

Securities Industry Association
Sarbanes Oxley from the IT Practitioner's Point of View

October, 2004

- **Influences on Bear Stearns' approach**
- **Bear Stearns IT Strategy**

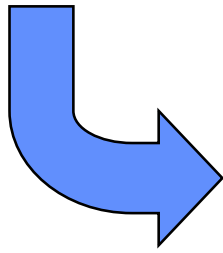
SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

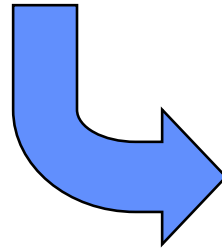
- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the **effectiveness of the internal control structure and procedures** of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

COSO



COBIT



Industry Standard

Consultant Recommendations

- **Control Environment**

The tone is set at the top!

- **Risk Assessment**

Internal control risks

- **Control Activities**

General controls plus application controls

- **Information and Communication**

Roles and responsibilities awareness

- **Monitoring**

Metrics

Control Objectives for Information Technology

***COBIT
Control
Objectives***



COBIT Control Objectives	COSO Component				
	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					■



***COSO
Components***



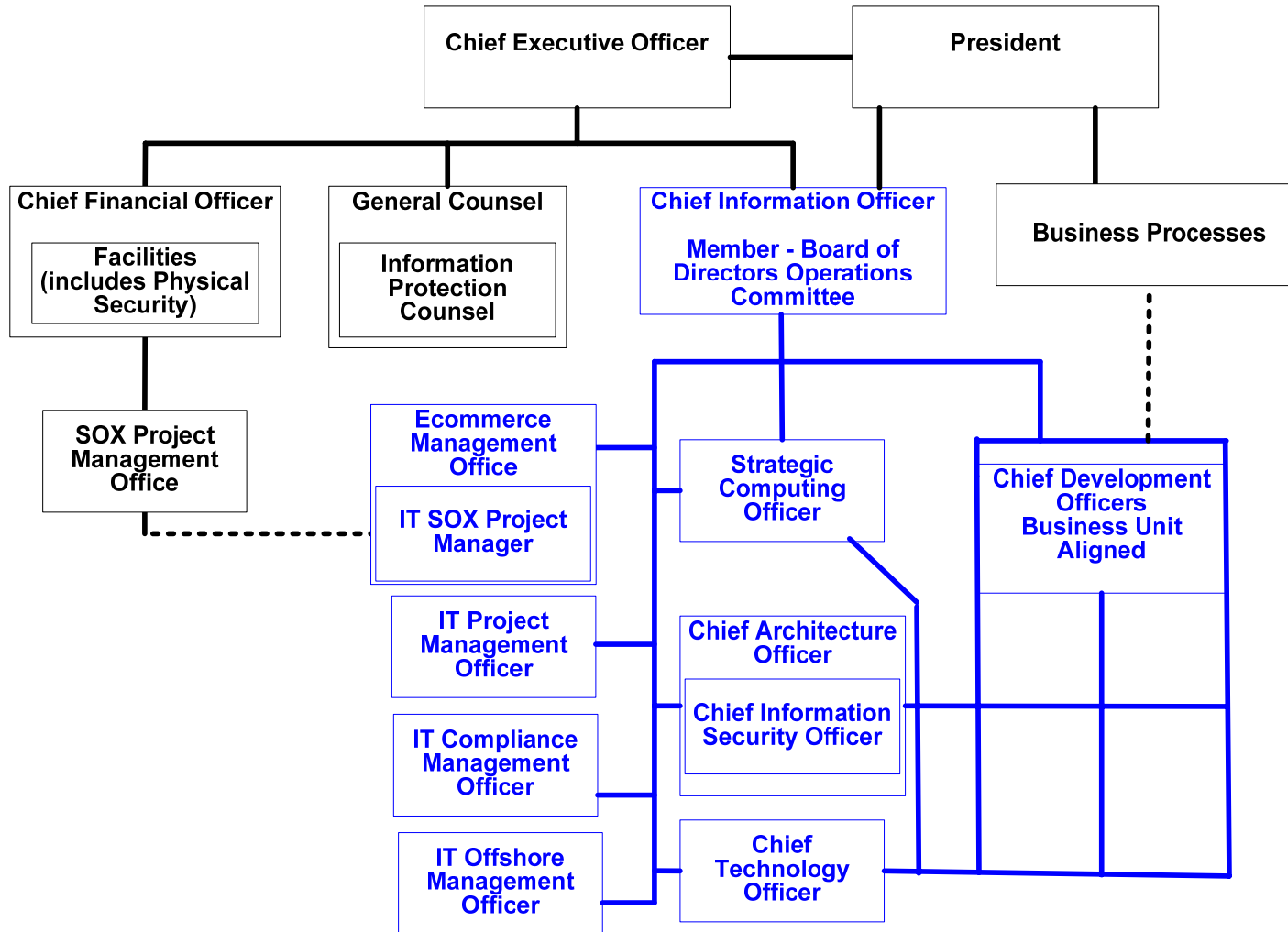
***Controls that
focus on COSO
objectives***

***Source: IT Control Objectives for Sarbanes-Oxley
The IT Governance Institute, an ISACA Research Foundation Organization***

“The SEC regulations that affect Sarbanes-Oxley are undeniably complicated, and implementation will be both time-consuming and costly. In proceeding with an IT control program, there are two important considerations that should be taken into account:

1. There is **no need to reinvent the wheel**; virtually all public companies have some semblance of IT control. While they may be informal and lacking sufficient documentation, IT controls generally exist in areas such as security and availability.
2. Many companies will be able to tailor existing IT control processes to comply with the provisions of Sarbanes-Oxley. **Frequently, it is the consistency and quality of control documentation and evidential matter that is lacking, but the general process is often in place**, only requiring some modification.”

BSC IT Roles and Responsibilities



Key IT SOX Roles and Responsibilities

SOX IT Liaison

SOX IT Committee

SOX IT Liaison (committee chair)

Internal Audit's IT Division

Information Security Group

IT Compliance Management Office

IT Assessors – Accountable Directors

IT Reviewers – CXOs or Direct Reports

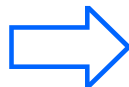
- 1. Determine the scope of your SOX effort**
- 2. Evaluate current control structure with respect to systems in scope**
- 3. Develop action plan to mitigate identified gaps**
- 4. Implement required controls and update documentation**
- 5. Validate and certify controls**

Step 1: Determine the scope of your SOX Effort

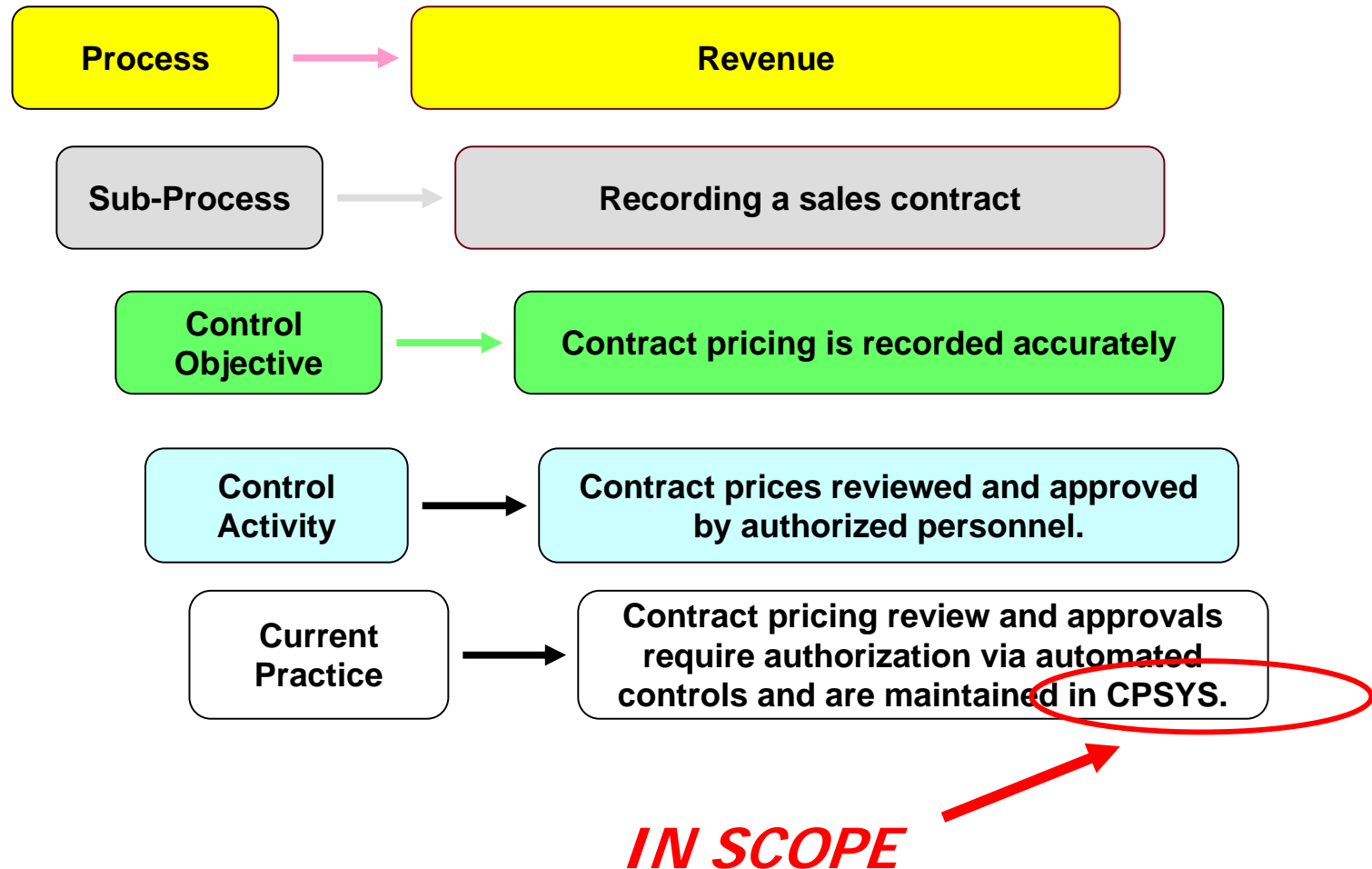
- ⇒ ***Start with the business control structure and processes for financial reporting***
- ⇒ ***Reduce the processes to a set of procedures***
- ⇒ ***Identify the control objectives that are supported by those procedures***
- ⇒ ***Identify the applications as known to the business to support their controls***

This is done by the SOX PMO. As we follow this process, the IT Liaison compiles:

a list of applications



Example: Determining the scope of SOX Effort



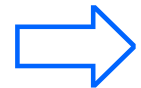
Step 2. Evaluate control structure with respect to scope

Start with the list of applications

- ⇒ ***Identify IT control objectives common to all applications with reference to current Policies and Procedures***
- ⇒ ***Review Control Objectives with Internal and External audit***
- ⇒ ***Identify the control practices for each application with reference to Control Objectives***
- ⇒ ***Collect documentation on control practices that are common to all applications, these are General Controls***
- ⇒ ***Collect documentation on control practices common to applications of common architecture, these are Application Controls***

As this step was completed, we compiled:

a list of control objectives and associated control practices



Example: Control structure with respect to scope

**GENERAL
CONTROLS**

**APPLICATION
CONTROLS**

Application: CPSYS (Contract Pricing System)

IT Governor: Jeannette Santos, Senior Managing Director, IT Pricing Development

IT Manager: Carol Godwin, Vice President, IT Pricing Development

Change Control Administrator: Kristin Klark, Associate Director, IT Quality Assurance

Recovery Administrator: Josh Smith, Associate Director, IT Operations

Description: CPSYS allows sales to enter proposed and change pricing for contract printing and contract negotiation. Once contracts are signed, legal uses CPSYS to compare to the signed contract and accepts as revenue.

Application Component list:

Component Name: GUI (various applications)

Platform: Motif/X-Windows/ accessed through Hummingbird Exceed on Wintel

Specifics: Startup executables on network file share //ntshare/cpsys

Support Team: IT Wintel Administration

Component Name: Database

Platform: Sybase DBMS

Specifics: Sybase ASE server CPSYSDB1 on Sun Solaris machine cpsyssol1

Support Team: IT UNIX and Sybase Administration

Change Control Overview: Developers use Clearcase for source code versioning. QA compiles and delivers to IT Wintel and/or UNIX Administration with corresponding install instruction.

Source Code Repository: Clearcase on ccserv1

Access Control Overview: Users login to the X-Windows GUI via single-sign-on, it retrieves the Sybase password which is unknown to the user. Entitlements are stored in Sybase. Certain business users can add or remove SSO users from the application and also change their roles and privileges.

Network Access Category: Internal

Primary Password Repository: Single-Sign-On

Secondary Repository: Sybase

User Admin Team:

Access Admin

User Admin Team:

Sybase Admin

Entitlement Repository:

Sybase

User Admin Team:

Business users under Sam Jones

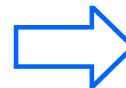
Step 3: Develop action plan to mitigate gaps

Start with the list of control objectives and documentation on associated practices.

- ⇒ **Identify any application that does not meet control objectives, that is, documentation on corresponding practice is missing or inadequate to cover control objective.**
- ⇒ **Notify CXOs of deficient applications that they must change current practice and update documentation.**
- ⇒ **Identify metrics that show progress in gap mitigation.**
- ⇒ **Review planned practices and implementation timeframe to ensure they are compliant.**

When this step was completed, we had:

actionable plans and visible metrics



Example: Develop action plan to mitigate gaps

Identify any application that does not meet control objectives, that is, practices are missing or inadequate.



Notify CXOs of deficient applications that they must change current practice.



Identify metrics that show progress in gap mitigation.



Review planned practices and implementation timeframe to ensure they are compliant.



Enough time to schedule communication with Senior Managers

Enough time for a development lifecycle

The day external audit needs to start testing to assess SOX Compliance

Example SOX IT Committee Lists

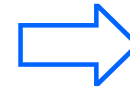
<i>Control Objective</i>	<i>General</i>	<i>Control Practice</i>
<i>Logical security tools and techniques are implemented, configured, and administered to enable restriction of access to data and programs.</i>	<i>Network</i>	<i>Firewalls restrict traffic into the Internal Network from all external sources to application that require strong authentication.</i>

<i>Control Objective</i>	<i>Application</i>	<i>Control Practice</i>
<i>Logical security tools and techniques are implemented, configured, and administered to enable restriction of access to data and programs.</i>	<i>Client/Server (CPSYS, CSAPP2, etc)</i>	<i>Strong authentication is provided via Single-Sign-On. OS and DBMS Security configured at group level. Entitlements configured via BU-administered screen that updates DB2 table.</i>

Step 4: Implement Required Controls, Update Documentation

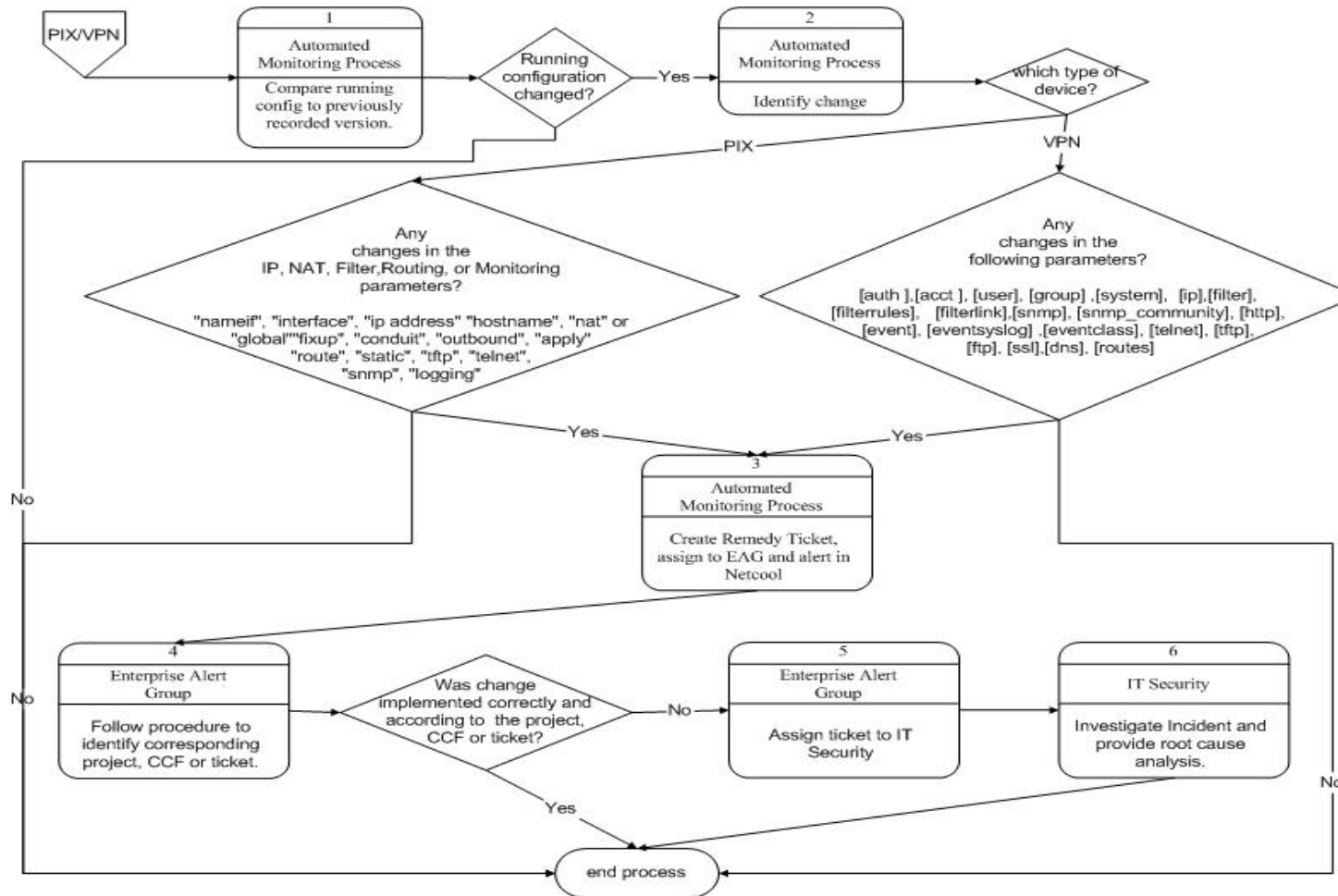
- ⇒ ***Start with the actionable plans for gap mitigation.***
- ⇒ ***Publish metrics.***
- ⇒ ***Identify Documentation.***

When this step is completed, we have:

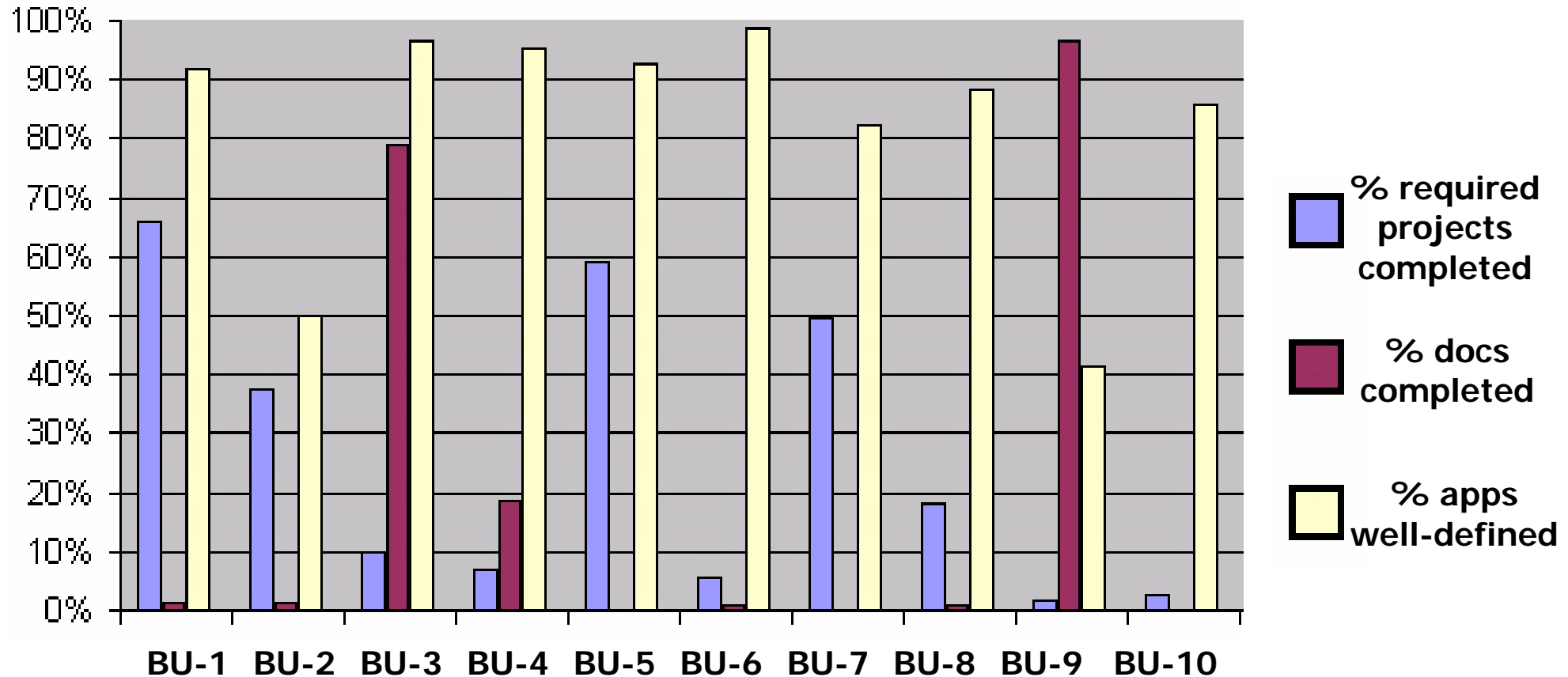


documentation and awareness

Example CXO Documentation – Control Practice Description



Example Compliance Metrics



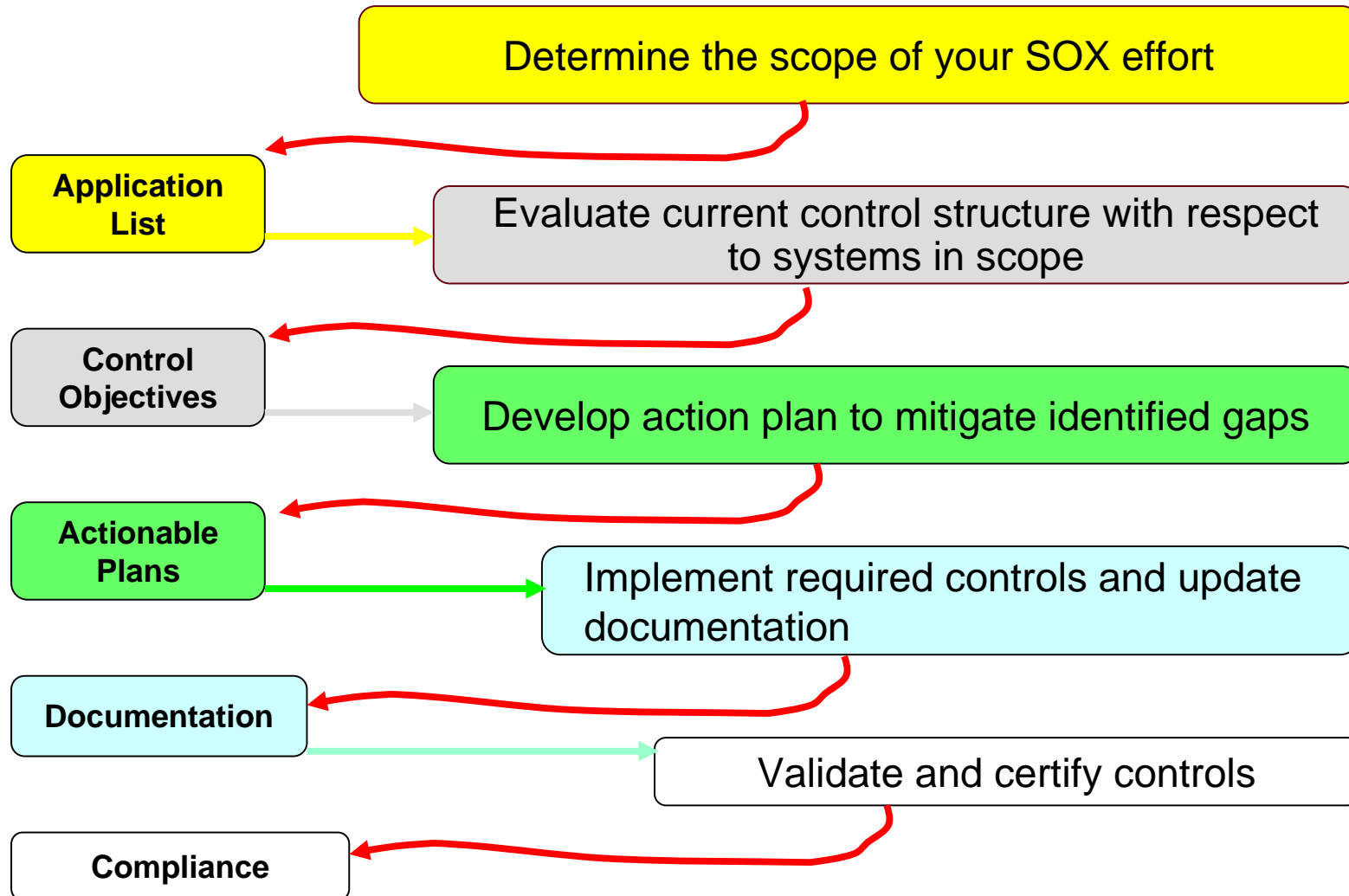
Step 5: Validate and certify controls

- ⇒ ***Start with the documentation on control objectives as well as the documentation on the servers and software that comprise the applications and all associated control practices.***
- ⇒ ***Test all general controls.***
- ⇒ ***Test all the control practices associated with each application infrastructure type to ensure that they exist and are consistently implemented.***
- ⇒ ***Do this periodically and document test results.***

When this step is completed, you have:

 ***compliance***

Putting it all together



For more information....

Useful sites:

www.pcaobus.org

www.sec.gov/spotlight/sarbanes-oxley.htm

www.coso.org

www.isaca.org

www.ffiec.gov