

March 31, 2005

## Enterprise Agility—SOX and Enterprise Information Integration

By Rick Dove, Consultant, UtiliPoint International; Chairman, Paradigm Shift International

Attestation under Sarbanes-Oxley is making new friends of auditors and management. They hang together, now - so to speak. Little consolation for either: honest errors will continue to happen, so will fraud.

The intent of Sarbanes-Oxley (SOX) can be characterized as risk reduction: reduce errors, inhibit fraud, and provide shareholders with transparent equal-access to material knowledge. But implementation is principally procedural controls and documentation, under threat of penalty. The vague parts of SOX are where the real leverage lies: principles of intent, and corporate transparency.

Procedural controls are necessary. Good procedural controls, well documented, may even mitigate liability - somewhat. But procedural controls are passive, and will neither eliminate error and fraud in financial statements, nor eliminate uncertainty and risk in doing business. Nor will timely reporting of material events protect the auditor and manager if discovery is late. Attesting to the efficacy of controls and the presence of their documentation is necessary under SOX, but insufficient.

There is no substitute for detective work. Auditors with expertise and experience can smell a problem when patterns don't seem quite right, and focus their investigation to great effect. Those without this sixth-sense rely on statistical methods to uncover anomalies or provide some sense of comfort. New compliance intensity is increasing the ranks of the less experienced, and increasing audit-accuracy risk as a result.

The typical ERP system claims to have all that matters, and provides the auditor a convenient centralized data store for exploration and sampling. It also provides the fraudster an equally convenient point for manipulation, and the error a solid camouflage in system-wide propagation.

Regardless of ERP, all Utilities have a plethora of independent departmental systems. Most of these departmental systems are isolated, and lack automated communication with other enterprise systems. Yet each has source data that should be in agreement with the enterprise financial systems.

Tapping these isolated data bases can verify reported financial data, and expose risks, data inconsistencies and data anomalies. For instance:

- Asset Management Systems, Geographical Information Systems (GIS), and Operations and Maintenance Systems (O&M) contain overlapping source data on the presence and condition of generation, transmission, and distribution assets.
- The Customer Information System (CIS), Billing System, and GIS contain overlapping information about revenue and revenue sources.
- The Work Order Management System, Engineering Design System, and Project Management System contain overlapping information on regulatory and environmental compliance progress.

**Key point:** SOX is to be interpreted and implemented for intent, not for procedure. The intent is to minimize the opportunity and instance of undetected fraud and mistake. Ignoring potential evidence just because it resides in something as far from the auditor's mind as the GIS database, for instance, is asking for trouble. The GIS system has the lock on asset presence and current valuation truth, as well as confirmation that actual meters and transmission lines correspond to revenue in financial systems.

William Donaldson, SEC Chairman, quoted in an Edison Electric Institute report<sup>1</sup>: "Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies' DNA." Jerry Edwards, of the Federal Reserve Board, in an unofficial PCAOB Roundtable Transcript<sup>2</sup>: "I think [the] discussion here is beneficial to the board and should be considered in trying to build your final approach. ... there may be a kind of an accumulation of control evidence that may actually turn out to be, when looked at in its entirety, significant. ... the final language that you develop [should] allow for broader consideration of a number of different control items which might very well, in their totality, rise to the degree of significance. Also, I think that it's important that the external auditor look at at least some sample of the controls that are not necessarily deemed to be key or significant controls, just to ensure that something hasn't been missed and that there's not some possibilities for potential problems there."

Isolated systems are generally considered a problem by management - information that must be transferred from one application or database to another, or extracted for reports and analysis, requires intervention by IT personnel



to construct custom database queries. However, access aside for the moment, the auditor may view these isolated databases as a valuable sampling resource, an effective control against fraud collusion, and a defacto separation of responsibility in the SOX intent.

**Access is the issue.** Each one of these databases has a different application front end, a different user interface, a different underlying data structure, and often vendor-proprietary or company home-grown data representations.

For the auditor, enterprise-wide data transparency is the holy grail - ideally facilitated by what I'll call an *Auditor's Portal* - with point-and-click exploration, automated cross-database consistency checks, exhaustive sampling options, and integral analytics and report generation. Better yet, a capability to verify period cut-off accuracy, to compare current period detail-data with prior periods, and to sound the alarm in advance of a material event. With such a portal, audit accuracy would be less dependent on expertise and experience, attestation risk would be reduced, and much better results would take much less time. Auditors in wonderland - where SOX attestation is not an issue, and all the auditors are above average.

So why isn't this in every auditor's tool box? Principally for the same reasons something similar isn't in every manager's tool box. Enterprise-wide data transparency is incompatible with legacy IT infrastructure, and major infrastructure migration options are generally unaffordable, highly disruptive, and not without considerable risk.

Some day the so-called Service Oriented Architecture (SOA) will be here, and things will be different - we are promised. All business processes will be supported by a collection of loosely-coupled IT applications, communicating in a common language, through a common exchange, and able to request and access anything on demand - with authorization of course. When SOA finds its way into general usage, effective audit tools will be easy to accommodate. An auditor's portal will be the auditor's personal tool, with remote access from anywhere. Audit advice and consultation on-demand will be location and time independent. Pending problems will be brought to the auditor's attention immediately, before they become material events. The same notifications and access will be available to management - transforming auditors from the bearers of bad tidings under conflicting pressures, into advisors and problem solvers. And auditors will sleep at night.

In the meantime ... Three companies offer approaches that demand both respect and investigation: ACL, MetaMatrix, and 4DataLink. All have in common the ability to access and correlate data in disparate and unconnected databases. ACL offers a cross-industry focused auditor's tool of some renown. MetaMatrix offers a cross-industry technology approach that promises an alternate and affordable way to integrate enterprise information. 4DataLink offers a utility focused approach with graphical views of data integrated across disparate databases.

**ACL**<sup>3</sup> provides an audit focused software package that has achieved the widest general usage among auditors in all industries. ACL claims they can provide interfaces to all databases of interest to the auditor, from ERP to the ever present financial spreadsheets. They provide automated tools for comparing data in different databases, monitoring data consistency, sounding the alarm when things go awry, and special analytics for the auditor's tricks-of-the-trade.

**MetaMatrix**<sup>4</sup> takes credit for coining the phrase Enterprise Information Integration (EII). This is an important technological concept that bears some discussion, and a concept compatible with SOA as it develops. In short, the EII approach does not attempt to integrate the various enterprise application packages for direct communication, but rather builds a model of what is contained in those application databases. Unlike data warehousing, it does not duplicate what is contained elsewhere, but rather maps the nature and meaning of what is contained elsewhere. It is a model of the enterprise data, with links into each of the databases of interest. It can present to a user an integrated view of data without reproducing all of that data in a centralized database. The breakthrough value here is that customized inter-application interfaces do not have to be developed - which is where the major expense and risk of an integrated infrastructure rears its ugly head. To my knowledge no company has employed the MetaMatrix approach for assisting the audit function. Perhaps an Auditor's Portal can not justify a MetaMatrix implementation alone. But a company with this capability already installed for other purposes should not have much in the way of incremental expense.

Now to the two agility connections: 1) EII can provide affordable and unprecedented enterprise transparency - something SOX demands, and one of the three cornerstones of enterprise agility; and 2) EII can be implemented gradually and non-intrusively - providing graceful, incremental infrastructure integration. The data model can be broadened one database at a time, to fit the enterprise annual budgetary appetite - and adding application databases to the model does not require alteration or downtime to the application. There is no risk of disruption. Strong EII provides more than an integrated view of otherwise disparate data - it can provide automated bi-directional linkage between application databases, propagating data from one to another as and when desired.

What a concept! Agility is all about the ability to change effectively. It would seem that the block on infrastructure integration has a potential solution that demands investigation.

**4DataLink**<sup>5</sup> has a mature EII model approach, specifically for utilities. Their core technology is an integrated data model that provides user-custom graphical and analytical views across application databases as if they were all one. They didn't develop this with auditor's in mind. But there it is. It would be a simple matter for any of their customers to get a self-service thin-client portal catering to the auditor's interests. Like MetaMatrix, maybe not justified for the auditor's needs alone. Unlike MetaMatrix, 4DataLink's enterprise data model maintains a time-stamped history of data changes - they can reproduce an accurate view of the past at any point in time. For the auditor, this can show precise period cutoff status, at start of period as well as end of period.

There are at least 45 Utilities that already have 4DataLink's capability - latent - but just waiting for auditing to demand some respect. These Utilities have equivalent self-service portals used by the regulatory compliance office, the CFO, the CEO, marketing, and various operational and engineering functions that need an accurate view of current and past status, enterprise wide. Until recently their customer base was all in Latin America, where serious privatization and re-regulation developed the need for this capability. At electric Utilities the need was new regulatory compliance, where penalties exist if individual customer-outage detail can not be accurately documented and audited - anytime after any occurrence. For telecommunication utilities the need was marketing and sales driven, where installed demographics, potential for new services, and sales programs leveraged information integration to simulate what-if service-extension scenarios.

### Transparency - Basics of an Auditor's Portal

An Auditor's Portal would leverage the fact that the enterprise has multiple databases, which are controlled by different departments and contain redundant information. Meaningful transparency can not be selective.

William L. Livingston, a member of the Institute of Internal Auditors with PE certification and extensive power-industry experience, counts 27 mentions of transparency in Sarbanes-Oxley. In his response to proposed OECD guidelines<sup>6</sup> he says: "In its first year of operations, in a brilliant move, the PCAOB clearly and dramatically transferred the responsibility for transparency compliance to internal audit of internal control. After designating internal audit as the principal gatekeeper, the explicit onus on internal audit was reinforced by mandating that transparency compliance be maintained on a contemporaneous basis."

An Auditor's Portal, implemented on an EII technology base, has the potential to address the necessary transparency and, at the same time, provide a powerful enterprise control mechanism in its own right. So where is this Auditor's Portal? All the technical ingredients are present. Perhaps SOX will be the impetus for both informed management as well as knowledgeable audit - reducing the risk of walking around in the dark. But then, some prefer it that way.

The discussion above is an excerpt from a work-in-process on meeting Sarbanes-Oxley compliance *intent*, enabled by EII technology. If you know of other EII approaches that should be considered, please contact [dove@utilipoint.com](mailto:dove@utilipoint.com).

#### ----- References -----

1. [A Guide to Enhanced Corporate Governance and Financial Reporting in the Energy and Utility Industry](#), Edison Electric Institute, Dec 2003, [http://www.eei.org/industry\\_issues/finance\\_and\\_accounting/finance/restoring\\_investor\\_confidence/corporate\\_governance.pdf](http://www.eei.org/industry_issues/finance_and_accounting/finance/restoring_investor_confidence/corporate_governance.pdf)
2. [Unofficial transcript of the Public Company Accounting Oversight Board Roundtable July 29, 2003](#), PCAOB, [http://www.pcaobus.org/Rules\\_of\\_the\\_Board/Documents/2003-07-29\\_Roundtable\\_Transcript.pdf](http://www.pcaobus.org/Rules_of_the_Board/Documents/2003-07-29_Roundtable_Transcript.pdf)
3. [ACL](#), [www.acl.com](http://www.acl.com)
4. [MetaMatrix](#), [www.metamatrix.com](http://www.metamatrix.com)
5. [4DataLink](#), <http://www.4DataLink.com>
6. ["Corporate Governance of State-Owned Enterprises - Comment Letter on Draft OECD Guidelines,"](#) [www.parshift.com/Speakers/Speak024.htm](http://www.parshift.com/Speakers/Speak024.htm)

*Rick Dove is a recognized thought leader and change agent for agile enterprise and agile systems of all kinds. He co-led the seminal effort that defined agility in the early nineties as the survival need of the new millennium. He subsequently organized and led the Agility Forum's industry-collaborative work that identified and defined concepts and principles for achieving agility in all aspects of enterprise. He's developed and managed deployment of agile enterprise business processes and IT infrastructure. He is a prolific writer and frequent speaker on the subject, and the author of Response Ability: The Language, Structure, and Culture of The Agile Enterprise (Wiley 2001) and Value Propositioning—Perception and Misperception in Decision Making (Iceni Books 2005).*