

Seradex White Paper

A Discussion of Issues in the Manufacturing OrderStream

Internal Controls, Fraud Detection and ERP

Recently the SEC adopted Section 404 of the Sarbanes Oxley Act. This law requires each annual report of a company to contain

1. A statement of management's responsibility for establishing and maintaining an adequate internal controls and
2. Management's assessment of the effectiveness of the company's internal control structure and procedures for financial reporting.
3. The company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures

Sarbanes Oxley requires that internal controls be extensively documented and this is a significant exercise. This brief review will look at some issues that should be considered in setting up internal controls in an ERP environment.

Internal Controls: reviewing the practices, transactions, procedures and processes used to control the financial transactions and protecting a company's property and assets.

This paper will examine how the internal auditor working specifically with the Seradex ERP system can implement internal controls and detect fraudulent

transactions. The general approach should be applicable to most ERP systems.

What is SERADEX ERP?

Seradex is an ERP application processing data from a database. It offers flexible configuration and security options. Seradex links data in real time across the traditional business functions such as sales-production-inventory-procurement and finance

An important point to note is to realize that Seradex ERP is an application program, like Microsoft Excel or Word. It typically sits between the end user and a database management system (such as SQL Server) and controls the adding, changing and deleting of data from that database.

Seradex ERP is a very flexible system that is configured to meet the organizational needs and requirements. This adds to the complexity of auditing the system because not only do you need to know how Seradex ERP works but also how your company is using Seradex.

One important feature characteristic of the Seradex ERP system is that user access is dependent on the Windows network security setting for each user and group. By setting up groups with highly detailed access parameters users can be easily setup and added to the appropriate group reducing security administration efforts.

Seradex ERP and Internal Controls

Seradex ERP dictates that operational data and financial data are totally integrated. More people are able to enter transactions without review or checking by a supervisor. Many organizations give users very wide access to data without necessarily analyzing specific work requirements.

Note: Without careful consideration this wide access can weaken internal controls by violating the segregation of duties concept.

ERP systems change the role of middle management for transaction review and authorization. Questioning and follow up formerly done by middle managers is commonly reduced when an ERP system is implemented.

There are several implications and considerations to the internal controls possible in Seradex ERP. These can be segregated into the following categories:

- Network Security and User Identities
- User and Group Setup
- Security authorization issues
- Use of Active Directory
- Administrative user management
- Password control
- Customer / Supplier Access
- User Controls
- Server, Network and Firewall controls
- Patch policy on Servers and Workstations

- System Controls
- Reconciliation of control accounts to subsidiary ledgers – Accounts Payable, Accounts Receivable, Inventory, Invoicing, Vendor Invoicing

- Reconciliations of data to external information – bank reconciliation, accounts payable statement reconciliations
- Cost centre and responsibility accounting
- Management review and budgetary control
- Review and authorization of non-routine transactions
- Validation checks
- Validation of data input in particular transactions
- Properly designed and validated reports with authority checks
- Matching of documents prior to “closing out” e.g. purchase order – receiving documentation – invoice
- Master file control
- Independent review of master file changes
- Independent master file creation to transactional responsibilities Identifying redundant master

Auditing for Fraud

Auditors have a responsibility to minimize opportunities by ensuring that adequate internal controls are in place. If internal controls are weak in a particular area the next step would be to consider red flags. A red flag is an indicator that some kind of irregularity is occurring and that something may be wrong. It does not prove that fraud has occurred but if a red flag is identified more detailed transaction examination is required.

Identifying Red Flags

Some example of red flags could include:

- Actual expenses far exceeding budgeted or prior years expenses
- Expenses out of historic norms
- Significant manual entries made to asset and expense accounts
- Addresses, telephone numbers and other data that link employees to vendor master records
- Ratios are not making sense: ex. ratio of overtime expenses to sales,
- Unexplained price increases in material costs (kickback scheme)
- Excessive Inventory quantity and cost adjustments

Manual database queries can be developed to examine the inventory audit trail, adjustment details, phone number and address comparisons of employees and vendors to provide identify further transactions for examination. All transactions in Seradex record the network user who created or changed the transaction as well as time and date stamps.

Accounts Payable in SERADDEX ERP

Purchasing and accounts payable represents a major area for fraud because it results in the physical disbursement of cash to suppliers.

Seradex ERP offers excellent built in tools to avoid fraudulent activity in the accounts payable function:

Seradex offers three ways matching between Purchase Order, Receiving and Vendor Invoicing. This is followed by check preparation. Ideally each of these transactions should be done by separate individuals to ensure

segregation of duties. An invoice voucher can be printed and reviewed for each check over a threshold amount to additional review.

An invoice voucher can be printed for any purchase from a one time vendor or any PO for a "Special" item. Establish procedures on when a vendor master is required. Requiring a PO offers more control than entering a miscellaneous payable directly into A/P as more people have to be involved in the transaction. These transactions need more thorough controls and testing.

Vendor Master File changes should be a separate function from Purchasing to ensure segregation of duties
Duplicate invoice control - the system will review invoices posted to a particular vendor code and highlight whether the current invoice is the same as a previous one.

Fraud Tests in the Accounts Payable Cycle

Some things to test for in this cycle include developing queries for identifying high risk vendors and payments:

- Transactions where the same user created the PO, Receipt and Approved the Vendor Invoice
- PO's where the person changing the PO is different that the person issuing the PO
- Any PO for a non inventory item or service item that is >\$XXX.
- Service expenditures don't involve asset that has to be produced later. This includes expenditures for consulting, advertising or marketing
- Any PO to a one time vendor that is >\$XXX
- Transactions where the Vendor was created by the user issuing the PO

Seradex ERP has challenged the role of internal auditors and it requires auditors to learn new skill sets - some of which are fairly technical and involve directly accessing data in the system.

Security Authorizations

At the heart of internal control is security access to the ERP system. Defined policies on who sets users up and what groups they belong to is critical. Make sure network logs are switched on for full tracking. This allows you to check who logged on at what workstation. Queries can be developed to list all users that logged on to each workstation and at what time. Information on which workstations logged onto Seradex is easily available. These can be correlated to the time of individual transactions in Seradex ERP. These logs will also identify which data files were copied to the local workstations.

Most users are not aware that these capabilities exist.

Severely limit users who are granted administrative rights and ensure users only have access to the information they require. Often a short cut is taken and the easiest answer is to give all personnel very wide access if authorizations are set too narrow, users will require significant Help Desk resources.

Password Control

The system can enforce minimum password lengths and enforce password expiry on a regular basis.

Patch Management Policy

Document the frequency of patch updates for servers and workstations.

Data Access

In these days of DVD burners, USB keys that can hold 1 Gigabyte of data, stringent control over corporate data needs to be established. Unauthorized users could easily take customer lists, sales history, product information and pricing home in their shirt pockets.

Remote Users

Remote users accessing the system through VPN connections need to be securely authenticated.

Seradex Inc.
4460 Harvester Rd.
Burlington, ON
L7L 4X2
Tel: 905-332-5051
mcorker@seradex.com
www.seradex.com

