

Relevante

Accounting & Technology Consultants

Impact of
Sarbanes Oxley Act of 2002
on IT Departments

Presented by

Fred Kaplan, MBA, CBM

Director of Financial Consulting
Relevante, Inc.

- **History, Benefits & Deadlines of the Sarbanes Oxley Act of 2002**
- **Key Provisions of Sarbanes Oxley Act**
- **Key Requirements for implementing SOX provisions in IT**
- **Control Frameworks**
- **IT Implications & Challenges to SOX Compliance**
- **IT Management's Responsibilities for SOX Compliance**
 - **Infrastructure**
 - **Security**
- **Costs, Effectiveness & Future Technology Initiatives for Compliance with Sox**

- **In response to the Arthur Anderson, Enron and WorldCom debacle, the Sarbanes-Oxley Act seeks to**
 - Restore the public confidence in both public accounting and publicly traded securities
 - Assure ethical business practices through heightened levels of executive awareness and accountability

Benefits of Effective Internal Control over Financial Reporting

Relevante

Accounting & Technology Consultants

- **Improved effectiveness and efficiency of internal control processes**
- **Better information for investors**
- **Enhanced investor confidence**
- **Improved quality of financial reporting**

Impact of
Sarbanes Oxley Act of 2002
on IT Departments

- **FYE on or after November 15, 2004**
 - US accelerated filers
 - Public equity float of \$75 million and up
- **FYE on or after July 15, 2006 – all other public entities**
(previously 7/15/05 – was extended one year in 3/2005)
- **Non-public – could have impact**
 - Preparing for IPO
 - Vendor to public entity

- ***Section 302* – Corporate Responsibility for Financial Reports**
- ***Section 404* - Management Assessment of Internal Controls**
- ***Section 409* – Real Time Disclosures**
- ***Section 906* - Corporate Responsibility for Financial Reports – Penalty Enhancements**

- **Certifications required in periodic financial statements**
 - Review of reports by signing officers
 - No false or misleading statements or omissions
 - Information presents the financial condition & results in all material respects
 - Responsibility of signing officers for enforcing internal controls
 - List of deficiencies in internal controls
 - Significant changes in internal controls

- **Management's responsibility to establish & maintain a system of internal controls**
- **Identification of framework for evaluation of internal controls**
- **Disclosure of material weaknesses in internal control**
- **Opinion on adequacy of internal controls by external auditors**

- **Expanded disclosure requirements under amended SEC form 8-K**
- **In most cases, Form 8-K to be filed within 4 business days after a triggering event**
- **New Qualifying triggering events**
 - Entry into a material definitive agreement
 - Termination of a material definitive agreement
 - Creation of a direct financial obligation or an obligation under an off balance sheet arrangement
 - Costs associated with exit or disposal activities
 - Material Impairments
 - Notice of delisting or failure to satisfy a continued listing rule or standard

Accelerated filing Deadlines

Report	2002	2003	Filed after 12/15/2005
10-K	90 days	75 days	60 days
10-Q	45 days	40 days	35 days

Key Requirements for implementing SOX provisions in IT (1)

- **Understanding the organization's internal control program and its financial reporting process**
- **Selecting an appropriate control framework**
- **Mapping the IT systems that support internal control and the financial reporting process to the financial statements.**
- **Identifying risks related to these IT systems.**
- **Designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness**

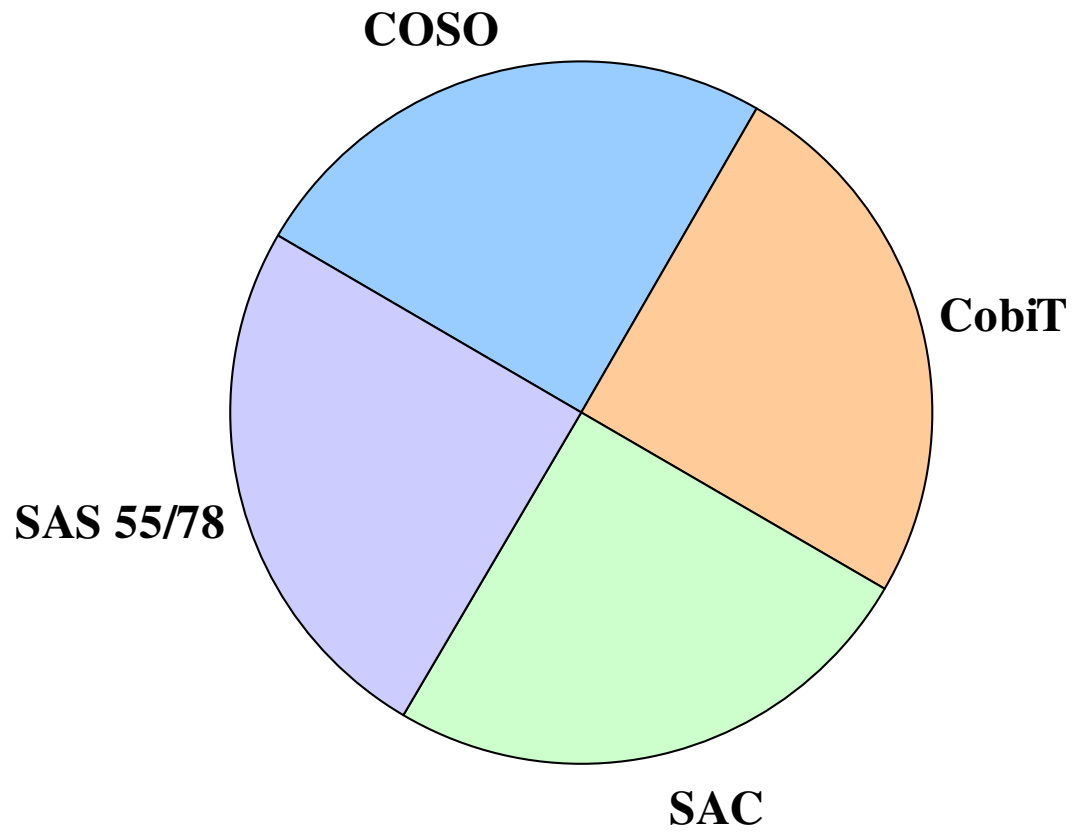
Key Requirements for implementing PCAOB Control Framework in IT (2)

Relevante

Accounting & Technology Consultants

- **Documenting & testing IT controls**
- **Ensuring that IT controls are updated & changed, as necessary to correspond with changes in internal control or financial reporting processes**
- **Monitoring IT controls for effective operation over time**

Impact of
Sarbanes Oxley Act of 2002
on IT Departments



Comparison of Internal Control Frameworks

Parameter	COBIT	SAC	COSO	SAS's 55/78
Primary Audience	Management, Users, ISA's	Internal Auditors	Management	External Auditors
Organizational IC objectives	<ul style="list-style-type: none"> • Efficient Ops • Confidentiality • Integrity • Reliable financial reporting • Compliance with laws 	<ul style="list-style-type: none"> • Efficient Ops • Reliable financial reporting • Compliance with laws 	<ul style="list-style-type: none"> • Efficient Ops • Reliable financial reporting • Compliance with laws 	<ul style="list-style-type: none"> • Efficient Ops • Reliable financial reporting • Compliance with laws
Focus	IT	IT	Overall Entity	Financial Statement
IC Effectiveness Evaluated	For a period of Time	For a period of Time	At a point in time	For a period of Time
Responsibility of IC system	Management	Management	Management	Management

- **Control Environment**
- **Risk Assessment**
- **Control Activities**
- **Information and Communication**
- **Monitoring**

- 1. Acquire or develop application software**
- 2. Acquire technology infrastructure**
- 3. Develop and maintain policies and procedures**
- 4. Install and test application software and technology infrastructure**
- 5. Manage changes**

- 6. Define and manage service levels.**
- 7. Manage third-party services**
- 8. Ensure systems security**
- 9. Manage the configuration**
- 10. Manage problems and incidents**
- 11. Manage data**
- 12. Manage Operations**

- **Certification of the completeness, accuracy & integrity of reporting data**
- **Creating an audit trail back to originating system**
- **Integration of non financial information**
- **Management of user access to information**

- **Effective Data Capture due to fragmentation of data across several systems & department boundaries**
- **Manual processes & Excel spreadsheets used to aggregate underlying data**
- **Building effective access control rules**
- **Implementation of change requests**

- **Requirement of large amount of information in the periodic reports quickly**
- **Need for reduction in the level of manual activities in the financial reporting & consolidation process**
- **Rapid, Mass deployment of information**

- **Automation of problem and opportunity identification**
- **Proactive Intelligence**
- **Real Time Access to information**

- **Multiple, non integrated applications**
- **Disconnected spreadsheets to reformat, edit information extracted from transaction processing systems**
- **Non integrated business intelligence solutions that enable many different views of data to be presented from different versions of source data**
- **Custom built add-on products, that read or write data directly to the application database tables**

- **Data transfer errors**
- **Transactions not logged**
- **Difficulty in tracing transaction sources**
- **Bypassing of secure posting routines**
- **Tendency to maintain multiple local sources for the same data**

- **Invest in controls**
- **Address end-to-end business processes**
 - Order to Cash
 - Procure to Pay
- **Disintegration of legacy applications (ERP, CRM & SCM)**
- **Disjointed process ownership**

- **Servers where financial data is stored, and all other servers and desktops that have access to them**
- **Must be securely locked down**
- **Access controls must be demonstrated**
- **Detailed audit reports must be performed on an ongoing basis**
- **Automated process may be mandated**

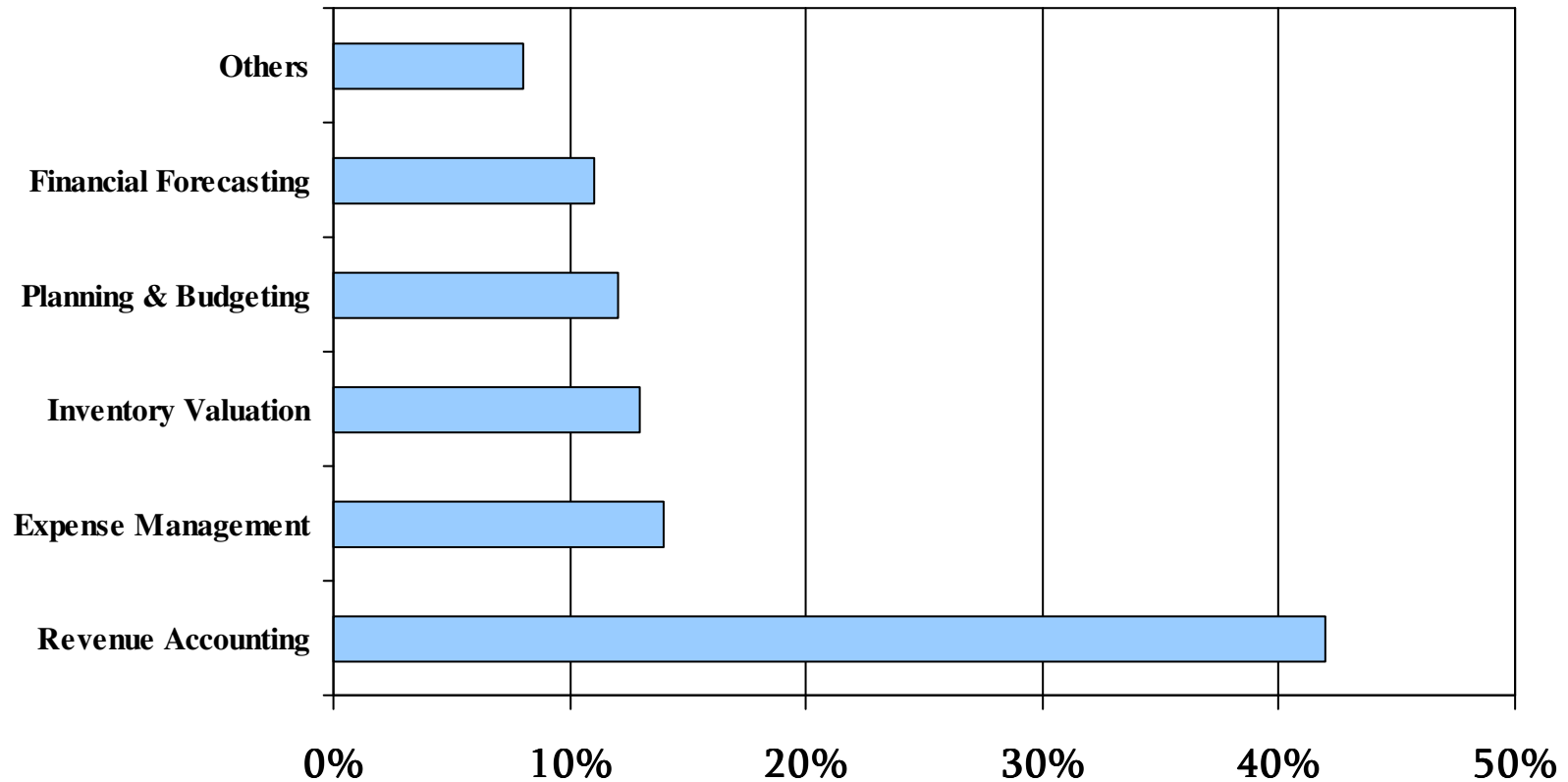
- **Establish and adopt policies**
- **Train IT staff and users**
- **Establish controls to ensure policy standards are met**
- **Take action when controls fail**

- **Physically secure devices**
- **Secure offline storage (backup tapes, etc.)**
- **Secure system admin accounts and groups**
- **Require regular password changes**
- **Require complex passwords**
- **Disallow frequent reuse of passwords**
- **Assign lowest possible permissions to all Windows accounts**
- **Secure installation files and media**

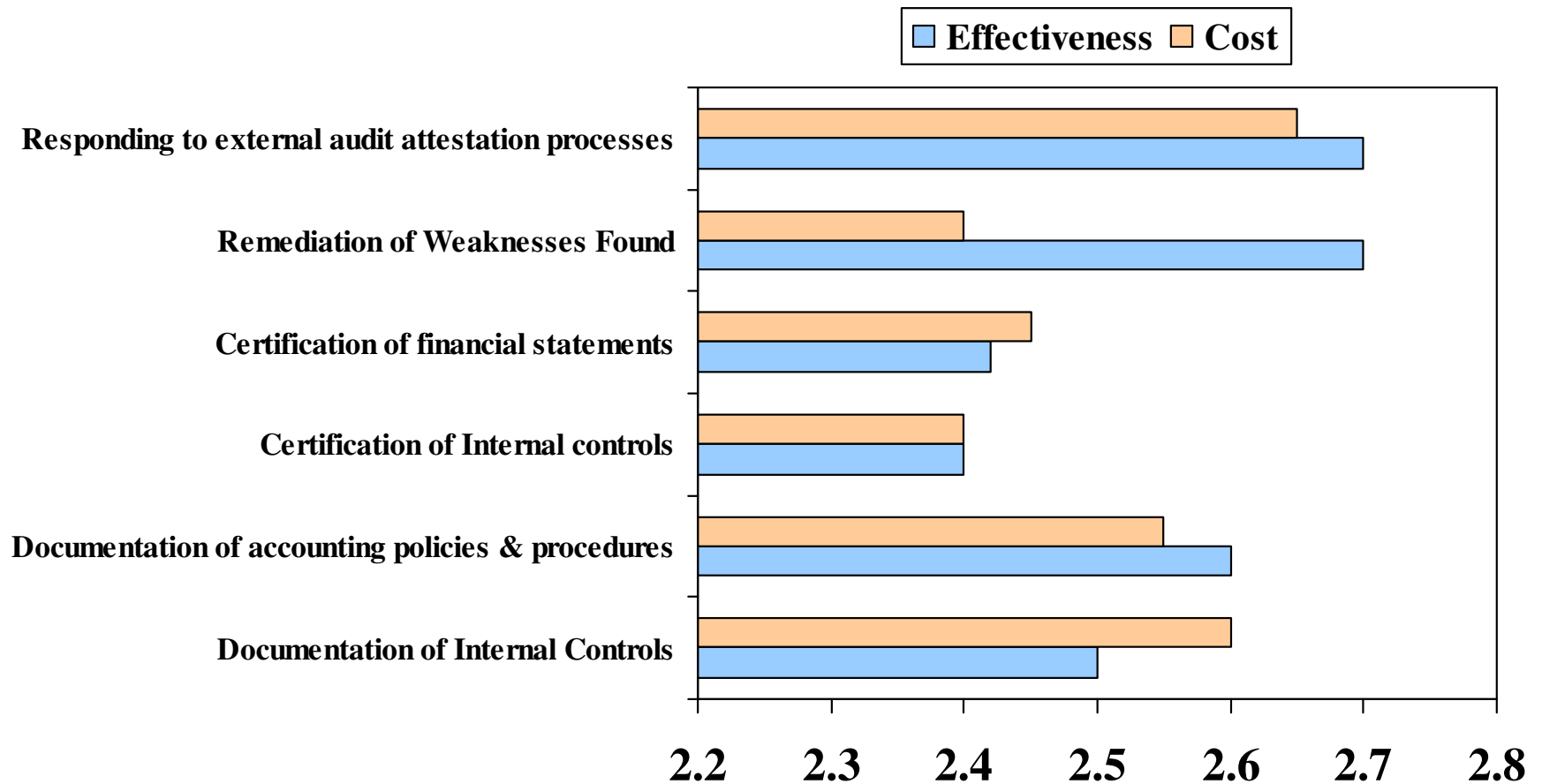
- **Implement current service packs and hot fixes as quickly as possible – AFTER ADEQUATE TESTING**
- **Keep anti-virus and anti - spyware software up to date**
- **Implement firewalls between Internet and private network**
- **Enable security logging**
- **Prepare disaster and even procedures**

- **Implement Smart cards**
- **Encrypt network traffic**
- **Encrypt file systems**
- **Implement firewalls within private network to isolate networks and activities**

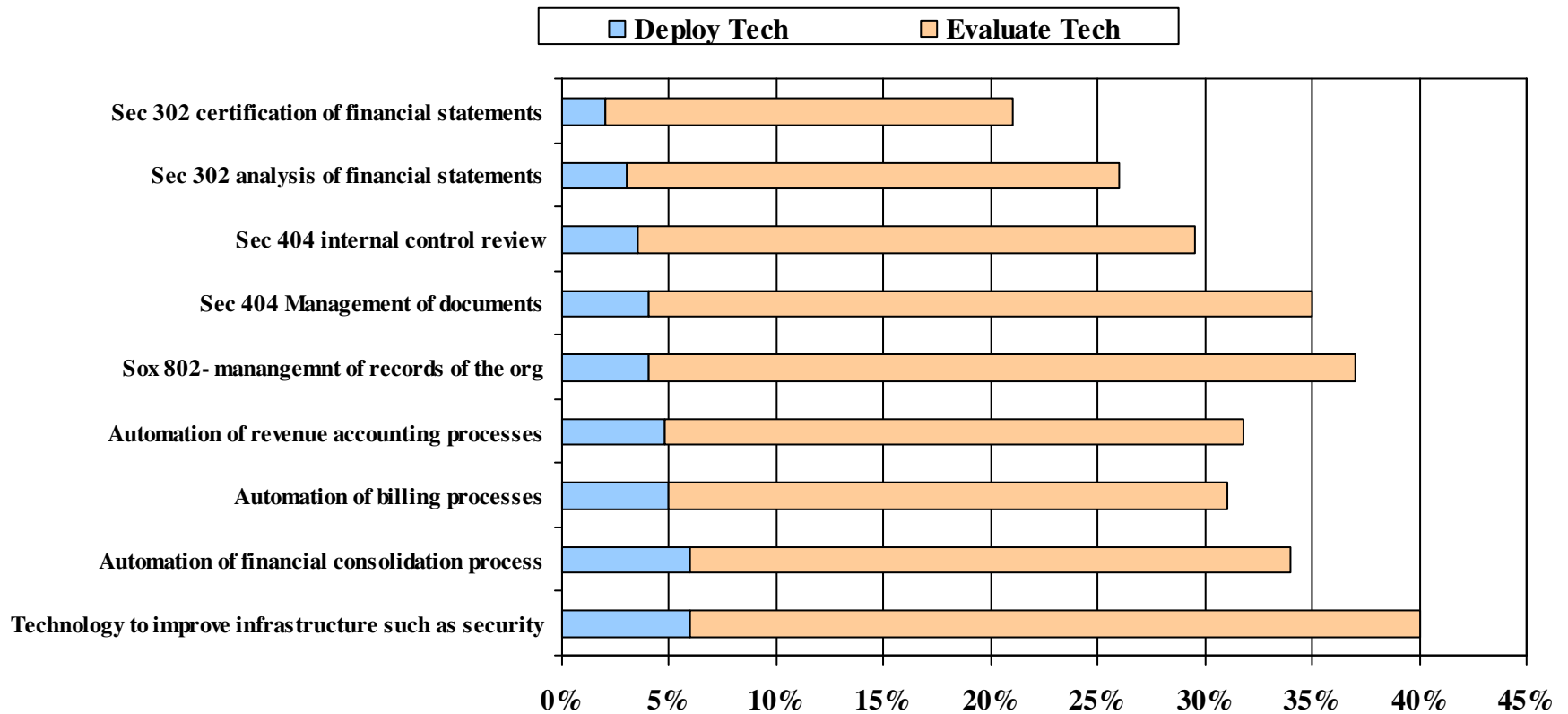
Financial Processes that present the most risk of restating financial results in an organization



Sarbox Compliance Costs & Effectiveness



Plans for improving SOX processes using technology at public & private companies



Thank You



Impact of
Sarbanes Oxley Act of 2002
on IT Departments