

Auditing EH&S Software Systems After Implementation

Control # 666

Prepared by Jill Barson Gilbert, QEP

President, Lexicon Systems, LLC, P.O. Box 890433, Houston, TX 77289-0433

JBGilbert@Lexicon-Systems.com

ABSTRACT

Just about every business, from small to large, uses some type of software solution to automate environment, health & safety (EH&S) processes. Most organizations direct their energies towards implementation and do not spend adequate time planning, developing evaluation criteria and success metrics or performing a quality check after implementing an EH&S software solution. After spending thousands, or sometimes millions, of dollars on information technology, organizations should ensure that these resources were well spent, that the system meets user needs and that it adds value to the organization.

A Post Implementation Audit (PIA) is a thorough evaluation of the benefits of the software solution. A PIA can show the “hard” benefits such as the changes in Return on Investment from the original business case and savings as a result of implementing the solution. A PIA also can show the “soft” benefits such as improved communications, more consistent data, easier access to data, data sharing among different groups, more effective environmental management systems and improved regulatory compliance.

Organizations that embrace Quality Management Systems and Environmental Management Systems standards understand that audits are part of the Plan – Do – Check – Act cycle of continuous improvement. Information Technology (IT) systems are dynamic, and should be evaluated after their implementation to verify their value to the organization. Those that develop a systems scorecard up front—define project objectives, approach, how IT, business areas and management are involved, expected costs and benefits—can minimize the surprises when a PIA is done. This paper provides advice for conducting successful PIAs.

INTRODUCTION

Just about every business, from small to large, uses some type of software solution to automate environment, health & safety processes. Most organizations direct their energies towards implementation and do not spend adequate time planning, developing evaluation criteria and success metrics or performing a quality check after implementing an EH&S software solution. After spending thousands, or sometimes millions, of dollars on information technology, organizations should ensure that their resources were well spent, that the system meets user needs and that it adds value to the organization.

A PIA is a thorough evaluation of the benefits of the software solution. A PIA can show the “hard” financial benefits such as Return on Investment (ROI) and “soft” organizational and image benefits such as improved compliance.

WHY AUDIT EH&S MANAGEMENT INFORMATION SYSTEMS?

An Audit is An Audit

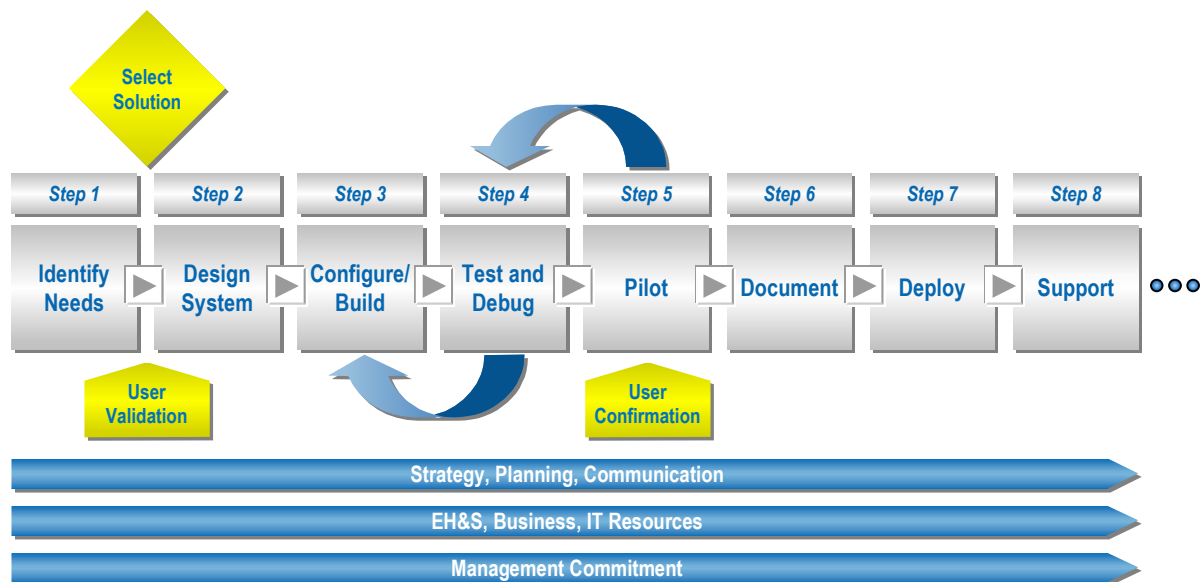
From an audit perspective, EH&S systems are no different from other management information systems. Organizations that invest significant resources on systems should ensure that the systems add value and serve their intended purpose. According to a recent *CIO Magazine* article only 20 percent of IT shops in the general population perform post-implementation audits.

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 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 incorporate learning back into project practices.”¹

Why Not Audit?

Why not audit EH&S IT systems once they are implemented? The 80 percent 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 systems life cycle (Figure 1).

Figure 1. Systems Life Cycle



In Step 1 of the Systems Life Cycle, a business analyst works with a cross-functional team of EH&S, IT, management and users to identify the stakeholder needs and translate these into detailed requirements. These business requirements carry through the System Design, Configuration, Testing and Pilot (Steps 2-5) and provide the backbone for the Documentation (Step 7). In effect, the requirements developed in the first step serve as the basis for acceptance of the implementation from a “features and functionality” standpoint. Following Software Deployment (implementation) in Step 7, help desk staff document the need for system enhancements or “fixes” and the cycle begins again. Three components must support this Life Cycle: 1) strategy, planning and communication; 2) application of EH&S, Business and IT resources; and 3) management commitment. These three components are essential to the success of a PIA.

Other reasons why companies do not perform PIAs are because they fear the audit results will reflect poorly on them or because of internal politics. Organizational politics can pose a real challenge and can work against the benefits of even the most well-planned and well-executed audit.

EH&S Regulatory Compliance Initiatives

It makes good business sense to audit a management information system that stores data needed to demonstrate compliance. The volume and complexity of EH&S data, coupled with complex reporting requirements, present a good case for a PIA. Periodic audits of the EH&S Management Information System (EMIS) can detect problems in the business processes that generate the data, and potential errors due to the number of parties that “touch” the data. For example:

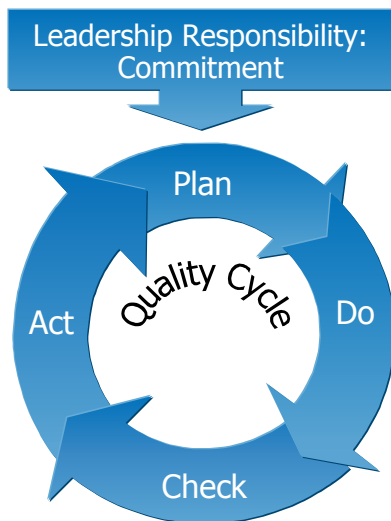
- » The federal Title V air permit program requires a “Responsible Official,” typically at the senior management level, to document compliance with every requirement in the permit. It follows that this Responsible Official wants to know that the information used to develop this semiannual compliance certification is accurate and complete.
- » The Occupational Safety and Health Administration (OSHA) Hazard Communication program requires companies that manufacture or distribute chemicals to provide current Material Safety Data Sheets (MSDS) to their customers. Imagine the product liability if there is not a method of periodically auditing the MSDS management system to ensure that the MSDS are accurate, complete, and up-to-date.
- » Emergency Planning and Community Right-to-Know Act (EPCRA, or SARA Title III) requires annual Tier Two reports of the quantity and location of hazardous substances stored onsite. This law also requires annual Toxic Release Inventory (TRI) reports that quantify emissions of hazardous substances to air, water, land; for processing as fuel; or for recycling. Preparing a TRI report requires data from throughout the business enterprise—purchasing, accounting, research & development, manufacturing, distribution, etc.

Voluntary EH&S Initiatives

ISO 9001 and ISO 14001

Management Information Systems in effect, are 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 (Figure 2).

Figure 2. Continuous Improvement Cycle



An overwhelming percent of software implementations fail, due to poor (or no) planning and poor implementation. Following the Continuous Improvement Cycle can help organizations ensure the success of their system implementation. The following five points explain how this cycle applies to EH&S management information systems.

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

Plan. At this stage the organization plans the system, incorporating EH&S requirements to meet business objectives. The organization also defines success criteria that can serve as audit criteria.

Do. The organization implements the EMIS, hopefully according to plan, incorporating the EH&S business requirements. Users begin to employ the system to automate day-to-day tasks and management reports. System rollout is an iterative process, with a series of system and user acceptance tests.

Check. Management systems that leverage information technology (IT) are dynamic. Organizations should evaluate EH&S management information systems after implementation to verify their value to the organization. Audits occur during the “Check” phase of the Continuous Improvement Cycle, based on a predefined set of success criteria.

Act. Based on audit findings, the organization adjustments to the system, which might include changes to the way users employ the software, changes to the software itself or technology upgrades. And the cycle continues.

Responsible Care[®] Management System

The American Chemistry Council (ACC) requires its members to subscribe to their Responsible Care program. ACC member companies must have their Responsible Care Management System (RCMS) in place by the end of 2004.

RC 14001

The Responsible Care 14001 initiative allows ACC member companies to undergo a combined Responsible Care Management System audit and an ISO 14001 Environmental Management Systems Audit.

POST IMPLEMENTATION AUDITS

What is a PIA?

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

Ideally, the audit team conducts the audit using predefined criteria. Organizations that develop a systems scorecard up front—define project objectives, approach, how IT, business areas and management are involved, expected costs and benefits—can minimize the surprises when a PIA is done.

Who Should Conduct the PIA?

Organizations differ regarding the makeup of the PIA team. Audit team members can come from one or more of the following groups:

- IT members of the project implementation team
- Business members of the project implementation team
- IT and/or subject matter experts independent of the project implementation team
- Internal audit department staff
- Software vendors

It is good business practice to have an independent party (one not involved in the implementation) lead the audit team. Ideally, the audit team will include some IT and business members of the project team. Sometimes it makes sense for software vendors to participate as team members or in audit interviews. Both software vendors and their clients can benefit from lessons learned and recommendations for improvements to the software and its implementation.

What Questions Should the Auditors Ask?

In her article on Post Implementation Audits, Levinson recommends that the auditors ask questions in five topic areas:²

1. System Functionality
2. System Security
3. Implementation Process
4. Post Implementation Issues
5. Results

System Functionality

System features and the resulting functionality are the elements most apparent to IT, business management and end-users. If the system works well, people are happy. If the system does not work well, the IT department and business management rapidly hears of user discontent. The PIA should ask, how does the system work? Does the system effectively automate previously manual processes? Is the system user-friendly, and do people use the system? Does the system need enhancements, such as additional modules, inputs or outputs to serve its intended purpose?

System Security

Today, with corporate espionage, malicious “hacking” and the introduction of commercial software applications delivered over the Internet, security concerns are greater than ever. System security can cover the physical security of the hardware, i.e., 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 ask, does the system have adequate physical security in addition to security that guards 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, and 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?

Implementation Process

Since 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 to apply 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 (EH&S, 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? Were users and system administrators adequately trained 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 it to be successful? What methodology was used, and did it work well? 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 there a problem with hardware or software failure?

Post Implementation Issues

As mentioned earlier, a Management Information System is a dynamic entity. It requires ongoing support and maintenance to remain effective. Appropriate PIA questions in this area include, what type of help desk system is 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 measure the system against predefined project objectives described in the business case. Questions might address metrics such as Return on Investment (ROI), hard benefits and soft benefits.

TEN TIPS FOR POST-IMPLEMENTATION AUDITS³

- ☑ *Commit to continuous improvement* – be willing to use what you learn to make the system perform better and add value to the organization.
- ☑ *Get the right people involved* – management, EH&S, IT, operations and business representatives; internal and external resources; software vendors and independent consultants as needed.
- ☑ *Select the right projects to audit* – select a project that uses technology that you expect to be around for a while vs. something about to be phased out. Select projects that have senior management support, and those where a PIA truly can add value. Start out with a small project with clearly defined business objectives, where you can show conclusive results.
- ☑ *Time the audit properly* – select a system that has been deployed long enough to identify typical “new system” issues that often result. Also, time the audit so that the audit team and those being audited can spend adequate time to conduct a thorough audit.
- ☑ *Collect adequate documentation* – collect facts to support findings, such as completed questionnaires, notes on discussions with users and system administrators, copies of methodology. Ask for copies of the business case and expected benefits, copies of the project schedule, milestones and deliverables; business and technical requirements; changes to the project plan; and cost data.
- ☑ *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 guideline. While objective results are good, do not discount feelings, as “people” issues are a significant contributor to the success of an implementation.

- ☑ *Act on audit findings* – not only act on findings, but also have a mechanism in place to track and communicate actions to stakeholders.
- ☑ *Focus on solutions, not on placing blame* – focusing on solutions gets the team involved in improvements that can help them better use the system.
- ☑ *Share and apply lessons learned* – the identification and use of best practices (and “worst practices”) will aid continuous improvement of the system being audited, as well as other systems.
- ☑ *Incorporate PIAs as part of your systems methodology* – the implementation is not complete when the system goes “live,” and periodic audits are part of the Plan – Do – Check – Act Continuous Improvement Cycle.

CONCLUSIONS

Organizations that embrace Quality Management Systems and Environmental Management Systems standards understand that audits are part of the Plan – Do – Check – Act cycle of continuous improvement. IT systems are dynamic, and should be evaluated after their implementation to verify their value to the organization. Those that develop a systems scorecard up front—define project objectives, approach, how IT, business areas and management are involved, expected costs and benefits—can minimize the surprises when a PIA is done.

Organizations that are serious about audits and willing to the time and money can benefit from their investment. Lessons learned during the PIA can make the system work more effectively, perhaps extending its useful life. In addition, best practices identified during the audit can help to enhance the probability of success of future system implementations. In both cases, the organization and the system users profit.

REFERENCES

1. Levinson, Meredith, “It Ain’t Over... Until You Do The Post-Implementation Audit,” *CIO Magazine*, 01 October 2003.
2. Ibid. This paper adds recommendations based on the author’s experience with business requirements analysis, software development and software implementation.
3. Gilbert, Jill Barson, “Post Implementation Actions,” IT Insight column, *EM*, December 2003. This paper expands upon the checklist in the column.

KEY WORDS

Audit, EH&S Management Information System, EIMS, EMIS, Environmental

Information Management System, Environmental Management Information System,
Environmental Management System, Information Technology, Management Systems,
Management Information Systems, Methodology, PIA, Post Implementation Audit,
Project Management, Project Management Methodology, Quality Management Systems