Sarbanes–Oxley Tools: Why do they fail?

Notice

Notes & Disclaimer

Document Version 1.6

Companies or products mentioned herein are trademarks of their respective trademarks owners.

Note: In some cases products & company names are interchangeably used.

The author regrets inadvertent publication of an email from ISACA listserv in the previous version of the document without permission of the person concerned. That email and the name of person has been removed from the document.

The author was pointed to some errors in version 1.0 of this document related to IBM product architecture. Those errors have been rectified as well.

Disclosure: The vendors have not been given an opportunity to put their point of view before publication of the document.

Disclosure: The author is associated with a company which has its own Sarbanes Oxley web based tool. However this report has been published entirely in the author's personal capacity in exercise of his rights to creative freedom, and no permission has been sought or given by the author's employer to publish the report.

Distribution: The document can be freely distributed and reproduced without alteration.

Table of Contents

Author Background

Rohit Tripathy

Rohit Tripathy works as a Sarbanes-Oxley consultant, and was previously employed with Ernst & Young. The views expressed in this analysis document are totally personal and do not reflect direct or implied opinion of any organization he is associated with, any of his clients or his previous employer Ernst & Young. You can get in touch with the author at **rohit.tripathy@gmail.com**

Introduction

Document Background

I have been involved in 6 different Sarbanes-Oxley (SOX) implementation projects as a consultant, out of which three clients went for a tool based SOX implementation project. In each case, my client spent more than USD 150,000 to procure a web based SOX tool from a leading Sarbanes-Oxley tool vendor. In all three cases, the SOX project team ended up spending inexcusable amount of time feeding data/documents and maintaining the Internal Controls structures into the tool. Finally the clients gave up, they stopped using the tool, and went back to Excel sheets and Word documents. The tool implementation failed. This has moved me to analyze the leading vendors of Sarbanes-Oxley tool and come up with conditions where the tool implementation can fail. I am myself shocked by the results of the analysis. None of the top tool vendors have a fully workable product. It seems in the rush of Sarbanes-Oxley craze, the vendors offered poorly designed solutions to the market, without carrying out a thorough REQUIREMENT ANALYSIS.

Before I start I will quickly list the problems with the current crop of major Sarbanes-Oxley tools:

Problems at a quick glance:

- Account-Process-Risk-Control Hierarchy problem
- Excel Sheet Column Definition problem
- Control Multitude problem
- Process Narratives Maintenance problem
- Control Level Access and Audit problem
- Tool itself not compliant to Sarbanes-Oxley IT controls problem
- Tool offering compliance for Incorrect Sarbanes-Oxley Act clause problem
- Fixed Workflow problem
- Follower problem
- Application Performance problem
- Tool homogeneity problem
- Old wine in new bottle Syndrome
- Complexity of Installation problem
- Other problems

Account-Process-Risk-Control Hierarchy problem

Paisley Consulting was the first one to define a fixed hierarchy of Account-Process-Risk-Control on the basis of their interpretation of COSO framework. COSO framework gives the flexibility of choosing hierarchy to end implementing organization. However, Paisley's *Risk Navigator* did not offer the same flexibility to its users. Subsequently, every other compliance tool vendor aped Paisley Consulting and incorporated Account-Process-Risk-Control fixed hierarchy in the tool, or a variation of it. This hierarchy is not at all suitable for Operational Internal Controls, Strategic Internal Controls, and IT Internal Controls. Even for Financial Internal Controls, this hierarchy is not suitable in a number of cases, like Treasury Management, General Ledger Controls (A general ledger cannot be mapped to any account. It is itself a summary of all accounts). A deployable SOX tool should have the flexibility of letting end users decide creating hierarchies.

Excel Sheet Column Definition problem

A Sarbanes-Oxley implementation project generates a lot of excel sheets. In most implementations, the excel sheets contain fields that describe Control Objectives, Control Procedures, Testing Procedures, Testing Results, and auditor assessment. In some implementations fields describing whether a control is key, Control owner, testing frequency, Control risks are used. For a mid to large size organization, at least 250 excel sheets are generated. This number can go up more than 1000 for a large organization. Mostly, a Sarbanes-Oxley engagement begins before a tool is procured. So the sheet formats are decided prior to tool procurement. If the tool has fixed hierarchy, and fixed control description fields, it will not be able to fit in pre-generated excel sheets. An organization that procures a tool with fixed Control Description formats will end up going back to excel sheets.

Control Multitude problem

Each sheet has on an average 8 - 10 key controls which has to be tested. This translates to about close to 2500 controls for a 250 excel sheet organization. If the tool gives a view that lists only one control at a time, a Sarbanes-Oxley implementation team will have to go to 2500 different screens to complete first round of data entry. There are at least 4 iterations for every control as the internal and external auditors insist on changes. To accomplish this, for a single edit view tool: the team will have to go to at least 10,000 screens to update the control data in the tool. The complications arise when periodic testing process begins. Controls may have to be tested daily, weekly, monthly, quarterly or annually. So if a Sarbanes-Oxley implementation has 2,500 key

controls, the testing team will have to visit each of them individually depending upon the frequency of testing. Most of the tests are have a transaction sample size typically 5% of population size or 25 in number. This is a mammoth task for the testing team. The story does not end there. These controls have to be revisited by the control owner who is responsible to validate testing results, and later by the Internal and external auditor. So, the Sarbanes-Oxley tools MUST NOT give edit access to a control one at a time. If the tool does that, it is humanly impossible to use it.

Process Narratives Maintenance problem

At the very start of a Sarbanes-Oxley project, most of the processes that have an impact on ICFR (Internal Controls on Financial Reporting) are documented typically in a Microsoft Word doc format. These processes are either Financial like Account Receivables, General Ledger, Purchases/Payables or Information Technology processes like IT Administration, Application User Management, Change Controls etc. These process word documents are called Process Narratives. The process narratives are of continuously evolving nature, especially when the Sarbanes-Oxley implementation phase is going on. Assuming if three persons are working on one document, the critical need of the tool is that ONLY ONE person should be able to edit a word document at a time. Other wise, there will be three versions of the same document, with incremental information in each. This problem was solved by the software community on large project by a check-in/check-out version control mechanism. Only one person can take out the document from the repository using check-out process, and if a document has been checked out by someone, no one else can edit it. That document can be retrieved only for *read only* purposes by others till the person who checked out the document checks it back in. There after another person can check the document out for his editing. As a Sarbanes-Oxley implementation team, consisting of more than 15 persons, handling 50 or more process narratives, version control with edit locking-in capabilities is an essential requirement for the tool.

Another related issue is that vendors who don't understand auditing process offer a PROCESS MAPPING functionality rather than PROCESS NARRATIVE MAINTAINING functionality. The initial process documentation for SOX relates to describing the whole process and listing key controls in that process, and not process maps. The process documentation goes through a number of iterations. This cannot be achieved using a PROCESS MAPPING functionality.

Control Level Access and Audit problem

For a web based tool where edit access to controls is shared by various people, it is very important that the access should be granted at a Control

Level. One should be able to restrict edit access to a control to a designated person. Otherwise the integrity of Control information can be violated by anyone having access to application. If Control level *access control features* are not present in a Sarbanes-Oxley tool, better control is exercised with data in remaining distributed format like Excel sheets and Word, the control of which lies with the Compliance Officer rather than in centralized database format with poor access control on Intranet. Also all textual changes to any control field should be audited and be reproducible, and the SOX tool should list what was the change made by which person.

Tool itself not compliant to Sarbanes-Oxley IT controls problem

Most of the Sarbanes-Oxley compliance tools are themselves not compliant to Sarbanes-Oxley IT controls. If IT application under SOX review does not have password controls, the IT auditor will make the IT managers life miserable. It's ironical that most of the Sarbanes-Oxley tools themselves don't have minimal features like ability to denying concurrent login to users, account lockout after failed login attempts, and inactivity timeout features. Other tools do not have even basic password controls like ability to set complexity requirements and minimal password lengths.

Tool offering compliance for Incorrect Sarbanes-Oxley Act clause problem

Sarbanes-Oxley Act has seven major clauses.

- **Section 301(4)**: Whistle Blower protection
- **Section 302**: CEO/CFO certification of external auditor attestation of internal controls
- **Section 401**: Off balance sheet item disclosure to SEC
- **Section 404**: Periodic evaluation of ICFR (Internal Controls over Financial Reporting)
- **Section 409**: Real time disclosure of material events in 8-K filings with SEC
- **Section 802**: Record Retention Procedures, and violation penalties
- **Section 906**: Corporate Responsibility for Financial Reports, and penalties

The biggest pain point for Organizations has come in due to Section 404 which states that all internal controls should be periodically tested as per PCAOB guidelines. The only place a tool can make significant difference to Sarbanes-Oxley act compliance costs is if they tool addresses Section 404.

Some tool vendors have made a pitch for Section 802 compliance which provides upto 20 years imprisonment for altering, destroying, mutilating, concealing, falsifying records, documents or tangible objects with the intent

to obstruct, impede or influence a legal investigation. Section 802 compliance is not a tool issue. A lot of workpapers are paper based, they have to be signed off by auditors, will continue to remain paper based. As per the Sarbanes-Oxley act Section 802, these audit workpapers and records should not be tampered. A tool that is based in premise of electronic document retention as per Section 802 will always be incomplete.

Fixed Workflow problem

Most of the times when the workflow feature offered by SOX tools, it is simply the Document Workflow system with edit-review-approve-certify cycles. There are two problems with that: for one, different organizations have different document workflows, and a tool with fixed workflow cannot accommodate variability. The other problem is that workflows go beyond document workflows. A workflow is a queue of activities that flows from one step to another on performance of the previous activity. Each of these activities can be assigned to a person. Typically in a true workflow system, these activities are unitary application functionalities, or a web form. What vendors claim as workflow capability are in practice no more than fixed web forms based document workflows whose order cannot be changed by end users.

Follower problem

Paisley Consulting was the first product to go off the block with its *Risk Navigator* product. A lot of products thereafter have simply copied or extended Paisley Consulting's interpretation and taxonomy of Sarbanes-Oxley Act. The original definition was itself incomplete, so the tools following thereafter have carried forward the problems present originally.

Application Performance problem

The performance of tools is a very critical factor in successful implementation of the tool. For instance Lotus Notes/domino based architectures are known to be notoriously slow. A tool must have an acceptable response time to fetch control information.

Tool homogeneity problem

Many vendors have done a complex integration of two or more products. Both of them have to be separately installed, and it adds to the complexity of solution offering.

Old Wine in New Bottle Syndrome problem

Many vendors have repackaged and classified their pre-sox offerings are a Sarbanes-Oxley product. We are going to analyze the history of every vendor, and how have they evolved their Sarbanes-Oxley product.

Complexity of Installation problem

Many tools are complex to install and set up, and they need vendor assistance every time they are installed.

Handysoft - *SOXA Accelerator*

Company Background

Handysoft is a Vienna, VA based company with key promoters having South Korean linkages. The company was incorporated in 1991. The company is among the leading Business Productivity Measurement (BPM) vendors. Handysoft has a set of tools called *BizFlow* which helps in getting BPM implemented. Handysoft Sarbanes-Oxley offering is called *SOXA accelerator*. Technologically Handysoft is inclined towards Java based technologies.

SOXA accelerator has been designed by a team headed by Caffrey H.J. Lee. Mr. Lee holds a Bachelor of Arts in Business Administration from Hanshin University in Korea. Mr. Lee is also responsible for *BizFlow* BPM platform. *SOXA accelerator* is a hard coded Workflow created on *BizFlow* platform that gives workflow features and is integrated with Plumtree CMS (Content Management Service) that gives document repository features. It also includes Business Objects 10(Crystal Reports) for dashboard reporting.

Handysoft Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	Fail
Excel Sheet Column Definition problem	Fail
Complexity of Installation problem	Fail
Control Multitude problem	Fail
Process Narratives Maintenance problem	Success
Control Level Access and Audit problem	Success
Follower problem	Fail
Application Performance problem	Fail
Tool homogeneity problem	Fail
Old wine in new bottle Syndrome	Fail
Other problems	Fail

Account-Process-Risk-Control Hierarchy problem

The flow for Handysoft's *SOXA accelerator* begins by defining a project team. Once the project team is in place, the team defines the organization's significant financial accounts and corresponding processes. With that information, the team can automate the collection and evaluation of information about financial controls, risk assessments, and issues using the *SOXA accelerator*'s customizable Sarbanes-Oxley workflows. Process owners are assigned; they are responsible for defining risks and controls, and for associating control data and documentation with the process. *BizFlow* notifies the process owner via e-mail and creates a task for the user to complete the risk evaluation and define the controls for the process they have been assigned.

This Handysoft has created a fixed workflow on Account-Process-Risk-Control hierarchy, and consequently it suffers from Account-Process-Risk-Control hierarchy problem.

Excel Sheet Column Definition problem

As Handysoft is a hard coded BPM solution, the control, risk and test field descriptions are fixed. Therefore the tool suffers from *Excel* Sheet column definition problem.

Complexity of Installation problem

Installation of *SOXA accelerator* version 2 is very complex. *BizFlow* and *Plumtree* have to be both independently installed, and then integrated. At a minimum, there are three application servers (*Plumtree* Portal Application, *Plumtree* collaboration server, Handysoft *BizFlow* application server), three separate databases (Collaboration Server Database, *Plumtree* Database, *BizFlow/SOXA* database), and an optional server (Document Repository). Please note that multiple application servers and database servers can be installed in one machine, so *SOXA accelerator* may not need at least 6 different machines. But the speed of the application with such a complex set transaction flow is expected to be very slow. The integration between *Plumtree* and *BizFlow* has been achieved through web services, which is still not a proven enterprise concept in terms of speed and scalability. With such a complex architecture, maintenance will always be an issue, and feature upgradation cannot be rapidly achieved. The vendor support would always be needed should anything go wrong with the installation. The *BizFlow* database is a Java based JDBC connected database, *Plumtree* database is ODBC/XML connected database. The technology is not homogenous.

Control Multitude problem

The application offers one control at a time access control. So it suffers from Control Multitude problem. This gets compounded by the fact that each control has an individual access control, and a role defined workflow. For 2500 controls, around 20,000 views would be needed.

Process Narratives Maintenance problem

The tool has check-in/check-out mechanism of version control. So it does not suffer from Process Narratives Maintenance problems.

Control Level Access and Audit problem

SOXA accelerator is a process centric fixed workflow application. Access to a control is obtained at process design stage only to Control Owners. So *SOXA accelerator* does not suffer from control level access and audit problem.

Follower problem

The product seems heavily influenced by Paisley Consulting *Risk Navigator*, and OpenPages *SOX Express*. It has taken the same approach of definition Account/Process, Control Objectives, Risks etc., and offers no new insight or unique features that not available in other tools.

Application Performance problem

Due to the heterogeneity of the offering, this suffers from Application Performance problem.

Tool homogeneity problem

As Handysoft is a complex integration of three separate products, it suffers from Tool homogeneity problem.

Old Wine in New Bottle problem

The tool repackages Handysoft's pre-SOX days *BizFlow* BPM application. So it suffers from Old Wine in new bottle problem.

Other problems

Fixed Roles: The tool has defined fixed roles inside the application: 404 Assessment Project Lead, Account & Process Evaluators, Process Owners, Control Evaluators, Control Testers, 404 Assessment Approvers, Roll-up lead, Roll-up approvers. The tool should have provided for flexible roles. If an organization has already implemented SOX, and not defined the roles as per tool roles, a lot of process re-engineering would be required.

Import problem: Existing excel sheets cannot be easily imported into the application. Each excel sheet has to be broken down into separate control objectives, risks, controls, and testing procedure as per fixed field definition by Handysoft, and then individually uploaded in the system.

Fixed Reports: The tool offers Documentation Status, Testing and Evaluation status, Assessment status, and process assessment. The user cannot configure any custom report beyond what has been provided by Handysoft unless he pays Consulting Dollars to Handysoft.

Fixed Platform: It runs only on Microsoft platform.

Openpages – *SOX Express*

Company Background

Openpages was incorporated in 1996. Initially it used to offer Web content management services, using a product called *ContentWare* that offered a suite of products for creating, managing, and deploying content to Web sites, wireless devices, and print publications. Thats how the company came on to be known as OpenPages (Content Management of webpages). Openpages was a late entrant with its mission of building Enterprise Content Management Systems and found the market stagnant. So in 2002, with the coming of Sarbanes-Oxley Act in the US, the CEO Mike Duffy (Sales background) and Santanu Paul(CTO, technology background), pushed the company into creating a compliance solution called *Sarbanes-Oxley Express*. *SOX Express* design was led by Santanu Paul, who came on board when OpenPages acquired Viveca which was a provider of services for B2B content and online catalogs. In 2003 Santanu Paul left OpenPages to start a company in India.

Openpages purchased PwC *Internal Controls Workbench*(*ICW*) and acquired 375 clients with them in April 14, 2004. *ICW* was not integrated with *SOX Express*, so that the technological complexity of *SOX Express* does not go up. However *SOX Express* offers integration with another PwC product called *TeamMate*. The PwC *ICW* clients were encouraged to move to *SOX express*, and *ICW* support was diluted. OpenPages' platform includes J2EE-based workflow, document management, content management and multi-channel publishing upon which compliance solutions are built.

Technology Background:

The framework for *Sarbanes-Oxley Express* has been provided by OpenPages Server (OP4). OpenPages has a technology bias towards Java 2 Enterprise Technology (J2EE) which has now been widely recognized as a very slow platform due to interpretation based architecture. *SOX Express* is a J2EE based product.

Openpages Performance Matrix	
Test Case	**Result**
Account-Process-Risk-Control Hierarchy problem	**Fail**
Excel Sheet Column Definition problem	**Fail**
Control Multitude problem	**Fail**
Process Narratives Maintenance problem	**Fail**
Control Level Access and Audit problem	**Success**
Fixed Workflow problem	**Fail**
Follower problem	**Success**
Application Performance problem	**Fail**
Tool homogeneity problem	**Fail**
Old wine in new bottle Syndrome	**Success**

Account-Process-Risk-Control Hierarchy problem

Openpages provides Section 404 compliance through an entity called IC Documentation. The hierarchy of IC documentation is Business Entity, Accounts, Processes, Risks, Controls, & Tests. Openpages was among the first big products on block along with Paisley Consulting, so this hierarchy has been copied by every other SOX Compliance product vendor. So it suffers from Account-Process-Risk-Control hierarchy problem.

Excel Sheet Column Definition problem

Sarbanes-Oxley Express has fixed definitions for the entities it has defined. These entities are Business Entity, Accounts, Processes, Risks, Controls, & Tests. The fields for each of them are fixed as well. So OpenPages suffers from Excel Sheet Column Definition problem.

Control Multitude problem

Sarbanes-Oxley Express has multiple controls at a time view access, but single control at a time edit access. So it suffers from Control Multitude problem.

Process Narratives Maintenance problem

Sarbanes-Oxley Express lets users attach files at process, risks, controls and test levels. However these files are not governed through a version control system. So it suffers from Process Narratives Maintenance problem.

Control Level Access and Audit problem

Sarbanes-Oxley Express has control level access and audit control. So it does not suffer from Control Level Access and Audit problem.

Fixed Workflow problem

SOX express has fixed workflows from Section 302 and Section 404. Process owners first provide sub-certification for their areas of jurisdiction. Sub-certifications are then "rolled-up" throughout the company and approved by managers at each business level. *SOX Express* then presents a final certification report for attestation assurance from corporate officers. So it suffers from Fixed Workflow problem.

Follower problem

Sarbanes-Oxley Express was an early solution provider. The fixed entity definition though inspired by Paisley Consulting was its own. So it does not suffer from follower problem.

Application Performance problem

Sarbanes-Oxley express is based on J2EE technology. This has been known to be a slow platform. So *Sarbanes-Oxley express* is expected to be slow.

Tool homogeneity problem

Openpages integrates with *Cognos* for Dashboard graphing and Reporting. Openpages acquired two products from PwC, *TeamMate* and *ICW*. It offers product integration/interoperatability with *TeamMate*. However *ICW* has not been integrated, *ICW* clients have been encouraged to migrate from *ICW* to *Sarbanes-Oxley express*. So it suffers from Tool homogeneity problem.

Old Wine in New Bottle problem

Sarbanes-Oxley Express is a totally redesigned product though the technology platform has remained J2EE. It is not a repackaged product. So it does not suffer from old wine in new bottle syndrome.

Paisley Consulting – *Risk Navigator*

Company Background

Paisley Consulting is a Cokato, Minneapolis, Minnesota based company. It was incorporated in 1995. Paisley's claim to fame was *AutoAudit* workpaper system which was a hit product in desktop audit product space. The original promoters of Paisley Consulting are Tim and Stacey Welu. Tim was in sales and marketing with Hormel Foods in Austin, Minnesota before starting Paisley Consulting while Stacy had an auditing background. Stacy is a Certified Lotus Professional (CLP), which explains Paisley's initial leaning towards Lotus Notes based technology platform as evident in *SNAP reporter*. The J2EE tilt was given by Jay Dorenkamp – the Chief Technology Officer. Jay got introduced to J2EE technology from Lawson Software where Jay was vice president of technology development for Lawson Software, a supplier of financial, human resources, supply chain, and business intelligence applications, where he was responsible for the company's core technology platform and its evolution to J2EE-based standards.

Paisley was among the first to move into SOX compliance tool space when it release *Risk Navigator* in February 2003, within 7 months of Sarbanes-Oxley act being passed.

Paisley Consulting is responsible for all the problems compliance tool implementation space is facing. They were the first one to define Account-Process-Risk-Control Hierarchy, which is Paisley's interpretation of COSO specification released by Threadway Committee of Sponsoring Organizations. Starting with OpenPages which released *Sarbanes-Oxley express* in June 2003, all subsequent compliance tool vendors blindly aped the *Risk Navigator*'s way of looking at Section 404 tool solution.

Paisley Consulting Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	Fail
Excel Sheet Column Definition problem	Fail
Control Multitude problem	Fail
Process Narratives Maintenance problem	Fail
Control Level Access and Audit problem	Success
Tool itself not compliant to Sarbanes-Oxley IT controls problem	Fail
Fixed Workflow problem	Fail
Follower problem	Success
Application Performance problem	Fail
Old wine in new bottle Syndrome	Partial Fail
Complexity of Installation problem	Fail
Feature Gaps	Fail
Other problems	Fail

Account-Process-Risk-Control Hierarchy problem

Paisley Consulting was the first one to define a fixed hierarchy of Account-Process-Risk-Control on the basis of their interpretation of COSO framework. COSO framework gives the flexibility of choosing hierarchy to end implementing organization. However, Paisley's *Risk Navigator* did not offer the same flexibility to its users. Subsequently, every other compliance tool vendor aped Paisley Consulting and incorporated Account-Process-Risk-Control fixed hierarchy in the tool. This hierarchy is not at all suitable for Operational Internal Controls, Strategic internal Controls, and IT internal controls (What is account in an IT control?). Even for Financial Internal Controls, this hierarchy is not suitable in a number of cases, like Treasury Management, General Ledger Controls (A general ledger cannot be mapped to any account. It is itself summary of all accounts). A deployable tool should have the flexibility of setting the hierarchy to users.

Excel Sheet Column Definition problem

Importing existing control data in *Risk Navigator* is a very complex process. Since the control description fields have been fixed by Paisley, it suffers from Excel Sheet Column Definition problem.

Control Multitude problem

Maintenance of data in *Risk Navigator* is a well documented and acknowledged problem. Users have to navigate through humongous number of screens before data could be updated in the tool. It offers one control edit screen at a time to the user. So it suffers from Control Multitude problem.

Process Narratives Maintenance problem

Sarbanes-Oxley Express lets users attach files at process, risks, controls and test levels. However these files are not governed through a version control system. So it suffers from Process Narratives Maintenance problem.

Control Level Access and Audit problem

Sarbanes-Oxley Express has control level access and audit control. So it does not suffer from Control Level Access and Audit problem.

Tool itself not compliant to Sarbanes-Oxley IT controls problem

Risk Navigator does not have denying concurrent logins functionality, account lockout controls & session timeout controls. So the tool is itself not compliant to Sarbanes-Oxley Act IT controls.

Fixed Workflow problem

Paisley has the following fixed workflows:

- Create Accountability and Ownership
- Assessing Controls
- Monitoring and Review
- Issue Tracking and Resolution
- Reporting and Reference
- Management Certifications
- Security

So it suffers from fixed workflow problem. It is interesting to note that Paisley's interpretation of workflow is different from general industry definition of workflow which is: *" Workflow is the operational aspect of a work procedure: how tasks are structured, who performs them, what their relative order is, how they are synchronized, how information flows to support the tasks and how tasks are being tracked ".*

Follower problem

Paisley Consulting is the originator of Account-Process-Control-Risk hierarchy. It is the only tool that cannot be truly called as follower. It does not suffer from follower problem.

Application Performance problem

Paisley's *Risk Navigator* is based on J2EE technology. Most of the enterprise applications based on J2EE architecture are slow. Paisley speed issues are very well known in Auditor Community.

Old Wine in New Bottle problem

Paisley was among the first movers in web based Sarbanes-Oxley tool market. So it can be considered as a front runner in this market. *SNAP reporter* was a Lotus Notes based charting and reporting tool. It is well known that Lotus Notes based applications are notorious for their slow speeds. *SNAP reporter* has been remodeled in J2EE technology and made a part of *Risk Navigator*. So it suffers partially from Old wine in new bottle syndrome.

Complexity of Installation problem

Installation of *Risk Navigator* involves installation of a J2EE application server, *Risk Navigator* JAR files, a database, *SNAP reporter*. It normally takes a week to install and upload hierarchy definition on Paisley.

Feature Gaps

Version Control and **Workflow** features are not present in *Risk Navigator*.

Oracle – *Internal Controls Manager*

Company Background

Oracle *ICM* is a half baked product. This is a product designed by half understanding of auditing processes. First of all, the product makes the assumption that an organization is simply a collection of processes. Each process has a number of controls, say 20.. and those controls have risks associated with them. Each of the control has to be retested. A glaring omission in this understanding is that Process instead of Organization structure is the starting point. So, in this flow if Account Receivable is a process, it would have various organization units as its children. You can't say: show me all processes under Western Region for North American Computers. You can only say: Show all regions for Account Receivables process. This is a major logical flaw. Typically an audit is done region wise, and not process wise. This approach can work only for the case where the organization is process centric rather than region centric. That is to say: For US, Japan and Italy, Accounts Receivables(AR) are being handled by Global AR department. In my consulting career, I have never seen such an organization. Most organizations are region centric, i.e., there is an AR department for US, and there is an AR department for Japan.

Another critical logic flaw: Oracle ICM has defined Assertions at Control level. A basic course in auditing would have substantiated that as per Statement of Accountant Standard, SAS 31, assertions are related to Financial Accounts, that is, any line item in Balance Sheet, Profit & Loss Account, or Funds Flow statement. Assertions have no existence at Controls level. Let me set the basics right for the designers of Oracle ICM: Against each account in a financial statement, there are assertions. When those assertions are tested by auditors, they look for internal controls that ensure that assertion objectives are met. So the flow is Accounts->Assertions->Internal Controls. What Oracle has done: Internal controls->Assertions. This means you will first define a control, and then try to figure out which assertion it relates to. Unfortunately this is not how Auditing as a profession works.

Control Objectives are not a input text field but a checkbox of pre-configured options. the options I could make out are: Effectiveness and Efficiency of operations, Reliability of Financial Statements, Compliance with Applicable Laws and Regulations, Safeguarding Information and Systems. In this approach, if the number of objectives goes to 200, it will be impossible to present it to user. Control Objectives should not have been offered as a user selectable checkbox. This approach has limited room to accommodate User defined Control Objective.

At this state of product, I think I am not mentally ready to even evaluate this product any further. **This product is not fit for commercial usage.**

Stellent – *Sarbanes-Oxley solution*

Company Background

Stellent Inc was started in 1995, in Minnesota. It started off as an Enterprise Content Management Tool for manage workflows for website platform management. The driver behind Stellent *Sarbanes-Oxley solution* was the former CEO Vernon Hanzlik, and later Executive Vice President, Compliance Solutions. He managed the strategy and execution behind bringing Stellent's compliance applications. His previous large scale technical exposure was with Lee Data Corporation where he used to do Product Management for the IBM 3270 market. Mr. Hanzlik held a bachelor degree in business administration from University of Wisconsin-Stout. Mr Hanzlik has severed his employment agreement with Stellent.

The company is a publicly listed company. Its greatest year was during the height of Dot-com boom in 2000-2001 when the company's revenues jumped from USD 17 million to USD 53 million in a single year. However with the tech meltdown, the license sales revenues slipped to USD 40 million in 2003. It simultaneously grew its services offering, which grew to USD 25 million in 2003.

Stellent Technical solutions are based on J2EE platform. Stellent compliance solution is called Stellent Sarbanes-Oxley solution which is a variant of their content management solution in terms of architecture and design. It was an early mover in this space, and released the solution in August 2003.

Stellent Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	Partial Fail
Excel Sheet Column Definition problem	Fail
Control Multitude problem	Fail
Process Narratives Maintenance problem	Success
Control Level Access and Audit problem	Success
Fixed Workflow problem	Fail
Follower problem	Fail
Application Performance problem	Fail
Old wine in new bottle Syndrome	Fail
Complexity of Installation problem	Fail
Other problems	Fail

Account-Process-Risk-Control Hierarchy problem

Stellent has tried to carve out a mixture between COSO components, and financial components. It does not have an ACCOUNT concept. It follows Process-Policy-Risk-Control fixed cycle. The basic entities in Stellent for a POLICY are COSO components, Assertions, Risks, Controls, Matrix, Reviews, Attachments, Issues and History. Ironically, it has ASSERTION support but no ACCOUNT support. So it has done a partial implementation of Paisley's Account-Process-Risk-Control flow.

Excel Sheet Column Definition problem

In any Content Management Solution based Compliance product, the fields will have to be necessarily fixed. All the fields in Stellent are fixed. For instance, the risk fields are Risk Significance, Risk Type, Risk Likelihood, Risk Rating. There is no way an organizations existing excel sheet could be imported into this tool. For instance, if an organization has implemented its control sheets with Risk definition different from Risk Significance, Risk Type, Risk Livelihood and Risk Rating, the tool is not suitable. The tool suffers from Excel Sheet Column Definition problem.

Control Multitude problem

The basic entity for control enforcement in Stellent *Sarbanes-Oxley solution* is a POLICY rather than a CONTROL. However it supports controls. Controls have to be fed in through unitary screens. So it suffers from Control Multitude problem.

Process Narratives Maintenance problem

Content Management Systems generally have good version control systems for documents. So is the case with Stellent's *Sarbanes-Oxley solution*. This product does not suffer from Process Narratives Maintenance problem.

Control Level Access and Audit problem

A Content Management System is a document workflow. In Content Management Systems, access control is enforced by assigning ownership to a step in workflow. So if a control has been defined as a step in workflow, ownership, and consequently access could be controlled. Stellent does not suffer from Control level access problem. Stellent also has good auditing capabilities. So it does not suffer from auditing problem as well.

Fixed Workflow problem

As explained previously, a Content Management System is itself a fixed document workflow. So it suffers from fixed workflow problem.

Follower problem

Stellent as a product is definitely inspired by Paisley Consulting's *Risk Navigator*. So it suffers from follower problem.

Application Performance problem

Stellent has built using a service-oriented architecture (SOA) that exposes application programming interfaces (APIs) as Web services, supporting the Simple Object Access Protocol (SOAP) and Web Service Description Language (WSDL) standards. Web services are generally slow, and if you add J2EE on top of that, you would have an application performance issue.

Old Wine in New Bottle problem

Stellent has repackaged its existing Content Management System, and after modifications repositioned it as a *Sarbanes-Oxley solution*. So it suffers from Old wine in new bottle syndrome.

Complexity of Installation problem

To install Stellent, a J2EE application server, java installable and the database will have to be installed. A typical installation and minimum configuration time for such a product would be 1 week.

Other problems

The compliance product division is going through an internal top level executive turbulence. The designer of product Mr Hazlik has severed his employment agreement with Stellent. He was followed by Dean Berg. Currently Stephanie Maziol is the Director of compliance solution.

Protiviti – *SarbOx Portal*

Company Background

Protiviti is a wholly owned subsidiary of Robert Half International with 30 offices in the United States and six international locations. The *SarbOx Portal* is one of two proprietary information-technology (IT) tools the company has developed to help its clients comply with Section 404 of the Sarbanes-Oxley Act. Protiviti is a Sarbanes-Oxley consulting service provider as well as a tool vendor. Protiviti reaped a heavy windfall from Sarbanes-Oxley consulting projects. Revenues jumped to $133 million in 2003, and $352 million in 2004, representing about an eighth of California-based Robert Half's $2.7 billion total. In the first quarter of 2005, Protiviti fees hit $111 million.

Since the design of the tool has come from a team that has worked on ground and does not have any technological bias, the tool flows are simple, and feature overkill seems not to have been done. The flow begins with feeding organization structure through Organization Modeling, and then identifies financial reporting elements within it. Business processes that affect those financial reporting elements are then defined, and risk is then carried out in each of those business processes. This is a welcome break from Account-Process-Risk-Control hierarchy. The ability to start from Organization Modeling rather than account modeling enables a majority of controls to be mapped. However there are a couple of problems as well. First of all there are three levels of mapping needed. The problem with the tool is that *SarbOx Portal* has been designed as a repository of documents. So key control/risk information has to be fed as a document rather storing it directly as a field in database. This implies content search is difficult, and control data retrieval is tough.

SarbOx Portal was built using Microsoft's .NET framework. Protiviti *SarbOx portal* uses MS SQL 2000 as the database.

Protiviti Performance Matrix	
Test Case	**Result**
Account-Process-Risk-Control Hierarchy problem	**Success**
Excel Sheet Column Definition problem	**Fail**
Control Multitude problem	**Fail**
Process Narratives Maintenance problem	**Fail**
Control Level Access and Audit problem	**Fail**
Tool itself not compliant to Sarbanes-Oxley IT controls problem	**Fail**
Fixed Workflow problem	**Not Applicable**
Follower problem	**Success**
Application Performance problem	**Success**
Tool homogeneity problem	**Success**
Old wine in new bottle Syndrome	**Success**
Complexity of Installation problem	**Success**
Feature Gaps	**Fail**
Other problems	**Fail**

Account-Process-Risk-Control Hierarchy problem

The tool has its own unique hierarchy of Organization Structure, Financial Model, Process Classification Scheme, Risk Control Matrix. As explained earlier, the starting point is the organization structure rather than Financial structure. This gives the tool tremendous flexibility over Account-Process-Risk-Control hierarchy structure. The tool does not suffer from Account-Process-Risk-Control hierarchy problem.

Excel Sheet Column Definition problem

The product architecture and variety of maps that exist will make it impossible to import an existing excel control sheet in the application. It is advised that this product should be procured before a Sarbanes-Oxley compliance project is started. if the procurement is done subsequent to the engagement, it will become impossible to work with the tool. The tool suffers from Excel sheet column definition problem.

Control Multitude problem

Control as an entity does not have an independent existence in *Sarbox Portal*. It exists in the form of RC matrix (Risk Control) matrix. The data entry points to RC matrix are unitary. So the tool suffers from Control Multitude problem.

Process Narratives Maintenance problem

SarbOx portal has several points where documents can be attached, i.e. at Financial Model level, Risk Information level, Organization level. So version control system has not been built into the product. The tool suffers from Process Narratives maintenance problem.

Control Level Access and Audit problem

Access control in the application is role based. The roles in the system are Admins, All users, Content-Financial, Content-Organization, Content-PCS, Content-Risk, Document Formats, Documenter, External Audit, Librarian, ProjectTeam, RC Matrix and Report. Management of access control is difficult in the application. I suspect the admin will end up making most of the users members of majority of the roles. Otherwise a full time person would be needed to do role management in this application.

Tool itself not compliant to Sarbanes-Oxley IT controls problem

The tool does not have even basic password level controls. There are no password length or complexity features, no account lock-out after failed login attempts, no session timeout etc. *SarbOx Portal* is itself not compliant to Sarbanes-Oxley IT controls.

Fixed Workflow problem

There is no workflow concept in this tool. In a lot of ways this is better than BPM tool vendors introducing artificial and pseudo workflows which end up complicating the tool operation.

Follower problem

This tool under no means a copy of Paisley's *Risk Navigator* or OpenPages *SOX Express*. It has defined its own hierarchy which is different and better than *Risk Navigator* or *SOX Express*. It does not suffer from the follower problem.

Application Performance problem

The tool has been designed on .NET platform. There have been users' complaints that .NET is slow, but in any case it is much faster than J2EE applications. Also the product architecture is simple, so architectural constraints are lesser. So the tool does not suffer from Application Performance problem.

Tool homogeneity problem

The only third party integration is with Crystal Reports for showing dashboards, which is not a very complex integration. The tool does not suffer from Tool homogeneity problem.

Old Wine in New Bottle problem

Since Protiviti was not in existence before 2002, *SarbOx Portal* is a totally new and redesigned product. It does not suffer from old wine in new bottle syndrome.

Complexity of Installation problem

Installation of the tool needs installing .NET framework on a Windows machine, installing *SarbOx portal*, installing crystal reports plug-in, installing MS SQL 2000 database, and then configuring each of them. This is certainly not complex when compared to all J2EE based product installations. *SarbOx portal* does not suffer from Complexity of Installation problem.

Feature Gaps

Protiviti is a simple system. In many cases a simple but sharp solution may yield better results than a feature heavy but a confusing product. It does not have versioning capabilities, Issue tracking mechanisms, Control Self assessment etc.

Other problems

Risk information is added into the system as a document rather than as a database field. This architecture causes problems in doing reports in risk field and getting risk count.

Risk Representation: Risks are represented as types, i.e., every conceivable risk has to be added as a type first and then it has to be mapped to every process.

Complex mapping scheme: There are several system configuration maps: Organization Structure-Financial Model map, Financial model-Process map, PCS-Organization map. The multi layered mapping process creates difficulty in aggregate data management. Ideally the tool should have had only a single mapping operation (It is difficult to achieve in the tool as it has three separate entities Organization Model, Financial Model & Process Model).

Certus – *302/404*

Company Background

Certus was started in March 2001 with the name of nthOrbit with initial focus on developing real-time, supply-chain software. In 2003, Certus (Then Nth Orbit) jumped into Sarbanes-Oxley bandwagon when in May it released *Certus* as a compliance management product. The product was an integration between *Vignette* which was an Enterprise Content Management Software and *Webmethods* which is a workflow solution. The key promoter of Certus was Vani kola. Before Nth orbit, she was the CEO of RightWorks which was sold to ICG technologies at the height of Internet boom at 22 million dollar cash and 635 million dollars in stock.

Certus 302/404 is a amalgated product which integrated two independently standing products: *Vignette* (For Documents/Record management/CMS) and *Webmethods* (for workflows and alerting.) It is a J2EE based product. The *Certus-Vignette* integration is achieved through a program called "*Certus-Vignette Link*".

Certus Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	Fail
Excel Sheet Column Definition problem	Fail
Control Multitude problem	Fail
Process Narratives Maintenance problem	Success
Control Level Access and Audit problem	Fail
Fixed Workflow problem	Fail
Follower problem	Fail
Application Performance problem	Fail
Tool homogeneity problem	Fail
Old wine in new bottle Syndrome	Success
Complexity of Installation problem	Fail
Feature Gaps	Fail
Other problems	Fail

Account-Process-Risk-Control Hierarchy problem

Certus has fixed a hierarchy of Account-Process-Risk-Control. So it suffers from Account-Process-Risk-Control hierarchy problem. Also, *Certus* has got the context of ASSERTIONS wrong. It associates assertions to Controls and Risks instead of associating it to accounts.

Excel Sheet Column Definition problem

Certus has fixed fields for accounts, processes, business entity, and risks. It offers limited flexibility for control definition. So it suffers from Excel Sheet Column Definition problem.

Control Multitude problem

Certus has one screen at a time edit access for Controls definition. So it suffers from Control Multitude problem. However, they do have a screen where all controls associated with a process can be simultaneously viewed.

Process Narratives Maintenance problem

Certus is a marriage between independent third party products to get fast time to market. It used *Vignette* for Document & Records management. *Vignette* has good versioning capabilities. So the product does not suffer from Process Narratives Maintenance problem.

Control Level Access and Audit problem

Certus does not have Control level access. Also the auditing features are weak. It suffers from Control Control Access and Audit problem.

Fixed Workflow problem

Certus uses *Webmethods* to define fixed workflows. So it intrinsically suffers from Fixed Workflow problem.

Follower problem

Certus product philosophy seems deeply inspired from Paisley Consulting's *Risk Navigator*. There is a very strong correlation between product features and workflows between the two products. For instance, common taxonomy for Issue management features has been used in both products. So it suffers from follower problem.

Application Performance problem

Certus is a marriage between independent third party products to get fast time to market. It used *Vignette* for Document & Records management. It used *Webmethods* for Workflow and alerting. The performance of amalgated products in J2EE technologies are generally slow, so the tool suffers from Application Performance problem.

Tool Homogeneity problem

Certus 302/404 is a amalgated product which integrated two independently standing products: Vignette (for Documents/Record management/CMS) and *Webmethods*(for workflows and alerting.) It is a J2EE based product. The *Certus-Vignette* integration is achieved through a program called "*Certus-Vignette Link*". So *Certus* fails Tool Homogeneity problem.

Old Wine in New Bottle problem

Certus started as a supply chain management company. However its compliance product has been conceived and designed after the promulgation of the Sarbanes-Oxley Act. Its supply chain product has not been reused in *Certus 302/404*.

Complexity of Installation problem

Certus does not have a homogenous solution. It has tried to integrate two existing market products and tried to position it as a compliance solution. *Certus* is a marriage between independent third party products to arrive to a solution with fast time to market. It used *Vignette* for Document & Records management. It used *Webmethods* for Workflow. Installation of *Certus* is separate installation of *Vignette*, *Webmethods*, *Certus* Integration patch. The product has multiple databases, multiple application servers. Maintenance of this application will be very difficult.

Feature Gaps

Certus does not have Control Self Assessment functionality.

Other problems

If any one of the three companies: Certus, *Vignette* and *Webmethods* cease business operations, the product maintenance will be severely affected.

Movaris – *OneClose*

Company Background

Movaris is a venture capital funded company based out of Cupertino, California. Movaris offers *Movaris OneClose* (previously known as *Movaris Certainty*). Movaris as a company has worn several hats. It started as a paperless office solution provider. For sometime it was a BPM company. Later it became a financial records transaction company until Sarbanes-Oxley act happened, after which it extended its operations to provide internal control services through Financial Statement transaction processing. The fundamental concept in Movaris offering is that internal controls must be attested/verified before a financial close operation is done. Thus it intends to make Internal Controls attestation a line function before quarterly closure of accounts. Movaris Certainty was released in September 2003. This product was renamed to *OneClose* in October 2005.

Movaris is not a typical web based SOX compliance product, as it has a totally different philosophy of approaching SOX 302/404 compliance. A central assumption in Movaris is that each control must be linked to at least one financial statement (Balance Sheet/Profit & Loss Account/Cash Flow Statement) item before it can be incorporated into the system. This approach has the advantage that every control gets directly linked with a financial statement item. However, it becomes impossible to map indirect controls like IT controls, and controls that are operable above the financial statements like General Ledger controls, or operational controls. A lot of process re-engineering/reclassification would be needed before this tool can be incorporated in any organization. Compliance operations in this product can be successfully done only for those clients who carry out their financial accounting/closures already through Movaris. It is doubtful that companies would junk their investment in existing GL/central accounting systems just to obtain better compliance. It is not anticipated that double closures would be done by companies, once in their core financial systems and again in Movaris *OneClose* platform. This seems best suited for customers who are already using Movaris financial transaction services.

The technology platform for Movaris has been driven by Mr Steven Yankovich. Prior to founding Movaris, Mr. Yankovich was responsible for developing the software/hardware design environment at HAL Computer Systems for six years. Earlier, he managed the technical support and quality assurance team at Aida, an engineering software startup that was later sold to Teradyne, for five years. Before that, Mr. Yankovich developed the design environment at American Super Computers, Inc.

Movaris Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	NA (* see below)
Excel Sheet Column Definition problem	NA*
Control Multitude problem	Fail
Process Narratives Maintenance problem	NA*
Control Level Access and Audit problem	NA*
Fixed Workflow problem	Fail
Follower problem	Success
Old wine in new bottle Syndrome	Fail
Complexity of Installation problem	Partial Fail
Feature Gaps	Fail
Other problems	Fail

***** *Movaris OneClose* is a Java based enterprise application. Since ***Movaris OneClose*** **is not a generic Sarbanes-Oxley compliance product, a lot of issues with generic Sarbanes-Oxley solution are not applicable.**

Account-Process-Risk-Control Hierarchy problem

Movaris has a hierarchy of Financial Statement Item-Risk-Control. It has completely done away with Account-Process-Risk-Control concept, so this problem is not applicable.

Excel Sheet Column Definition problem

An essential requirement for implementation of this product is that Financial Statements be imported into the application. Each control in an excel sheet would have to be individually mapped to an item in financial statement. If organizations objective is replacement of their existing excel sheets, this is not a suitable product. However if companies are totally starting afresh, they can use this philosophy. Excel Sheet column definition problem is not applicable for Movaris.

Control Multitude problem

OneClose has one control at a time edit screen. Each of the controls are linked to an item in Financial statement. It suffers from Control Multitude problem.

Process Narratives Maintenance problem

It allows attachment of evidence files only in form of attach evidence, such as the reconciliation template, a bank statement, or a general ledger screenshot. Since there is no concept like process, process narratives cannot be maintained in Movaris. Version control is irrelevant in *OneClose*. Movaris is not suitable for Process documentation. Process Narratives Maintenance problem is not applicable in case of Movaris.

Control Level Access and Audit problem

Access control is enforced through roles in a financial statement. Control Level Access and Audit problem is not applicable in case of Movaris.

Fixed Workflow problem

The *OneClose* application is itself a fixed financial workflow. So it suffers from fixed workflow problem.

Follower problem

Movaris certainly has its own unique Sarbanes-Oxley compliance solution. It cannot be accused of suffering from follower problem.

Old Wine in New Bottle problem

Movaris Process server, Movaris Dashboard etc are products that have been constructed by Movaris well before Sarbanes-Oxley act came into place. Since Movaris has rejigged its old service offering to a SOX compliance solution, it suffers from old wine in new bottle syndrome.

Complexity of Installation problem

To install Movaris *OneClose* the following has to be installed:

- Java Development Kit
- Servlet Exec/AS from New Atlanta which is an application server(has to be separately procured)
- A database: Oracle, DB2 or MS SQL server

A minimal installation will take at least a week. It partially suffers from complexity of installation problem.

Feature Gaps

No Process Documentation version control system.

Other problems

The application server used is Servelet Exec/AS 4.2 or version 5.0 for Windows software from New Atlanta. This has to be separately purchased in addition to Movaris. It offers only two frameworks COSO and COSO ERM which is prepackaged into the product. Reporting is outside the product through Crystal Reports.

IBM – *Workplace for Business Controls and Reporting*

Company Background

IBM as a company needs no background. It was a late entrant to Sarbanes-Oxley compliance market when it launched a J2EE based compliance tool called IBM *Workplace for Business Controls and Reporting* in October 2003. The tool links needs Lotus Notes infrastructure for messaging/collaboration capabilities. IBM under previous Chairman Lou Gerstner's leadership made a hostile acquisition of Jim Manzi's Lotus Development Corporation for USD 3.5 Billion at 64.50 USD per share in 1995 when the Lotus stock was trading at only USD 32 per share. It seems that IBM is till now trying to protect its investment in Lotus technology. In 1995 Lotus was a great concept when Internet Standards were evolving, but it no longer holds true in the new millennium. Lotus Notes was indeed one of the first to offer enterprise level collaboration and messaging capabilities. However one of the biggest flaws of Lotus notes was its performance. The other problem was its scalability. Lotus Notes operates on a proprietary protocol and on a non standard web TCP/UDP port 1352. As a result Lotus Domino/Notes based architecture needs a company to install the whole server infrastructure at every location where Notes services are needed. This causes another compound problem of trying to ensure uniformity of separate database in every location through replication mechanisms. Subsequently ultra lightweight collaboration/messaging technologies have evolved, but with the amount of investment made by IBM, it seems stuck to a 1995 pre-web days technology.

The leadership for IBM's Sarbanes-Oxley solution has been provided by Larry Bowden who is Vice President, IBM Workplace Software Solutions and works from Somers, NY. Previously Larry was Vice President of Portal Solutions and Lotus Products for IBM's Lotus Software brand, so the tool has distinct Lotus Notes based flavor. Mr. Bowden was also instrumental in aggressively pushing *WebSphere* Portal product line in his earlier role. It was quite natural that *WebSphere* Portal product crept into IBM's *workplace for business controls and Reporting*. *WebSphere* is another J2EE based application server technology. As said earlier, all J2EE based technologies are expected to have performance issues inherently. Larry holds a BS degree in engineering and an MBA, both from the University of Denver.

IBM Performance Matrix

Test Case	Result
Account-Process-Risk-Control Hierarchy problem	Success
Excel Sheet Column Definition problem	Fail
Control Multitude problem	Fail
Process Narratives Maintenance problem	Success
Control Level Access and Audit problem	Success
Tool itself not compliant to Sarbanes-Oxley IT controls problem	Fail
Fixed Workflow problem	Fail
Follower problem	Success
Application Performance problem	Fail
Tool homogeneity problem	Fail
Old wine in new bottle Syndrome	Success
Complexity of Installation problem	Fail
Feature Gaps	Fail
Other problems	Fail

Account-Process-Risk-Control Hierarchy problem

IBM Workplace for Business Controls and Reporting hierarchy structure is Process → Subprocess → Objective → Risk → Control → Procedure. The product designers have done a good job in ensuring that Financial modeling carried out not through a leaf in the defined hierarchy tree, but as an optional modeling item. This makes the system flexible to address any type of Control modeling requirements. Another good feature in the product is that Financial statements could be optionally mapped to Sub-process. The financial statements supported are Income statement, Balance sheet, Disclosures. It would have been good if the designers could have supported Cash flow statements as well. The product does not suffer from Account-Process-Risk-Control hierarchy problem.

Excel Sheet Column Definition problem

All the definiton fields in Process → Subprocess → Objective → Risk → Control → Procedure are fixed. So this tool suffers from Excel Sheet Column Definition problem.

Control Multitude problem

The control data entry procedure is as follows. When the user opens a control object in the evaluation phase, the control data attributes are displayed along with the procedure results. The procedure results include the procedure name, procedure owner, procedure evaluation date, and procedure conclusion. The control evaluator can evaluate the control based on the summary procedure information or can "drill down" into a procedure if they want more detailed information about a procedure. The control is rated as effective or ineffective. The control evaluation frequency, next evaluation date, and the rationale for the next evaluation date are set. In this scheme, control data has to be entered one at a time. So control multitude problem exists in the tool.

Process Narratives Maintenance problem

IBM Workplace for Business Controls and Reporting has versioning and archiving capabilities. So it does not suffer from Process Narratives Maintenance problem.

Control Level Access and Audit problem

IBM's hierachy is Process → Subprocess → Objective → Risk → Control → Procedure. Ownership is defined and delegated at Control and Procedure level. The solution provides very good data auditing features. The product does not suffer from Control level access and audit problem.

Tool itself not compliant to Sarbanes-Oxley IT controls problem

As this product is a complex mixture of several individual IBM products, there are several layers where users would have to be created and configured. In such a scenario to obtain Sarbanes-Oxley IT controls compliance, the tool must ensure that at every layer wherever a user is created, password controls, account lockout controls and session timeout controls must be present. For the purpose of this document, I will take up end users created through the main application ie Business Controls & Reporting. For such users: password controls, account lockout controls and session timeout controls are not present. **This brings a client procuring the product to a paradoxical situation: He will become non-compliant to Sarbanes-Oxley IT controls if he procures and installs Sarbanes-Oxley solution from IBM.**

Fixed Workflow problem

Workflow as a separate entity is not an important application component in this compliance solution. So this is not applicable. It has an embedded workflow that can help reduce the risk of errors by streamlining user reviews and approvals. So it suffers from fixed workflow syndrome.

Follower problem

The tool design has been freshly thought. So it does not suffer from follower problem.

Application Performance problem

J2EE based application server along with Lotus Notes based architecture will ensure that the tool will have application performance issues.

Tool homogeneity problem

Apart from the database and the LDAP server, the tool packages *WebSphere* Portal and Application Server, DB2 client, Content Manager, Business Controls & Reporting, Crystal Enterprise. This is in no way homogenous. So the tool suffers from lack of homogeneity.

Old Wine in New Bottle problem

IBM Workplace for Business Controls and Reporting is a totally redesigned product, albeit on IBM platform only. So it is not old wine in new bottle.

Complexity of Installation problem

To install *IBM workplace for business controls and Reporting*, the following components must be installed.

- DB2 Database Server
- LDAP Server
- *WebSphere* Portal and Application Server
- DB2 client
- Content Manager
- The main compliance solution: Business Controls & Reporting
- Crystal Enterprise

This is an amazingly complex installation. God save the client.

Feature Gaps

It does not have Issue tracking mechanisms.

Other problems

The solution has fixed roles. These roles are

- Super users
- Business unit/process/subprocess owners
- Control owners
- Procedure owners
- Auditors

If an organization's implementation of compliance is not done through this role structure, it will become difficult to fit in the solution.

Peoplesoft – *Internal Controls Enforcer*

Company Background

Peoplesoft was acquired by Oracle in January, 2005. It is very strange to observe that same company is releasing two competing products, Oracle *Internal Controls Manager*(*IC Manager*), and PeopleSoft Internal Controls Enforcer(IC Enforcer). I pity the customers of Oracle, what should they assume Oracle wants to sell them, *Oracle Internal Controls Manager*(*ICM*), or *PeopleSoft's Internal Controls Enforcer*(*IC Enforcer*). In the interest of customers like my clients, I request Oracle to come up with a clear stand on which compliance product it intends to back up.

I did not have sufficient data to analyze PeopleSoft's *IC Enforcer*. So I can't make any judgment on PeopleSoft. However I will point readers to the summary of contents of an independent analysis of *IC Enforcer* carried out by Forrester. I will remind readers of this document that normally I don't subscribe to the view presented by third parties unless I verify the accuracy of contents myself. In this case, I don't have enough evidence to verify Forrester's analysis on *PeopleSoft's Internal Controls Enforcer*. So I don't endorse the views of Forrester. Copyrights to succeeding section belong to Forrester

Link to Forrester's Analysis

http://www.forrester.com/Research/Document/Excerpt/0,7211,36844,00.html

Conclusion

Concluding Remarks

Of all the problems listed above, none of the tools have successfully addressed The Excel Sheet Column Definition problem and the Control Multitude problem, which in my view are most important problems. So as things stand now, if one goes for a tool based implementation, selects a tool from the list given above, the probability is very high that the tool based implementation will fail.