



Introduction to
AUTOMATION VALIDATION FOR PUBLIC COMPANIES
Pertaining to Sarbanes-Oxley Regulations

Presented by
Alan S. Kaplan
President / CTO, Xactis Corporation

At a recent panel discussion addressing 750 top CIO's, the statement was made:

“The Greatest Risk to SOX Compliance is in your automation.”

And all panel members agreed.

BACKGROUND ON CONGRESSIONAL TECHNOLOGY CHALLENGES

As an understandable reaction to financial fraud and corporate scandals, Congress has mandated new regulations for which compliance is technically challenging and perhaps not even feasible in the real world of IT. This is not the first time they did this.

Congress once mandated “*KNOW YOUR CUSTOMER*” to the Department of Education so that students who cheat the government would not get any further financial assistance. A great idea to save money and catch cheaters!

- The project was to combine 12 systems to accomplish this worthy goal. The price was 2.2 million dollars and the contract was issued to CSC.
- The GAO sensed the project was not technically possible.
- Analyzing source code and data proved it and the contract was cancelled.
- The taxpayers saved most of the money and a scandal was averted.

Now they have legislated another technically challenging mandate. But technically speaking, SOX Compliance is really:

- An elusive goal – not a destination
- A risk to be managed – not solved
- A highly evolving scenario, with changes that affect your professional operations and personal security – Sarbanes Oxley – Section 404

Recently queried a large accounting firm about their SOX compliance methodology as it relates to IS Audit, and only got a blank stare in response. But the truth is “The Greatest Sarbanes Risk We Face is in the Automation” as follows:

- Reviewers and auditors have traditionally relied on bank statements, interviews and documentation reviews to assess regulatory related risks and to assist management with sufficient controls to be compliant with regulations.
- Some sample testing is the common technique used to partially validate automated processes and rules embedded in the IT systems.

- As the roles and complexity of enterprise information systems has grown, a new need is emerging to have online controls and business intelligence systems governing financial reporting.
- But only the most knowledgeable companies and IT Governors know that in-depth system analysis is required to validate these automated processes, rules, and data –pertaining to regulations requiring more integrated and accurate information about their controls under Sec. 404 (including enhanced worm, virus and intrusion detection).

Managers, Compliance Officers and IT providers are scrambling to package tools and services to help their customers reach compliance; but no matter which controls are chosen, the risk of the initiative will depend on:

- Compliance Initiative support and budget
- Compliance Officers that are well-trained and given authority over autonomous entities with the organization
- Effective monitoring of customers, transactions and accounts
- Effective monitoring for insider misconduct
- Effective reporting to management and regulators
- Diligence and Enhanced Due Diligence
- Compliance Information Integration
- Data Management Skills – including data quality to facilitate meaningful integration
- Documentation of policies, procedures and personnel
- Documentation of automated systems
- Audit – validating the adequacy and effectiveness of controls!

MITIGATING RISKS THROUGH AUTOMATION VALIDATION

The purpose of audits is to validate adequacy and effectiveness of controls – to mitigate risks through Information system review, and independent validation and verification.

The audit / review / IV&V process must:

- Be viewed with prestige and in a positive way
- Bring together all of the company to do what is nearly impossible: team building
- Analyze controls
- Document rules and processes in the automation
- Document the data lineage from reports
- Have access to and check historical data to see what the people and automated systems are catching and what they are missing
- Effectively and proactively handle external audits to minimize penalties for infractions



FINANCIAL INFORMATION VALIDATION METHODOLOGY

Step One	Identify Critical Information End-items
Step Two	Trace Data Lineage Back to Origins
Step Three	Determine the Meaning and Validate the Quality of the Original Data
Step Four	Validate Application Processes, Business Rules and Related Controls and Verify Automation Security
Step Five	Follow Data Lineage Forward to Validate Mappings, Transformations and Data Quality
Step Six	Verify Security at Data Consumption Points
Step Seven	Validate End-to-end System Security

SUMMARY – YOUR GREATEST RISK TOWARD COMPLIANCE

- Reviewers and auditors have traditionally relied on interviews and documentation reviews to assess regulatory related risks and to assist management in becoming compliant.
- Sample testing is the common technique used to partially validate automated processes and rules embedded in the IT systems.
- As the roles and complexity of enterprise information systems has grown, a new need is emerging to have in-depth system analysis to validate these automated processes, rules and data as they pertain to new regulations requiring more integrated and accurate information.
- IT providers are scrambling to package tools and services to help their customers reach compliance; but no matter which applications are chosen, the success or failure of the initiative will depend on data quality and integration.