

SOX Readiness: How to Comply in a Changing, Technologically Complex World

Deborah Frazer Somerville, President
FSC LLC

Steve Shofner, Senior Manager
Armanino LLP

Andy Snook, President
Fastpath, Inc.

Agenda: 9:00 – 10:15 a.m.

- Introductions and logistics
- Presentation 1: SOX – How to succeed in compliance – and live to tell the story
- 10:05 – 10:15 a.m. - Break

Agenda: 10:15 a.m. – 12:00 noon

- Presentation 2: Testing Automated Controls
- Presentation 3: Demystifying risk management in ERP systems
- 11:55 – Transition to lunch

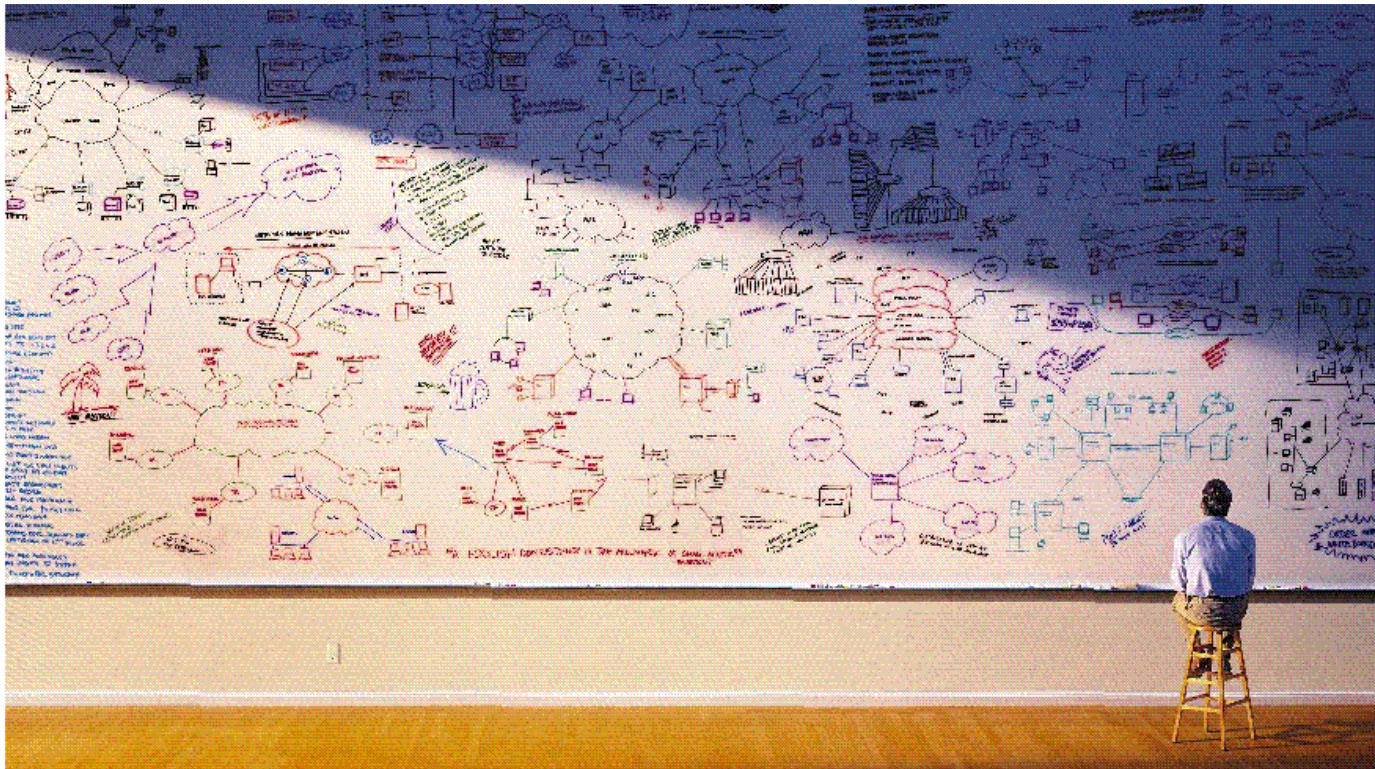
Agenda 12:00 noon – 2:00 p.m.

- 12:00 noon – 1 p.m. – Lunch and networking
- 1:00 – 2:00 p.m. – Expert Panel Q&A

SOX READINESS – HOW TO SUCCEED IN COMPLIANCE – AND LIVE TO TELL THE STORY

DEBORAH SOMERVILLE
FSC

SOX Readiness – Where to begin?



SOX 404 Requirements

- Top Line Requirements
 - Management is required to provide a written report on the effectiveness of internal controls over financial reporting
 - The company's auditors are required perform an independent assessment on the effectiveness of internal controls over financial reporting as part of their integrated audit
- Company Requirements
 - Controls must be:
 - suitably designed
 - appropriately documented
 - tested
- Auditors' Requirements
 - Understand company's control objectives and structure
 - Assess completeness and effectiveness of control structure
 - Test control structure to confirm effectiveness

Phases of SOX 404 Program

- Phase I - Perform Planning and Risk Assessment
- Phase II – Develop Process Documentation
- Phase III - Evaluate Effectiveness of Controls
- Phase IV – Remediation and Summarize Results

Phases of SOX 404 Program

- Phase 1
 - Planning, scoping, risk assessment, prioritization of higher risk areas, develop timeline
- Phase 2
 - Design of controls, identification of gaps
 - Phased approach based on risk
 - Can be spread over time based on company requirements
- Phase 3
 - Perform test of controls – flexible approach to start with limited testing and move to more robust sample sizes
- Phase 4
 - Assess findings, remediate

PCAOB Audit Practice Alert No. 11

- In response to significant audit deficiencies frequently cited in PCAOB inspection reports
 - Risk assessment and the audit of internal control
 - Selecting controls to test
 - Testing management review controls
 - Information Technology considerations, including system-generated data and reports
 - Roll-forward of controls tested at an interim date
 - Using the work of others
 - Evaluating identified control deficiencies

Two Cited Deficiencies Directly Impact Audit Clients

- Testing management review controls
- Audit firms have failed to sufficiently:
 - Test the design and operating effectiveness of management review controls that are used to monitor the results of operations
 - Evaluate the precision of management review controls

Factors That Can Affect Level of Precision

- Objective of review
- Level of aggregation
- Consistency of performance
- Correlation to relevant assertions
- Predictability of expectations
- Criteria for investigation

Two Cited Deficiencies Directly Impact Audit Clients, cont'd

- Information Technology (IT) considerations, including system-generated data and reports
 - Generally, **how** does the control owner **know** the report they are using is **complete** and **accurate**
- Examples of uses of IT that significantly affect internal control
 - Risks of material misstatement resulting from IT processes/systems
 - Important controls that depend on the effectiveness of IT controls, e.g., **system-generated reports**
 - Important IT controls, e.g., automated controls that address risks of material misstatement and IT general controls (ITGCs)

What does this mean for your SOX program?

- Enhanced rigor when carrying out control activities is required
- Examples:
 - Single sign-offs as evidence of review no longer adequate
 - Indications of follow through must be present, e.g., **initials at variances reviewed; documentation reviewed attached to reconciliation**
 - Reviewers must annotate documentation with tick marks: **on items verified, on parameters used to generate reports, etc.**
 - Defining what is considered a system-generated report will be important
 - Extracts downloaded to Excel and analyzed – yes
 - A checklist created in Excel - no

How To Get Started

- Develop overall Project Timeline and include all four phases, specifically:
 - Planning, scoping and risk assessment
 - Document design of business process (BP) - revenue, record to report, external reporting, purchase to pay, treasury, payroll, etc. - controls, including narratives, Risk and Control Matrices
 - Conduct test of design and perform gap analysis; design remediation as appropriate
 - Document Entity Level Controls (ELC), mapping to COSO 2013
 - Document Information Technology General Controls (ITGC), mapping to COBIT 5 (and COBIT 5 to COSO 2013...)
 - Develop test plans and perform testing – BP, ELC, ITGC
 - Summarize and report to management
 - Initial draft of Management Assessment of Internal Controls memo and Management Evaluation of Controls memo

Appendix

- COSO 2013 and COBIT 5
 - Mapping of the 17 Principles to COBIT 5

COSO Principle 1

- The organization demonstrates a commitment to integrity and ethical values.
- COBIT 5 Coverage:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - APO01 Manage the IT Management Framework
 - APO07 Manage Human Resources

COSO Principle 2

- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- COBIT 5 Coverage:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - EDM02 Ensure Benefits Delivery
 - EDM03 Ensure Risk Optimization
 - EDM04 Ensure Resource Optimization
 - EDM05 Ensure Stakeholder Transparency

COSO Principle 3

- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- COBIT 5 Coverage:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - APO01 Manage the IT Management Framework

COSO Principle 4

- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- COBIT 5 Coverage:
 - APO01 Manage the IT Management Framework
 - APO07 Manage Human Resources

COSO PRINCIPLE 5

- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
- COBIT 5 Coverage:
 - All COBIT 5 Processes

COSO PRINCIPLE 6

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- COBIT 5 Coverage:
 - All COBIT 5 Processes

COSO PRINCIPLE 7

- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
- COBIT 5 Coverage:
 - EDM03 Ensure Risk Optimization
 - APO12 Manage Risk

COSO PRINCIPLE 8

- The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- COBIT 5 Coverage:
 - EDM01 Ensure Governance Framework Setting and Maintenance
 - APO01 Manage the IT Management Framework
 - APO07 Manage Human Resources
 - MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

COSO PRINCIPLE 9

- The organization identifies and assesses changes that could significantly impact the system of internal control.
- COBIT 5 Coverage:
 - APO01 Manage the IT Management Framework
 - BAI02 Manage Requirements Definition
 - BAI05 Manage Organizational Change Enablement
 - BAI06 Manage Changes
 - BAI07 Manage Change Acceptance and Transitioning

COSO PRINCIPLE 10

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- COBIT 5 Coverage:
 - All COBIT 5 Processes

COSO PRINCIPLE 11

- The organization selects and develops general control activities over technology to support the achievement of objectives.
- COBIT 5 Coverage:
 - DSS06 Manage Business Process Controls

COSO PRINCIPLE 12

- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
- COBIT 5 Coverage:
 - APO01 Manage the IT Management Framework

COSO PRINCIPLE 13

- The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
- COBIT 5 Coverage:
 - APO11 Manage Quality
 - MEA01 Monitor, Evaluate and Assess Performance and Conformance
 - MEA02 Monitor, Evaluate and Assess the System of Internal Control

COSO PRINCIPLE 14

- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
- COBIT 5 Coverage:
 - APO01 Manage the IT Management Framework

COSO PRINCIPLE 15

- The organization communicates with external parties regarding matters affecting the functioning of internal control.
- COBIT 5 Coverage:
 - EDM05 Ensure Stakeholder Transparency

COSO PRINCIPLE 16

- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- COBIT 5 Coverage:
 - MEA02 Monitor, Evaluate and Assess the System of Internal Control

COSO PRINCIPLE 17

- The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
- COBIT 5 Coverage:
 - EDM05 Ensure Stakeholder Transparency
 - MEA02 Monitor, Evaluate and Assess the System of Internal Control

TESTING AUTOMATED CONTROLS

STEVE SHOFNER

ARMANINO

Audit Objectives

- Financial Objectives
 - Existence or Occurrence
 - Completeness
 - Valuation or Allocation
 - Rights & Obligations
 - Presentation & Disclosure
- IT & Operational Objectives
 - Security
 - Availability
 - Confidentiality
 - Integrity
 - Scalability
 - Reliability
 - Effectiveness
 - Efficiency

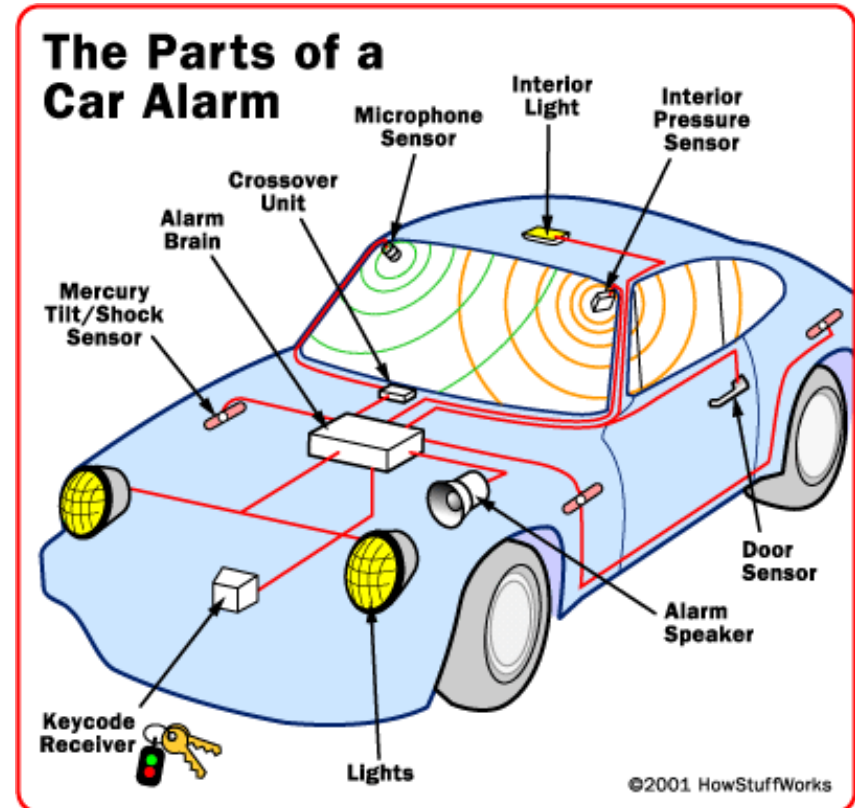
Compliance Audits Could Include Objectives From Both

Types of Controls

- Automated Controls
 - These are programmed financial controls
 - They are very strong: the programmed logic will function the same way every time, as long as the logic is not changed
 - Test of one versus a statistical test of many
- Partially-Automated Controls
 - People-enabled controls
 - People rely on information from IT systems (also referred to as Electronic Evidence) for the control to function
- Manual Controls (no IT-Dependence)
 - People enable the control
 - Controls that are 100% independent of IT systems

Other Ways To Categorize Controls

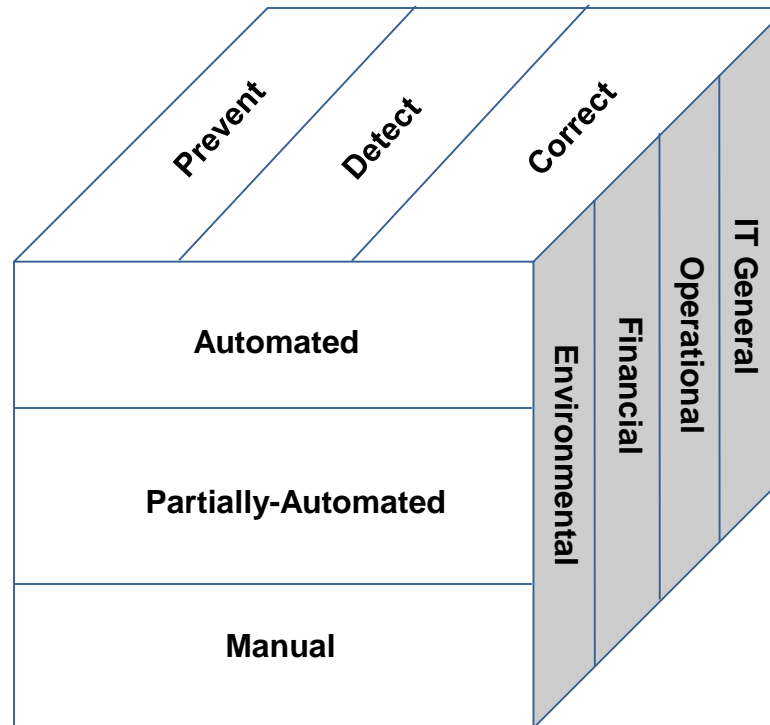
- Prevent Controls
 - The locks on your car doors
- Detect Controls
 - Your car alarm
- Correct Controls
 - Your auto insurance
 - A LoJack system (a device that transmits a signal used by law enforcement to locate your stolen car)



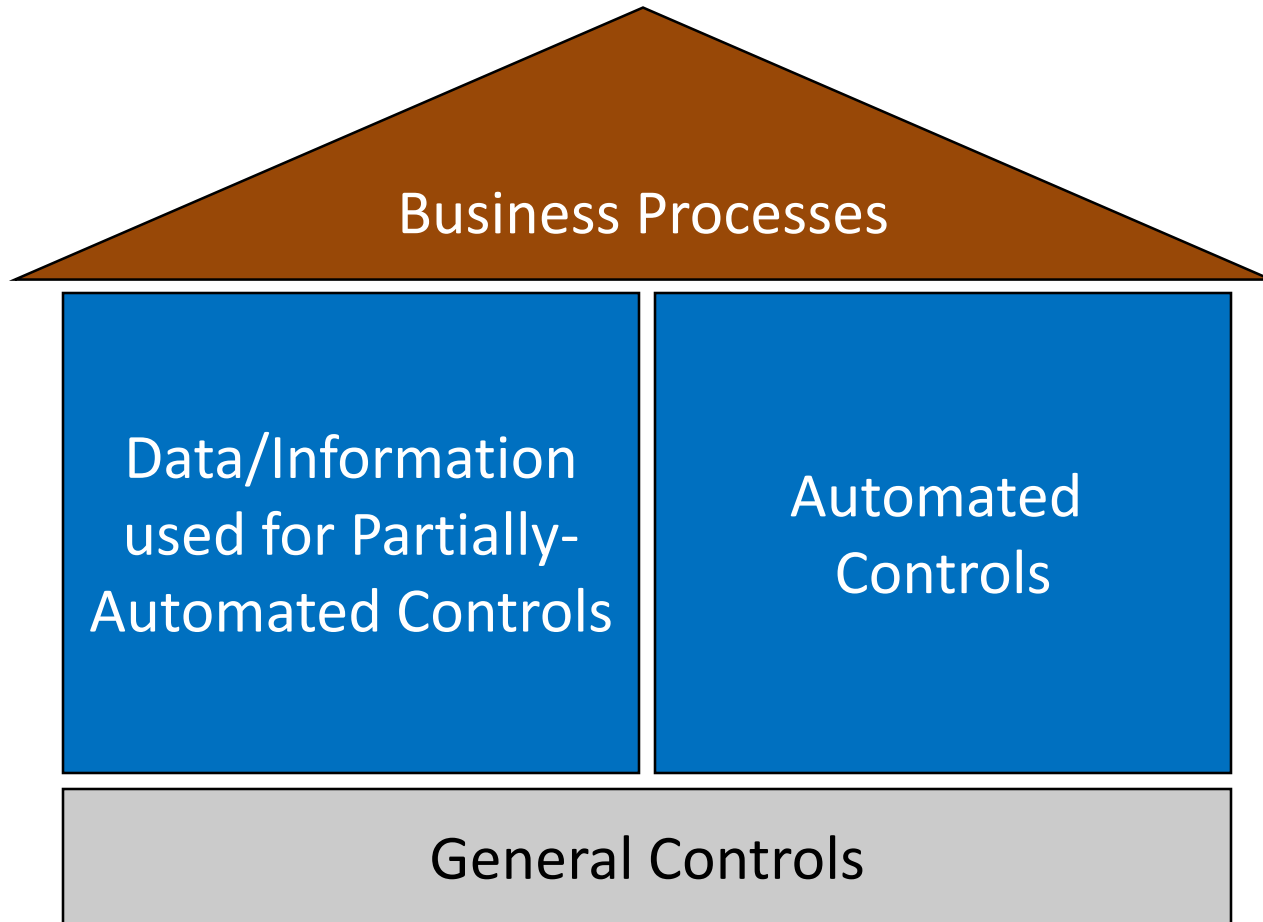
More Ways To Categorize Controls

- Environmental Controls
 - (a.k.a. “Governance”)
- Financial Controls
- Operational Controls
- IT General Controls
 - User Administration
 - Change Management
 - IT Operations
 - Physical Environment

Controls: Multidimensional

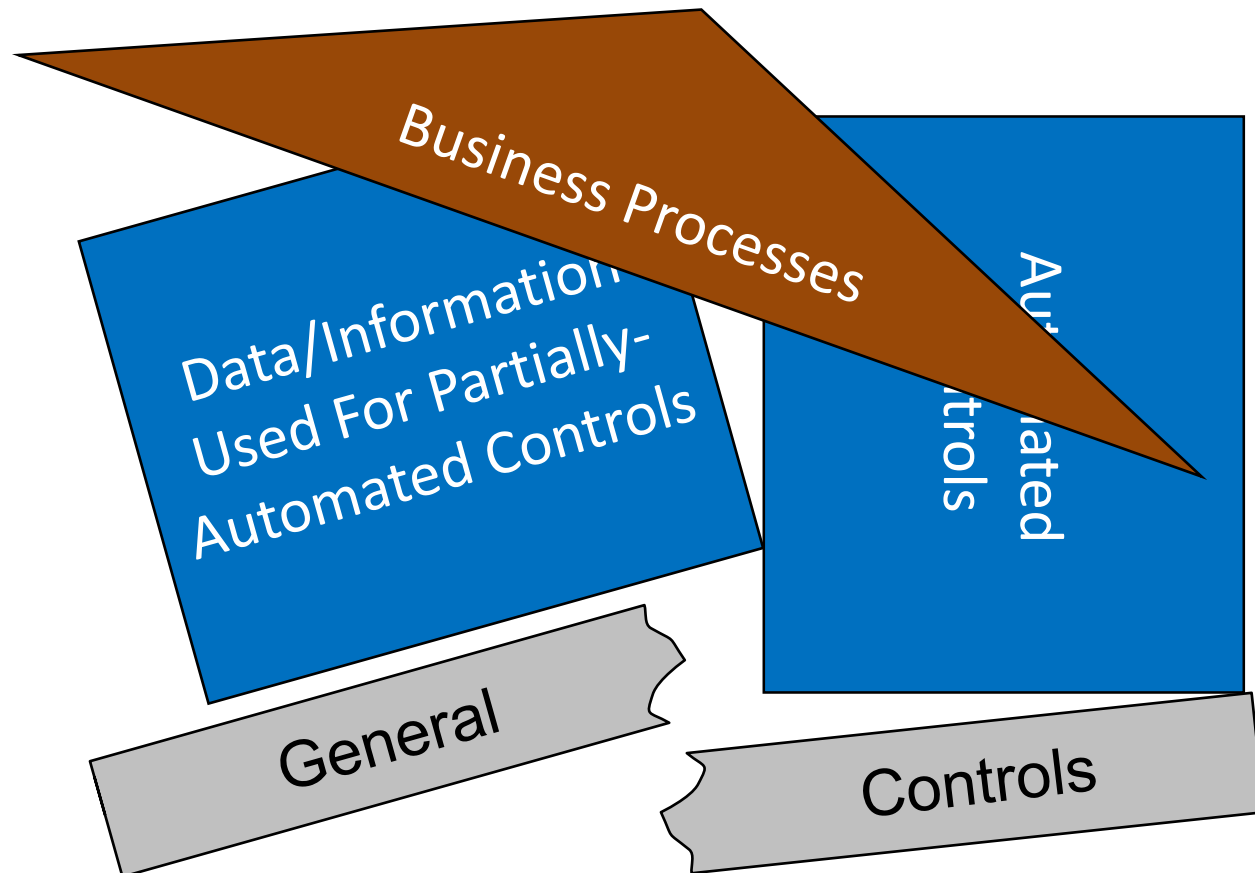


Reliance on Data and Related IT Systems



Reliance on Data and Related IT Systems

Potential For Significant Problems Exists



Automated Controls – We LOVE them!

- Automated Controls
 - These are programmed financial controls
 - They are very strong: The programmed logic will function the same way every time, as long as the logic is not changed
 - **They are easier to test: a test of one versus a test of many**

'Sample-Based' Test Strategy

- Obtain a population (a list of all transactions)
 - Ensure the completeness of the population
 - Ensure the accuracy of the population
- Possibly ensure the client has ensured the completeness and accuracy of the reporting they use
- Analyze the population size, frequency, etc. and select a sample of transactions
- Obtain documentation supporting the control activity for each sample selected
- Identify (potential) exceptions and discuss with control owners

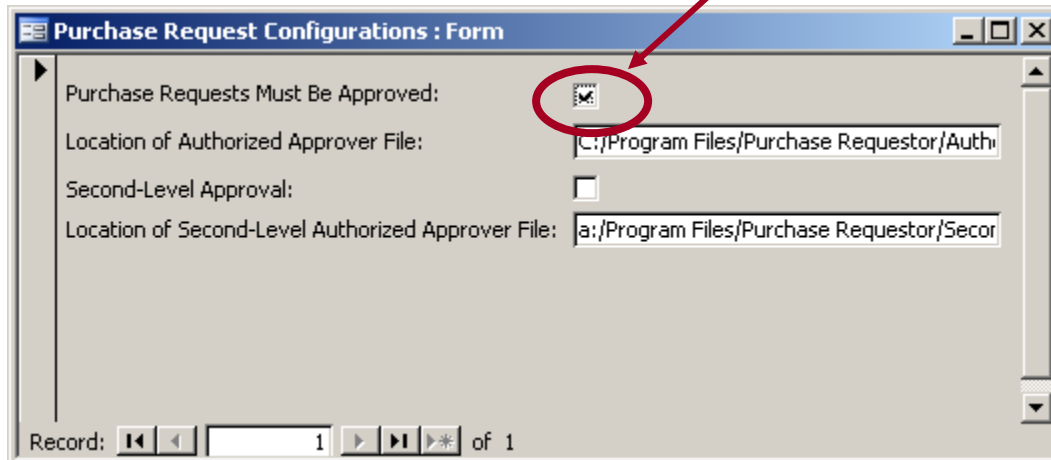
This approach introduces a level of 'audit risk,' resulting from the "Luck of the draw" with your sample selection

Automated Control Test Strategy

- Determine the programmed logic
 - Usually a configuration setting
 - Sometimes setting is “unconfigurable” (programmed into the application, and cannot be changed without changing program code)
- Follow one example of each *type* of transaction
 - This confirms that there isn’t anything ‘upstream’ or ‘downstream’ that may affect the outcome

Automated Controls: Test Strategy

- Example:
 - All Purchase Requests must be approved by a Manager or above
- 1. Get a screen-shot of the configuration setup screen showing this control is configured:



Purchase Request Configurations : Form

Purchase Requests Must Be Approved:

Location of Authorized Approver File: C:/Program Files/Purchase Requestor/Authv

Second-Level Approval:

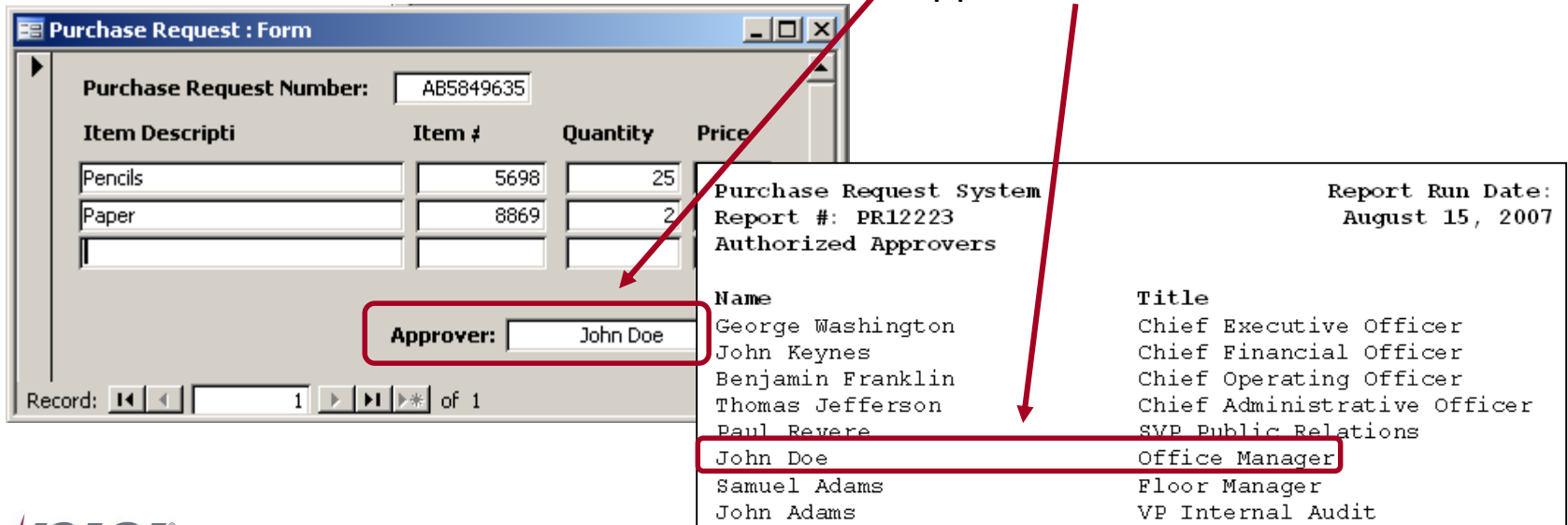
Location of Second-Level Authorized Approver File: a:/Program Files/Purchase Requestor/Secor

Record: 1 of 1

Automated Controls: Test Strategy

- Example:
 - All Purchase Requests must be approved by a Manager or above

 1. Get a screen-shot of the configuration setup screen showing this control is configured.
 2. Observe one completed purchase request and validate that the approver was on the authorized approver list.



Purchase Request : Form

Purchase Request Number: AB5849635

Item Descripti	Item #	Quantity	Price
Pencils	5698	25	
Paper	8869	2	

Approver: John Doe

Record: 1 of 1

Purchase Request System
Report #: PR12223
Authorized Approvers

Name	Title
George Washington	Chief Executive Officer
John Keynes	Chief Financial Officer
Benjamin Franklin	Chief Operating Officer
Thomas Jefferson	Chief Administrative Officer
Paul Revere	SVP Public Relations
John Doe	Office Manager
Samuel Adams	Floor Manager
John Adams	VP Internal Audit

Report Run Date: August 15, 2007

Automated Controls: Test Strategy

- Example:
 - All Purchase Requests must be approved by a Manager or above
1. Get a screen-shot of the configuration setup screen showing this control is configured.
 2. Observe one completed purchase request and validate that the approver was on the authorized approver list.
 3. You're done!



**Any (more)
Questions?**

**DEMYSTIFYING RISK MANAGEMENT IN
ERP SYSTEMS
ANDY SNOOK
FASTPATH**

Agenda

- Common challenges
- Working together: audit + IT + business process owners
- Application security
- Segregation of duties
- Audit trails

“Security refers to the features around user application permissions whilst Controls refers to the process controls within and external to the application.

The goal is an environment that uses a blend of Security & Control measures to mitigate risks that are operational or financial in nature”.

What we see at our clients

- Access security is low priority for the project team
- Process controls are not part of the consideration
- Security design is the domain of IT/Sys Admin and business is not aware
- No on-going monitoring of process controls
- No consideration of segregation of duties
- Dilution of 'go-live' security design
- Inability to report on current security setup
- Expensive customisations in place of S&C features

Working Together: Audit, IT and BPOs



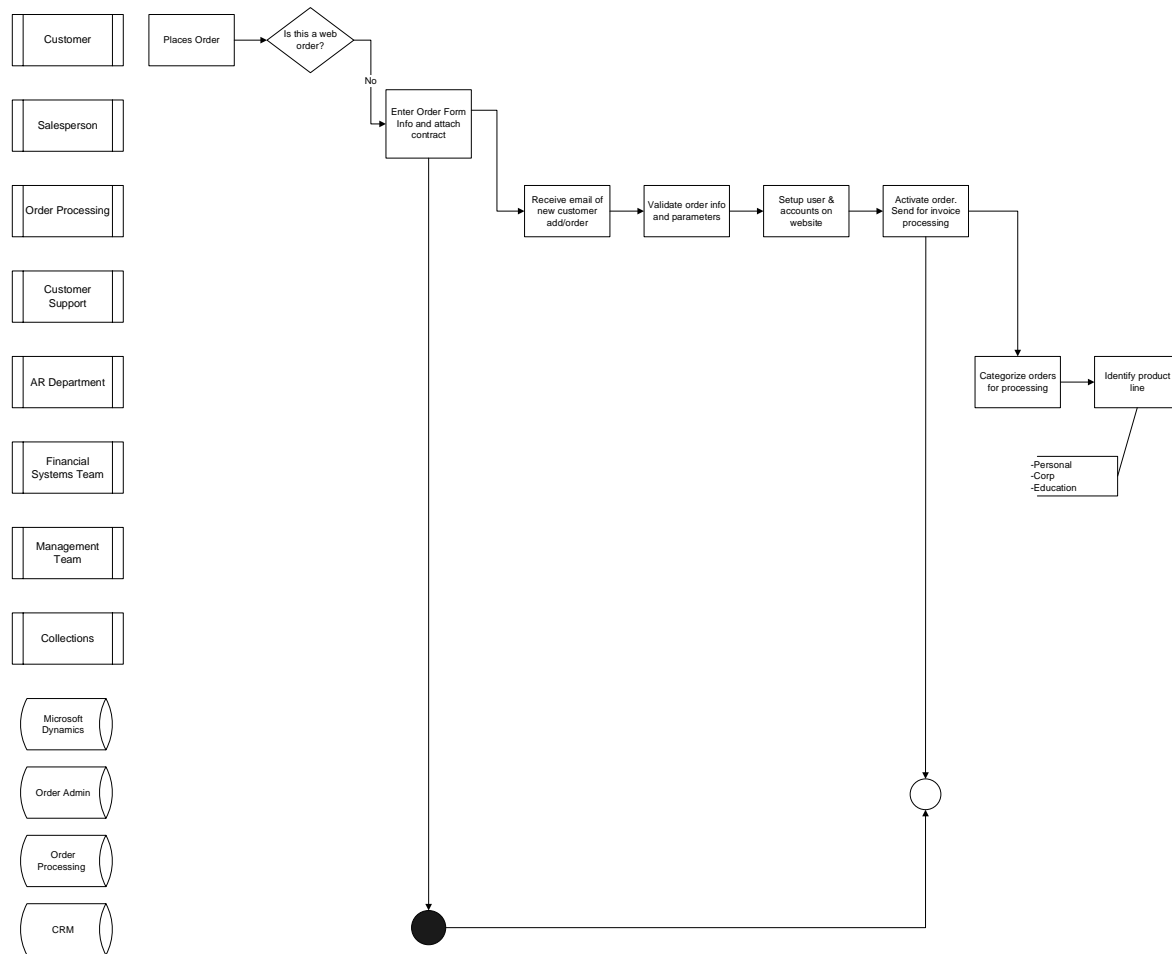
Working Together: Audit, IT and BPOs

- ERPs sit in the middle of IT and BPOs
- BPOs unsure of the underlying security
- IT unsure of the business process requirements/risks
- Few people have holistic view of process
 - Processing requirements
 - Financial
 - Roles
 - Systems, data, integrations
 - Risks

Working Together: Audit, IT and BPOs

- Identify the processes that are in scope
- Use business process maps to unite the teams
- Involve audit, IT and BPOs in mapping
- Include roles, systems and risks in map
- Provides basis for documentation, training, auditing

Map the process



Translate process and risk to ERP systems

- Base application security on business process maps
- Identify high risk business processes
- Determine functionality required for high risk processes
- Define risks, reviews, reviewers and periodicity
- Provide evidence that reviews are being done

3 Key Questions

- ▶ Who has access?
- ▶ Where are the risks in that access?
- ▶ What was done with the access?

Application Security – Who has access?

- Take a risk based approach
 - Analyze by function not by user or risk
 - Average system has over 5000 access points
 - Average system has 30-40 high risk access points
 - 500 vs. 1,000,000

Application Security – Who has access?

- Customers
- Vendors
- Item/Inventory
- Pricing
- HR
- Payroll
- Process disbursements (check run)
- Release/Approve purchase order
- Goods receipt
- Enter vendor invoices
- Post journal entries
- Open/Close GL accounts
- Ship customer orders
- Accounts Receivable transactions (post cash, credits)
- Credit & Collection (credit limits, hold, release)
- Customer order entry
- Process/Modify customer invoices
- Process credit memos
- Write-off customer accounts
- Record labor hours
- Payroll payment (check run)
- Prepare payroll (calculation/approval)
- Open/Close Fiscal Periods
- Maintain Users/User Security Privileges
- System/ Module Configuration – Settings
- Code changes

Application Security– Who has access?

- Take a risk based approach
 - Analyze by function not by user or risk
 - Average system has over 5000 access points
 - Average system has 30-40 high risk access points
 - 500 vs. 1,000,000
- Understand administrative access
- Application security vs. database security

Segregation of Duties

- Preventative vs. productivity
- Build a rule set of potential conflicts
- Identify Conflicts
- Mitigation
- 3 key questions
 - What are your rules?
 - Where are your risks?
 - What are you doing about it?

Audit trails – What did they do with that access?

- Take a risk based approach
 - Focus on key areas – Vendors, configuration, cash receipts, code changes, etc.
 - Focus on key fields – Payment terms, addresses, pricing, etc.
- Who changed it?
- When was it changed?
- Was it changed the right way?

Manual Journal Entries

- Direct impact on financial statements
- Easiest way to work around other controls
- Journal entry testing
- Focus on 5 W's
 - Who
 - What
 - Where
 - When
 - Why

Conclusion

- Bring finance and IT together
- Define processes and risks
- Take a risk based approach

Questions?