

The Deloitte logo is displayed in white text on a dark blue background. The word "Deloitte" is in a bold, sans-serif font, followed by a small yellow dot.

Deloitte.

Sustained Internal Control Compliance.

An Overview of Internal Control Solutions and Technologies

ISACA – Ottawa Chapter
January 16, 2006

Presenters: Carlton Wan & Mike Abbott

Audit • Tax • Consulting • Financial Advisory.

Introduction

- Facilitator introduction
 - Mike Abbott
 - Carlton Wan
- Participant introduction / demographics:
- How many of you:
 - Are from organizations that have gone through Internal Control Certification activities?
 - Are from organizations that are going through Internal Control Certification activities?
 - Have implemented some form of compliance tool? Are considering an implementation?

Agenda

- Introductions
- Current Climate
- Technology architecture for sustaining compliance
- Compliance Tools
 - Internal Control Management/ Financial Compliance Process Management
 - Security and Continuous Control Monitoring
- Benefits and Lessons Learned
- Concluding Thoughts
- Q&A

Current Climate

Reviewing the current climate

United States

- Sarbanes and Oxley's goal: to quell a volatile situation
 - Frequent corporate scandals arising
 - Rapidly falling market confidence
 - The public demanding corrective action
 - Sarbanes-Oxley Act of 2002 (SOX)
- Section 404 — “Management Assessment of Internal Controls” — is particularly onerous for businesses
 - Identify financial reporting risks
 - Ascertain related controls
 - Assess their effectiveness
 - Fix any control deficiencies
 - Re-test and re-document
 - SEC delayed deadlines due to daunting complexity

Reviewing the current climate

Canada

- CSA multilateral instruments 52-109 and 52-111 were introduced as the Canadian public company response.
 - Essentially mirrors requirements introduced by SOX; except different compliance dates.
- Government's response
 - Office of the Comptroller General (OCG) re-established as a key element to strengthen government wide comptrollership and oversight.
 - Treasury Board Secretariat introduced measures aimed at strengthening transparency and accountability (which has included departmental and agency financial statement audits).

Reviewing the current climate

- First conformance dates in the US have now passed
- Initial trepidation was justified
 - Section 404 work was often difficult and chaotic - ***a significant drain on resources (time, personnel and dollars)***
- Common conclusion by management: This kind of monumental effort simply cannot be sustained in perpetuity

Where are organizations spending time?

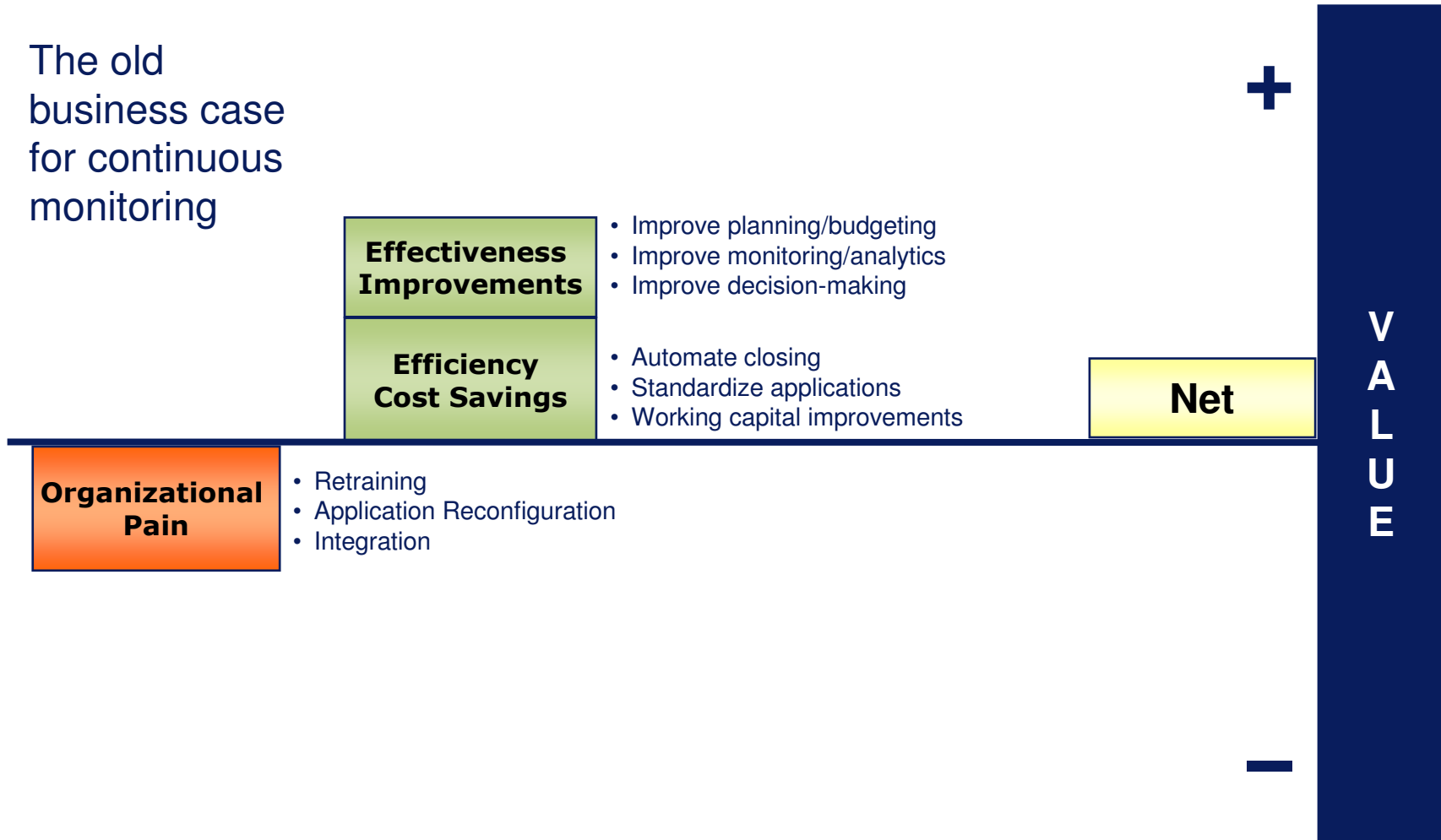
- Initial Scoping
- Process Documentation (including general IT controls)
- Control Testing
- Remediation of Control Weaknesses
- Certification
- On-going testing and certification

Organizations have used all sorts of tools, techniques and resources, from manual to automated to achieve desired results.

Internal Control Certification point of view

Before 2000 Market Collapse

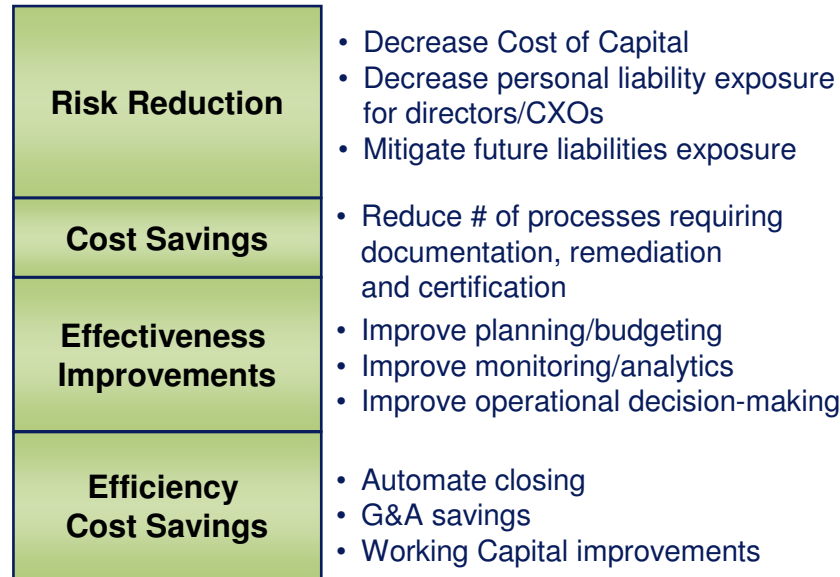
The old business case for continuous monitoring



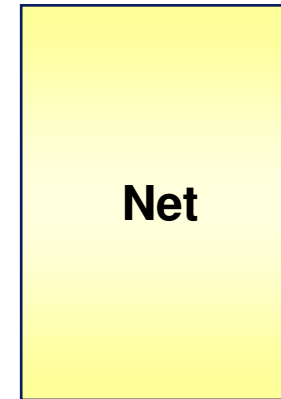
Internal Control Certification point of view

Case for Moving Beyond Compliance is Compelling

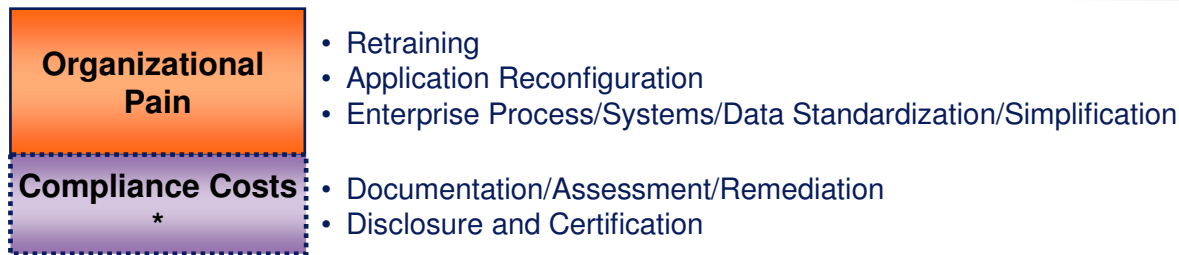
The **NEW**
business case



+



**V
A
L
U
E**

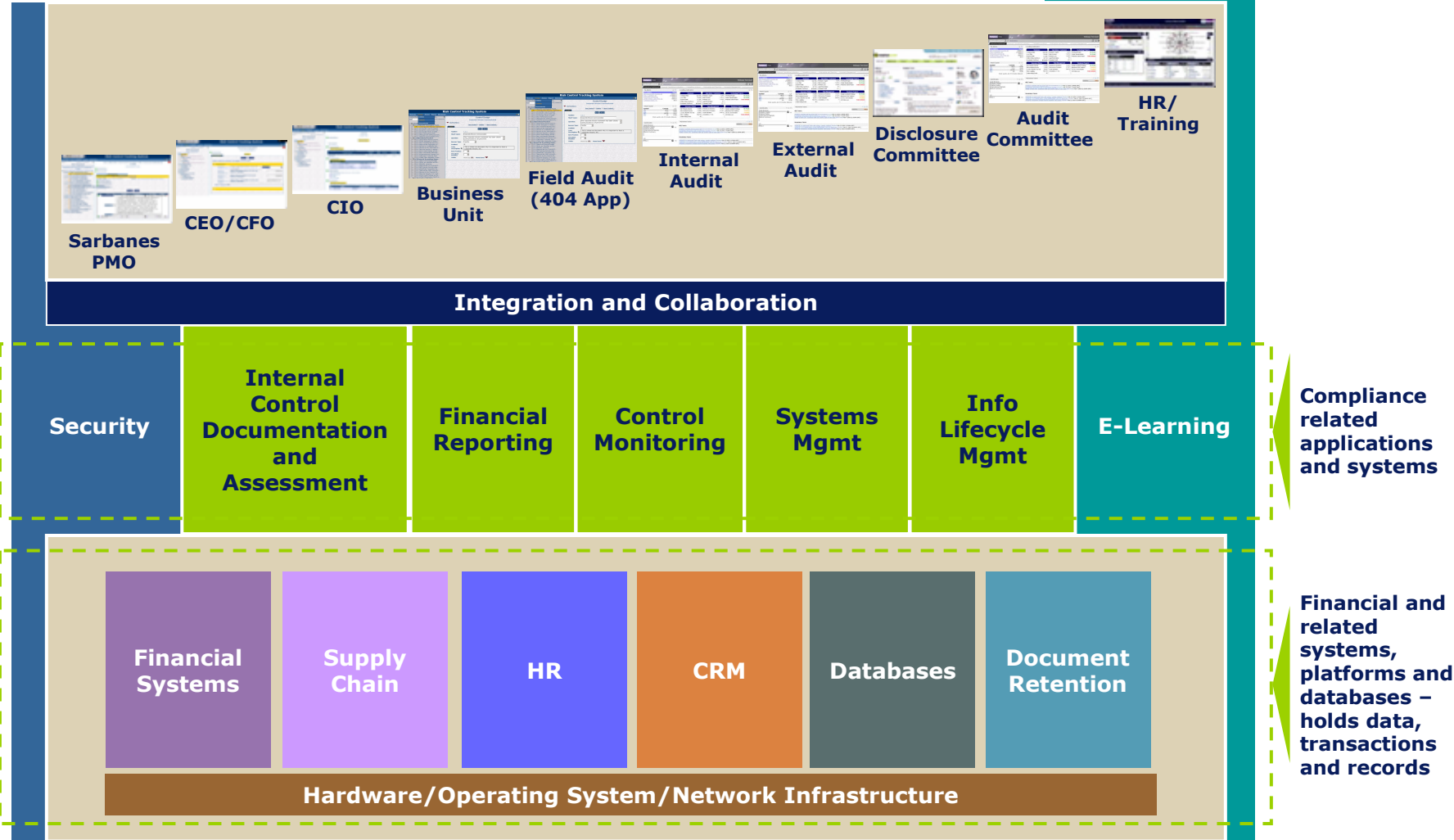


-

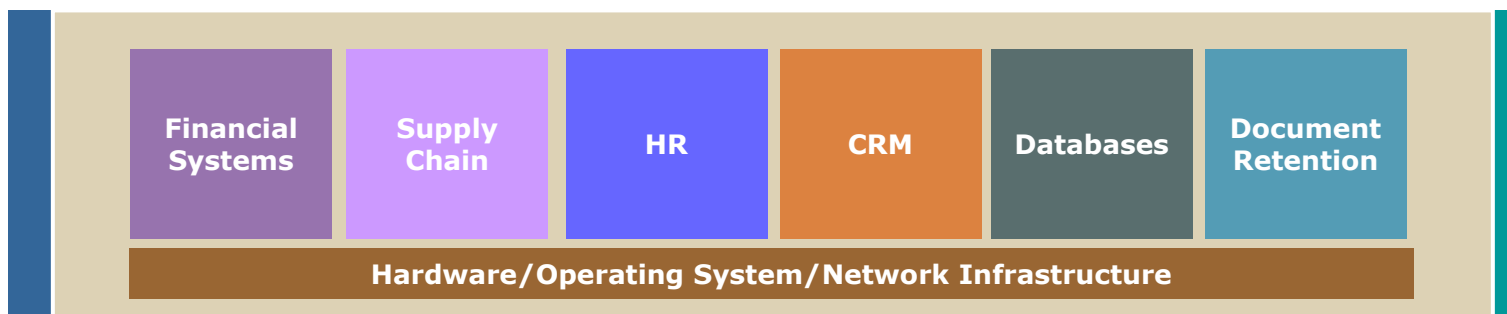
(*assuming standardization/simplification initiative)

Technology Architecture for Sustained Compliance

End-state technology architecture for sustaining compliance



Financial system layer



This layer primarily contains the financial systems, data and transactions, but also includes systems and databases that collect, manage and store related information, such as customer and employee information.

This includes vendors such as Ariba, EMC, IBM, Oracle/PeopleSoft, SAP, Siebel.

Compliance application layer



This layer contains the applications that support the sustainable compliance activities

- Companies will not implement all of these capabilities simultaneously, rather they will focus on areas that provide the greatest benefit to their compliance efforts (e.g. reducing cost, complexity and risk)
- Some functionality may already be present with existing technology in use by a company; this technology will be leveraged to aid the sustained compliance efforts
- The need for new functionality will cause companies to license, implement, and integrate new technologies into their infrastructure

Compliance Tools

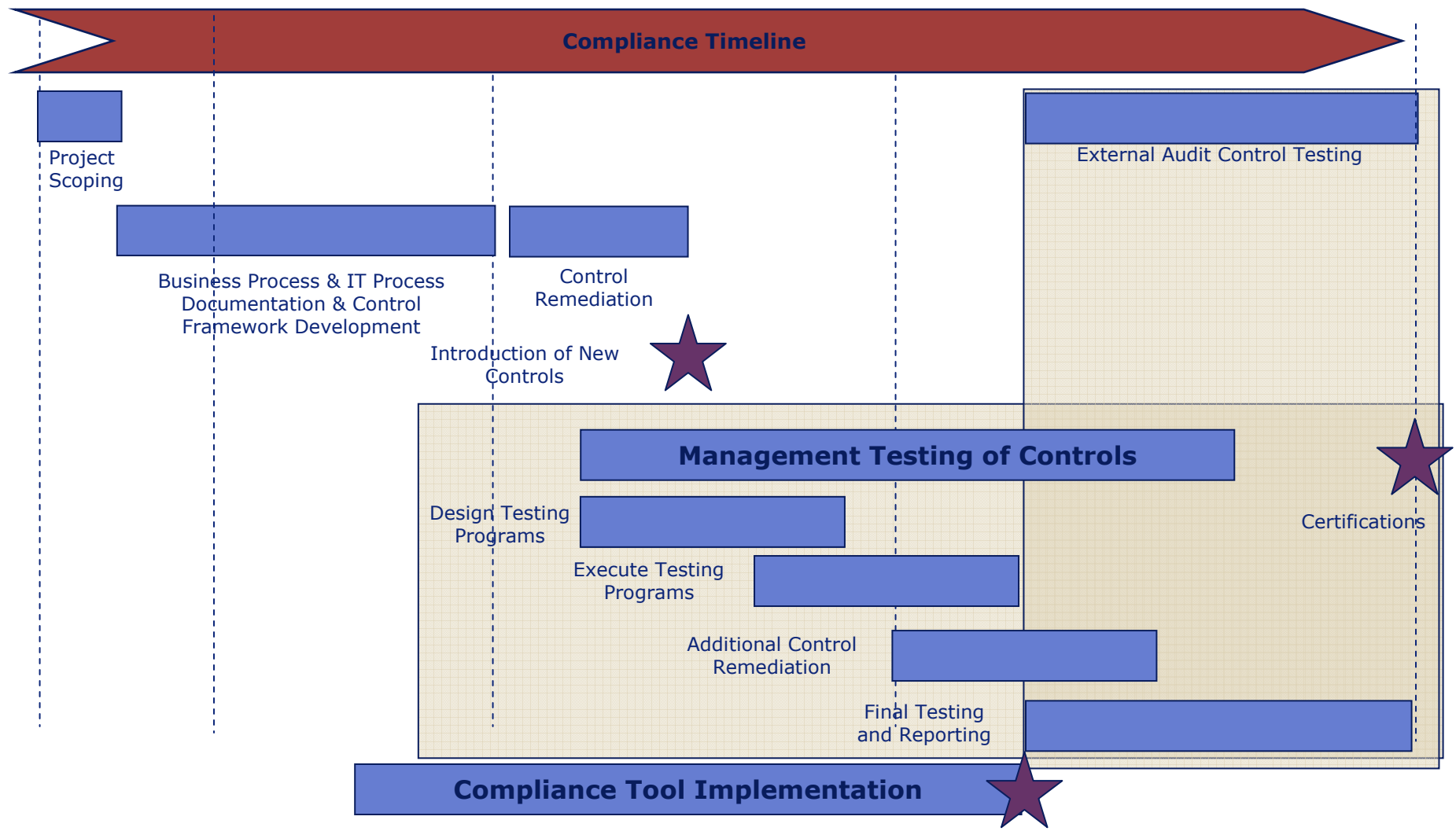
Internal Control and Audit Tools

- The market has been flooded with software solutions, tools and products; however the market remains, at best, a maturing environment.
- Some vendors advertised their solutions as “SOX Compliant”.
 - Due to a general lack of understanding of SOX and other internal control certification requirements in the marketplace.
 - No solution, by itself, can be a SOX compliant tool, but at best, be part of a compliance solution
- As market matures more research is being conducted on the various strengths and weaknesses of the tools (e.g. Gartner)
- What are the types of tools?
 - Audit management
 - Continuous Auditing
 - Control Assessments & Evaluation
 - Data Analysis
 - Risk Analysis
 - Segregation of Duties management
 - SOX compliance
- There are many tools that can and are being implemented as part of compliance programs.

Overview of Internal Control Tools

- From a sustained compliance perspective, vendors can be broadly defined in the following areas:
 - Internal Control Management/ Financial Compliance Process Management
 - Internal control management products offer Internal Control documentation, testing and reporting capabilities.
 - Internal control management products tend to be internal control repositories and databases of an organization.
 - Assessment of internal controls in these tools differentiate between both design and effectiveness of internal controls.
 - Security and Control Monitoring
 - These products are more specialized as either Segregation of Duties management tools and/or continuous control monitoring tools.
 - The key differentiator on these tools vs. Internal Control Monitoring is that Security and Control Monitoring tools are in themselves, internal controls (Monitoring and control activity layer of the COSO model).

What is Financial Compliance Process Management?



Internal Control Documentation and Assessment



Addresses the overall requirements needed by an organization to facilitate on-going internal control documentation and assessment.

Documentation and Assessment	Functionality	Sample Vendors
Organizational Configuration	Model the hierarchical company structure to reflect accounts and business processes within business units.	SAP, Oracle, Peoplesoft, IBM, Microsoft, Paisley, Qumas, Open Pages, Movaris, Certus, Office applications 80-20 Software and other boutique solutions.
Internal Control Frameworks	Database is structured to enable the documentation of internal control frameworks based on the concept of risks/control objectives to control activities and techniques. Used for both business process and general computer controls.	
Internal Control Testing	Database is structured to enable the capture, cataloging and summarization of internal control testing programs and results.	
Internal Control Remediation and Reporting	Tool enables the recording, tracking and management of internal control weaknesses or other issues.	
Differences	Workflow, issue management, conclude frameworks, database structure (control activities; objectives; testing results; remediation; reporting) and costs.	

Common Vendor Evaluation Points

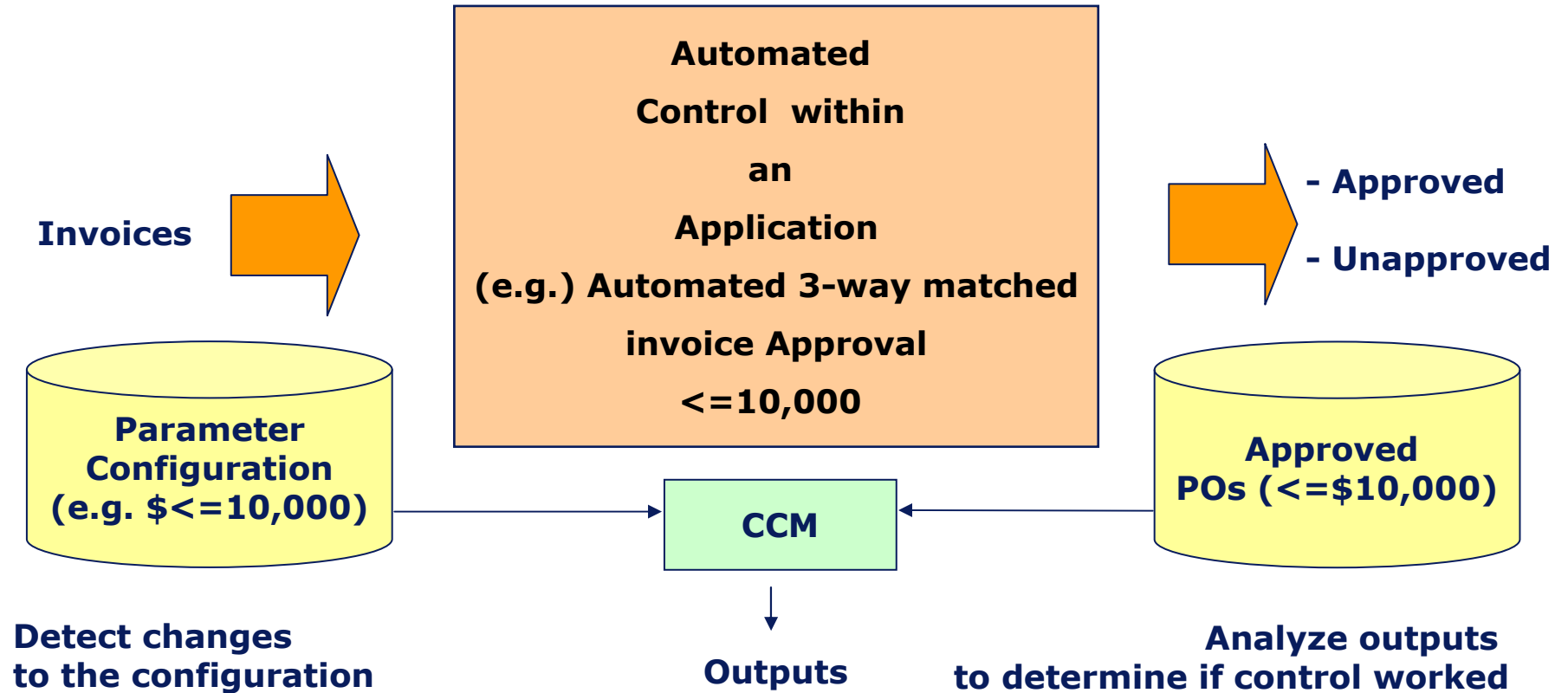
- Organizational Structure
- Control Framework (ability to track by COSO and COBIT)
- Data Migration (ability to leverage existing documentation)
- Reporting abilities (Executive and Operational)
- Document Content Management
- Assessment (Workflow, Approver, Reviewer)
- Security functions (any tool must have appropriate controls)
- Audit Trails
- Integration with existing software
- Price

What is continuous controls monitoring?

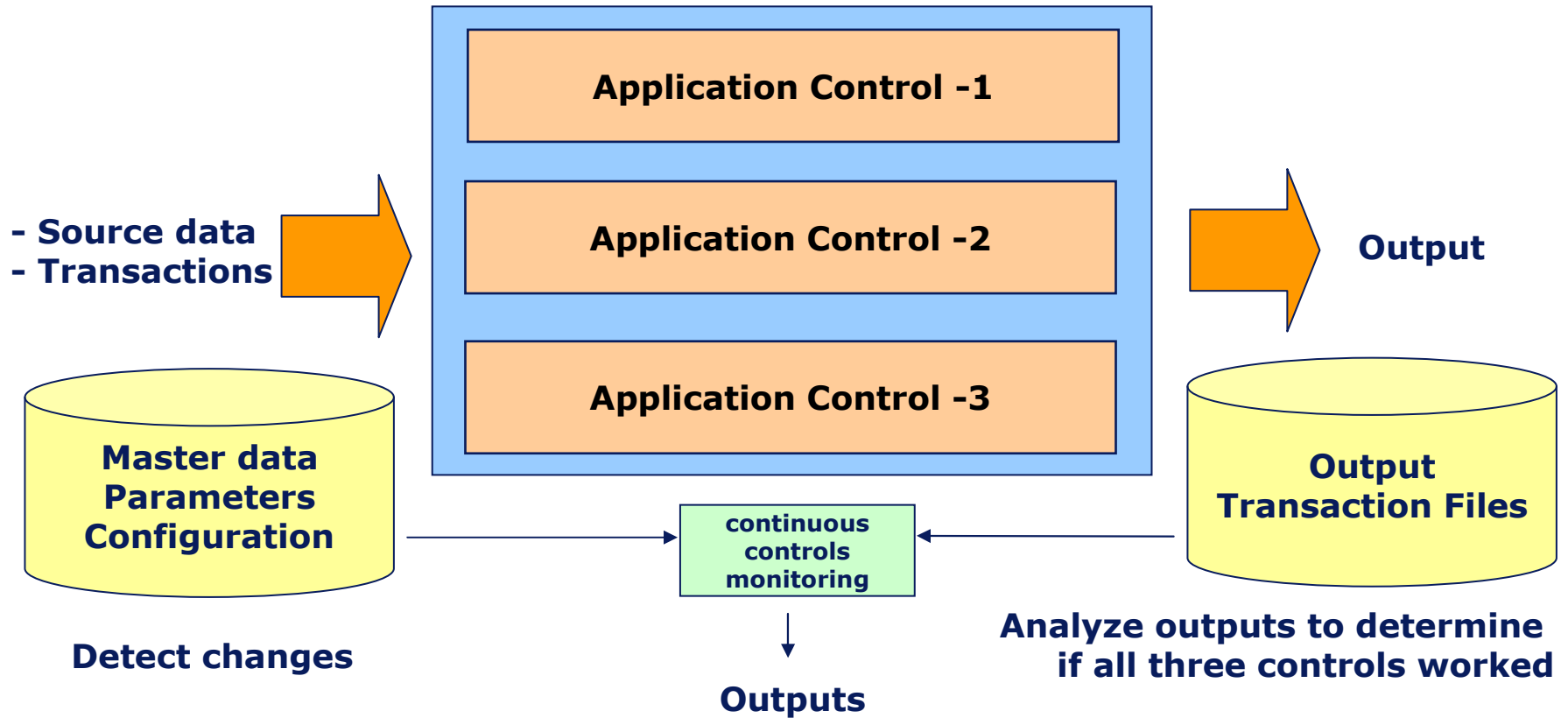
- Techniques used to:
 - Detect changes in the configuration of controls
 - Analyse data to identify exceptions that do not meet business rules, policies or other criteria indicative of a control failure

...on a real-time or near real-time basis

The continuous controls monitoring concept...



Using continuous controls monitoring to test multiple controls...



The key is to identify the logical control clusters

Ready to use modules from vendors do this for standard processes (e.g.) Payables

Control monitoring



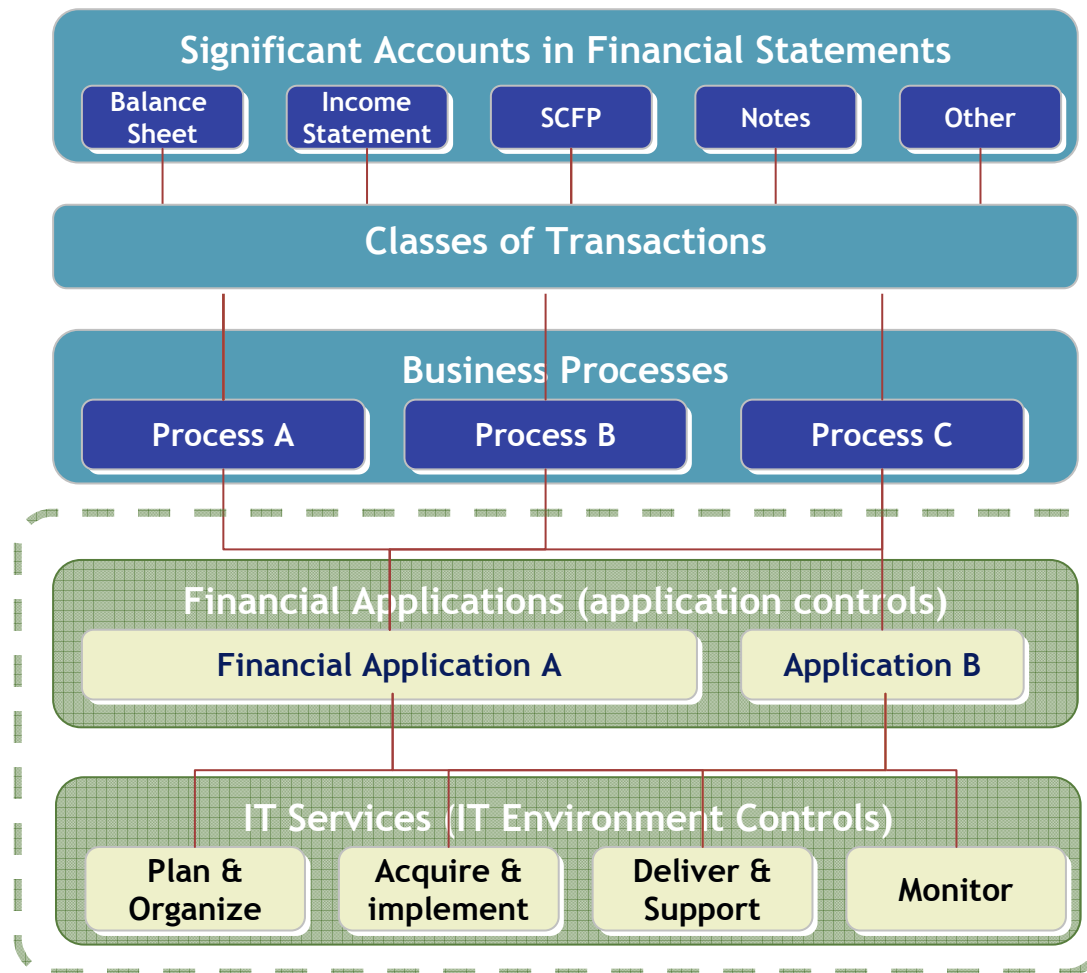
Addresses the as-needed automatic monitoring for activities such as a transaction’s adherence to policies and defined controls, fraud prevention, segregation of duties and changes in controls

Monitoring Activities	Functionality	Sample Vendors
Changes in Control	Monitoring changes in the parameters in control configuration tables	Applimation, Cendura, Computer Associates
Segregation of Duties & User Access	Ability to know who has access to various transactions and/or modules; an access matrix for defining incompatible transactions/functions; monitoring access tables for potential access conflicts; monitoring who has accessed transactions, modules and content	Approva, Applimation, Computer Associates, Courion, IBM, Logical Apps, Oblix, Oracle/PeopleSoft, SAP, Sun Microsystems, Virsa
Transaction Monitoring	Analyzing transactions for anomalies outside the parameters of controls, monitoring for completeness and accuracy of transactions, and other unusual transactions outside tolerance levels	ACL, Cognos, Hyperion, IBM, Oracle/PeopleSoft, SAP, SAS, WebMethods
Process Monitoring	Monitoring manual process such as reconciliations, periodic closings, compliance certifications	Certus, IBM, Movaris, Oracle/PeopleSoft, SAP, WebMethods

What's in scope?

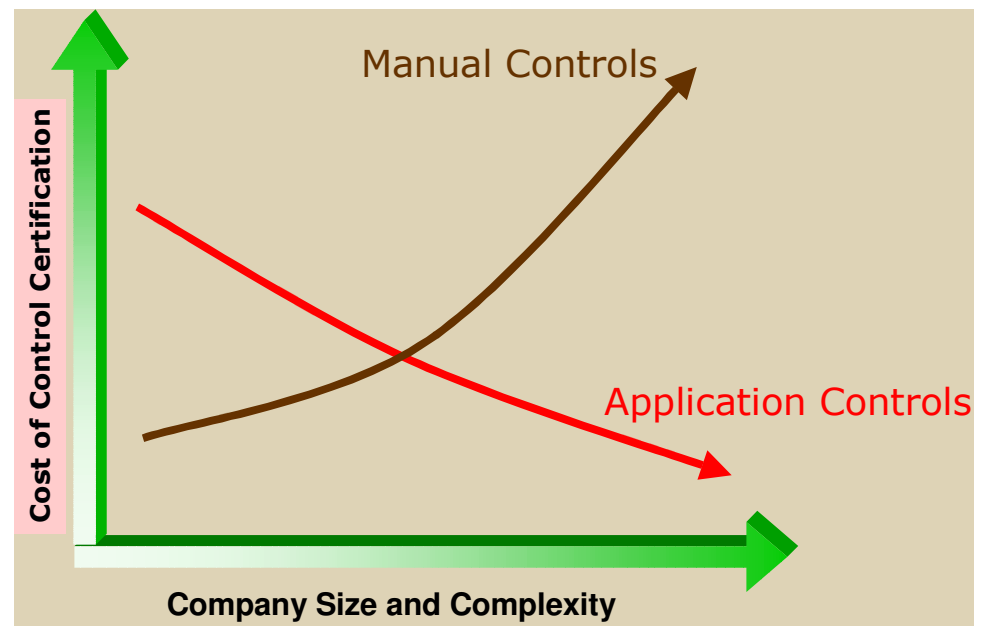
- Need to include/consider both application and general controls
- General controls:
 - Most immediate benefits are likely to be where currently some form of automation has been implemented; leverage it.
Examples:
 - Change / Problem management tools
 - Network, platform and database level surveillance tools
- Application controls:
 - Most immediate benefits are likely to be in standard processes (e.g. Payroll, Accounts payable) where vendor tools are available
 - Complex home grown applications where controls testing can be complex and effort intensive
 - Network intensive applications (e.g. transaction approval and payment systems) test of outputs against criteria tends to be easier

Applicability to both application and general controls



Application controls – a key element of sustained compliance

- Sustained compliance requires the optimization of key controls
 - Ensuring continuous control effectiveness
 - Minimizing reliance on typically unreliable manual procedures and activities
 - Minimizing the cost of effectiveness assessment
- The value of application controls increases with the size and complexity of an organization



Types of controls – which ones are candidates for continuous monitoring?

	SYSTEM/AUTOMATED	MANUAL
DETECTIVE	<ul style="list-style-type: none"> • Exception edit reports • Interface controls • Conversion controls • Automated reconciliation controls • KPI's 	<ul style="list-style-type: none"> • Reconciliations • Management review • KPI's (Key Performance Indicator) • Reconciliation controls
	AUDIT TRAILS/MONITORING	
PREVENTIVE	<ul style="list-style-type: none"> • Access controls • Edit/Validation controls • Tolerance/Limits • Segregation of duties • Config. controls • General IT controls 	<ul style="list-style-type: none"> • Policies/Procedures • Authorization controls • Management review • Segregation of duties • Physical access controls • General IT controls

Benefits and Lessons Learned

The Benefits

- Reduces the costs of ongoing compliance
 - Automates labour-intensive testing of controls
 - Allows limited resources to focus on investigating and resolving exceptions rather than performing repetitive testing procedures
 - Repeatable process

- Effectively managing risks
 - 100% testing of transactions versus sampling approach
 - Provides assurance throughout the year rather than point in time
 - Can identify design as well as operating effectiveness deficiencies
 - Timely identification of control issues

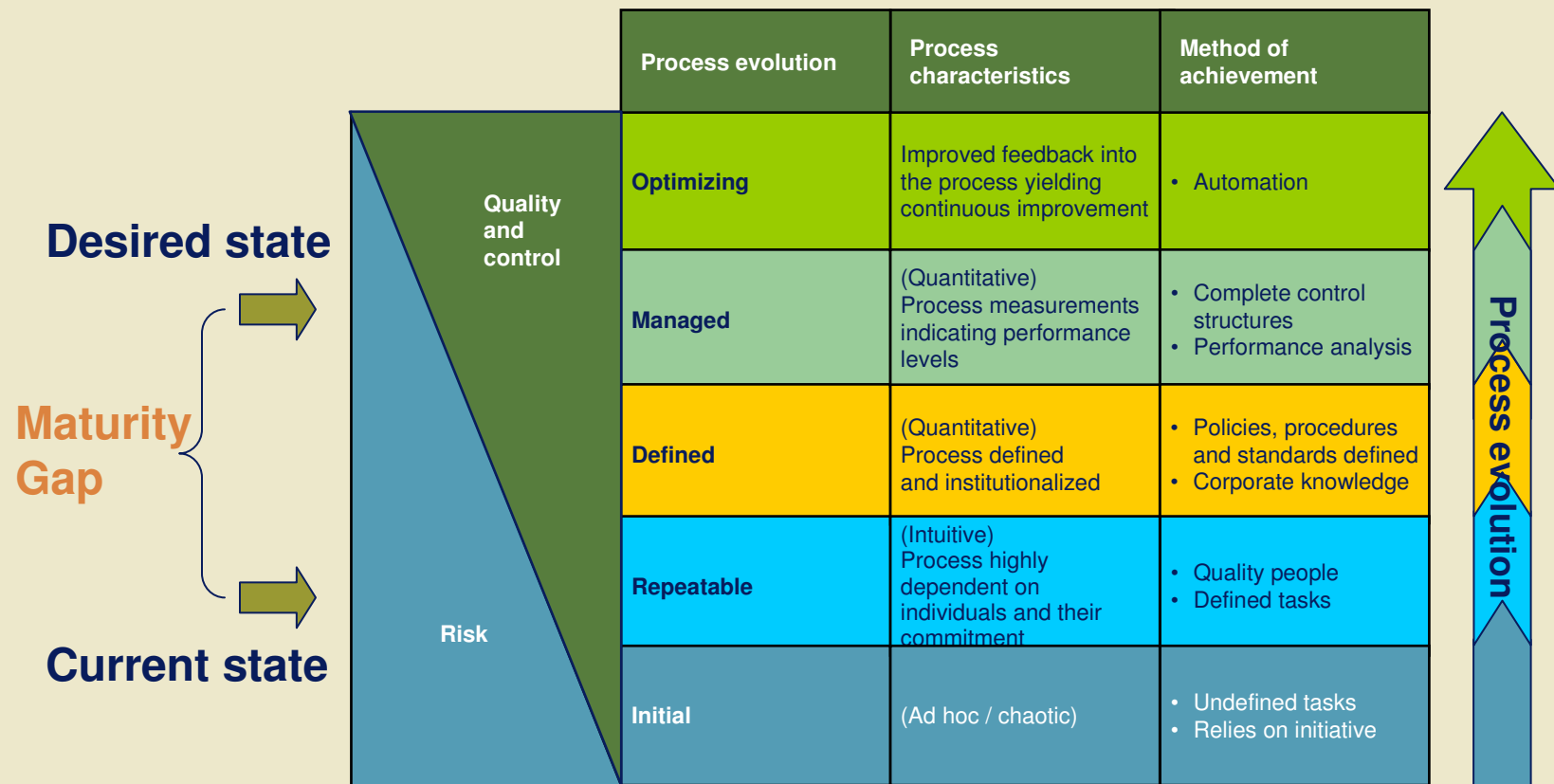
Lessons Learned - Year 1

Many companies have approached initial certification and compliance as a project and have not started to address the broader issues of sustained compliance.

- Significant time, money, and resources have been expended to achieve first year SOX compliance
 - 11% of companies reported Material Weaknesses
 - Many companies **missed** filing deadlines
 - Almost all had significant deficiencies
 - Market reaction is moderate
- Costs and effort of compliance was consistently underestimated
- In spite of initial plans, significant effort was required in Q3 and Q4 to meet deadline
- “Makeshift methods” were implemented to document, evaluate, test, and remediate controls;
- First-wave technologies were implemented to fill the gap and assist in the documentation effort;
- Process and technology solutions have not been implemented to respond to internal and external changes which may impact the effectiveness of internal controls;
- Well-designed, repeatable processes have not yet been established;
- Roles and responsibilities have not been clearly defined and integrated into the day-to-day activities of affected employees;
- Focus was primarily on achieving year-one compliance with little energy dedicated to understanding and developing a framework to sustain compliance.

Capability maturity model

Identify existing and desired capabilities



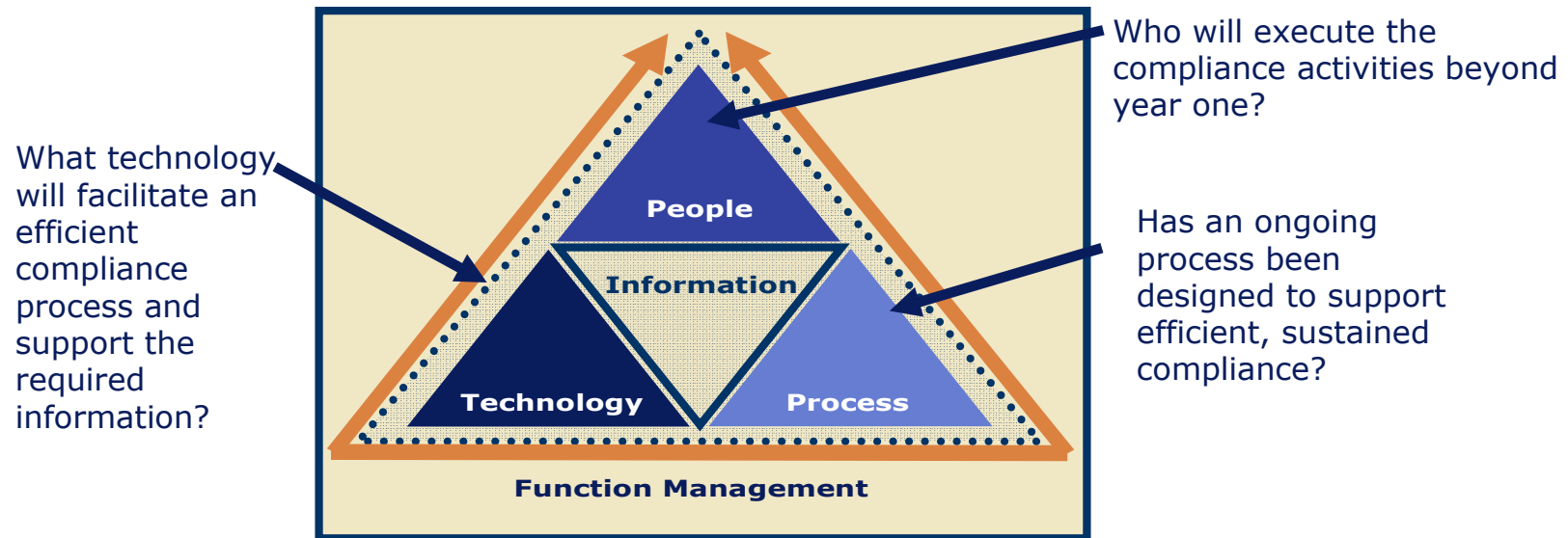
Build on what's already in place

Concluding Thoughts

Concluding Thoughts

- In order to achieve sustainable compliance, companies need to build an efficient and effective compliance infrastructure that enables repeatable, reliable actions to deliver high information quality.
- Compliance is not the end game – Not to be misunderstood – compliance is critical, simply stated you have no choice, but a much greater reward awaits those companies both savvy and strategic enough to see the journey for what it really is.
- Perform thorough research BEFORE buying any solutions – (e.g. Gartner research reports, other customers of the vendor)

Elements of the Sustainment Framework



Questions??

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 6,100 people in 47 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

Member of
Deloitte Touche Tohmatsu