

Audit Your New EHS Software System

A post-implementation audit of the environmental, health and safety management information system evaluates how well the software meets user needs and its value to the organization.

JILL BARSON GILBERT, QEP
LEXICON SYSTEMS, LLC

JUST ABOUT EVERY BUSINESS, FROM SMALL to large, uses some type of software to automate environmental, health and safety (EHS) processes. Most organizations focus on implementation and do not spend enough time planning, developing evaluation criteria and success metrics, or performing a quality check after implementing new EHS software.

A post-implementation audit (PIA) is a thorough evaluation of the benefits of the software solution. A PIA can quantify the tangible benefits, such as the changes in return on investment from the original business case and direct savings realized as a result of implementing the solution. A PIA can also identify intangible benefits, such as improved communications, more-consistent data, easier

access to data, improved data sharing among different groups, more-effective environmental management systems, and improved regulatory compliance. This article offers advice for conducting successful PIAs.

Why audit an EHS management information system?

From an audit perspective, EHS systems are no different from other management information systems (MISs). Organizations that invest significant resources on information technology (IT) should ensure that the systems add value and serve their intended purpose.

According to a recent *CIO Magazine* article, only 20% of IT shops in the general population perform post-implementation audits. Yet, "PIAs are among a resourceful company's best tools for proving the value of high-cost, mission-critical IT investments and for gleaning project management best practices, which CIOs [chief information officers] can then apply to subsequent projects. Companies ... have found ways to overcome political and resource hurdles to make audits a routine project management practice. They've figured out the best timing for audits, who should conduct them, how to make the findings actionable and how to

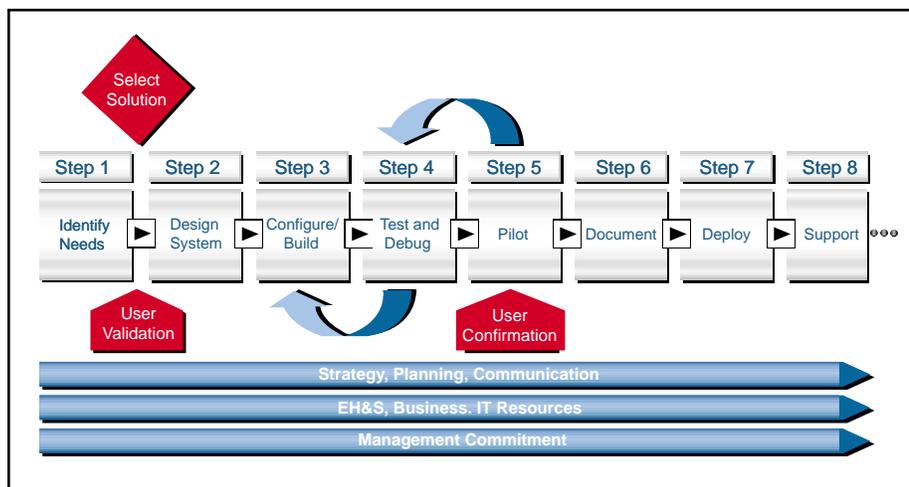


Figure 1. Lifecycle of an MIS project.

incorporate learning back into project practices. (1)”

The 80% of companies that do not conduct PIAs blame the time required to conduct the audits, the drain on resources, and the need for good documentation throughout the entire system lifecycle. (Other reasons include fear that the audit results will reflect poorly on them, and that internal politics stand in the way.)

In Step 1 of the system lifecycle (Figure 1), a business analyst works with a cross-functional team of EHS, IT, management and user representatives to identify stakeholder needs and translate them into detailed requirements. These business requirements carry through the system design, configuration, testing and pilot phases (Steps 2–5) and provide the foundation for the documentation (Step 6). In effect, the requirements developed in the first step serve as the basis for acceptance of the implementation from a “features and functionality” standpoint. After software implementation (Step 7), as they provide ongoing user support (Step 8), the help-desk staff document the need for system enhancements or “fixes,” and the cycle begins again.

Three components must support this lifecycle: strategy, planning and communication; application of EHS, business and IT resources; and management commitment. These three components are essential to the success of a PIA.

The volume and complexity of EHS data, coupled with complex reporting requirements, make a good case for performing a PIA. Periodic audits of the EHS management information system (EMIS) can detect problems in the business processes that generate the data, as well as potential errors due to the number of parties that handle the data.

PIA basics

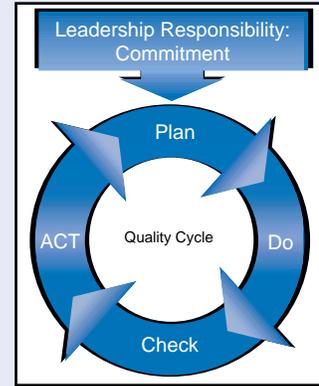
In concept, an MIS audit is much like any other audit — it checks the performance of the system against a set of metrics. A PIA is just that — an audit of a computerized data-management system conducted after the system is fully operational, usually after it has been “road tested” for a while.

The audit team should conduct the audit using predefined criteria. Developing a systems scorecard up-front — defining the project’s objectives, its approach, how IT, business areas and management will be involved, and the expected costs and benefits — can minimize surprises later when the PIA is performed.

The makeup of the PIA team varies from one organization to another. It is good business practice to select an independent party (one not involved in the implementation) to lead the team. The audit team should include some IT staff and repre-

PIA and the Plan-Do-Check-Act Cycle

Management information systems are, in effect, automated management systems. Organizations that embrace quality management systems (ISO 9001) and environmental management systems (ISO 14001) standards understand that audits are part of the Plan-Do-Check-Act cycle of continuous improvement.



An overwhelming proportion of software implementations fail due to poor (or no) planning and poor implementation. Organizations can help ensure success by applying the continuous improvement cycle to their EMIS as follows:

Leadership commitment. The organization must visibly demonstrate management commitment before embarking upon a systems initiative. Since EHS data come from all aspects of the enterprise, leadership commitment is a significant element.

Plan. At this stage, the organization plans the system, incorporating EHS requirements to meet business objectives. It also defines success metrics that can serve as audit criteria.

Do. The EMIS is implemented during this phase. Users begin to employ the system to automate day-to-day tasks and the production of management reports. System rollout is an iterative process that includes a series of system and user-acceptance tests.

Check. Management systems that leverage information technology are dynamic. Based on the predefined success criteria, the organization should evaluate the EMIS after implementation to verify its value to the business.

Act. Based on the audit findings, adjustments are made to the system. These might include changes to the way users employ the software, changes to the software itself, or technology upgrades.

sentatives of various business units who were members of the project implementation team, as well as some IT and/or subject matter experts who were *not* part of the implementation team. Software vendors may participate either as team members or in audit interviews; they and their clients can benefit

from lessons learned and recommendations for improvements to the software and its implementation.

Auditors should ask questions in five topic areas (2):

- system functionality
- system security
- the implementation process
- post-implementation issues
- results.

System functionality

System features and the resulting functionality are the elements most apparent to IT, business management and users. If the system works well, people are happy. If the system does not work well, the IT department and business management quickly hear of user discontent.

The PIA should ask how the system works. Does the system effectively automate processes that were previously done manually? Is the system user-friendly, and do people use the system? Does it need enhancements, such as additional modules, inputs or outputs, to serve its intended purpose?

System security

Vulnerability to corporate espionage, malicious hacking and the introduction of commercial software via the Internet make security concerns more important than ever. System security can refer to the physical security of the hardware (*i.e.*, the servers that house the software application), access to the software by users and system administrators, and secure data-backup and -recovery systems.

The PIA should evaluate whether the system has adequate physical security, as well as security to control access to the software. Who can access the software, how can they access it, and what types of user permissions do they have? Are the data protected from intrusion? Is there a method of tracking who has created or updated the data? How are data backed up, how often, and where are backups stored?

The implementation process

Because the cost and resources applied to implementation can far exceed the cost of the hardware and software applications, a PIA that includes questions on the implementation process can document valuable lessons learned that can be applied to future projects. PIA questions in this area are similar to a project “post-mortem” and should address people, process and technology issues.

People. Was management support for the project evident? Were the right people (EHS, operations, management, IT) involved in the implementation? Were they adequately trained on the software, and did they have the appropriate skills? Was the appropriate staffing level applied to meet project peaks and valleys? Did users and system administra-

tors receive adequate training on how to use the system?

Process. What went well? What did not go well, and what was the root cause? Were the project scope, schedule and budget well-planned to allow for success? What methodology was used, and how well did it work? Was the implementation completed on-time and on-budget? What kind of implementation documentation was provided?

Technology. Were the appropriate IT tools available to allow the team to implement the software? Was hardware or software failure a problem?

Post-implementation issues

As mentioned earlier, an MIS is dynamic. It requires ongoing support and maintenance to remain effective.

Appropriate PIA questions in this area include: What type of help-desk system was in place immediately after the system rollout? What help-desk system will be in place as the system and its users mature? What is the process for logging problems? Have system enhancements been made? How are system changes approved and tracked?

Results

The bottom line is whether the system performs as intended. In this portion of the PIA, the auditors evaluate the system against the predefined project objectives described in the business case. Questions might address metrics such as ROI and other quantifiable benefits, as well as less-tangible benefits.

Ten tips for performing PIAs (2)

1. *Commit to continuous improvement.* Be willing to use what you learn to make the system perform better and add value to the organization.

2. *Get the right people involved* — management, EHS, IT, operations and business representatives; internal and external resources; software vendors; and independent consultants as needed.

3. *Select the right projects to audit.* Choose a project that uses technology that is expected to be around for a while, rather than something about to be phased out. Select projects that have senior management support, and those where a PIA can truly add value. Start with a small project with clearly defined business objectives, where you can show conclusive results.

4. *Time the audit properly.* Select a system that has been deployed long enough to identify typical “new system” issues that often result. In addition, schedule the audit so that the team and those being audited can spend adequate time to do a thorough job.

5. *Collect adequate documentation.* Gather facts to support findings, such as completed questionnaires, notes on

discussions with users and system administrators, and copies of methodologies (*e.g.*, the methodologies used for gathering business requirements, project management, implementation, project documentation). Ask for copies of the business case and expected benefits; the project schedule, milestones and deliverables; business and technical requirements; changes to the project plan; and cost data.

6. *Collect quantifiable results* — the more objective, the better. Use the defined objectives in the business case, as well as the detailed business requirements, as your guide. But even though objective results are good, do not discount feelings, because “people issues” are a significant contributor to the success of an implementation.

7. *Act on the audit findings.* Also have a mechanism in place to track and communicate actions to stakeholders.

8. *Focus on solutions, not on placing blame.* Focusing on solutions gets the team involved in improvements that can help them better use the system.

9. *Share and apply lessons learned.* The identification and use of best practices (and identification and avoidance of worst practices) will aid continuous improvement of the system being audited, as well as other systems.

10. *Incorporate PIAs as part of your IT systems culture.* The implementation is not complete when the system “goes live.” Periodic audits are part of the Plan – Do – Check – Act continuous improvement cycle. 

Literature Cited

1. **Levinson, M.**, “It Ain’t Over ... Until You Do The Post-Implementation Audit,” *CIO Magazine* (Oct. 1, 2003).
2. **Gilbert, J. B.**, “Post Implementation Actions,” IT Insight column, *EM*, Published by the Air and Waste Management Association (Dec. 2003).

JILL BARSON GILBERT, QEP, is president and founder of Lexicon Systems, LLC, headquartered in Houston, TX (E-mail: jbgilbert@lexicon-systems.com; Website: www.Lexicon-Systems.com), where she consults to corporate clients, software companies and investment firms in four key areas: information systems and information technology; business planning and strategy; product and services marketing; and project management and execution. She has more than 25 years of practice in industry, consulting and software/services product management. Previous positions include director of product management for Oracle Corp.’s EHS applications, director of strategy for T3, Inc., and director of EHS management information systems for InteGreyted International, LLC. Previously, she had a long EHS management consulting career with Pilko & Associates, Inc., after starting her environmental and industrial hygiene career with Diamond Shamrock Corp. She earned an MS in environmental management from the Univ. of San Francisco and a Bachelor of Arts from Miami Univ., and completed the Rice Program for Managers; in addition, she is a Qualified Environmental Professional (QEP). She has been an active member of the Air & Waste Management Assn. (A&WMA), where she was vice president and board member. She currently serves on the A&WMA Editorial Advisory Committee, and writes the IT Insight column in the organization’s *EM* magazine.