InternalAuditor GLOBAL PERSPECTIVES ON RISK, CONTROL, AND GOVERNANCE

Auditing IT Project Management

By actively participating in the IT project management life cycle, internal auditors can improve the quality and effectiveness of critical business applications, while keeping costs to a minimum.

KK Mookhey
Principal Consultant, NII Consulting

Use of reliable technology is critical for the success and competitiveness of organizations around the world. In these companies, IT activities can be completely internalized, outsourced, or both. Whether an organization outsources or performs any or all IT functions internally, a crucial aspect of the IT department's success is the ability to manage projects of different sizes and complexity levels that use multiple applications. As the business grows and offers more services and products to an ever-increasing consumer base, the technology requirements also will continue to grow. Consequently, the IT department may find itself unable to adapt to the new business landscape. Internal auditors can help IT departments address ongoing business changes and growth by providing recommendations that enhance key areas of the IT project management life cycle.

KEY PROJECT MANAGEMENT AREAS

Regardless of the organization's size and the services it provides, internal auditors should be aware of symptoms that show systemic problems with the IT department's project management approach. Usually, the presence of some or all of the symptoms below can signal that something is wrong:

Business users are unhappy with the quality and timeliness of the IT project's delivery.
The IT department blames users for not stating their requirements and expectations clearly.
The organization experiences frequent time and cost overruns on critical projects.
Questions related to project criticality elicit different responses from the IT department and senior managers.
Specific business opportunities are lost because IT systems or applications are not able to meet their goals.
There is a low level of awareness and slow adoption of IT best practices.

While there are different ways to prevent these problems, globally accepted best practices are available to help organizations manage IT projects effectively. The more popular among these are:

The Project Management Institute's Project Management Body of Knowledge (PMBOK), one of the most widely referenced guides for project management. It is consistent with other management standards such as the International Organization for Standardization's (ISO's) 9001 Standard and the Capability Maturity Model Integration (CMMI).
Projects IN Controlled Environments (PRINCE2), a structured approach to project management that has become popular in the United Kingdom, where it is the de facto standard for project management.

Along with these best practices, internal auditors can use the IT department's published project management standards and processes as the basis for the audit. At a minimum, key areas to be reviewed for any IT project include: user requirements, prioritization and scheduling, planning, resource management, training, monitoring and tracking, risk management, quality control checks, and delivery.

User Requirements

Identifying what the user wants should be the first step of any IT project. Inaccurately identifying user requirements can result in project delays or, worse, the project's cancellation. As a result, auditors need to review the process followed to gather user requirements and the functionality and features that the system must deliver.

Often users state their requirements in generic terms or in terms of the objectives they want the software to achieve — for instance, a system that facilitates compliance with the Basel II Framework. Converting broad statements such as this into specific system functionality and features can be a daunting task. The auditor, therefore, should recommend that once the development team captures user requirements and documents them, users formally commit to the stated requirements. Users must also resist increasing requirements once the system design and estimates have been frozen.

Essential points that must be covered when gathering user requirements include identifying:

1. The system's objectives.
2. The stakeholders and affected parties.
3. Specific system features.
4. Reports that must be available.
5. The user and privilege matrix.
6. Specific security requirements.
7. Legal and regulatory requirements.
8. The environment in which the system will be deployed.
9. The types of manuals that need to be developed.
10. Other systems with which the new application needs to be compatible or integrated.

Prioritization and Scheduling

Dissonance often occurs between the IT department and senior managers regarding the criticality of certain projects. For instance, for a bank, the feature to allow customers to receive credit card transaction alerts on their mobile phones might provide tremendous savings by reducing the percentage of fraud, but the IT department might perceive this project as an unnecessary feature involving substantial reprogramming efforts. As a result, many IT departments have to allocate limited resources and juggle existing priorities when faced with requests for new features, enhancements, or products. Unfortunately, this may result in assigning existing projects a lower priority, thus completing them later than expected.

To avoid knee-jerk decisions that result in ad hoc reprioritization and rescheduling of projects, auditors must determine whether:

1. There is an established communication channel between the IT department and the rest of the organization to ensure proper project portfolio management. This is usually done by establishing a team of IT personnel and managers from the business unit requesting the change.
2. There is a healthy dialogue among senior managers to ensure IT strategies and goals are aligned with overall business objectives and priorities. In highly dynamic business environments, companywide goals and strategies can change from one quarter to the next. Therefore, this high-level dialogue helps ensure the IT department is able to adjust its workload to the changing business landscape.
3. Project priorities and schedules are decided and signed off by both parties. The assigned business manager and IT project manager must work together to finalize project priorities and delivery schedules taking into account:

The strategic and competitive advantage of the project to the organization.
The financial benefits from a quick project rollout.
The complexity of the project and technologies used.

Build-buy Analysis. During this part of the prioritization and scheduling process, the organization should perform a build-buy analysis to decide whether it should acquire a commercial software product or create one in-house. Basic deciding factors include each of the product's strategic advantages, risks, and capabilities. For example:

Does building the system in-house deliver strategic advantage to the organization (i.e., would it give the company a competitive edge)?
Is it a maintenance project or a new initiative that requires significant work?
Are specific technical skills required for the project's completion? If so, do they exist in-house?
Does the organization have the right project management skills based on the project's size, complexity, and nature?
Based on initial estimated project timelines, can the organization complete it on time based on market or regulatory requirements?
Does the requested product exist? If so, are well-established vendors available?
Could the organization experience any integration issues if a solution is purchased?
If customization is required, is the vendor willing to perform it?

In addition, auditors need to consider the tool's information security aspect, if outsourced, because critical data might be shared with the third-party. Finally, auditors should verify whether a build-buy analysis was completed before embarking on a large project to ensure the decision to build an application in-house or buy it from a vendor is most appropriate given the existing IT environment and resources.

Project Planning

When planning IT projects, different kinds of project estimates should take place such as completion time lines, the number of people required to perform the work, and estimated costs. Regardless, estimates should always be based on the nature of the organization and the project, the skills of the development team, and the technology platforms used in the organization (e.g., COBOL, C++, or Java). It is important for auditors to keep in mind, however, that project estimates, especially for software development projects, are usually complex. For example, a maintenance-type project will be completed much faster than a new project on the same technology platform.

For the estimate, the IT project manager should adopt a known or customized methodology, depending on what is more suitable based on the IT and business environment and skill sets. One of the more common estimate techniques for software development projects is the function point analysis (FPA) methodology, which focuses on measuring the size of an information system based on the functionality it delivers to users.

Because projects can be re-estimated throughout their life cycle, the project management team will usually devise an initial figure based on preliminary discussions with the client. As discussions progress and user requirements are more clearly defined, the team will accurately adjust estimates. The question then is: Which estimate should the team be held accountable for? This estimate should be the one delivered immediately after the user requirements are completely outlined or when the software design phase is completed.

When looking at project methodology estimates, auditors should review the following:

- Is the methodology well-defined, easy to use, and consistently used across teams and projects?
- Is there a periodic review of the methodology that considers the changing nature of projects, the business environment, and existing technologies?
- Is the methodology adaptable to projects with different technologies, development principles, and complexities?

The auditor also must look at historical records to determine variances between estimates and actual project execution time lines. While variations are normal, any significant differences might indicate that the estimated methodology is flawed and is not in line with actual execution time liness or that the project's execution is weak (i.e., projects are not delivered on committed time lines).

Variances are usually accompanied by the presence of scope creep (i.e., users who constantly change their requirements and expectations), which greatly increases the actual effort required to deliver the project successfully. Finally, variances also could be the result of incorrectly identifying user requirements, because while users typically speak in terms of overall business needs, development teams speak in terms of modules and technology features.

Resource Management

Once estimates are completed, project managers should allocate the necessary resources to the project. Resource allocation evaluates the technical and managerial skills needed for the project, comparing these skills with those available in the organization, and allocates time to specific project components. If the necessary skills are not available in the IT department, additional staff can be hired permanently on a contract basis until the project's completion or temporarily through an external vendor.

During this phase, internal auditors need to answer the following questions:

- What is the IT team's current workload?
- Is there a process in place to periodically assess capacity use and future capacity requirements? This question can be answered by using a skills' matrix to quickly determine available skills and those in short supply, based on upcoming project requirements. The skills' matrix must be updated regularly.
- Do staffing agreements exist with established vendors that can supply people with needed technical skills?
- Is the organization capable of handling emergency situations, such as a sudden increase in demand?
- What is the perception of the entire team (i.e., unit leaders, the project manager, team leader, and team members) with regard to resource management throughout the entire project?

Training

Resource management can be successful only if the delivery teams are trained adequately on the technologies and capabilities required to execute the project successfully. As part of the review cycle, auditors need to determine the following:

- Does the project have a training plan?
- Does the project's capacity planning process work with the training plan in terms of required skills and any skill upgrades needed to execute the project internally?
- Besides technology-focused training, does the plan address other critical areas such as project management, communication, and leadership skills?
- Is there a feedback mechanism to monitor training effectiveness?

It is important to monitor team members to understand how they feel about the process. Often critical problems associated with the project and resource management phase become evident if the client organization is given a chance to freely express its opinions.

Project Monitoring

The key to successful project management is not just planning the project effectively, but also the processes used to monitor the project's execution. In this area, the auditor should assess the following:

- On a daily basis, is there a method for logging the work done (e.g., are timesheets used to log hours worked or is data captured in a project management tool)?
- Are processes in place to monitor projects (e.g., meetings with project managers, meetings with users, and documentation)?
- How are variances tracked, escalated, and brought under control?
- How are variances handled in terms of quality and type of deliverables?

What mechanisms exist to highlight variances? Do these fit into a performance management system to continuously increase productivity and improve quality?
How is productivity measured over the short- and long-term?

Project Risk Management

Every medium to large project carries risks that need to be assessed and managed. Common risk elements auditors need to keep in mind include inaccuracies in gathering user requirements, scope creep due to users increasing requirements once the design is frozen, lack of proper skills to develop the system, and under- or over-estimating the project's costs, needed resources, and completion deadline. In addition, project funding or sponsorship withdrawal, lack of proper testing leading to defective products, insecure design or development that leads to data compromises, and lack of proper user training or inadequate system documentation are risks that could negatively impact the project's completion and success. Auditors, therefore, should evaluate the following aspects:

Is there a risk methodology? If so, what is it, what risks are taken into consideration, and how are risks ranked and prioritized?
Is risk management performed differently based on the project's size and criticality?
Are there contingency and mitigation plans?
How often are risks reassed?
Who makes risk treatment decisions?
What follow-up and monitoring mechanism is in place?

Quality Control and Testing

Another important aspect of overall project management is the quality processes. The IT project management team may decide to adopt different globally accepted quality standards — such as the ISO 9001 Standard, Six Sigma, or CMMI, or a combination of these — to deliver a high-quality project.

The most important aspect of quality control is testing the application, which usually entails dedicated teams and specialized tools in larger projects. Common testing phases include:

The design review, a review of the tool's high-level design to ensure it meets user requirements.
Module testing at the module level to ensure it meets functional specifications.
Load testing to ensure the application functions in environments with a large number of users and transactions.
Integration testing to determine how application modules integrate with other modules or systems.
Regression testing to ensure modifications and fixed bugs don't result in the application loss of functionality.
Source code reviews, which consist of automated or manual code reviews to ensure they adhere to coding guidelines and security requirements.
User acceptance testing, the final stage of testing before deployment, to determine the user's satisfaction with the tool.
Post-implementation reviews to determine if the delivered system meets user requirements.

As part of the quality control and testing phase, auditors need to review the following:

During which phases of the project's execution should quality checks be in place, and how effective are these checks?
During which phases of the project's execution are quality checks in place?
Can the number and type of quality checks be modified based on the project's complexity and criticality?
Are thresholds defined for an acceptable percentage of defects?
Is a root-cause analysis performed when thresholds are exceeded?

When answering these questions, auditors need to keep in mind that the sooner defects are noted in a project, the lower the cost of fixing them. In fact, the cost of fixing defects rises exponentially as the project moves from the design phase to the development, testing, and deployment stages. For instance, the cost of fixing a defect introduced in the requirements stage when discovered at post-release phase is 10 to 100 times the cost of fixing the defect during the requirements stage.

Time Introduced	Time Detected				
	Requirements	Architecture	Construction	System Test	Post-release
Requirements	1	3	5-10	10	10-100
Architecture	-	1	10	15	25-100
Construction	-	-	1	10	10-25

Table 1. The cost for fixing a defect found at a particular stage based on its first occurrence (Source: *Code Complete*, 2004, 2nd edition)

Finally, auditors should perform a quantitative analysis to determine the number of defects discovered at each stage of the project's life cycle versus the total output of the IT department using a metric that is based on the project's size. Auditors also should review how soon and how effectively user-reported problems are resolved.

Delivery

The final stage in the project management life cycle is the product's delivery and sign-off. In this stage, auditors must

assess:

- The delivery process. This evaluation differs based on the type of project (e.g., was the product developed in-house or purchased from an external vendor or is it an infrastructure upgrade)?
- How user sign-off is obtained.
- The user and technical documentation supplied with the product.
- User feedback on the project.
- How the feedback was processed to improve the project's execution.

By proactively participating in each of these stages, auditors will be able to significantly improve the quality and effectiveness of the IT project throughout its entire life cycle.

MOVING FORWARD

Strong project management practices are critical to the successful execution of IT projects and, consequently, to the overall competitiveness of any organization. Periodic audits of the project management process ensure that systemic flaws are identified and fixed and the process is improved. As a result, every aspect of the project management life cycle is equally important and must be reviewed thoroughly.

For more information, auditors should consult the following resources:

- The Project Management Institute's Web site, which has a number of resources for project managers.
- Wikke41's Project Management Best Practices page.
- The Project Management Auditing Guide, available on Audinet.org.
- The Treasury Board of Canada's Project Management Audit Web page.
- ProDetec's Project Management Processes and Quality Checklist.
- ISO's 10006: 2003 Standard, Quality Management Systems - Guidelines for Quality Management in Projects.

KK Mookhey is the founder and principal consultant of NII Consulting, an IT security consulting firm in Mumbai, India, that offers ethical hacking, security auditing, ISO 27001, business continuity management, and security implementation services. Under his guidance, NII Consulting also builds software for auditors and security professionals. Mookhey has worked on research projects for ISACA and has published several articles and white papers. He also has led teams on numerous security audit and implementation assignments and has trained people from the Big Four accounting firms and Fortune 500 companies on IT security issues.