The Importance of IT Controls to Sarbanes-Oxley Compliance

15 December 2003

Presenters

Chris Fox, CA

- Sr. Manager, Internal Audit Services
  PricewaterhouseCoopers LLP

Paul Zonneveld, CA, CISA, CISSP

- Sr. Manager, Control Assurance
  Deloitte

©2003 IT Governance Institute

Agenda

- Setting the stage
- The role of IT in Sarbanes-Oxley 404 (SOA)
- Understanding the proposed rules
- IT Control objectives for Sarbanes-Oxley
- A readiness roadmap
- Summing up
- Comments from discussion document
- Closing remarks and Q&A

©2003 IT Governance Institute

Setting the Stage

©2003 IT Governance Institute

Setting the Stage

- Internal control is now the law.
  - The Sarbanes-Oxley Act of 2002 was created to restore investor confidence in the public markets.
  - The Act requires management to establish and maintain internal control—and requires the independent auditors to evaluate.
  - Compliance for internal control attestation will be within the next few years for most companies.
- Preparing for compliance is a significant task.
  - Processes need to be identified and controls need to be documented and tested.
- Current auditor rules require consideration of "IT."
  - Most organizations want to know "what is required" for compliance.
  - ITGI publication provides a road map (www.itgi.org).
  - Each situation will be unique and there is no "one size fits all."

©2003 IT Governance Institute

The Role of Information Technology in Internal Control over Financial Reporting

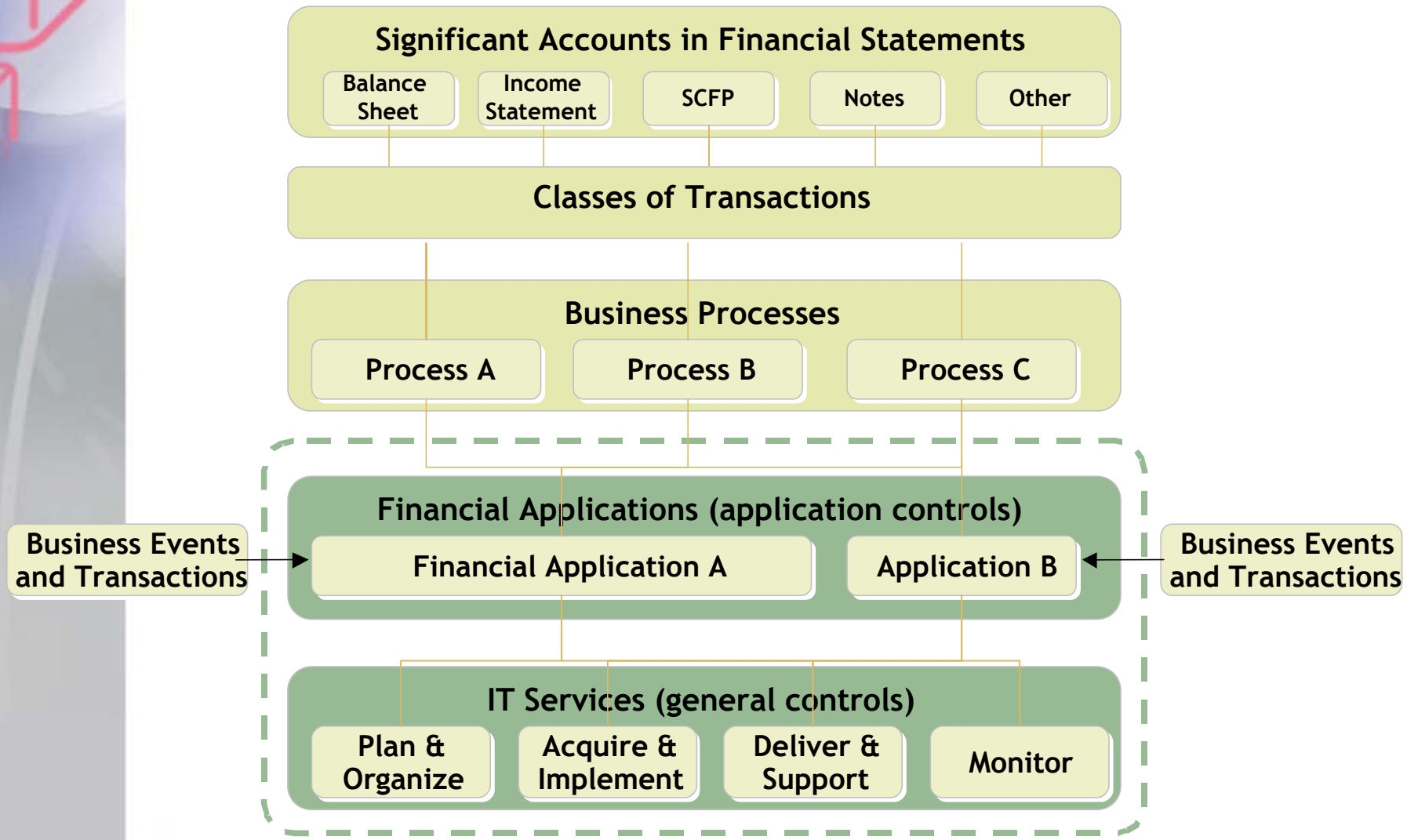
©2003 IT Governance Institute

The Role of Information Technology in Internal Control over Financial Reporting

- For most organizations, IT is pervasive to the financial reporting process.
- Financial applications are commonly used to initiate, record, process and report transactions.
- Relevant IT controls include those that are embedded in financial applications (application controls), as well as those present in IT platforms that support such financial applications (general computer controls).

©2003 IT Governance Institute

The Role of Information Technology in Internal Control over Financial Reporting (cont'd)



©2003 IT Governance Institute

Understanding the Proposed Rules

©2003 IT Governance Institute

PCAOB Releases

Release No.	Release Name	Status
2003-03	Board Funding: Establishment of Accounting Support Fee	Final - 4/18/2003
2003-04	Establishment of Interim Professional Standards	N/A - 4/18/2003
2003-07	Registration System for Public Accounting Firms	Final - 5/6/2003
2003-08	Ethics Code for Board Members, Staff, Designated Contractors and Consultants	Final - 6/30/2003
2003-09	Compliance with Auditing and Related Professional Practice Standards – Advisory Groups	Final - 6/30/2003
2003-15	Investigations and Adjudications	Final - 9/30/2003
2003-16	Withdrawal from Registration	Final - 9/30/2003
2003-19	Inspections of Registered Public Accounting Firms	Final – 10/7/2003
2003-17	An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements	Proposed – Comment date 11/21/2003
2003-18	Certain Terms Used in Auditing and Related Professional Practice Standards	Proposed – Comment date 11/6/2003
2003-20	Oversight of Non-US Public Accounting Firms	N/A
2203-21	Reference in Auditors' Reports to the Standards of the PCAOB	Proposed – Comment date 12/4/2003
2203-22	Proposed Technical Amendments to Interim Standards Rules	Proposed – Comment date 12/4/2003
2203-23	Proposed Auditing Standard on Audit Documentation and Proposed Amendment to Interim Auditing Standards	Proposed – Comment date 1/20/2004
2203-24	Proposed Rule on Oversight of Non-US Firms	Proposed – Comment date 1/26/2004

©2003 IT Governance Institute

Understanding the Proposed Rules

Auditors and management are required to document and assess the effectiveness of IT controls over the financial reporting process.

PCAOB Audit Standard (proposed)

- Significant reference to IT general and application controls
- Specific reference to tracing transaction through the system and identifying where controls exists within the system
- Specific reference to program development, program changes, computer operations, and access to programs and data

COSO Internal Control Framework (most commonly adopted)

- Risk assessment process identifies internal control risks related to data integrity, system security, system availability and data confidentiality
- Control activities process identifies application controls and general controls
  - Application controls include completeness, accuracy, authorization, availability and validity of transactions
  - General controls include operations and management, infrastructure, security, acquisition and maintenance, oversight and monitoring

©2003 IT Governance Institute

Understanding the Proposed Rules (cont'd)

The PCAOB rules are quite clear that audits must follow transactions through the system, not around it.

- (paragraph 48)
  "The auditor should obtain an understanding of the design of specific controls by applying procedures that include…tracing transactions through the information system relevant to financial reporting"

- (paragraph 79)
  The audit should trace all types of transactions and events, both recurring and unusual from origination through the company's information systems until they are reflected in the company's financial reports…walkthroughs provide evidence to:
  - Confirm understanding of the process flow of transactions
  - Confirm understanding of the design of controls—including those related to detection of fraud
  - Determine whether all points in the process where misstatements related to each relevant financial statement assertion that could occur have been identified
  - Evaluate effectiveness of design of controls and
  - Confirm whether controls have been placed in operation

- Similar statements are provided in paragraphs 81 and 82.

©2003 IT Governance Institute

Understanding the Proposed Rules (cont'd)

PCAOB statements on the importance of IT application controls:

- (paragraph 69)
  "The auditor should identify each significant process over each major class of transactions affecting significant accounts or groups of accounts…
  - Understand the flow of transactions.
  - Identify points within a process where a misstatement related to each relevant financial statement could arise.
  - Identify controls implemented to address these misstatements.
  - Identify controls that management has implemented over prevention or detection of unauthorized acquisition, use or disposition of company's assets."
- (paragraph 71)
  "Understanding the Period End Financial Reporting Process. Includes the following:
  - The procedures used to enter transaction totals into the general ledger
  - The procedures used to initiate, record and process journal entries in the GL
  - Other procedures used to record recurring/nonrecurring adjustments to the financial statements such as consolidating adjustments, report combinations and classifications"
- Similar statements are provided in paragraphs 102, 123, B26, B-1, B-4

©2003 IT Governance Institute

Understanding the Proposed Rules (cont'd)

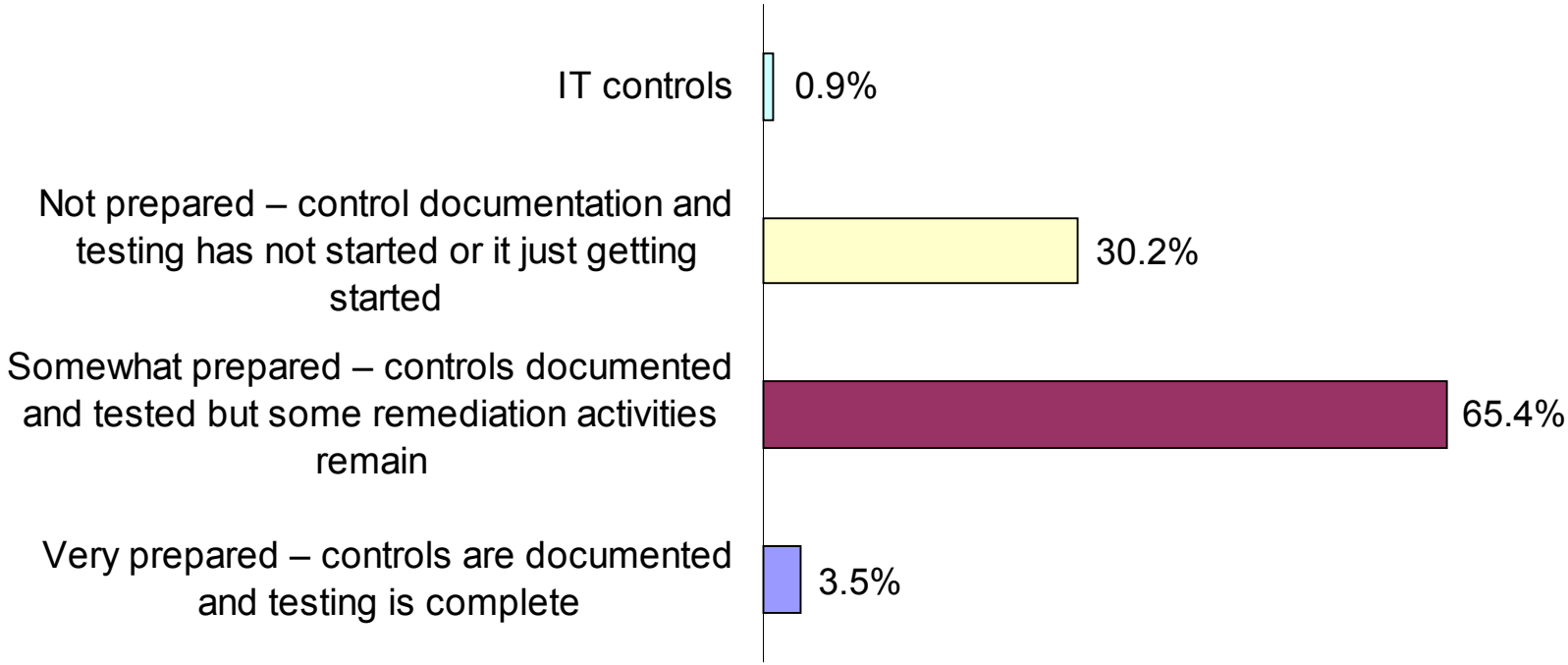
PCAOB statements on the importance of IT general controls:

- (paragraph 41)
  "…determining which controls should be tested… generally, such controls include… information technology general controls, on which other controls are dependent"
- (paragraph 51)
  "…information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively"
- (paragraph 74)
  "…the risk that the controls might not be operating effectively. Factors that affect whether the control might not be operating effectively include the following:
  - The degree to which the control relies on the effectiveness of other controls (for example, the control environment or information technology general controls)
  - Whether the control relies on performance by an individual or is automated"
- Similar statements are provided in paragraphs 104, 120, B22, B-1, B-4

©2003 IT Governance Institute

Polling Question #1

How ready do you think your organization is regarding Sarbanes-Oxley compliance?



©2003 IT Governance Institute

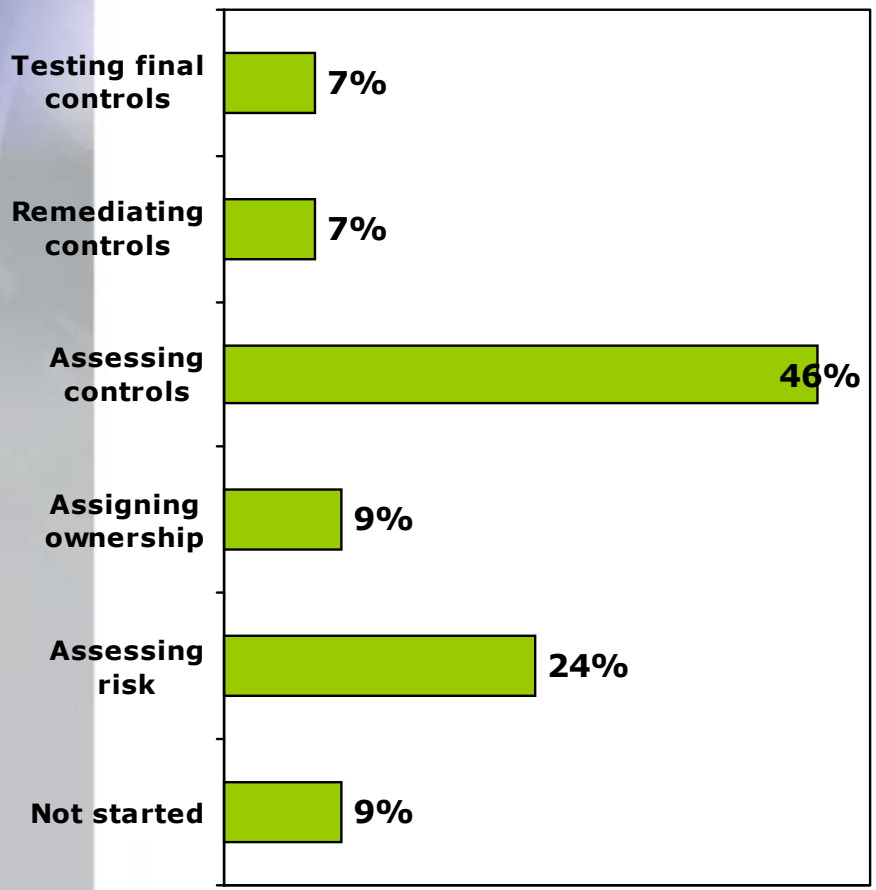
Comments from the IT Industry

©2003 IT Governance Institute

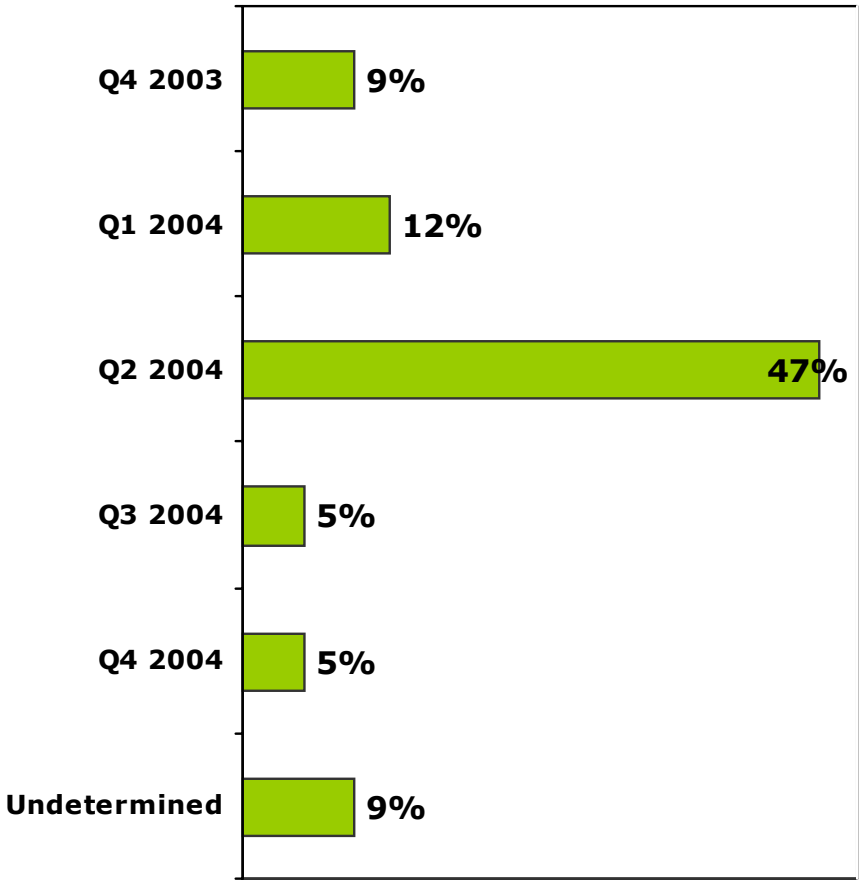
Comments from the IT Industry

Most IT organizations are progressing but have a lot of work to do.

Progress Towards Compliance



Target Date for Completion



©2003 IT Governance Institute

Source: Corporate Executive Board - Working Council Member Survey, November 2003

Comments from the IT Industry

- The risk:
  - "…many IT executives reportedly don't believe Sarbanes-Oxley has anything to do with IS operations. They couldn't be more wrong."—Gartner, 2003
  - "You may think the Sarbanes-Oxley legislation has nothing to do with you. You'd be wrong."—CIO Magazine
  - "85 percent of companies predict that SOA will require them to make changes to their IT and application infrastructure."—AMR Research
- Leading CIOs recognize that they need to address the SOA issue before it addresses them.
- The challenge:
  - Few CIOs have a strategy to respond.
  - Few CIOs have the resources to respond.
  - Few CIOs know what technologies will help.

©2003 IT Governance Institute

Recent Comments

- "With CEOs and CFOs now being held accountable for the accuracy of the financial reporting at their companies, "they are looking for ways to distribute that responsibility downward through their organizations," McLaughlin said. That includes asking IT managers to certify the systems used to process financial data" - Computerworld - November 2003
- "In an informal survey by CIO of the top 19 companies on the Fortune 100 list, most executives viewed compliance with Sarbanes-Oxley as a finance issue, not a systems issue. A few acknowledged a potential role for IT but insisted it was premature for the CIO to be involved…They are dangerously mistaken.." – CIO Magazine – November 2003
- "Even with the one-year grace period … most organizations will struggle to meet Sarbanes-Oxley Act (SOX) compliance deadlines" - META Group – August 2003
- "On 10 December 2003, the government of the Netherlands announced a new code of corporate governance. Two days earlier, the German government had announced that it would set up an independent auditing body to review the accounts of publicly quoted companies… The Dutch code of conduct and the proposed German legislation echo the U.S. Sarbanes-Oxley Act, which is now having broad consequences for U.S. companies. Similar legislation is being drawn up in the United Kingdom" – Gartner - December 2003.

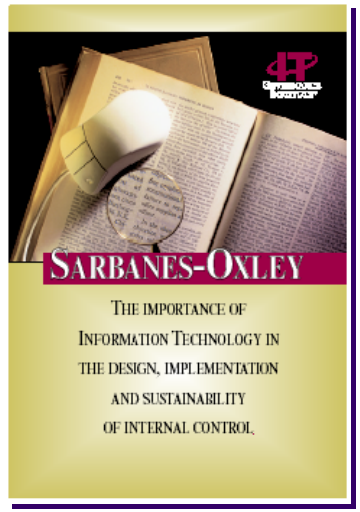
©2003 IT Governance Institute

IT Control Objectives for Sarbanes-Oxley

©2003 IT Governance Institute

IT Control Objectives for Sarbanes-Oxley

- The IT Governance Institute® (www.itgi.org) has recently published guidance for IT professionals on how to address Sarbanes-Oxley from an IT perspective
  - *"IT Control Objectives for Sarbanes-Oxley—The Importance of Information Technology in the Design, Implementation and Sustainability of Internal Control"*

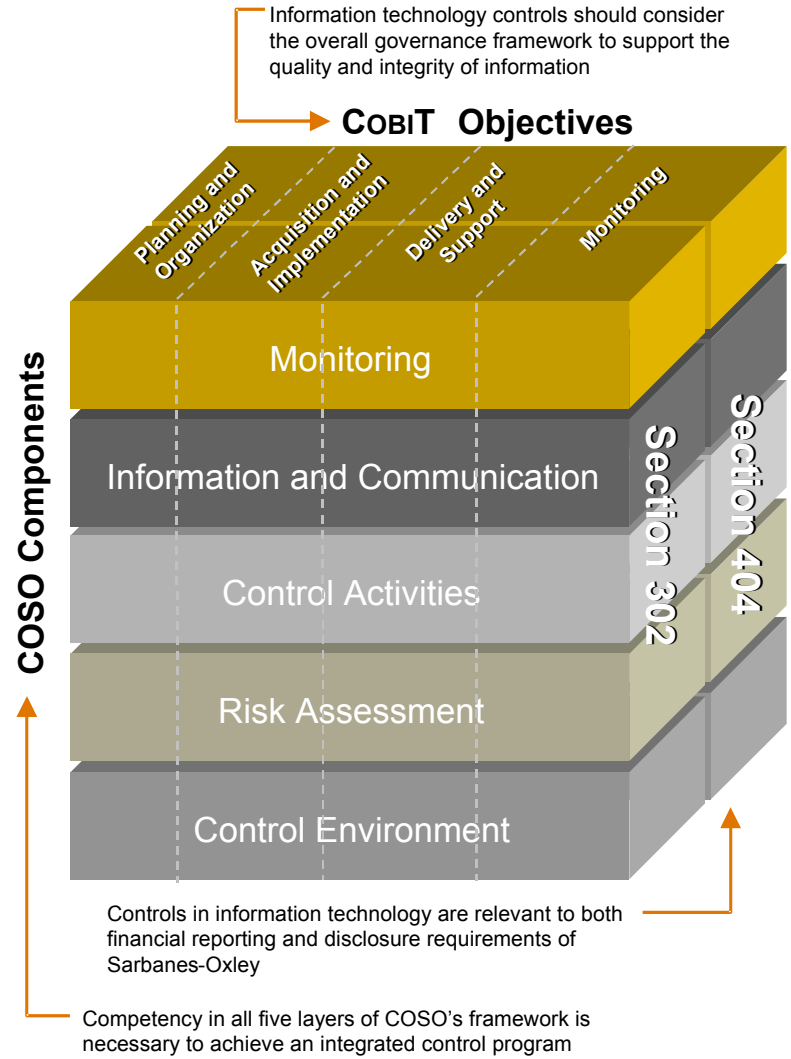


- The publication is the result of a joint effort of industry and auditors, with leadership from Deloitte and PwC
- The ITGI is a recognized global leader in IT governance, control and assurance
- Other control guidelines were reviewed and reconciled to this approach during the development process, including ISO 17799, Common Criteria, ITIL and SysTrust

©2003 IT Governance Institute

IT Control Objectives for Sarbanes-Oxley (cont'd)

- COSO is the control framework of choice for Sarbanes-Oxley compliance.
  - All five layers must be considered when evaluating internal control.
- COBIT is a widely accepted IT control framework (ITGI).
  - COBIT provides four domains of IT control.
  - COBIT controls address the five layers of COSO.
- With the development of this approach, organizations can be confident that they are taking an approach that reflects COSO requirements.



©2003 IT Governance Institute

IT Control Objectives for Sarbanes-Oxley (cont'd)

- The ITGI publication provides guidance to IT professionals on how to meet the Sarbanes-Oxley challenge.
- Detailed control objectives are provided for each COBIT domain and mapped to their respective COSO component.
- The publication provides a basis to establish IT controls for Sarbanes-Oxley.
- Organizations should assess their requirements on an individual basis and tailor their approach accordingly.

COBIT Objectives → **COSO Components**

CobiT Control Objectives	COSO Component: Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Planning & Organization					
Define a strategic IT plan		●		●	●
Define the information architecture			●	●	
Determine technological direction					
Define the IT organization and relationships	●			●	
Manage the IT investment					
Communicate management aims and direction	●			●	●
Manage human resources	●			●	
Ensure compliance with external requirements				●	●
Assess risks		●			
Manage projects					
Manage quality	●		●	●	●
Acquisition & Implementation					
Identify automated solutions					
Acquire and maintain application software			●		
Acquire and maintain technology infrastructure			●		
Develop and maintain procedures			●	●	
Install and accredit systems			●		
Manage changes			●		●
Delivery & Support					
Define and manage service levels	●		●		●
Manage third-party services	●	●	●		●
Manage performance and capacity			●		
Ensure continuous service			●		●
Ensure systems security			●	●	●
Identify and allocate costs					
Educate and train users	●			●	
Assist and advise customers					
Manage the configuration			●	●	
Manage problems and incidents			●	●	●
Manage data			●	●	
Manage facilities			●		
Manage operations			●	●	
Monitoring					
Monitor the processes				●	●
Assess internal control adequacy					●
Obtain independent assurance	●				●
Provide for independent audit					

IT Control Objectives for Sarbanes-Oxley (cont'd)

- COBIT provides a rich framework, with 34 IT processes and 318 detailed control objectives.
- The COBIT SOA framework identified a subset of these areas for the purpose of focusing on Sarbanes-Oxley requirements:
  - 27 IT processes
  - 134 control objectives
  - Not all of these processes and control objectives may be necessary for every company
- Several COBIT IT processes and related control objectives were eliminated if they:
  - Were too detailed (e.g., encryption specifications)
  - Were directed at specific technologies rather than general control principles (e.g., mainframe specifications)
  - Were focused on efficiency objectives (e.g., technology direction, automated solutions)

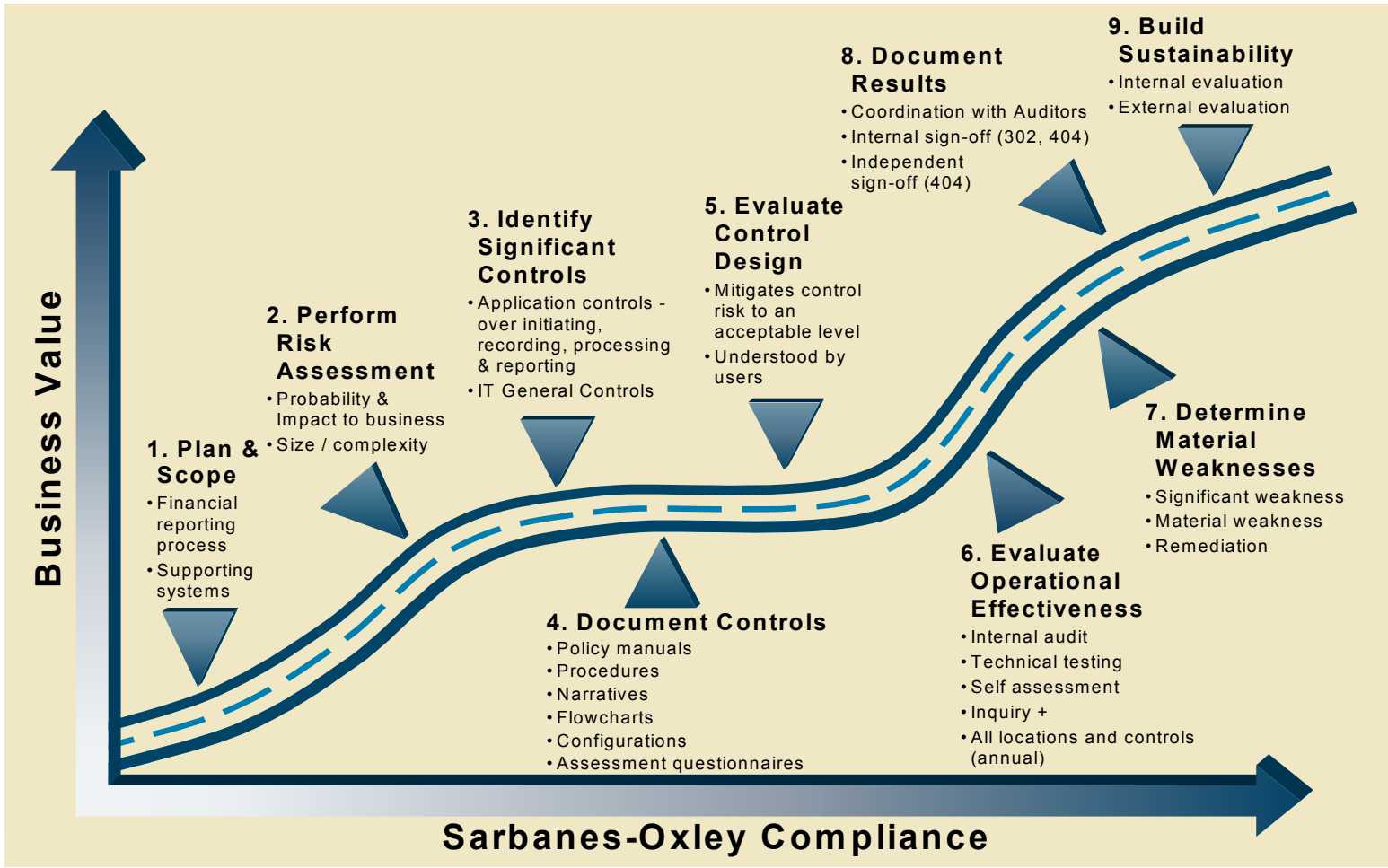
©2003 IT Governance Institute

A Readiness Roadmap

©2003 IT Governance Institute

A Readiness Roadmap

The following solution roadmap provides a guide to Section 404 readiness efforts.



©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Plan and Scope

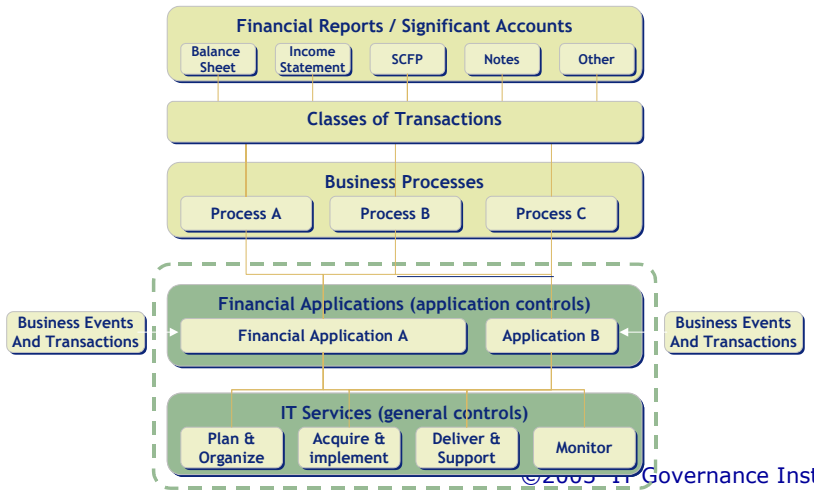
Understand the financial reporting process and identify the information systems and related IT resources that are used.

Key Components

- Financial reporting process
  - Initiating
  - Recording
  - Processing
  - Reporting
- Classes of transactions
- Nonrouting and nonsystematic

Key Considerations

- Enabling and changing accounting policies in accounting systems
- Prevention, identification and detection of fraud



©2005 IT Governance Institute

A Readiness Roadmap (cont'd)
Perform Risk Assessment

Identify risks associated with the information systems and related IT resources (i.e., what could go wrong?).

Key Components

- IT risks
  - Quality and integrity failure
  - Security failure
  - Availability failure
- Risk assessment
  - Probability of failure
  - Impact to the business

Key Considerations

- Specific risk areas
  - Data validation
  - Data conversion
  - Interfaces
  - Management reports
  - Complex or critical calculations
  - Spreadsheets

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Identify Significant Controls

Identify controls over security, availability and processing integrity across the four COBIT domains.

Key Components

- Application and general controls
- IT controls
  - Processing integrity
  - Security (e.g., segregation of duties)
  - Availability
- IT process activities
  - Systems planning and organization
  - Acquisition and implementation
  - Delivery and support
  - Monitoring

Key Considerations

- Entity level—Planning and organization
- Process/activity level—acquisition, implementation, support and monitoring
- Consider what is performed vs what is documented—May need to enhance documentation
- Understand how IT is organized and identify controls accordingly
- Perform control workshops to kick off—controls unlikely a primary focus and communication will be key

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Document Controls

Document the control process sufficient to support management's assertion as well as the independent audit.

Key Components

- Process description
- Risk assessment
- Control objective
- Control activity
- Test of the control
- Conclusions and remediation plans

Key Considerations

- Keep documentation current
- Report gaps in documentation
- Sufficient to support management assertion

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Evaluation Control Design

Controls should be designed to reduce the risk of error to an acceptable level—consider the COBIT capability model.

Key Components

- Sufficient to demonstrate
  - Control design to prevent or detect material errors
  - Conclusion that tests were appropriately conducted
  - Results appropriately evaluated
- Consider people, process and technology

Key Considerations

- Preventive vs. detective
- Automated vs. manual
- Controls are defined, managed, measured and repeatable

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Evaluate Operational Effectiveness

Test controls to ensure that they are operating as designed and consistently over a period of time.

Key Components

- Application controls and general controls
- Performance
  - Performed by knowledgeable person
  - Performed consistently
  - Appropriately monitored
  - Weaknesses followed up on a timely basis

Key Considerations

- Period of time vs. point in time
- Audit evidence—Inquiry alone is not enough
- Service organizations—SAS70

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Determine Control Deficiencies

Identify deficiencies and establish an action plan to remediate and test prior to the compliance deadline.

Key Components

- Impact to the financial statements
  - Is it more than inconsequential?
- Likelihood of occurrence
  - Is there more than a remote likelihood of occurrence?
- Isolated weaknesses vs. systematic weaknesses

Key Considerations

- Isolated errors vs. systematic errors
- Has an impact assessment been performed to determine the importance to the financial reporting process?
- May need to revisit control design or operation if deficiencies are observed

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Document Results

Based on the results of testing, prepare an assertion on the effectiveness of internal control which will be audited by the independent auditors.

Key Components

- Evaluate operational effectiveness of internal controls over financial reporting
- Disclose all known control deficiencies and weaknesses
- Disclose acts of fraud

Key Considerations

- Show-stoppers
  - Material weaknesses
  - Significant deficiencies

©2003 IT Governance Institute

A Readiness Roadmap (cont'd)
Build Sustainability

Establish a "center of excellence" model to support ongoing Sarbanes-Oxley compliance.

Key Components

- Continuous effectiveness of internal control
- Monitoring activities
- Change management
- Knowledge capture and transfer

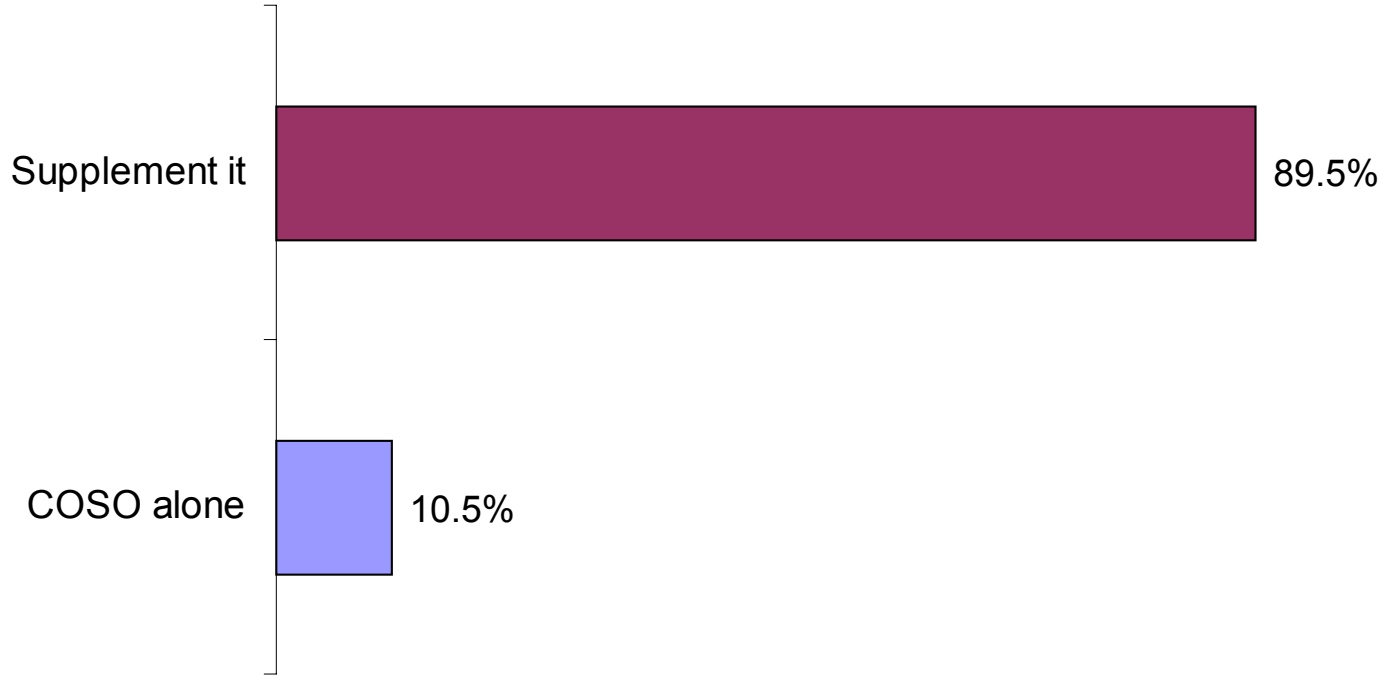
Key Considerations

- Continuous improvement process
- Rules are evolving—stay tuned

©2003 IT Governance Institute

Polling Question #2

Do you plan to use COSO solely to implement Sarbanes-Oxley compliance within your enterprise, or do you plan to supplement it with other best practices or standards?



©2003 IT Governance Institute

Summing Up

©2003 IT Governance Institute

Summing up

- With the dependence on IT for reliable financial reporting processes, IT plays a key role in compliance with Section 404 of Sarbanes-Oxley
- For many IT organizations Sarbanes-Oxley is simply a codification of existing responsibilities. These IT control responsibilities already exist, however Sarbanes-Oxley may require addition formalization and significant efforts to document and test.
- Companies should ensure IT has an active role in Sarbanes-Oxley efforts
  - Participate on the compliance steering committee
  - Understand the financial reporting process and communicate the dependency on IT (applications, infrastructure, security, etc.)
  - Establish IT's role in ensuring controls over the financial reporting process
  - Document IT risks and controls related to the financial reporting process
  - Regularly test controls and remediate significant weaknesses
  - Establish monitoring activities to ensure the effectiveness of IT controls over time

©2003 IT Governance Institute

Questions?

©2003 IT Governance Institute