What IT Auditors Can Learn From COSO's Internal Control over Financial Reporting Guidance for Smaller Public Companies

Presented by Sirius Solutions

ISACA Monthly Meeting

Thursday, September 21, 2006

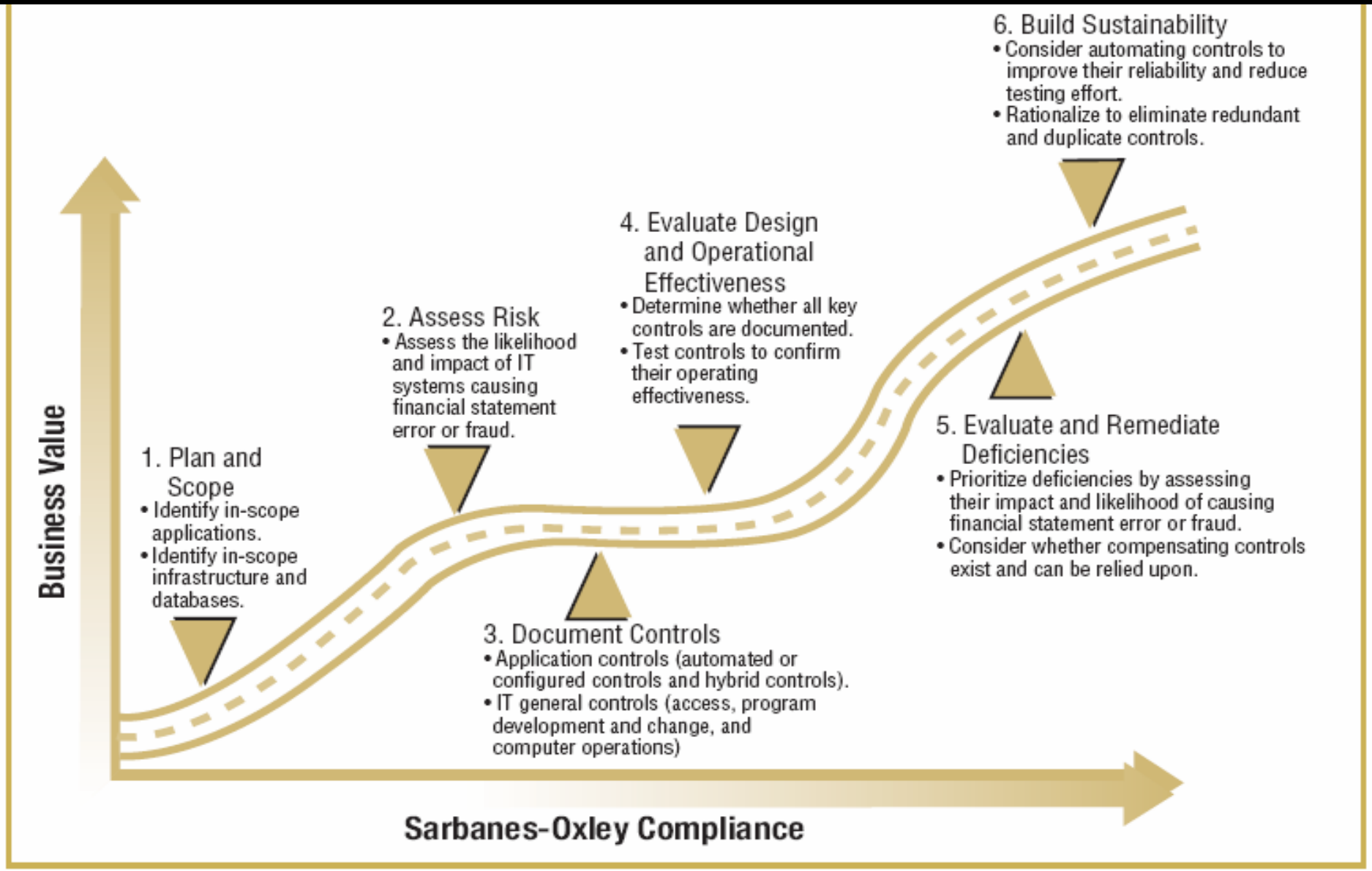
Presentation Agenda

- **An Overview of Sarbanes-Oxley**
- **SOX Compliance Roadmap**
- **What is COSO?**
- **What is COBIT?**
- **Alignment with PCAOB to COBIT**
- **Stages of Control Reliability**
- **ICE and Residual Risk Analyses**
- **Characteristics of "Smaller" Public Companies**
- **Complexity of "Smaller" Public Companies**
- **Categories of IT Controls**
- **Control Considerations for "Smaller" Public Companies**
- **Question & Answer Segment**

Overview of Sarbanes-Oxley Act

- **In general, the certification requirements require companies to formalize control structures, improve controls and establish monitoring programs to enable CEOs and CFOs to make evaluations and report conclusions in public SEC filings.**
  - **Section 302:** Requires quarterly certification by the CEO/CFO regarding the completeness and accuracy of quarterly reports as well as the nature and effectiveness of disclosure controls and procedures supporting the quality of information included in such reports.
  - **Section 404:** Requires an annual assertion by the CEO/CFO regarding the effectiveness of internal control over financial reporting and safeguarding of assets. It also requires an attestation by the independent auditor as to the accuracy of management's assessment.

SOX Compliance Roadmap



Source: IT Control Objectives for Sarbanes-Oxley, 2nd Edition. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Financial Reporting and Disclosure.

SIRIUS SOLUTIONS

What is COSO?

The Committee of Sponsoring Organizations of the Treadway Commission

COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

COSO Framework

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

SIRIUS SOLUTIONS

What is COBIT?

Control OBjectives for Information and related Technology

COBIT (4th edition) is the most recent version of Control Objectives for Information and related Technology, and was first released by the **Information Systems Audit and Control Foundation** (ISACF) in 1996.

The 2nd edition, published in 1998, reflected an increase in the number of source documents, addressed high-level and detailed control objectives and the addition of the Implementation Tool Set.

The 3rd edition marked the entry of a new primary publisher for COBIT: the **IT Governance Institute**. The IT Governance Institute was formed by the **Information Systems Audit and Control Association** (ISACA) and its related Foundation in 1998 in order to advance the understanding and adoption of IT governance principles.

IT Governance *is defined as: a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risks versus return over IT and its processes.*

COBIT Relationship to COSO (*original ITGI guidance)

COBIT Control Objectives	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize					
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.	•		•	•	•
Acquire and Implement					
Identify automated solutions.					
Acquire and maintain application software.			•		
Acquire and maintain technology infrastructure.			•		
Develop and maintain procedures.			•	•	
Install and accredit systems.			•		
Manage changes.			•		•
Deliver and 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.			•	•	
Monitor and Evaluate					
Monitor the processes.				•	•
Assess internal control adequacy.					•
Obtain independent assurance.	•				•
Provide for independent audit.					

Source: IT Governance Institute - The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting. (June 2004)

Alignment with PCAOB and COBIT (* latest ITGI guidance)

Figure 1—Control Processes Mapping to PCAOB and CobiT

IT Control Objectives for Sarbanes-Oxley	CobiT	PCAOB IT General Control Heading			
	Mapping to CobiT 4.0 Processes	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and maintain application software.	AI2	●	●	●	●
2. Acquire and maintain technology infrastructure.	AI3	●	●	●	
3. Develop the IT processes, organization and relationships.	PO4	●	●	●	●
4. Install and accredit solutions and changes.	AI7	●	●	●	●
5. Manage changes.	AI6		●		●
6. Define and manage service levels.	DS1	●	●	●	●
7. Manage third-party services.	DS2	●	●	●	●
8. Ensure systems security.	DS5			●	●
9. Manage the configuration.	DS9			●	●
10. Manage problems and incidents.	DS8, DS10			●	
11. Manage data.	DS11			●	●
12. Manage the physical environment and operations.	DS12, DS13			●	●

In all, 12 IT control objectives, which align to the PCAOB Accounting Standard No. 2 and Control Objectives for Information and related Technology (COBIT), were defined for Sarbanes-Oxley. Figure 1 provides a high-level mapping of the IT control objectives for Sarbanes-Oxley, the PCAOB IT general controls and the COBIT 4.0 processes.

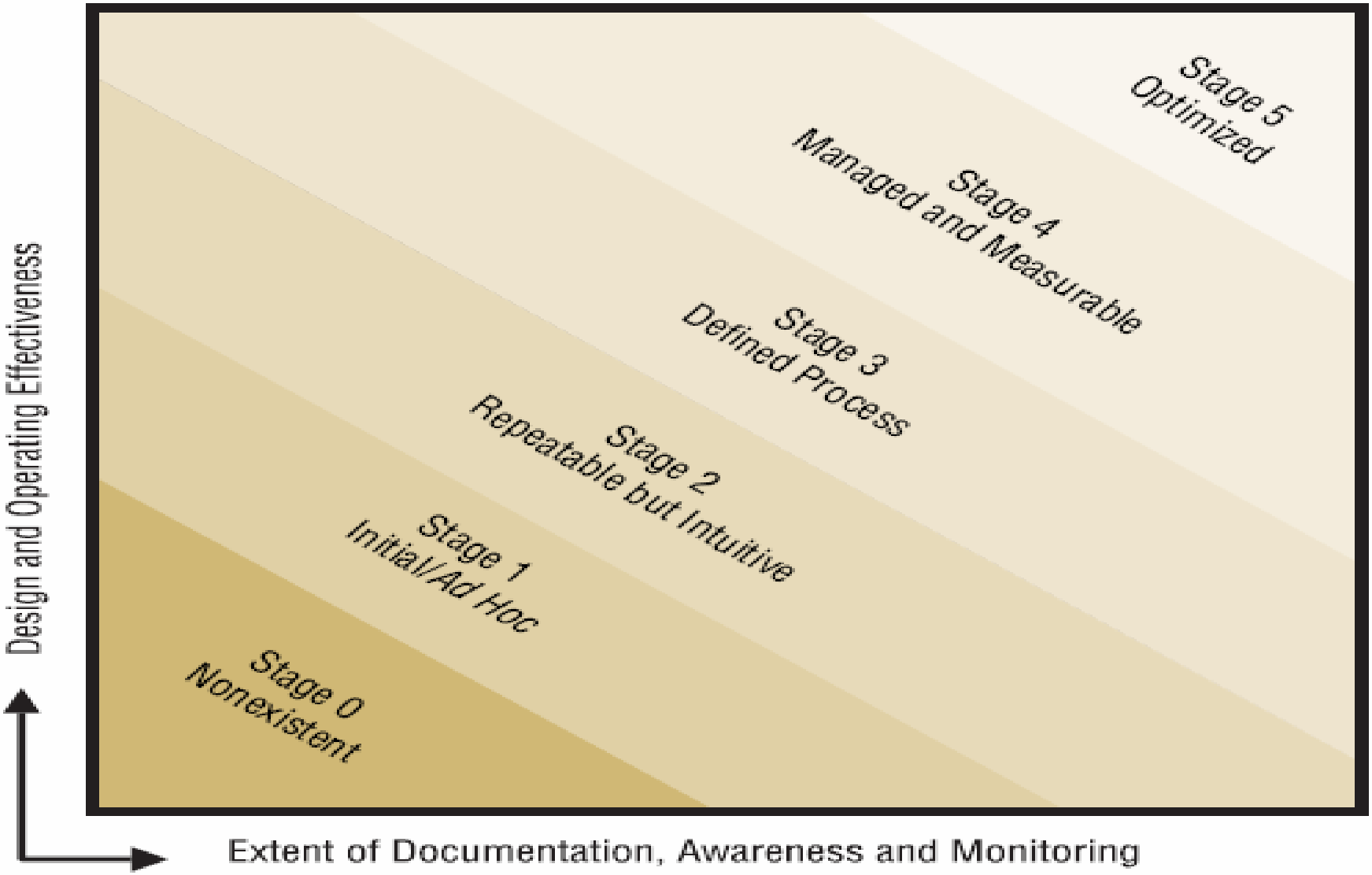
Source: IT Control Objectives for Sarbanes-Oxley, 2nd Edition. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Financial Reporting and Disclosure.

SIRIUS SOLUTIONS

COSO Component: Risk Assessment

SIRIUS SOLUTIONS

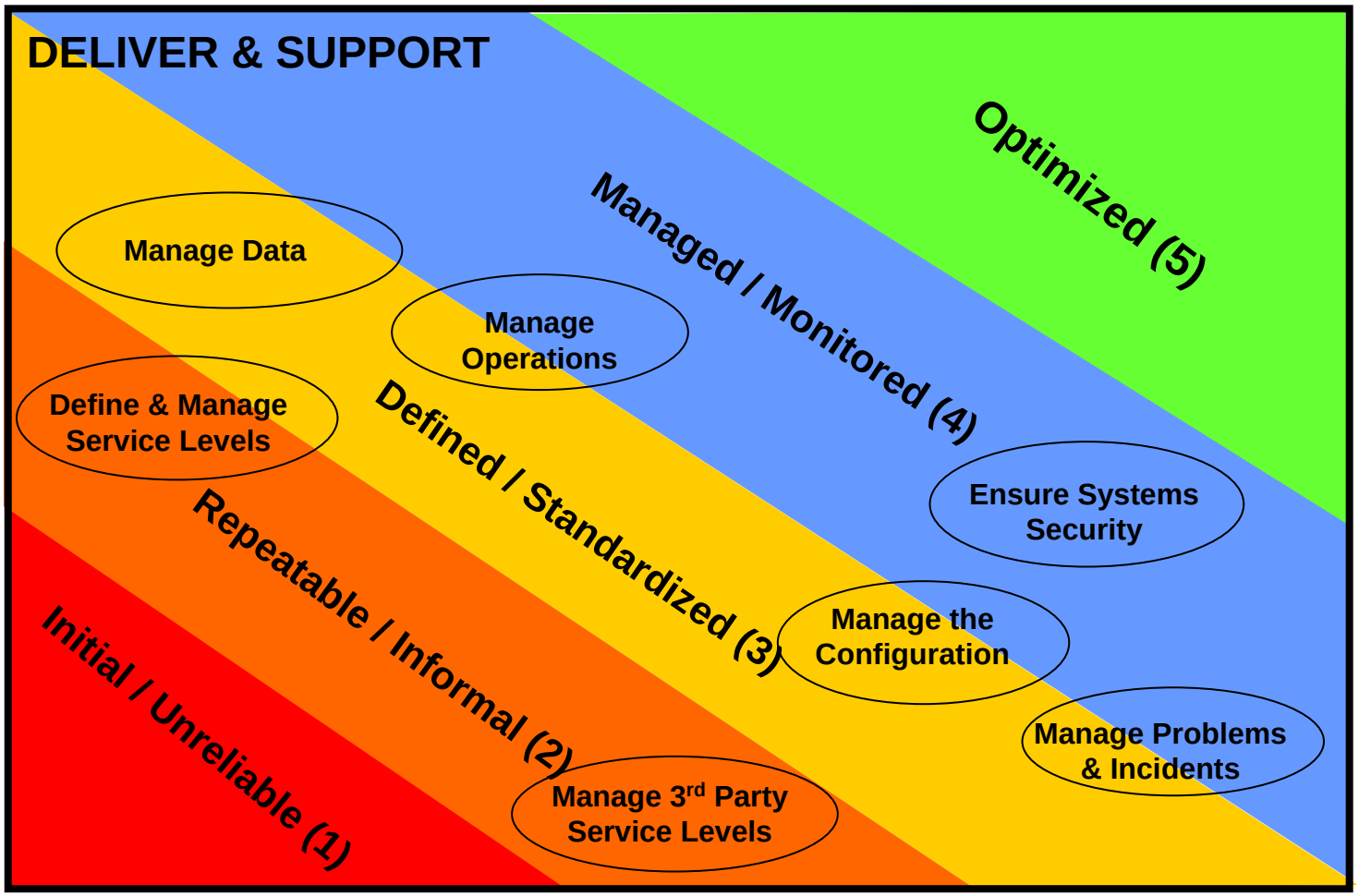
Stages of Control Reliability



Source: IT Control Objectives for Sarbanes-Oxley, 2nd Edition. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Financial Reporting and Disclosure.

SIRIUS SOLUTIONS

Internal Control Effectiveness Assessment by COBIT Objective



SIRIUS SOLUTIONS

Strategic IT Risk Assessment & Analysis

Impact		
1	No Impact	➢ Resolution of issues will be handled by junior management and staff ➢ <$10,000 impact on profitability ➢ No potential impact on shareholder value ➢ No impact on reputation
2	Minimal	➢ Resolution of issue will be handled by direct reports to subsidiary president ➢ $10,001 to $50,000 impact on profitability ➢ Financial impact can be absorbed under normal operating conditions ➢ There is a potential impact on shareholder value and reputation
3	Moderate	➢ Resolution of issues will handled by subsidiary president and direct reports to subsidiary president ➢ $50,001 to $250,000 impact on profitability ➢ Short-term impact on shareholder value and/or reputation
4	Significant	➢ Resolution of issue will be handled by Board, CEO and CFO ➢ $250,001 to $500,000 impact on profitability ➢ Serious impact on reputation and shareholder value with adverse publicity ➢ Key relationships are threatened
5	Catastrophic	➢ Sustained, long-term loss in shareholder value ➢ >$500,000 impact on profitability ➢ Loss of key relationships

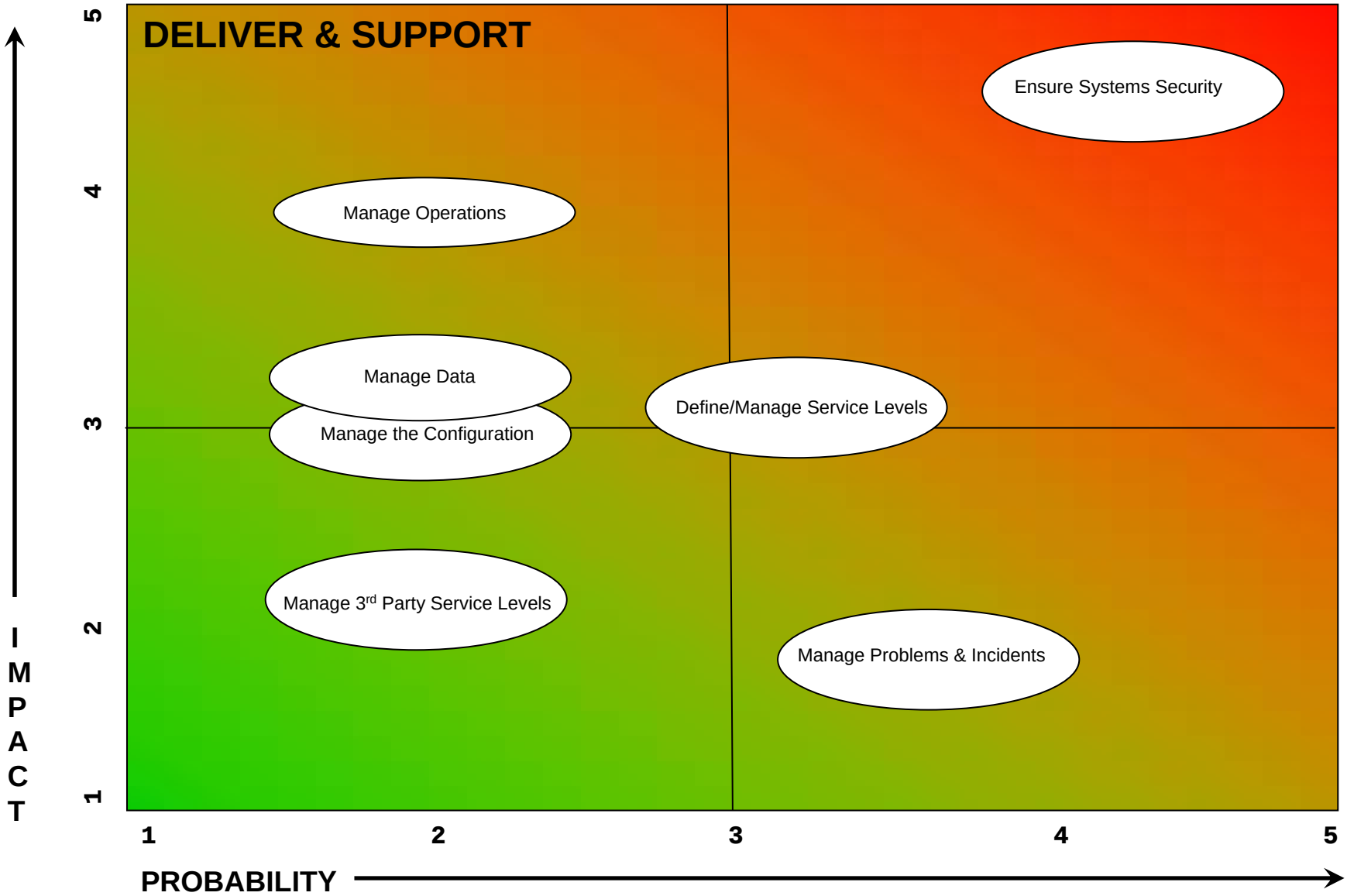
	Probability	
1	Remote	➢ Event may only occur in exceptional circumstance
2	Unlikely	➢ Event could occur
3	May	➢ Event should occur
4	Likely	➢ Event will probably occur
5	Will	➢ Event is expected to occur

Risk Residual Matrix

Ranking Components

SIRIUS SOLUTIONS

Residual Risk Matrix



SIRIUS SOLUTIONS

COSO Component: Control Environment

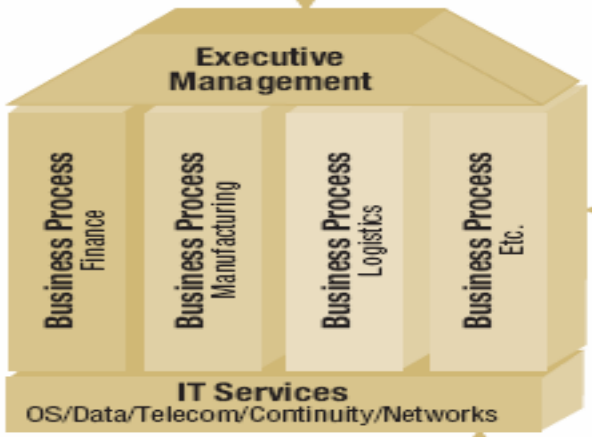
SIRIUS SOLUTIONS

Common Elements of Organizations

Entity-level Controls

Entity-level controls set the tone and culture of the organization. IT entity-level controls are part of a company's overall control environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit



Application Controls

Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP and Oracle as well as smaller off-the-shelf (OTS) systems like ACCPAC.

Controls include:
- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

IT General Controls

Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls

Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations

In understanding where IT controls exist within the typical company, consideration of at least three elements should be given: executive management, business processes and IT services.

Source: IT Control Objectives for Sarbanes-Oxley, 2nd Edition. The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Financial Reporting and Disclosure.

SIRIUS SOLUTIONS

COSO Component: Control Activities

SIRIUS SOLUTIONS

Characteristics of "Smaller" Companies

COSO's Internal Control over Financial Reporting Guidance for Smaller Public Companies, discloses the following characteristics for businesses referred to as "smaller" which include but are not limited to:

- Fewer lines of business, and fewer products within lines
- Concentration of marketing focus, by channel or geography
- Leadership by management with significant ownership interest or rights
- Fewer levels of management, with wider spans of control
- Less complex transaction processing systems
- Fewer personnel, many having a wider range of duties
- Limited ability to maintain deep resources in line as well as support staff positions such as legal, human resources, accounting and internal auditing

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Complexity

The nature of information technology related controls is largely a reflection of the degree of complexity of transaction processing, software development and related factors.

IT Control Area	Less Complex	More Complex
Transaction Processing	**Processing is such that input controls can be readily reconciled to the system output. Reliability of processing is achieved via manual user controls.**	**Transactions are subject to calculations or other manipulations using data or formulas, sometimes with multiple subsystems, where input is not reconcilable to system output. Reliability of processing is achieved via built in application controls, together with related manual user controls and IT general controls.**
System Development	**Packaged accounting software with straightforward functions with few processing options, or with standard, readily configurable processing options and controls. Reliability achieved through controls over vendor selection and package implementation.**	**Custom developed software or packaged software modified or supplemented to meet the company's processing needs. The software may require modification as additional features are provided to users or company needs change. Reliability achieved through program development and change controls.**

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Complexity continued

IT Control Area	Less Complex	More Complex
Connectivity	**Connectivity to external networks and / or the Internet is limited to e-mail applications.**	**Reliance on external connectivity, including the Internet, where the company transmits transactional data to and from the Internet.**
End-User Computing	**Spreadsheets serve as an electronic information warehouse, perhaps performing straightforward calculations using simple formulas.**	**Spreadsheets support complex calculations, valuations and modeling tools, perhaps using macros and linking multiple supporting spreadsheets.**

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Categorization of IT Controls

The following categorizes IT controls and is useful when considering an approach to assess design and effectiveness, based on the aforementioned degree(s) of complexity.

Systems Development – controls over design and implementation of systems that help ensure that systems are appropriately developed, configured, approved and migrated into production

System Changes – controls over modifications to systems, whether applications, supporting databases or operating systems, helping to ensure that changes are approved and properly tested and implemented

Security and Access – controls over critical applications, supporting databases, and networks that help management ensure that access is properly authorized an data is appropriately used, maintained and reported

Computer Operations – controls over day-to-day operations that help ensure that processing errors or improprieties are identified and corrected in a timely manner

Application Controls – controls built into applications to help ensure completeness and accuracy of transaction authorization, validity and processing, as well as related manual user controls

End-User Computing – controls over spreadsheet and other user-developed applications that address potential input, logic and interface errors

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies

June 2006

Systems Development

Systems Development in a Less Complex Environment

- Fewer significant changes to the processing environment
- Changes might include only operating system patches and packaged application upgrades
- Management should follow a process for selecting new packages which considers application controls, security features, data conversion requirements, testing, and backout plans
- Management may also rely on system change procedures for updates

System Development in a More Complex Environment

- Within a more complex environment management uses a broader range of system development policies and procedures that help ensure financial reporting related applications are designed, developed, tested, and installed in a properly controlled manner

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Change Management

Change Management in a Less Complex Environment

•Application, database, and job schedule changes may be limited to controls over proper installation of upgrades

•A patch management process may be used that includes testing prior to release of packaged software updates into production

•Contracts with a third party to test application and system patches

Change Management in a More Complex Environment

More complex environments typically have a wide variety of changes at the request of the business or initiated by the IT group. In these environments management:

•Develops change and incident management processes, with effective control procedures to help ensure changes are made properly

•Where the company utilized a network for user authentication and/or receiving data such as customer orders, appropriate controls are required to determine whether changes are done properly such that reporting objectives are achieved

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies

June 2006

Security and Access Controls

Security and Access Controls in a Less Complex Environment

In a less complex environment, access controls are focused on access to the network and access to application software. Database technology utilized by packaged application software is maintained through the application tools and interfaces. Access controls are monitored through IT operations or a security administrator, whose role is to perform the following tasks:

- Grants and maintains access at levels defined by management, including disabling default logon accounts
- Authenticates logon accounts
- Establishes general system access control including system default passwords, implements security patches in cooperation with IT operations, and disables unnecessary services
- Monitors and reports on security issues to IT management and information owners
- Performs re-certifications

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Security and Access Controls continued

Security and Access Controls in a More Complex Environment

More complex environments utilizing the network for user authentication and/or receiving data (i.e. customer orders) call for network controls. Within a more complex environment management:

- Secures access to critical applications, databases, operating systems, and networks
- Restricts access to authorized personnel by requiring appropriate identification and authentication. Server, telephone, network and power supply equipment are kept in a secured room or cabinet
- Receives and reviews reports on both security and processing problems and delivers to an appropriate, identified individual, with problem tracking mechanisms established

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Computer Operations

Computer Operations in a Less Complex Environment

- Within a less complex environment management backs up, retains, and stores critical financial data and programs
- Backup media are stored in secure locations, both on-site and off-site
- Backup media is tested periodically to assess recoverability

Computer Operations in a More Complex Environment

- Within a more complex environment management also establishes formal sign-off procedures to track items transferred offsite for back-up purposes
- Also established is a process to report operating issues, with regular or periodic review, by IT operations and company management
- Issues are analyzed to determine corrective actions, prioritized according to impact on the company
- An escalation process accelerates urgent issues to top management for resolution

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies

June 2006

Application Controls

Application Controls in a Less Complex Environment

- Management implements controls over data input to determine whether transactions are authorized, and transactions are processed correctly and completely, with rejected items captured and followed-up
- Implements controls over output to help ensure matters requiring user action are properly dealt with

Application Controls in a More Complex Environment

- Within a more complex environment management also uses data processing controls for accuracy, completeness, and timeliness of data during either batch or real-time processing by the application
- Controls over application programs and related computer operations are reviewed to determine that data are processed accurately through the application and that no data is added, lost, or altered during processing
- A formal data exception procedure exists for error handling, where management reviews all changes to data during the remediation process

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

End User Computing

Identifying and Securing End-User Computing Applications

Management identifies significant end-user applications, including spreadsheets, and other user-developed programs. Critical end-user applications are stored on secured file servers. Data integrity is ensured by locking or protecting cells to prevent inadvertent or intentional changes to standing data.

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
June 2006

Outsourced Operations

Reviewing Outsourced Operations

Some companies choose to outsource management of their information technology. Outsourced tasks may include those related to computer operations, change management and security and access controls. Management reviews general computer controls of critical third party vendors that host and/or support critical financial applications and/or information technology support functions. These controls may be evidenced by an independent third party review and report, such as a Type II SAS 70 report.

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies

June 2006

About Sirius Solutions

- **Headquartered in Houston, Texas**
- **Began operations in 1998**
- **Maintains a client list that includes leading global corporations**
- **Over 250 experienced professionals having significant management experience with Fortune 500 corporations and 'Big Four' accounting firms**
- **Professionals average more than 10 years experience in their respective fields: finance, risk, accounting, information technology, operations and process improvement, strategy, internal audit and tax**
- **In 2006, named by Inc. Magazine as the 33rd fastest growing private company in the United States; 1st in the consulting sector and the 2nd fastest growing company in Texas**
- **Our service offerings include:**
  - **Business Processes & Controls**
  - **Financial Reporting & Transaction Support**
  - **Management Information Systems, and**
  - **Energy Consulting.**

SIRIUS SOLUTIONS

THANK YOU

Charla Parker-Thompson, Firm Director
Business Process & Controls / Financial Systems Integrity
Sirius Solutions, L.L.L.P.
(713) 888-7113 office
(832) 545-7130 cell

Question & Answer Segment

SIRIUS SOLUTIONS