Title:	*Provenance and Compliance*
Author:	*John Ibbotson*
Version:	*1.0*
Date:	*29th September 2006*
Status:	*Public*

Summary

Businesses have to operate in an increasingly regulated environment where the penalties for breaching regulations can be very severe. Examples of regulated business areas include financial markets, pharmaceutical and food products, import and export of products and services in addition to rules relating to corporate governance. A key component of any compliance regime is the management of internal controls that can be subjected to internal and external audit processes. This paper briefly describes how Provenance may provide a solution to financial auditing as an example of a common internal control process.

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

Members of the PROVENANCE consortium:

- IBM United Kingdom Limited United Kingdom
- University of Southampton United Kingdom
- University of Wales, Cardiff United Kingdom
- Deutsches Zentrum fur Luft- und Raumfahrt e.V. Germany
- Universitat Politecnica de Catalunya Spain
- Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutató Intézet Hungary

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

1 Introduction

All companies are subject to the laws and regulations of the countries in which they operate. These laws may regulate the ways companies perform their operations or be specific to the products and services they provide. Regulations specific to company operations will include for example labour laws which govern their human resource activities, contract law, taxation and regulations that govern how and when they report financial information to their external investor. Compliance to these regulations has become increasingly important in recent years as a response to several major incidents of corporate malpractice.

In the case of regulations specific to products and services, the following are some examples:

1. Approval of drugs by national administrations in the pharmaceutical industry
2. Regulatory processes governing patient data confidentiality in healthcare
3. Regulations governing movement and storage of foodstuffs
4. Regulations governing the management and movement of animals
5. Regulations governing transactions in financial markets

The sources of these regulations are many and varied. They may be defined as part of a country's legal framework or set by a wider community such as the European Union. In either case, there are usually a set of internal control processes that a company or organisation must implement to ensure compliance to the imposed regulations. These controls can then be externally audited to show whether or not the organisation is compliant with the regulations.

In this use case, we consider the subject of financial reporting as an example of regulatory compliance. The COSO organisation (www.coso.org) has identified four internal financial control components that lead to improved financial reporting. These elements are:

1. A Control Environment within a company that is managed by the board of directors and an associated audit committee. It must set the financial management philosophy of the company and demonstrate integrity with a set of ethical values. It should define the company's organizational structure by assigning authority and responsibility and define its human resources policies and procedures.
2. Risk Assessment is a company wide objective which gets devolved into departmental process level objectives. The identification and analysis of financial and other risks has to be a continuous process and is fundamental to the management of change within a company.
3. Information and Communication. All pertinent information must be identified, captured and communicated in a form and timeframe to enable people to carry out their responsibilities. All channels of information both internal and external must be open and transparent.
4. Control Activities. These are policies and procedures that help ensure management directives are carried out and include a range of activities such as:
   a. Approvals authorisations, verifications and reconciliations
   b. Reviews of operating performance
   c. Asset security
   d. Segregation of duties

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

Provenance can be applied in the fourth of the above components in augmenting existing processes by documenting the processes (in this case financial) as they execute. We use the example of entries posted to a company's general accounting ledger to illustrate how this may be achieved.

2 An Accounting Example

The General Ledger is the core component of any company's accounting system. It contains the set of "books" containing records of all the financial transactions that flow through the company and therefore provides a permanent record of the financial history of the company. The General Ledger may contain other sub-ledgers for items such as cash, accounts receivable and accounts payable. All entries posted to these sub-ledgers will be reconciled and visible through the General Ledger account. The set of financial transactions contained within the General Ledger are periodically audited by external auditors who then certify the financial health of a company; the company is then able to report its financial results to external investors.

In addition to the transactions recorded in a General Ledger, companies must also describe the processes they use to update entries in the General Ledger. These transparency requirements are imposed to combat fraudulent transactions that may influence a company's financial state. In this case, an auditor has not only to certify the accounts of a company but also the processes used by the company in generating the accounts.

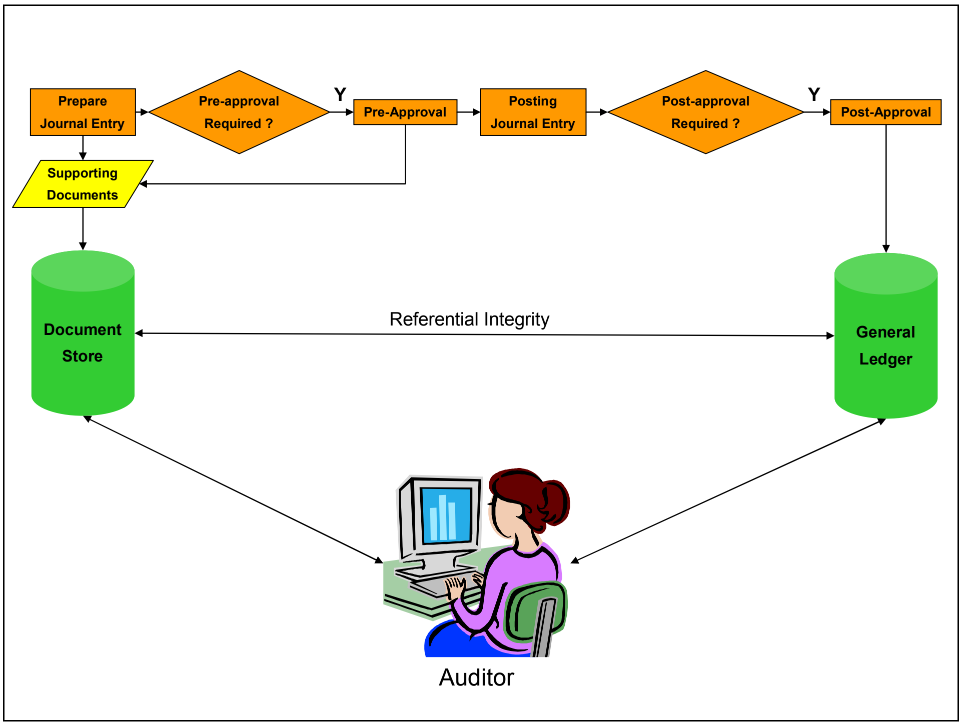

Figure 1 General Ledger entries with Audit

Figure 1 illustrates a business process that may be used to generate transactions in a company General Ledger. In this process, two databases are used. The first is the General Ledger where all financial transactions are recorded. The second is a Document Store where documents supporting the transactions are stored. These supporting documents may include bills of sale, receipts etc. The two databases are linked and referential integrity exists between them allowing entries in the General Ledger to be linked to its supporting documentation and vice versa. The process supporting the

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

General Ledger posting is an approval process where authorised users inspect and approve the updates before they are committed to the databases.

When auditing, an auditor has access to the General Ledger and supporting Document Store. The transactions are sampled and inspected and assuming no discrepancies are uncovered, the auditor can certify the accounts.

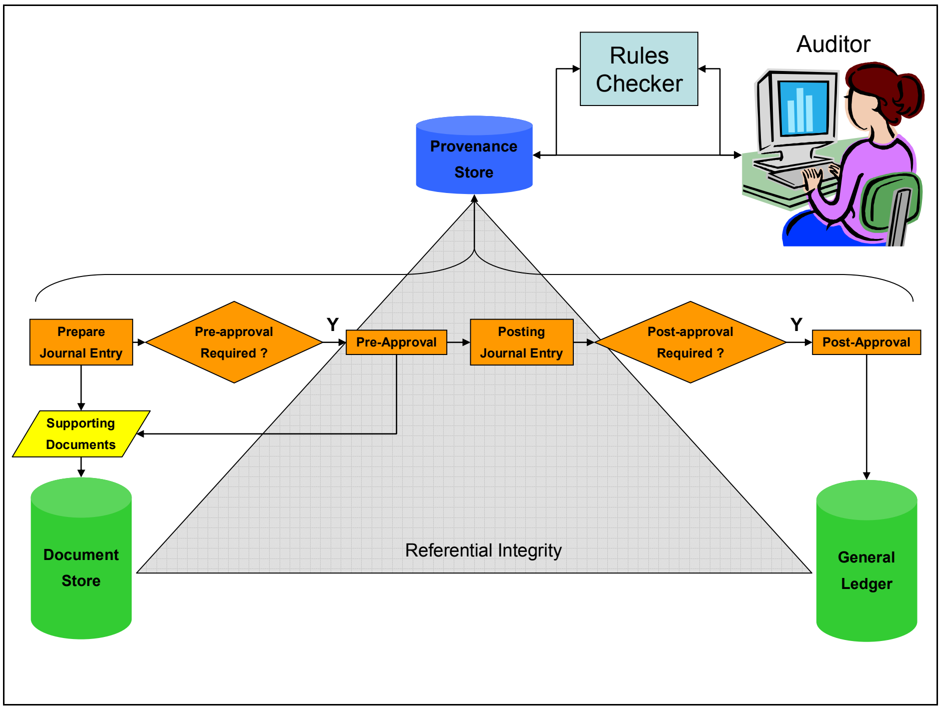

Figure 2 A Provenance Aware Process

Figure 2 illustrates the same process but it is now Provenance enabled. Each component of the accounting process is an actor that documents its execution in the Provenance Store. By including access to the Provenance Store, the auditor can now not only examine the transactions contained within the General Ledger and Document Store, but also inspect the documentation of the processes that created the transactions. In addition to directly querying the Provenance Store, an auditing application may also use a Rules Checker which can check whether a set of compliance rules relating to the accounting process have been violated or not.

The process documentation stored within the Provenance store may include the following information items within the Provenance data model:

1. Identifiers for each General Ledger transaction
2. The roles and identities of users preparing, approving and posting the General Ledger transactions
3. Timestamps recording when the individual process steps took place
4. Codes confirming that each process step completed satisfactorily
5. For security and protection against tampering, the Provenance documentation can be cryptographically signed

With this process documentation, an auditor may pose the following types of queries:

1. For a particular transaction in the General Ledger, did the users approving the transaction have sufficient authority?

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme

2. Were the defined steps in the accounting process followed sequentially?
3. Were the supporting documents for a particular transaction approved at the correct time?
4. Are there any transactions in the General Ledger that were inserted that did not follow the necessary process?
5. Have any transactions been altered since they were first entered into the General Ledger?

3 Conclusion

Companies are subject to a wide range of rules and regulations that apply directly to their internal operations and the products and services they provide. Compliance to these regulations are essential for a company to operate transparently and ethically in their particular markets. They are required to prove compliance to the imposed regulations through internal and external auditing processes.

These processes are usually manual where the auditors sample and inspect the process documentation generated by the company being audited. This is both time consuming and potentially subject to error. Applying the Provenance architecture and methodology to business processes as they execute has the potential to improve the quality of the auditing processes, improve the transparency of a company's compliance to the regulations and provide cost benefits which impact profitability.

The PROVENANCE project receives research funding from the European Community's Sixth Framework Programme