMI) • The Software Process Improvement and Capability dEtermination (SPICE)
Software Development Life Cycle (SDLC)	Provides a basis for identifying and assessing adherence to system development processes, as well as when to use or not use a particular approach.	• Waterfall • Rapid Application Development (RAD)
Project Management Best Practice Guides	Provides a foundation for developing an audit approach and a basis for assessing organizational and project-level performance.	• Project Management Body of Knowledge (PMBOK) • Projects in Controlled Environments (PRINCE2)
Automated Tools	Enables review of audit schedules, expenditures, resource allocation, issues, etc. If portfolio management tools are used, they enable the auditor to run reports listing all projects in order to risk-prioritize projects based on budgets and schedules, and to use metrics to identify "troubled projects."	• Schedule Management • Resource Management • Issue Tracking

Table 2. Project Methodology Components and Value to Auditor

Project Stakeholders

Internal auditors must understand how their organization identifies and includes stakeholders in IT projects. Stakeholders are the collection of people and groups that make the project happen. Projects simply cannot succeed without the proper stakeholders working together in a well-coordinated way. Executive stakeholders must provide strategic guidance, as well as financial, political, and emotional support. Business and IT user stakeholders ensure that the requirements and final product meet the intended business need. The number and types of stakeholders vary by organization and project. (See Appendix B for a list of typical stakeholders.)

Project Management Office (PMO) and the Internal Auditor

If the organization has a PMO, this will be a key starting point for the internal auditor to understand the organization's project management culture, methodologies, standards, and processes. Many organizations implement PMOs to help govern and influence project success across an organization. According to studies by the Project Management Institute, the top reasons for implementing a PMO are to improve project success rates, standardize practices, and lower costs. Although small organizations can manage projects effectively without a PMO, large organizations with a vast number of projects will find success unlikely without one.

Because of the critical role the PMO can play in a project management methodology, it is essential that the auditor develops and maintains a strong relationship with the PMO. PMOs may play a key role during project audits and may serve as a valuable liaison between internal auditing and project managers. Auditors can play an advisory role to the PMO by sharing their perspective on IT project risk and by setting auditing's expectations for the PMO and individual projects. IT project auditors should seek to understand the following:

- PMO's roles and functions
- Project management methodologies
- IT project cost and schedule performance data and trends
- IT project success/failure rates, statistics, metrics, and lessons learned
- Trends that are driving success or failure across all IT projects

They should also seek to obtain a listing of approved and funded IT projects annually — sorted by budget, risk, or other key factors — and a listing of major milestones and go-live dates for major system implementations.

Project Portfolio Management

Project portfolio management (PPM) refers to the collective management of projects to ensure that well-informed project investment decisions are made. Organizations use PPM to make better IT investment decisions, ensure adequate funding across business requirements, and elevate the role of IT in the organization by showing the value of all IT initiatives and projects. Internal auditors can use PPM to identify high-risk projects and the overall priorities of the organization.

Internal Auditors and Maturity Models

Generally speaking, maturity models exist to help organizations move from less mature processes to more mature processes. They help the organization identify current weaknesses and gaps in capability and identify its current level of maturity and then plot a strategy for improving to the next level of maturity. The general idea is to develop well defined, robust, and repeatable processes. There are specific maturity models for software development and project management. (See Appendix D for a summary of maturity models.)

Auditors can use maturity models as a basis for assessing an organization's project management and/or systems development processes. However, this probably only makes sense if the organization has already chosen a maturity model and is structuring its processes to be aligned with a model. If an organization plans to implement a maturity model for the first time, internal auditing could perform an initial audit against the proposed maturity standard. This would provide a baseline understanding for the organization to begin its use of the maturity model.

Auditors should view the use of maturity models by the organization as a very positive step in terms of improving the organization's IT project management approach. However, there is no requirement for an organization to use a maturity model, and many do not because of the cost and complexity.

Best Practices for IT Project Management

Best practices provide an ideal starting point for auditors to frame their risk assessment and audit approach. Best practices come from both general project management guides as well as those that are specific to IT development. Some widely accepted examples include:

- Project Management Body of Knowledge (PMBOK).[13]
- PRojects IN Controlled Environments (PRINCE2).[14]

---

[13] *Project Management Body of Knowledge (PMBOK), Project Management Institute, 2008.*

[14] *PRojects IN Controlled Environments (PRINCE2), United Kingdom's Office of Government Commerce (OGC), 2008.*

- Control Objectives for Information and related Technology (COBIT).[15]
- International Standards Organization (ISO) Standards.[16]

Internal auditors should not expect organizations to fully implement PMBOK, PRINCE2, COBIT, or any other large set of best practices. Rather, they should expect to see that these practices have been customized and integrated into the organization's project management methodology. Appendix E - General Project Management Best Practices gives more details on each of these best practices and frameworks.

Project Management Tools and Automation

Auditors should expect to see any number of automated tools for project management or teamwork being used on projects. Software may by used to manage entire portfolios containing hundreds of projects, and/or individual projects. Auditors may leverage these tools to obtain:

- Information on cost, schedule, and technical problems.
- Insight into project decision-making and issue-tracking.
- Information on resource utilization.

The following are some examples of project areas that may benefit from automation and tools.

Project Management

- Schedule management
- Cost management
- Requirements management
- Issue tracking
- Resource management
- Risk management
- Quality management
- Team collaboration/knowledge sharing

Systems Development

- Software defect tracking
- Software testing
- Source code management and version control

3.3 IT Solution Readiness

IT solutions have a natural development life cycle that includes a sequence of phases that must be followed in order to convert a management need into an IT system or application and to maintain the system in a controlled way. Typically, this sequence is referred to as a software life cycle (SLC) or software development life cycle (SDLC). (See Figure 3: Generic Software Development Life Cycle.)

Organizations may use their own software life cycle methodology for custom development or one provided by consultants or vendors for use with their products. SDLCs may vary by the type of technology being developed. They may be customized to meet any of the following development or implementation scenarios:

- Custom development using internal resources
- Custom development using fully or partly outsourced resources located on site or offsite (locally or in an offshore location)
- Vendor software packages implemented as-is with no customization
- Vendor software packages customized to meet specific requirements

Well-known types of SDLC models include Waterfall and Rapid Application Development.

Regardless, the internal auditors should expect to see some type of development life cycle and will need to determine whether it is appropriately followed. They'll then use the phases in the life cycle to determine when to perform the project audit and what controls to test.

The implementation phase of the project is often thought of as simply when the new system gets "turned on" in production; however, there are a series of critical steps and decisions that take place during the course of the project. Many project failures have been attributed to a lack of interim checkpoints, which should be established as part of the project

[15] *Control Objectives for Information and related Technology (COBIT), IT Governance Institute, 2008.*

[16] *International Standards Organization (ISO) Standards, ISO, 2008.*

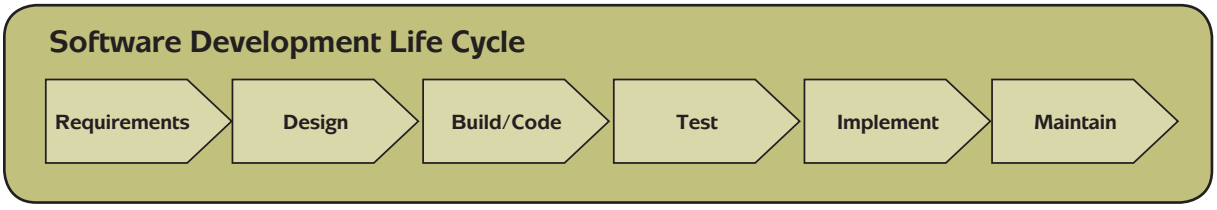


Figure 3. Generic Software Development Life Cycle

management methodology with the specific goal of the project team making a conscious decision to move forward with the project. Projects that are especially complex, such as an enterprise resource planning (ERP) system, should include specific decision points at the end of significant project milestones to ensure the project is on track.

External Consultant Assessment

During the solution or system implementation phase of the project it is quite common for the project management team to partner with an external firm or resource, especially for the implementation of a large package such as an ERP. Auditors should consider whether the viability of the external partner chosen has been reviewed especially for a project that will be lengthy. In addition, it is essential that the roles and responsibilities of all parties are well defined up front so that everyone will have a clear understanding of where accountability lies for the deliverables of the project.

Solution Design

During the solution design phase of the project, auditors should look to ensure that business requirements and both the existing and future business processes are taken into consideration. At the end of this phase, the project scope should be frozen, and all functionality should be prioritized in terms of what is required for the system launch. This prioritization is often referred to as the "must-have versus nice-to-have" decision. It's also typical during this phase for the project team to decide whether to build the solution in house or to buy an external package. Regardless of the decision made, it is imperative to ensure that both functional and security-related internal controls are considered so that they will be included in the solution up front.

Code, Build, and Data

Following the design phase, there should be a process to review the actual coding or building of the system. Within a system's life cycle, there may be many different internal rules or guidelines that the audit can follow. For example, a code development process review can be performed to determine whether robust and secure programming methods are being followed. Following the system build, the configurations or localizations will take place, followed by the conversion and/or loading of new or legacy data. In addition, the interfaces or connectivity to other systems in the organization will be set up. The data loading consideration is one of the most critical, in particular the preparation of any master data such as employee, customer, or vendor files. While it is important to ensure that there can be continuity of legacy information, it is imperative to start with data that has been clearly identified prior to loading to the new system. In other words, if there is duplicate or old data in the old system, the data should be cleansed before doing a conversion whenever possible.

Testing and Go-live

The next key step is the testing phase. It is essential to determine whether testing includes not only the end users, but also the workflows, security, and connectivity to other systems. Once testing is complete, there should be a checkpoint to decide on the readiness for go-live, or the launch in production. The go-live should not merely be considered as an event, but rather a phase in which a transition plan is in place to transition the new system from the project team to the team that ultimately will be responsible for ongoing operation and support. In this phase it is important for the project to take into account contingency or fall-back strategies to mitigate any unforeseen issues that arise with the final implementation. During this phase of the project there is usually significant pressure to show progress and meet deadlines and, as a result, some important aspects of the detail planning may be overlooked.

3.4 Organizational and Process Change Management

For any project, organizational and process change management is often the most important element to manage and, in fact, can present the most risk to a project. The most complex scenarios include both the change of a business process and the related information systems. Good project management governance processes, as illustrated in Figure 2, enable effective change management. Change management encompasses more of the soft, or intangible, aspects of a project, including understanding the magnitude of how the project will impact the organization and how it will change the way people work. From an audit perspective, this is where the integrated audit team becomes essential to ensure operational and technical aspects are assessed, with the right level of skills from the audit team.

Managing Communication

One of the most critical aspects of change management is managing communication in a broad sense, beginning with obtaining buy-in and representation from all stakeholders, marketing the benefits or reasons for the project, and managing the expectations of end users. For example, what processes will be impacted by the new system and what impact will the changes have on vendors or customers? These points should be stated clearly at the beginning of the project and must be managed well beyond post implementation.

Organizational Readiness

Organizational readiness entails assessing changes to the organization proposed by the new project and managing the level of resistance there will be to the change. This is especially true with projects that involve centralization of processing, such as a shared service center combined with the implementation of an ERP, or with those involving outsourcing. An assessment should be made on the skill set of existing staff members compared to changing or new roles, and determine whether processes or workflows are clearly defined, to gauge the readiness of the organization to accept the change.

Training

A key success factor for any new system implementation is ensuring that all users who will be impacted receive adequate training. The audit team should evaluate whether the training is complete, timely, and includes user guides that are not generic. In addition, training provided to the IT team and/or helpdesk personnel should be reviewed to determine whether it is adequate to support the new system.

Postlaunch Support

It is essential for auditors to ensure that a post go-live support plan is defined in terms of the support team organization, for both functional and technical issues. The support team should be analyzed to determine whether it is correctly sized for the go-live and postlaunch workload, which is usually much higher than normal. Additionally, contingency plans should be established in the event something goes wrong during the go-live period.

3.5 Post Implementation

Following the system go-live, there inevitably is a stabilization period. During this time, the users are getting acclimated to the system or new functionality, and any outstanding issues are being resolved. During this phase, there are key risks to watch for — many of which are related to change management aspects. In other words, the auditors must determine whether the new system is being used correctly and the functionality is meeting the requirements as intended. If many changes were made to the business processes along with the implementation of a new system, the stabilization period can take a relatively long time. A key consideration is to determine whether there is any prolonged resistance to change. For example, are users finding a work-around or short cuts because the new system is not as user-friendly as its predecessor? Discussions and interviews with users can be held to determine this.

A post implementation review can take a couple of different approaches. More detailed information on conducting a post-implementation review can be found in Section 4.3, on page 16.

4. Project Audit Planning

IT projects should be included in the annual internal audit plan using a systematic process. Figure 4: IT Project Planning Process depicts a logical workflow progression that uses a top-down approach to determine which projects to audit. It is consistent with the large audit planning process described in *GTAG 11: Developing the IT Audit Plan*.[17]

Internal auditors can add considerable value by evaluating both the IT and organizational aspects of IT-related projects. Key questions the internal auditor should consider include:

- How should IT project audits be incorporated into the annual audit plan?
- What is the appropriate role for the internal auditor?
- What projects should be audited and why?
- What type of project audit should the internal auditor perform?

4.1 IT Projects and the Annual Internal Audit Plan

To include projects in the annual audit plan or audit universe, internal auditing should have access to the organization's entire list of IT or technology-related projects. Ideally, there should be a list of all projects in a centralized system where auditors can run reports based on risk factors such as the cost of the project, schedule, project risk, project duration, etc. If no such list exists, questions regarding IT or technology-related projects can be raised during annual audit planning to both IT and key business functions. In addition, the PMO can be an invaluable source of information to aid auditors as they develop the audit universe and the annual audit plan, and as they plan audits of individual projects. The internal auditors should engage with the PMO as part of scoping and planning prior to conducting IT project audits.

The following points may be useful for auditors to consider when assessing the project risk at the organizational level and to determine how to include IT-related projects in the annual audit plan:

- A complete and accurate inventory of all projects — with enough supporting information to assess the risk at a high level — is unavailable.
- There are a large number of IT projects spread across the company.
- The organization lacks centralized methodologies and processes for project governance, including project management methodologies and system development life cycles.

[17] *GTAG 11: Developing the IT Audit Plan, pg. 3.*

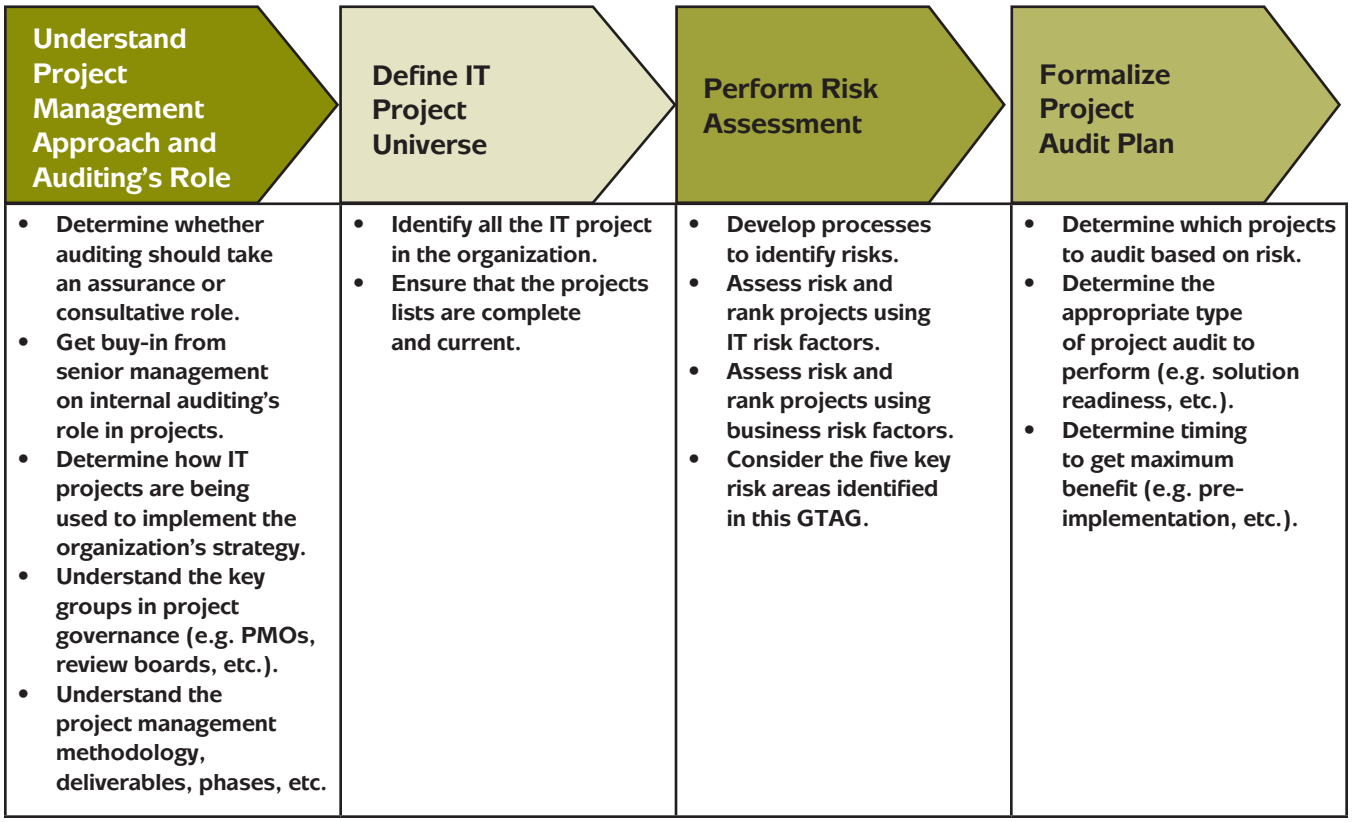


Figure 4. IT Project Planning Process, adapted from *GTAG 11: Developing the IT Audit Plan*.

- Senior management is overly confident in its ability to deliver projects effectively, yet cannot produce evidence of project inventories or centralized methods.
- Project managers and senior management believe that auditors cannot add value to projects and that project teams are too busy to deal with supporting a project audit because of lack of resources, impending deadlines, etc.

4.2 Internal Auditing's Role

When considering the internal auditor's role, a key point to keep in mind is the nature of the internal audit organization and whether the function is mandated to perform only assurance type engagements, or whether engagements that are more of an operational or consultative nature are also permitted. The IIA's *International Standards for the Professional Practice of Internal Auditing* provide the necessary guidance for the internal audit function to perform these roles.

Internal auditors can add significant value to a project by engaging early and supporting the project team throughout the project life cycle. They may be asked to support the project in various capacities, ranging from consultative reviews to formal audits. This can create the potential for perceived impairment of auditor independence. The IT auditor should provide reasonable assurance that his or her interest, if any, in the IT solution will not impair the objectivity of the review, and that his or her participation is one of providing advice without being responsible for making the decision. As an additional resource, the IT auditor may also consider Information Systems Audit and Control Association's (ISACA's) Guideline G17: Effect of Non-audit Roles on the IS Auditor's Independence.[18]

The sooner the auditor engages with a project, the better. Internal audits or assessments performed during the early phases of the project can be the most valuable because they can identify issues earlier and reduce cost. When auditors find issues, their recommendation often includes the addition of automated controls or possibly design changes. It has been well established in studies of software development that software fixes and adjustments are far cheaper to address in the early project stages, such as the design phase, rather than in the later stages of the project. Finding and fixing a software problem after delivery is often 100 times more expensive than finding and fixing it during the requirements or design phases.[19] Figure 5: Relative Costs to Fix Errors Throughout Life Cycle shows the dramatic relative cost of fixing software changes throughout the life of a project. This can be a major selling point in convincing senior management to support early internal audit involvement in the project.

---

[18] *IS Auditing Guideline G17: Effect of Non-audit Roles on the IS Auditor's Independence, Information Systems Audit and Control Association, 2003.*

[19] Reproduced by permission from Steven Rakitin, *Software Verification and Validation: A Practitioner's Guide*, Norwood, MA: Artech House Inc., 2001. © 2001 Artech House Inc.

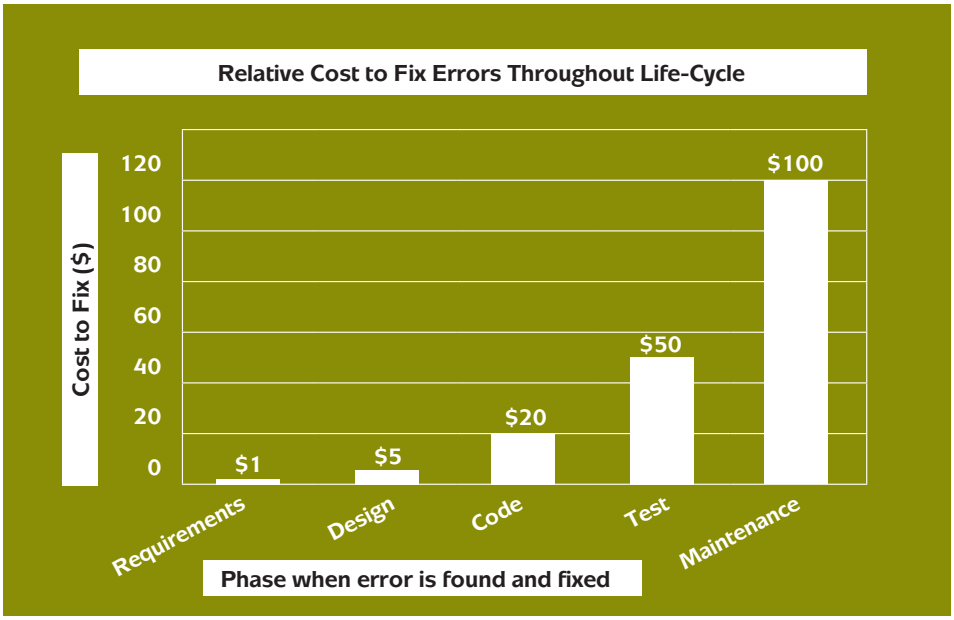


Figure 5. Relative Costs to Fix Errors Throughout Life Cycle. Adapted from *Software Verification and Validation for Practitioners and Managers, Second Edition*[19]

4.3 Types of Project Audits

Internal auditors may perform a variety of different reviews, depending on the project risk and needs of the organization. This GTAG highlights five of the most common types of project-related audits or assessments to consider:

- Project risk assessment to gauge likelihood of success.
- Readiness assessment during key phases or pre-launch.
- Post implementation review.
- Audit of a key project phase during the life of the project.
- Overall project management methodology assessment.

(Sample audit considerations for each can be found in Appendix F.)

The most important consideration for any type of internal audit review is staffing the engagement with the right skill set. This is where the benefits of an integrated internal audit team become very clear. Using an integrated team ensures that both the functional and technical risks of the project are included in the scope of the review. An integrated audit team should include skill sets of both a business and technical nature.

Risk Assessment

A risk assessment typically involves an overview of all project areas to identify the key risks that could impact project delivery and determine how well they are being tracked and mitigated. This type of review is also quite common if management believes the project is not progressing well, costs are exceeding the budget, or the project has already experienced delays.

Readiness Assessment

A readiness assessment is a review that takes place at a key stage of the project — usually upon completion of the business case, alignment phase, solution design phase, or pre-launch phase. The key objective for this type of review is to provide objective assurance on the completeness of each phase and to ensure management is aware of any newly identified risks or issues before moving forward to the next step.

Post-implementation Review

A post-implementation review takes place at some predetermined point after the new system has gone live. There are many different variables to consider regarding the target timing for this type of audit, including whether the system needs time to stabilize, how long the project team will be available to correct issues, vendor contractual considerations, and postlaunch issues raised by the users.

There are a couple of different approaches to performing a post-implementation project review. Its purpose can be to evaluate how well the project followed the organization's project methodology or SDLC, or to measure how well the new system is working. A post-implementation review likely would use an integrated audit approach because both the system and related business processes should be examined in tandem.

During the project initiation and development of the business case, many project benefits are noted. A benefits realization review is another type of post-implementation or post-project review that may be performed and would be geared toward measuring how well the project has achieved the benefits, savings, or efficiency gains it was intended to achieve. ISACA's Guideline G29: Post Implementation Review offers specific guidance on this type of review.[20]

Another approach is to audit the end results of the project back to the originally stated objectives, or to conduct an assessment of how the project went so that lessons learned can be captured for use on future projects. The audit team may also perform an end-to-end process review to include all aspects, or functionality, of both the business processes and the new information system. However the approach is designed, it is essential to allow an adequate stabilization period following the launch.

The duration of the stabilization period should be determined up front in the project plan. In general terms, the stabilization usually takes on average three to six months depending on the complexity of the system. It's also important for the auditors to keep in mind how quickly the project team will disband, and to identify who will take over the project documentation and manage the transition into a normal maintenance or continuous improvement phase. Auditing a project after the project team moves on can be quite difficult if there isn't adequate documentation available, or to understand why some decisions were made.

Key Phase Review

A key phase review, undertaken during the course of a project, is a proactive approach often used for high-risk projects. This can include SDLC or system design reviews, or participation by the internal auditor in a "gate" or specific project phase review, for example. The key objective is usually associated with assessing how closely the project management or SDLC methodologies are followed. As indicated above, internal auditing can work with project teams to address concerns before the system is moved into the production environment, when it is still relatively inexpensive to make corrections. Through early project involvement, internal auditing can raise questions and suggestions that influence a project in either a formal or informal way. There are two IS auditing guidelines from ISACA that can be referenced to guide the IT auditor in carrying out reviews of this nature:

---

[20] *IS Auditing Guideline G29: Post Implementation Review, Information Systems Audit and Control Association, 2004.*

(1) Guideline G17: Effect of Non-audit Roles on the IS Auditor's Independence,[21] and (2) Guideline G23: System Development Life Cycle (SDLC) Review.[22]

Project Management Methodology Assessment

Auditing the overall project management methodology can identify risks and point out weaknesses in the methodology that could help the entire organization improve. For organizations that have too many projects to audit individually, this type of review utilizes a more holistic approach. In addition, by auditing the methodology, the internal auditor will be better prepared to audit individual projects because the PMO audit will provide a strong basis for understanding the organization's practices.

Possible objectives of auditing project methodologies include:

- Assessing the adequacy of project management methodologies.
- Determining whether the methodology supports the full range of IT projects in the organization, from very small to very large.
- Assessing the effectiveness of management level support provided by the PMO. (This may be articulated in a PMO charter or mission statement.)
- Determining whether the PMO policies, standards, methodologies, and processes are implemented and executed consistently across all projects in the organization.
- Assessing the ability of the PMO to add the intended level of value.
- Determining whether the PMO has a complete inventory of all projects in the organization.
- Determining whether the PPM processes are working effectively.

Project Audit Reports

The report out from the audit team following a project review can vary depending on the type of review performed, and the stage of the project at which the audit team gets involved. The IIA's *International Standards for the Professional Practice of Internal Auditing 2400 series* provides guidance for communicating results; however, the type of review should be carefully considered when determining what format works best within the organization. For example, if the audit team is participating throughout the life of the project, status updates or memos to the project steering committee could be a format to consider. For a post-implementation review, especially if the full functionality of the system and underlying business processes are evaluated, the formal audit report format may be preferred.

4.4 External Auditor Considerations

Because IT and technology-related projects may have a critical impact on the organization's financial statements and operations, external auditors will want to know what major projects are underway in an organization. Specifically, they will be concerned with IT projects that could have a major impact on:

- Financial statement reporting (e.g., a new SAP general ledger system).
- Revenue generation (e.g., order processing).
- Inventory management.
- Major business or IT transformations that affect financial data or systems that produce financial data.
- Major regulatory requirements such as the U.S. Sarbanes-Oxley Act of 2002.

The CAE should engage with the external auditors to understand their perspectives on the risks associated with IT projects. A major risk for the organization is that the external auditor is unaware of major projects and highlights key control considerations of a project after the new system is already in production, when it is considerably more expensive to modify existing controls or implement new controls.

Conclusion

In conclusion, "auditors should consider projects to be opportunities to exploit their core competencies in new areas, while they help ensure the effective risk management, cost containment, and organizational success of projects," notes Richard B. Lanza in an article on technology project risks that appeared in *Internal Auditor* in 2002,[23] which is still very relevant today. The incorporation of projects into the audit universe helps internal audit to partner with both project managers and senior management and to have a positive impact towards future project success.

---

[21] *IS Auditing Guideline G17: Effect of Non-audit Roles on the IS Auditor's Independence, Information Systems Audit and Control Association, 2003.*

[22] *IS Auditing Guideline G23: System Development Life Cycle (SDLC) Review, Information Systems Audit and Control Association, 2003.*

[23] *"Technology Projects: The Riskiest Parts of the Business," Internal Auditor, May 15, 2002, Richard B. Lanza, CPA, PMP.*

Appendix A – Project Management

A.1 *Project Management Methodologies*

An IT project management methodology is like a toolkit for project teams. A good methodology explains the relationships among all the relevant project management and organizational processes. It is a comprehensive structure of repeatable processes that provides a road map on when, how, and what events should occur in what order. For IT projects, it is based on a combination of project management and system development best practices. Typically, it is composed of interrelated phases, activities, and tasks that are supported by documented milestones, guidelines, techniques/methods, templates, samples, and roles and responsibilities.

A methodology is necessary to:

- Provide a standard, repeatable model approach that can be used to deliver a project.
- Promote the use of best practices that will increase a project's probability of success.
- Define what is happening so that it can be improved. (According to the Software Engineering Institute (SEI), a process has to be defined before it can be improved or made repeatable.)
- Increase the chances of project success and reduce known risk areas.
- Provide a structure for project managers to manage their projects.
- Ensure best practices are systematically deployed across projects.
- Provide a structure for assessing the effectiveness of project outcomes and updating the methodology with those lessons learned.
- Provide a structure for consistently monitoring project performance against a consistent set of deliverable requirements and performance metrics.

Types of components typically found in a methodology include:

- **Frameworks –** composed of phases, activities, and tasks.
- **Guidelines –** define the activities required to generate deliverables.
- **Techniques/Methods –** provide guidance on how to perform activities.
- **Templates** and **Samples –** make it easier to apply recommended techniques.
- **Roles –** communicate who is responsible for what.
- **Project Plans –** lists the activities at both high and detail level for the project.

A.2 *Project Management Life Cycle*

According to the Project Management Institute, there are five phases in a project life cycle. The phases are linked by the outcomes they produce — the outcome of one is the input to another.

1. **Initiating** – Authorizing the project.
2. **Planning** – Defining and refining objectives and selecting the best of the alternative courses of action to attain the objectives that the project or phase was undertaken to address.
3. **Executing –** Coordinating people and other resources to carry out the plan.
4. **Controlling** – Ensuring that the project objectives are met by monitoring and measuring progress regularly to identify variances from the plan so that corrective action can be taken when necessary.
5. **Closing** – Formalizing acceptance of the project or phase and bringing it to an orderly end.

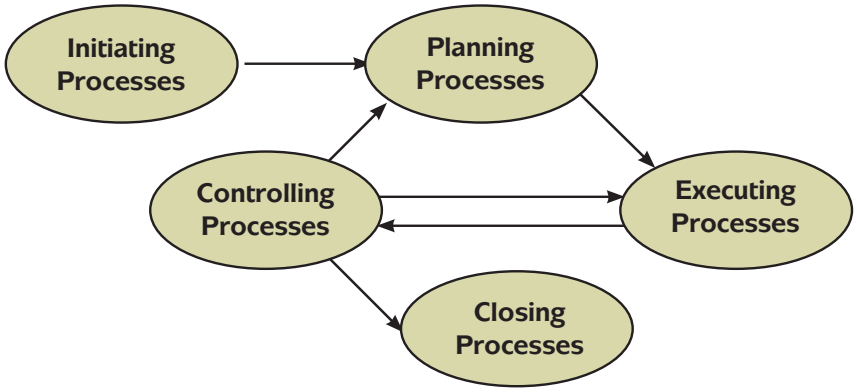


Figure 6. Major Project Life Cycle Process Groups. Source: Project Management Institute A *Guide to the Project Management Body of Knowledge* (*PMBOK® Guide*) - 2000 Edition, Project Management Institute Inc., 2000.

Appendix B – IT Project Stakeholders

The following is a list of potential stakeholders and their associated responsibilities. Not all of these roles will exist for every project, and there are many other possible roles.

Stakeholder	Responsibility
Steering Committee (Executive or Technical)	Executive leaders (business and IT) who influence guiding principles, strategy, and major decisions
Sponsor	Person who provides the financial resources or endorsement of the project
Project Manager	Person with overall project responsibility and clear lines of authority and accountability
User (Business, IT, etc.)	Those who use the outcome from the project
Project Team	The team that performs day-to-day work on the project, a mix of IT and business people
Influencers	Those not directly related to the use of the project, but due to their position, can have negative or positive influence
Project Management Office	The office that provides project managers or other team members, which may have direct or indirect responsibility for the outcome of the project
Compliance Review Boards	The team that assesses special compliance or policy requirements such as the U.S. Sarbanes-Oxley Act of 2002, local laws, etc.
IT Security	Those who ensure that the final system is designed with the IT security features to meet organizational security policies or best practices
IT Architecture Board	The team that ensures that the system will be compatible with existing or future infrastructure
Consultants and Vendors	Development consultants or the applicable system vendors (e.g., SAP, Peoplesoft, etc.)
Auditors (Finance, IT, External, and Internal)	Those who perform audits and provide auditor perspective on risk
Procurement	Those who buy project materials and labor

Appendix C – PMOs' Structure, Roles, and Responsibilities

Project management offices (PMOs) are typically organized and provide support in three ways:

Organizational Level	Type of Support Provided
Single Project	Supports or fully manages a single, very large project such as the Year 2000 problem or a global enterprise resource planning system implementation.
Business Unit	Supports many projects within a single business unit, usually within a larger, global organization that has many business units.
Strategic/Global	Supports all of the projects in an organization, regardless of which business unit owns the project.

The roles and responsibilities of PMOs vary by organization and may include some or all of the following:

- Provide project reporting and tracking.
- Ensure executive and/or user alignment and support.
- Drive process consistency and repeatability across projects.
- Provide projects with consulting and mentoring.
- Develop, implement, and maintain a framework for effective project management, including policies, standards, and methodologies.
- Provide project management training and mentoring.
- Provide the organization with a pool of project managers to manage projects.
- Conduct post-mortems of projects to capture and incorporate lessons learned.
- Help individual projects prepare for audits.
- Support the management of the organization's entire collection of projects, which may be referred to as project portfolio management.

Appendix D – Maturity Models

D.1 Capability Maturity Model

The first widely accepted maturity model was the Capability Maturity Model (CMM) developed by the Software Engineering Institute at Carnegie Mellon University in the United States. It was focused on software development.

CMM, and now many other models, use the following levels of maturity. The idea is to move from Level 1 to Level 5.

- **Level 1: Initial** – Few processes are defined.
- **Level 2: Repeatable** – Basic project management processes are established.
- **Level 3: Defined** – Projects use an approved tailored version of the organization's standard software process.
- **Level 4: Managed** – Detailed measures are defined and controlled.
- **Level 5: Optimizing** – Continuous improvement is enabled.

D.2 Project Management Maturity Models

Project management maturity models provide a process and structure for assessing current project management capabilities and developing a strategy for improvement. The following are two of the many examples of project management maturity models.

Maturity Model	Source	Description
The Portfolio, Program, and Project Management Maturity Model (P3M3)	United Kingdom's Office of Government Commerce (OGC)	Uses 32 Key Performance Areas as a basis for assessing and transitioning among the standard five layers of maturity.
Organizational Project Management Maturity Model (OPM3)	Project Management Institute (PMI)	Uses a highly structured approach for evaluating an organization's maturity based on three interlocking elements: knowledge, assessment, and improvement.

D.3 Systems Development Maturity Models

Systems development maturity models provide a process and structure for assessing current systems development capabilities and developing a strategy for improvement. The following are two of the many examples of systems development maturity models.

Maturity Model	Source	Description
Capability Maturity Model Integration for Development (CMMI)	Software Engineering Institute (SEI)	SEI developed the first major software development maturity model, and this is the next generation of that model.
The Software Process Improvement and Capability dEtermination (SPICE)	International Standards Organization (ISO)	Also known as ISO 15504, this standard provides a framework for the assessment of software processes, and is aimed at setting out a clear model for process comparison.

Appendix E – General Project Management Best Practices

E.1 PMBOK and PRINCE2

Project management best practices are primarily embodied in the following two guides:

Best Practice	Source	Description
The Project Management Body of Knowledge (PMBOK)	Project Management Institute (PMI)	An internally recognized standard (IEEE Std 1490-2003). It is the most broadly accepted set of project management practices in the world.
Projects in Controlled Environments (PRINCE2)	United Kingdom's Office of Government Commerce (OGC)	A structured approach to project management. It is the de-facto standard in the United Kingdom and other parts of Europe.

Neither of these guides specifically targets IT projects, nor are they meant to stand alone as project management tools. They are broad sets of fundamental practices and guidelines that are applicable across a wide range of industries and departments, and they're meant to be customized to the organization's needs. They are applicable whether an organization is building a bridge, developing a new service, or implementing a new software application. The PMBOK and PRINCE2 are different in many ways. However, both offer equally acceptable foundations for developing an IT project management framework.

PMBOK

According to the PMI, the PMBOK describes the sum of knowledge generally accepted within the profession of project management. "Generally accepted" means the knowledge and practices described are applicable to most projects most of the time, and there is widespread consensus about their value and usefulness. The overall purpose of the PMBOK is to provide a common lexicon within the project management profession and practice for talking and writing about project management.

The PMBOK begins with nine key project knowledge areas:

- Integration Management
- Scope Management
- Time Management
- Cost Management
- Quality Management
- Human Resource Management
- Communications Management
- Risk Management
- Procurement Management

These knowledge areas are further refined into 44 detailed processes. The PMBOK also provides guidance around project portfolio management and project management offices.

The PMBOK is consistent with standards from the International Organization for Standardization (ISO) and the Capability Maturity Model (CMM). The PMI manages the Project Management Professional (PMP) certification. Many government and financial organizations in the United States and the United Kingdom require their managers to be PMP certified.

PRINCE2

PRINCE2 is intended as a generic, customizable, end-to-end project management methodology. It has eight process areas:

- Business Case
- Organization
- Plans
- Controls
- Management of Risk
- Quality
- Configuration Management
- Change Control

PRINCE2 fits each process into a framework of essential components that should be applied throughout a project. It covers how to organize, manage, and control projects.

E.2 ISO Standards

The ISO standards incorporate and address project management best practices for specific industries or process areas, such as quality or construction management. However, ISO does not have a standard dedicated to general project management practices. The following are three examples of ISO standards that include project management practices.

- **ISO 1006:2003** provides guidance on quality in project management processes.
- **ISO 9001:2005** addresses quality with respect to service and product development.
- **ISO 15504** addresses project management maturity.

Internal auditors in organizations that use ISO standards should ensure they understand which ISO standards are relevant to their industry and their organization. There are too many ISO standards to discuss all of them in this GTAG.

E.3 COBIT Sections That Apply To Project Management

Control Objectives for Information and related Technology (COBIT) was developed by the IT Governance Institute, in association with the Information Systems Audit and Control Association. COBIT is a large and comprehensive IT governance framework that includes control objectives that could be used to manage IT projects.

When using COBIT to plan project audits, the internal auditor must determine which specific control objectives from COBIT best support the audit objectives. Here we highlight topics within COBIT's four domains that are most likely to be relevant during a project review, but others may apply as well.

Plan and Organize
- Ensure Compliance with External Requirements
- Manage Projects
- Manage Quality

Acquire and Implement
- Identify Automated Solutions
- Acquire and Maintain Application Software
- Acquire and Maintain Technology Infrastructure
- Develop and Maintain Procedures
- Install and Accredit Systems
- Manage Changes

Deliver and Support
- Define and Manage Service Levels
- Manage Third-party Services
- Manage Performance and Capacity
- Ensure Continuous Service
- Ensure Systems Security
- Educate and Train Users

Monitor and Evaluate
- Monitor and Evaluate IT Performance
- Monitor and Evaluate Internal Control

E.4 VAL IT

The Val IT Framework from the IT Governance Institute provides auditors with a powerful tool for assessing the business value of a project. Val IT offers a comprehensive, consistent, and coherent approach that helps all levels of management optimize the realization of value from IT investments.[24] Auditors can use this framework as a basis for structuring their audit program and assessing the business value of the project.

[24] *Val IT, IT Governance Institute, 2008.*

Appendix F – Internal Auditor's Questions for Reviewing an IT Project

The following table is a suggested list of audit questions that can be used in the assessment of the five key focus areas that have been highlighted throughout this GTAG. These questions have been adapted from a Lafarge internal audit work program.

Business Case and Alignment		
Area		**Criteria**
1 — Business Case- Investment / Benefit Realization		
1.1	Business case management	There is an agreed-upon business case for the project.
		It is updated, and includes lower levels of details as information becomes available.
		Realistic assumptions are being made about costs and benefits.
		Assumptions are documented and agreed-upon.
		Assumptions are actively proven or disproved as the project progresses, and appropriate action is taken as a result.
1.2	Project costs	The project management team is confident in the estimates.
		A standard estimating model is used for all common pieces of work.
		It is clear who needs to agree with and understand the model.
		Extra budget has been allocated to speed up or fast-track development projects to allow for testing out the approach, environment, etc.
		Estimates are included in the budget for both staff and nonstaff costs (hardware / software external/internal resources, developments, end-to-end testing, quality assurance, benefits realization follow-up, vendor costs, operational costs, etc.).
		There is a definition of what contingency is to be used. If an issue arises, there is a plan for how it will be addressed.
		The estimates have been reviewed by a qualified third party.
1.3	History	Changes in project costs have been made since the original business case.
		Changes have been made, if so, understand why.
1.4	Timing of costs	The estimated timing of costs is appropriate. Understand if it is possible to postpone some costs.
		Timing of costs has been changed, if so, understand why.
1.5	Type of benefits	Types of benefits (e.g., cost reduction, increased revenue, qualitative) are clearly articulated.
		The realization of benefits is dependant on external factors.
		How dependencies should be approached is defined.
		The benefits are aligned with the current scope of the project.

Business Case and Alignment		
Area		**Criteria**
1.6	Realization of benefits	It is clear how benefits will be measured (e.g., direct bottom line cost reduction, staff reduction or cost reallocation).
		The responsibility for achievement of benefits is clearly defined in terms of who will do what.
		The owners have approved the benefits as reasonable and achievable.
1.7	Time plan	A timeline for benefit realization is stated.
		The timing seems appropriate.
		Understand if there are any possibilities of accelerating the benefits realization.
2 — Project Plan and Approach		
2.1	Objective and scope	The scope of the project is clearly defined, and it includes sufficient level of detail.
		There is an up-to-date and communicated project charter.
		There is a common understanding of scope by both the business and the project.
		There is an agreed-upon procedure for changing the scope, which was designed at the outset of the project.
2.2	Estimates, timeline, and scope	The current estimates are clearly communicated to the project group, sponsor, steering group, and project office.
		Understand if estimates have changed over time, and why.
		The project has been reevaluated based on business case updates.
2.3	Organization	Each role in the project is defined.
		The project organization is defined.
		Everyone on the project knows and understands his or her role.
		Understand if there are any incentives attached to project success and the impact.
2.4	Deliverables	The content and structure of each deliverable of the phases are documented.
		The purpose of the deliverables are clearly understood and documented.
		All project signatories are aware of the required deliverables sign-off.
		The format of the deliverables been discussed and agreed-upon with the signatories.
		Appropriate experts have reviewed key deliverables.
2.5	Dependencies	Tasks outside the project are clearly documented and understood. The plans for these tasks have been developed and agreed-upon.
		Checkpoints are defined in advance, along with what will be produced.
		The planning assumptions are understood, documented, and agreed-upon.

Business Case and Alignment		
Area		**Criteria**
2.6	Time plan and activities	There is an overall project plan that links together all the sub-project plans.
		Every stream within the project has a detailed plan with visible milestones. Check if this only applies to critical areas.
		Each area has a clear view of the end result and what is required to get there.
		The main pieces of work have been identified and the relationship between them is documented.
		Each piece of work has a clear focus and owner.
		All inter-project and external dependencies have been identified and due dates and owners are defined.
		There is a fast track or pilot project to prove the methodology, deliverables, environment, etc.
		The pilot project run is small, discrete, and representative.
		The owners of the pieces of work have agreed to the plans.
		The planned days/weeks allow for holidays/training.
		The plan reflects learning curves/knowledge transfer.
		The plan allows for schedule contingency between each main piece of work as well as at the end of each phase.
		The plan includes sufficient lead-time for phase set-up tasks (e.g., environment, standards, and procedures.).
		Appropriate reviews and sign-off time is incorporated into the plan.
3 — Project Communication and Coordination		
3.1	Communication and change management	Everyone knows why we are doing this and the timeline of events.
		Everyone knows how it will affect him or her.
3.2	Organization	Each role in the organization is defined.
		Everyone knows how his or her role relates to the process on the whole.
3.3	Dependencies	All inter-department and external dependencies have been identified.
		Management is releasing the necessary resources to work on the project.
		Management is willing to halt other projects/areas of work if they conflict.
3.4	Shared Programs	The project has sponsors or representatives from each affected area.

Business Case and Alignment		
Area		**Criteria**
3.5	Current status	Understand the current status of the project with regard to time, cost, and scope, and whether there are any deviations from the project definition.
		Understand the key concerns with respect to status.
		Understand why any deviations have occurred.
		Reasons behind deviations were identified as risks before they occurred.
		Corrective actions have been taken to address deviations, risks, and issues.
3.6	Work plan	The work plan has been updated regularly.
		The project estimates are accurate and key milestones have been met on time.
		Key tasks to be completed are identified, and the critical path or must-have list for go-live has been identified.
		A plan to handle overruns if expected has been developed.
3.7	Risk handling	A risk assessment has been performed, documented, and communicated.
		It includes mitigation actions / contingency plans and those accountable.
		The risks are understood by the business.
		The risks and actions to mitigate them are proactively managed.
		Risks are reviewed regularly with the business.
		Issues have a clear owner for resolution.
3.8	Dependencies on other project/areas	The plan incorporates a mechanism for the coordination of changes resulting from other business/systems projects.
		Service level agreements have been specified for support areas.

IT Solution and Change Management		
Area		**Criteria**
4 — Process Design		
4.1	Business scope	Scope — in terms of business units, locations, and business rules — is defined and validated.
4.2	Process and supporting design	The process design is documented through business scenarios and business process design documents.
		Business scenarios are documented, tested successfully, and signed off by business representatives.
5 — Configuration and Developments		
5.1	Translation	All screens and customizing is documented.
5.2	Configuration	Configuration of critical tables are reviewed for completeness, and fully documented.

IT Solution and Change Management		
Area		**Criteria**
5.3	Programs	Functional design is complete, up to date, and agreed-upon with business representatives.
		Technical design is complete, according to specifications, and successfully unit-tested, and acceptance is tested by the project team.
		Specific programs are developed according to standards.
		Specific programs are unit tested.
		Programs are migrated to production platform or environment.
5.4	Interfaces	Functional designs for interfaces are complete, up-to-date, and agreed to.
		Technical designs for interfaces are complete and up-to-date.
		Reports are developed according to design, successfully unit-tested, and accepted by the project team.
		Interfaces are tested "end-to-end" with the production platform.
		The functional error-handling process is defined, developed, and tested.
		There are no outstanding "urgent" or "high" issues with interfaces.
6 — User Acceptance Tests		
6.1	User acceptance tests	All business scenarios are successfully executed and signed-off. All user acceptance tests are complete and scripts signed-off.
		There is adequate business involvement to ensure realistic testing.
6.2	Issues list	All functional gaps noted in the issues list are closed and resolutions are agreed.
6.3	Batch schedule	Daily, weekly, monthly, quarterly, and annual batch schedules are designed and validated with project and technical teams.
		Job failure instructions, from a functional perspective, are defined (e.g., skip job, rerun next day or hold schedule).
6.4	Issues remaining at go-live	Functional team leads have agreed with key business representatives which issues will not be fixed until after go-live, and work-arounds if necessary are defined.
		Where required, workarounds have been defined and communicated to the training and help desk/support groups.

IT Solution and Change Management		
Area		**Criteria**
7 — Data Conversion and Cut-over		
7.1	Data conversion plan	The data conversion plan and quality of converted data is proven through trial conversions and dry runs. Data owners for all data conversions are established.
		The data converted reconciles with data in the legacy systems.
		The quality of dry run-converted data is verified by data owners.
		The conversion plan dependencies and critical path are tested.
		Profiles required for manual data loads/checking are available and give required access.
		There are no outstanding "urgent" or "high" issues with the dry run.
7.2	Parallel data maintenance	Procedures for all data where parallel maintenance is required are written.
		Checks are in place to make sure parallel maintenance is carried out correctly.
7.3	Data loading	All pre go-live data loads are executed.
		Data converted reconciles with data in legacy systems.
		The quality of converted data is verified by data owners.
		There are no outstanding "urgent" or "high" issues with the data load.
7.4	Go-live plan	The go-live plan is developed and communicated to all impacted project and business personnel.
		The legacy batch schedule is ready.
		Legacy access profiles are amended to ensure users do not continue to use legacy systems by mistake.
		Timing and participants of go/no-go meetings are agreed-upon.
		Fallback plans are developed and agreed-upon.
7.5	Reconciliation	Financial balances reconcile to legacy systems. Balances are loaded and can be reconciled to legacy systems.
		Procedures are in place to explain or fix discrepancies.
8 — Technical Infrastructure		
8.1	User interface	All user locations are identified.
		The user interface is installed and has been checked on each PC.
		Logon procedures are checked.
		All update procedures are documented and communicated.
8.2	Printers	All printer locations are identified, and printers are set up and tested.
		All printers are established in the different systems.
		All printers can print from the different systems.

IT Solution and Change Management		
Area		**Criteria**
8.3	Electronic output	All fax and other electronic output formats are agreed-upon and tested.
		A production test is completed to outside fax line and electronic data interchange (EDI) recipients.
8.4	Batch schedule	Nightly and monthly batch schedules are checked.
		All server/directory destinations for interfaces are set up to point to production systems.
		There are no outstanding "urgent" or "high" issues.
8.5	Error handling procedures	Procedures for checking that errors are logged (batch interface) are in place.
		Batch interruption re-start procedures are agreed-upon and tested.
		Procedures for communicating errors to the business are agreed-upon.
8.6	Communication links	All communication links (e.g., LAN, WAN) are tested.
		Bandwidth supports peak data volumes.
		Fallback procedures are in place and tested.
8.7	System sizing	All infrastructure components that form part of the overall technical architecture is sized and tuned to accommodate peak activity and predicted growth rate.
		Hardware, software, and applications are tuned for go-live.
8.8	Performance tests	Performance tests have been conducted, and performance is acceptable for key business processes.
8.9	System performance	Post go-live, online, and batch system performance monitoring and tuning procedures are in place.
8.10	Disaster recovery	Procedures are in place for downtime, and a disaster recovery plan is in place.
		Procedures successfully tested.
8.11	Online system availability and maintenance slots	Online system availability and maintenance slots are agreed-upon with the business.
8.12	Security profiles	Security profiles are defined and implemented for IT support staff.
		The production environment is secured.
8.13	Interfaces	The interface technical set up is complete and tested.

Business and User Readiness		
Area		**Criteria**
9 — Business Simulation		
9.1	Preparation	All business scenarios are written (capitalize on user acceptance testing).
		The technical environment is ready.
		All necessary data are converted in the simulation environment.
		Users and profiles are ready.
9.2	Completion	All business scenarios with "urgent" or "high" issues are successfully executed.
		There is adequate business involvement to ensure realistic testing.
10 — Data Maintenance Post Go-live		
10.1	User ownership	Data types are inventoried and owners agreed-upon.
		The actual persons who will perform maintenance are appointed and trained.
10.2	Data maintenance	Procedures exist for each type of add/update.
		Procedures cover updating of any related trans-codification tables.
		Procedures have been communicated to all impacted users.
11 — Roles and profiles		
11.1	User profiles	Profile design is agreed-upon by the project team and business representatives.
		Profiles are developed and tested successfully.
		There are no outstanding "urgent" or "high" issues with profiles.
11.2	Business risks	Key business risks are identified and covered through systems features or procedures.
		There are no outstanding "high" issues.
11.3	System user access	All profiles are developed and tested for production and non-production environments.
		The business signs off on who receives what access.
		The business controls approval on segregation of duties.
		All user profiles are set up, including conversion and support roles.
11.4	Profile maintenance	Procedures for maintaining profiles after go-live are developed, approved, and distributed to impacted personnel.
12 — User Readiness and Training		
12.1	User impact	All users understand how their job will be impacted by the solution.
		All affected users have received job change information.
12.2	User training and competence	All affected users have attended training.
		Trainees have demonstrated competence in using the solution through the completion of training exercises.
		Extra coaching and support is scheduled for those users post go-live.

Business and User Readiness		
Area		**Criteria**
12.3	Interface errors	Users responsible for correcting interface errors have been identified and have been trained on the procedures.
12.4	Support tools	Users have access to support tools
12.5	New codes and form layouts	Customers/suppliers are informed of all new codes, form layouts, etc.

Implement - Transition - Post Implementation		
Area		**Criteria**
13 — Resource Staffing and Key Roles		
13.1	Competence requirements and fulfillment	The required skills are understood, documented, and updated.
		The required skills are covered by people assigned to the project.
		The project is competing with other projects/initiatives for key competencies/ resources. If so, understand the impact.
		There is a training program to build skills that are missing.
13.2	Competence localization	Key resources have been localized in the project premises, and/or the project team members are all located together.
13.3	Resource mix	The project has sufficient full-time resources.
		The internal vs. external resource mix is clear. There is a clear process for knowledge transfer if the external support is high.
		Agreements have been put in place for external resources (e.g., time and materials, or pay for realized benefits).
13.4	Staffing of key roles	The staffing of all areas receives sufficient priority — or is the skilled staff located in one key area?
		Knowledgeable resources are best placed to maximize their contribution to the project.
		The following roles are filled with staff with the right skills: technical architect, data architect, business architect, functional architect, and conversion/migration architect.
14 — Implementation Into Business Areas		
14.1	Roles projects/business areas	The business area understands their role in each phase of the project, and is prepared for the implementation.
		Each business area has a dedicated resource to work with the project.
		The decision-making process is clearly defined.
		The business area understands their role in the decision-making process.
14.2	Plans and resources	There are plans and resources for training, roll-out, follow-up, and sign-off.

Implement - Transition - Post Implementation		
Area		**Criteria**
15 — Implementation into IT Production and Maintenance		
15.1	IT production	There is a plan for transferring knowledge.
		The production team has agreed to a deployment plan.
		There are plans to ensure capacity.
15.2	IT maintenance	There is a plan for transferring knowledge.
		Maintenance has agreed to a deployment plan.
		There are plans to ensure capacity.
15.3	Implementation	The conversion dates been changed. If so, why?
16 — Transition to Support		
16.1	Support strategy	The overall support strategy is agreed-upon.
		The first-level support members are identified and trained on the required tools.
		The second-level support members are identified and trained on the required tools.
16.2	Change requests and fix procedures	The process for assessing and implementing change requests is agreed-upon and communicated (e.g., impact analysis, funding).
		The process for applying fixes and change requests is agreed-upon and communicated.
16.3	Support processes and contacts	Support numbers and guidelines for what information needs to be recorded if a problem is found have been communicated to users.
		The business is aware of on-site support contacts.
16.4	System usage, control measures, and review meetings	System usage measures (i.e., the system is being used, and it's working) are defined and agreed. Procedures are in place for capturing and reporting information.
		Daily post go-live review meetings are arranged.
17 — Business Continuation Plans		
17.1	Business continuation plans	Business continuation plans, in the event of loss of system, are developed and agreed-upon with project and business groups.
		Fallback plans are established to address procedures to take when the system becomes available again, to ensure items are not processed twice and financials are updated.
		Any required manual forms/other systems are in place to support fallbacks.
		The process for triggering fallback plans (i.e., who decides and who communicates) is defined and agreed-upon.

About the Authors

Steve Stein, CIA, PMP, CISA, CISSP, CFE, CGEIT
Steve Stein is the global IT audit manager for Hewlett-Packard's Internal Audit Department. He is responsible for the strategic planning and management of the IT audit function worldwide. Stein has 20 years of IT project management, consulting, and audit experience across many industries, including U.S. government, high-tech, and pharmaceuticals. He has extensive experience implementing and auditing SAP R/3 application implementations for global organizations, and assessing earned value project management systems. Stein was formerly a senior manager in KPMG's Information Risk Management group. He was awarded The Institute of Internal Auditors' William S. Smith Certificate of Honor in 2004 for his performance on the Certified Internal Auditor exam. He is a former U.S. Air Force Captain and graduate of the U.S. Air Force Academy, where he studied engineering and science.

Karine Wegrzynowicz, CIA, CISA
Karine Wegrzynowicz is an internal audit director with Lafarge Group Audit. Her responsibilities include oversight of auditing for IT and other operational functions on a global basis for Lafarge, a Paris-based international world leader in the building materials industry. Wegrzynowicz has more than 20 years of internal audit, IT, and operations experience in the airline, automotive and financial services industries. She has served The Institute of Internal Auditors and Information Systems Audit and Control Association at both the local chapter and international levels and is currently a member of The IIA's Advanced Technology Committee.

Reviewers
The IIA thanks the following individuals and organizations who provided valuable comments and added great value to this guide:

- Professional Practices Advisory Council:
  - Advanced Technology Committee
  - Board of Regents
  - Committee on Quality
  - Internal Auditing Standards Board
  - Professional Issues Committee
  - Ethics Committee
- IFACI (Unité de recherche informatique), France
- The IIA Norway (NIRF) IT Audit Speciality Group (IT nettverket)
- The Institute of Internal Auditors - UK & Ireland
- Ken Askelson, USA
- Clyde Batten, Nedbank Group Limited, South Africa
- Lily Bi, The Institute of Internal Auditors, USA
- Anders Blix, EDB Business Partner, Norway
- Lionel Guillou, Euroclear, Belgium
- F. M. Hallinan, Chevron Phillips Chemical Co. LLP, USA
- David Lione, Consultant, USA
- Michael Lynn, AXA Technology Services, USA
- Steve Mar, Resources Global Professionals, USA
- Tom Margosian, Ford Motor Co., USA
- Kurt Milne, IT Process Institute, USA
- Dr. Ulrich Hahn, independent audit expert, Germany
- Jacques Lourens, Nedbank Group Limited, South Africa
- Cesar Martinez, City of El Paso, USA
- Steve Hunt,Crowe Horwath LLP, USA
- James Reinhard, Simon Property Group Inc., USA
- Joe Zhou Xiaowei, General Motors, China

RSM McGladrey | McGladrey & Pullen

Accounting I Tax I Business Consulting | Certified Public Accountants

Looking for flexible IT audit staffing?

From small-scale, focused IT audit testing and assessment initiatives to larger-scope, complete IT audit co-sourcing assistance, our team of dedicated IT audit specialists help you achieve cost efficiencies that are more important than ever in today's economic climate. With more than 500 risk and operations professionals in nearly 100 offices nationwide, we're available wherever and whenever you need us.

Our full suite of co-sourced IT audit services includes:

- Co-sourced IT audit
- Project management/assessment
- SDLC reviews
- SAS 70 audit*
- IT security and controls assessment
- Penetration testing
- Business continuity assessment
- PCI Data Security Standard services
- Sarbanes-Oxley IT testing

www.rsmmcgladrey.com/IT-risk | TRMS@rsmi.com | 800.648.4030

RSM McGladrey | McGladrey & Pullen

Accounting I Tax I Business Consulting | Certified Public Accountants

RSM McGladrey is the official accounting, tax and business consulting firm of The PGA of America.

GTAG®

GTAG 12: Auditing IT Projects

Failure is not an option when it comes to your organization's IT projects. A project that goes over budget, falls behind schedule, does not achieve objectives, or is cancelled altogether can have a severe impact. Internal auditors can – and should – play a role in their organization's key IT projects!

The purpose of this GTAG is to provide you with an overview of techniques for effectively engaging with project teams and project management offices (PMOs) in order to assess the risks related to IT projects. This guide covers:

- How to outline a framework for assessing project related risk.
- Examples of common project management risks.
- How the internal audit function can actively participate in the review of projects while maintaining their independence.
- Five key components of IT projects for internal auditors to consider for building an audit approach.
- Top 10 factors for project success.
- Types of project audits.

This guide also includes sample questions for reviewing IT projects.

We'd like your feedback! Visit the GTAG 12 page under www.theiia.org/gtags to rate this Practice Guide and submit your comments.

The Institute of Internal Auditors

www.theiia.org

ISBN: 978-0-89413-663-4
Order Number: 2018.dl
IIA Member Free
Nonmember US $25

IPPF ALIGNED
International Professional Practices Framework

GTAGs are Practice Guides aligned under the International Professional Practices Framework