

Sarbanes Oxley and the Impact on Information Technology

By: Frank Padavano, IT Managing Director

About Accume Partners

- **Founded by Big Four partners in 1994**
- **Proprietary, risk-based internal audit approach**
- **Proven business model adds value**
 - **Professionals averaging nearly 20 years experience, deployed at competitive rates**
 - **Excellent reputation among clients, regulators, and the Big Four**
 - **Sarbanes-Oxley - Experience with over 100 SOX clients**



Background On Sarbanes Oxley (SOX)

- **New Law to Protect the Stock Holders**
- **Too Many “Enron’s” - Government and Accounting Board had to do something to improve confidence on the Health of our Market System**
- **PCAOB issued audit standard for the external auditor’s attestation opinion in July 2004**



3

Background On Sarbanes Oxley (SOX)

- **Requires an “Internal Control Report” that states:**
 - **Management’s responsibility to establish and maintain a system of internal controls governing financial reporting; and**
 - **The effectiveness of the financial reporting controls**
 - **Signed Acknowledgment by CEO and CFO**
- **Requires an attestation report by external auditors i.e. KPMG, PwC, Deloitte & Touche**



4

More About SOX

- **External Accountants need comfort that controls are in place and effective. Including Information Technology**
- **CIO's and IT Directors must also demonstrate that the IT controls are working**
- **Material Control breakdowns = disclosure in the Financial Statements**
- **Controls include process and technical controls to protect the Data**



5

How Does IT Get There

- **Management must Identify the Key Controls within each process**
- **Test Key Controls and Validate that they are effective**
- **Report Control Issues and action plan to correct**
- **Retest the controls to demonstrate that the corrected controls are working effectively**



6

IT Structured Approach

- **General Computer Controls**
- **Application Level Controls**
- **Third Party Service Providers**
- **Use of Spread Sheets**



7

General Computer Controls

- **Information Security**
 - **What is the Process in place to control and manage logical Access**
 - **Security Monitoring - How Does Management ensure that Access is correct and maintained**
 - **Is Employees access to process transactions consistent with functional Responsibility**



8

General Computer Controls

- **IT Governance**
 - **How Does Management ensure IT is meeting the Business Needs**
 - **Are there Segregation of Responsibilities Concerns**
 - **Hiring Practices for People, Training etc.**

General Computer Controls

- **Application Development**
 - **Separate Prod and Dev environments**
 - **Version Control**
 - **Unit Testing Changes**
 - **User Acceptance Testing**
 - **Migration - How Does IT move code**
 - **Who can move or modify production data and code**

General Computer Controls

- **System Software**
 - **O.S. Version - Supported**
 - **Patch Management**
 - **Virus Protection**

11



General Computer Controls

- **Network Management**
 - **Network OS - Security**
 - **Firewalls & Routers**
 - **Patch Management**
 - **Virus Protection**

12



General Computer Controls

- **Computer Operations**
 - **Data and Software Backup**
 - **Job Scheduling and Monitoring - File Transfers**
 - **Help Desk Support – Software?**
 - **End User Computing**
 - **Software Licensing**

13



Application Level Controls

- **In many Financial Business Processes, Key Controls are identified as “Automated” (e.g., A/P three-way match)**
- **These need to be jointly determined with IT and Financial to document and test**
- **Evidence should be Included in the Financial Business Process testing support**

14



Spreadsheets

- **Many companies rely on spreadsheets for financial reporting while having Elaborate Systems**
- **Inventory all Spreadsheets during Business Process Narrative with financial relevance (e.g., pricing models, journal entries, consolidations) and if possible obtain Server that the Spreadsheet (file) resides**

15



Spreadsheets

- **What we needs to be tested in IT:**
 - **Determine that all Files (as per Inventory of Spreadsheets) are on Server**
 - **Review Logical Security - who can do what to a Spreadsheet and evaluate access (segregation of duties)**
 - **Ensure all Files are backed up**

16



Spreadsheets

- **What should be tested by the Financial Folks:**
 - **Input Errors – Data entry or cut and paste**
 - **Logic Errors – Incorrect formulas**
 - **Interface Errors – Import or export issue**
 - **Version Control – Is the user's Spreadsheet on the server or on PC?**

Third Party Service Providers

- **Demonstrate controls are in-place and effective for Service Providers:**
 - **Not all Service Providers are included– Based on Materiality and Activity**
 - **How to get Comfortable – Either a Type II SAS 70 or a Site Visit**
 - **SAS 70 – Need to Review Opinion, Reported Issues and User Control's**

Critical Success Factors

- **Start Early**
 - **Compliance is a long-term project**
- **Top-Down Approach**
 - **Management must support the initiative**
- **Coordinated Team Effort**
 - **Management**
 - **External Auditor**
 - **Facilitator**
- **Tailor Approach to Specific Needs**
- **Leverage Technology Tools**
- **Communicate Progress Early and Often**



Lessons Learned

- **Need Better and More Frequent Communications with Financial team including Work paper consistency, need for IT resources**
- **Material Issues with Security and Change Control**
 - **Logical Security Access – User has the ability to process transactions inconsistent with functional responsibility**
 - **Change Control – Programmers can modify production software and production data**



Lessons Learned

- **Vendor Management – Lack of process. No SAS70 report or not reviewed.**
- **Not enough IT Auditors Exist to do all the work**
- **External IT Auditors used checklist approach and determined that there were deficiencies. Most were not applicable or had limited impact**



For more information, please contact:

Frank Padavano
Managing Director
609-322-5046
Fpadavano@accumepartners.com