ERP System Audit a Control Support
For Knowledge Management

Cristian AMANCEI, Traian SURCEL
Academy of Economic Studies, Bucharest, România
cristian.amancei@ie.ase.ro, traian.surcel@ase.ro

The ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, SCM, Financials, Projects, Human Resources and CRM; the audit of this systems is necessary in order to give reasonable assurance to the company on its core system. Obtained evidence evaluation can ensure whether the organization's IT&C system safeguard assets, maintains data integrity, and is operating effectively and efficiently to achieve the organization's goals or objectives. The audit process respecting the methodology based on: gathering information and plan; obtaining an understanding of internal controls; performing test of controls and substantive tests, develop a control support on quality of flow of information and knowledge from formal perspective, for Knowledge Management in large enterprises.
Keywords: *ERP systems, IT audit, information quality, knowledge management.*

Introduction

Enterprise resource planning ERP is the planning of how business resources materials, employees, customers etc. are acquired and moved from one state to another.

An ERP system supports most of the business system that maintains in a single database the data needed for a variety of business functions such as Manufacturing, Supply Chain Management, Financials, Projects, Human Resources and Customer Relationship Management.

Common database can allow every department of a business to store and retrieve information in real-time. The modular software design permits to a business to select the modules they need, mix and match modules from different vendors, and add new modules of their own to improve business performance.

IT Audit

IT system audit can generally be described as the process of obtaining and evaluating evidence to determine whether an IT system safeguards the organizational assets, uses resources efficiently, maintains data security and integrity and fulfils the business objectives effectively. During the audit, the auditors look for evidence that indicates:

• The organization has designed effective controls to address their compliance requirements and that there are no design deficiencies.

• The organization consistently applies the controls they have designed and that there are no operational deficiencies.

IT audit process normally involves the following steps:

• Planning
• Evaluation of controls
• Evidence collection and evaluation
• Reporting and follow up

Proper planning assists the auditor in:

• The direction and control of his work;
• Highlighting critical areas;
• Allocation of audit resources towards more important areas;
• Setting time frame and targets for review work;
• Obtaining sufficient, reliable and relevant audit evidence and
• Subsequently aid the auditing in decision making.

When planning the IT audit work, the auditor should take into account the type of the audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability.

Among the things to be considered are the independence and qualification of the pro-

vider of the audit evidence. For example, corroborative audit evidence from an independent third party can sometimes be more reliable than audit evidence from the organization being audited.

Physical audit evidence is generally more reliable than the representations of an individual.

The types of audit evidence, which the auditor should consider using, include:

• Observed process and existence of physical items

• Documentary audit evidence (including electronic records)

• Analysis(including IT enabled analysis using CAATs)

The report should be complete, accurate, objective, convincing, and as clear and concise as the subject permits. The report should include all significant audit findings. When a finding requires explanation, the auditor should describe the finding, its cause and its risk. IT audit is not effective if audits are performed and reports issued, but no follow-up is conducted to determine if audited organization has taken appropriate corrective action. The auditor should have a follow-up program to determine if agreed corrective actions have been implemented.

ERP Systems audit
The ERP systems audit is difficult to be performed, due to system complexity and implementation customizations required by the business profile and company management. In order to perform this audit we appreciate that the auditor has to define the major areas from the ERP system important on the audit mission and the prerequisites requests necessary for carrying out an audit for assessing security and privacy issues in ERP.

From the prerequisites requests we have selected the following:

• Understanding the business

• Understanding the enterprise structure

• Obtain access to the system

Understand the business
Understand the business and the risks specific to that business and its operations. This is the first basic step, not only in ERP audit, but

in any kind of audit.

Understand the enterprise structure
Understand the enterprise structure. The complexity of ERP arises from the fact that it attempts to encompass the entire business cycle of the enterprise, covering all major functions and all parts of the organization in its wake, including financial accounting, human resources and management information. The mapping of the various organization units is reflected in the enterprise structure in the ERP. An accurate understanding of the enterprise structure is the first step to carrying out an audit.

Obtain access to the system
Obtain access to the system. The audit of an ERP cannot be done by having someone generate reports and show them to the auditor. The information systems (IS) auditor should verify the various settings and data in the system by seeing them in the "live" system. For this, the auditor should obtain a user ID in the production system with read-only access to all modules and features. Needless to say, the auditor would need to have a good grasp of SAP and use the access with due care.

Discussing about the ERP audit, we believe that it's important to analyze the major areas of audit:

• Evaluating access control

• User ID evaluation

• Evaluation of configurations relating to business processes

• Change management

• Interfaces

• Privacy

Evaluating access control - all the data in the ERP are in one single database. Access to the data has to be secured not only at the application level, but also at the operating system, database and network levels through suitable controls. The IS auditor will review the network, OS and DBMS before evaluating the access controls in the application.

Access control evaluation in an ERP is a complex exercise and requires good skills with the particular ERP. Many ERPs use the concept of roles, assigning standard authorizations to the roles and attaching the roles to

users as per their job descriptions and duties required to be performed. Each role properties and the users defined for each role will be verified during the audit.

User ID evaluation - for auditing access control a list of authorized users and their privileges will be obtained. The IS auditor will also obtain the list of standard roles and the authorizations required for the roles.

The next step is to ascertain that all the authorized users have the appropriate privileges in line with their job responsibilities. To do this, the auditor should examine the roles that have been assigned to the various users, and ensure that the roles are in sync with their current job responsibilities. The next step is to identify from the system the authorizations and privileges associated with each of the roles in use, to ensure that roles, as defined in the system, are in line with what the role is expected to be.

It is good to approach access control evaluation from the perspective of critical functions and activities that would be required to be carried out only by specific authorized personnel. This would require a thorough knowledge of the ERP system to identify certain critical transactions. The IS auditor will query the system to determine the users who have authorization to execute such activities and options. The IS auditor will evaluate whether the list is aligned with the approved policies of the company.

Verification and evaluation of configurations relating to business processes - the process flow in every business activity and the possible options for carrying out these activities are decided by the configurations in the system.

Such configurations exist in every process and module. The best way to do this is to approach it from the business risk perspective and identify the configurations pertaining to those processes. Each of these configurations can be seen on the system by executing certain commands or following a certain path in the menu.

An audit program that lists these and the possible values and options of these are usually used to carry out this evaluation.

Change management - the way modifications are done to the programs and the configurations, the effective segregation between the development and production environments, the processes for testing, quality assurance and migration need to be reviewed by the auditor.

Interfaces - because ERPs invariably need to send or receive data from other systems. Interfaces can be simple batch uploads of data or real-time data movement from multiple systems to and from the ERP through an integration middleware platform. An interface has the potential to become a weak point that can compromise security. Audit scrutiny of interfaces is one of the important aspects of ERP security reviews. Controls should exist to validate data before upload and verify accuracy and integrity through control totals and logs

Privacy – because ERPs are such a large repository of different kinds of data that they can impact privacy issues in a significant way. Most ERPs have a human resources and personnel module, and such modules handle a lot of data about the employees of the company. The ERP can also hold information about customers, suppliers and partners.

Conclusion

There are ways to make the audit process more efficient and less difficult. These include:

• Develop metrics and procedures for different areas of the audit process in order to improve the efficiency in addressing those areas.

• Software development in order to permit automatic data extract and analysis, this measure will reduce the time allocate for system review and will improve the accuracy of the results.

• Take advantage of IT controls framework that are already developed, by defining own frameworks to address different cultural and business specifications.

Bibliography

[GRAB08] Bernard GRABOT, Anne MAYERE, Isabelle BAZET **ERP Systems**

and Organisational Change: A Socio-technical Insight, Springer Verlag Publishing House, 2008

[GRAN08]   Charles Le GRAND, Dan SAREL **Database Security, Compliance and Audit**, Information Control Systems Journal, Vol. 5, 2008

[ITGI4.1]   IT Governance Institute **Control Objectives for Information and related Technology**, v4.1, 2007

[IVAN05]   Ion   IVAN,   Gheorghe NOŞCA, Sergiu CAPISIZU **Auditul sistemelor informatice**, Editura ASE, Bucureşti, 2005

[KENT08]   Anderson KENT **A business Model for Information Security**, Information Control Systems Journal, Vol. 3, 2008

[LAUD07]   Kenneth   LAUDON,   Jane LAUDON **A Essentials of Management Information Systems**, Prentice Hall Publishing House, 2007

[SURC07]   Traian   SURCEL,   Cristian AMANCEI **The Information Security Management System, Development and Audit**, Proceedings of 8th International Conference on Informatics in Economy, IN-FORMATICS IN KNOWLEDGE SOCIE-TY, 17-18 May, 2007, Bucharest, ASE Publishing House

[SURC08]   Traian SURCEL, Ion IVAN, Cristian AMANCEI **The IT Audit – a Major Requirement for the Management Quality and Success in the European Business Context**, Proceedings of 4th International Scientific Conference, EUROPEAN INTEGRATION – NEW CHALLENGES FOR THE ROMANIAN ECONOMY, 30-31 May, 2008, Oradea, University of Oradea Publishing House