



# Sarbanes Oxley & CMMI



Mazars / Lamri



# Agenda

- What is Sarbanes Oxley?
- COSO Framework (1992 & 2004)
- What does SOX mean for IT?
- Control frameworks – what is available
- CMMI – how does it address the SOX agenda
- CMMI Based Appraisals – Giving Confidence
- Summary

# What is Sarbanes Oxley (SOX) ?

Single most important piece of legislation affecting  
**corporate governance, financial disclosure** and the  
practice of **public accounting** since the US securities  
laws of the early 1930s

# What is Sarbanes Oxley (SOX) ?

- US law passed in 2002
- **OBJECTIVE** - strengthen corporate governance and restore investor confidence.
- **WHY** - response to major corporate & accounting scandals in prominent companies in USA

# What Does SOX Address?

- New responsibilities for **boards of directors**
- New responsibilities for **management** of public companies,
- More powers for Security and Exchange Commission (**SEC**)
- Created the Public Company Accounting Oversight Board (**PCAOB**).
  - **Criminal Penalties for Corporate Management**

# What Does SOX Address?

## Section 302

## Section 404

Who	Management	<ul style="list-style-type: none"> <li>▪ Management</li> <li>▪ Independent auditors</li> </ul>
When	July 2002	Year-ends beginning 15 / 11 / 2004 * *
What	Management certification on company's internal control over financial reporting	<ul style="list-style-type: none"> <li>▪ Management Conclusion</li> <li>▪ Auditor Attestation</li> </ul>
Frequency	<ul style="list-style-type: none"> <li>▪ Quarterly</li> <li>▪ Annual</li> </ul>	Annual

# What Does SOX Mean for UK Companies?

## Public Companies

- US Listed or Listed Parent
- SEC Registrants

## Private Companies

- Entering a public market
- IPO
- Acquisition target
- Best in class - internal control framework
- Complex third parties/ relationship with US listed companies
- Dispersed shareholdings

- Voluntary Organisation
  - 1985 - Commission on Fraudulent Financial Reporting
  - SEC final rules refer to COSO
  - COSO framework – application of SOX
- 
- Original COSO framework      Internal Control
  - 2004 COSO framework      Integrated Enterprise

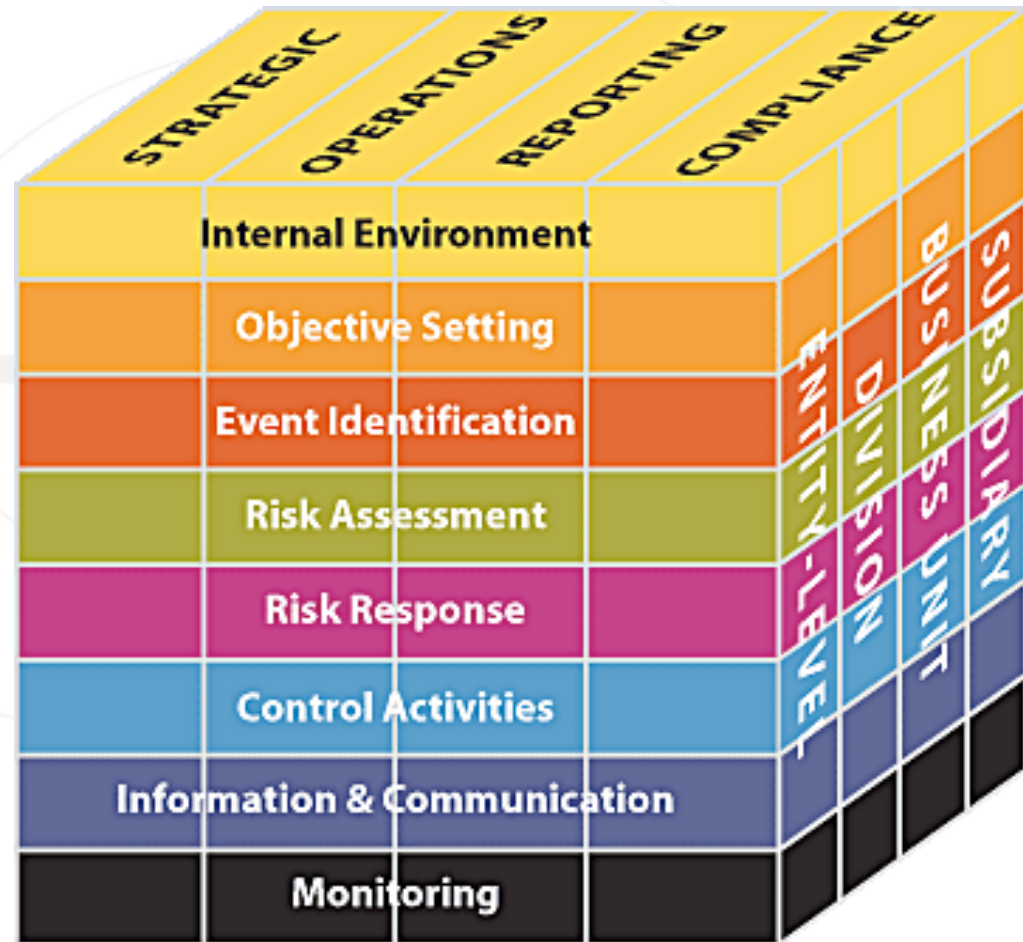
# COSO & Internal Control

1. The control environment
2. Risk assessment
3. Control activities.
4. Information and communication
5. Monitoring

1+2 +3 +4 +5 = integrated system of controls

# COSO & Integrated Framework

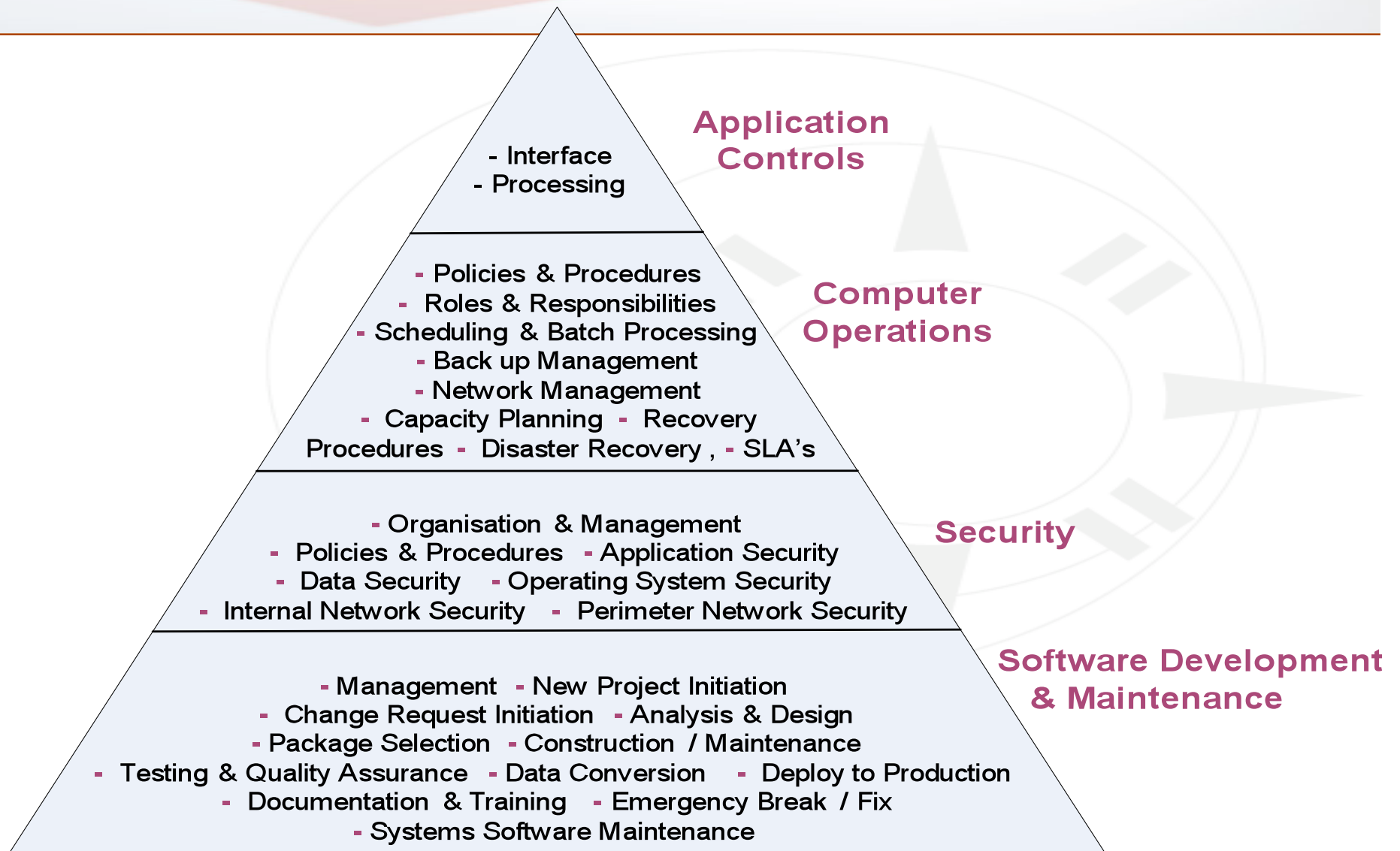
- 2004
  - Expands
  - Includes objective setting
- Entity objectives :
  - Strategic
  - Operations
  - Reporting
  - Compliance



# What Does it Mean for IT?

- IT is a key component of IT controls
- IT supports corporate reporting & compliance
- IT controls at
  - Company level
  - Business process level
  - IT function level
- 2004 PWC Survey – 46% increase in IT budget

# What Does it Mean for IT?



# What Does IT Mean for IT?

## Example – Application Interfaces

1. Interface can only be run once for each data set
2. Values are completely & accurately transferred from source to target
3. Only valid transactions are processed
4. Evidence of successful processing is recorded
5. In progress run errors are notified to the operator

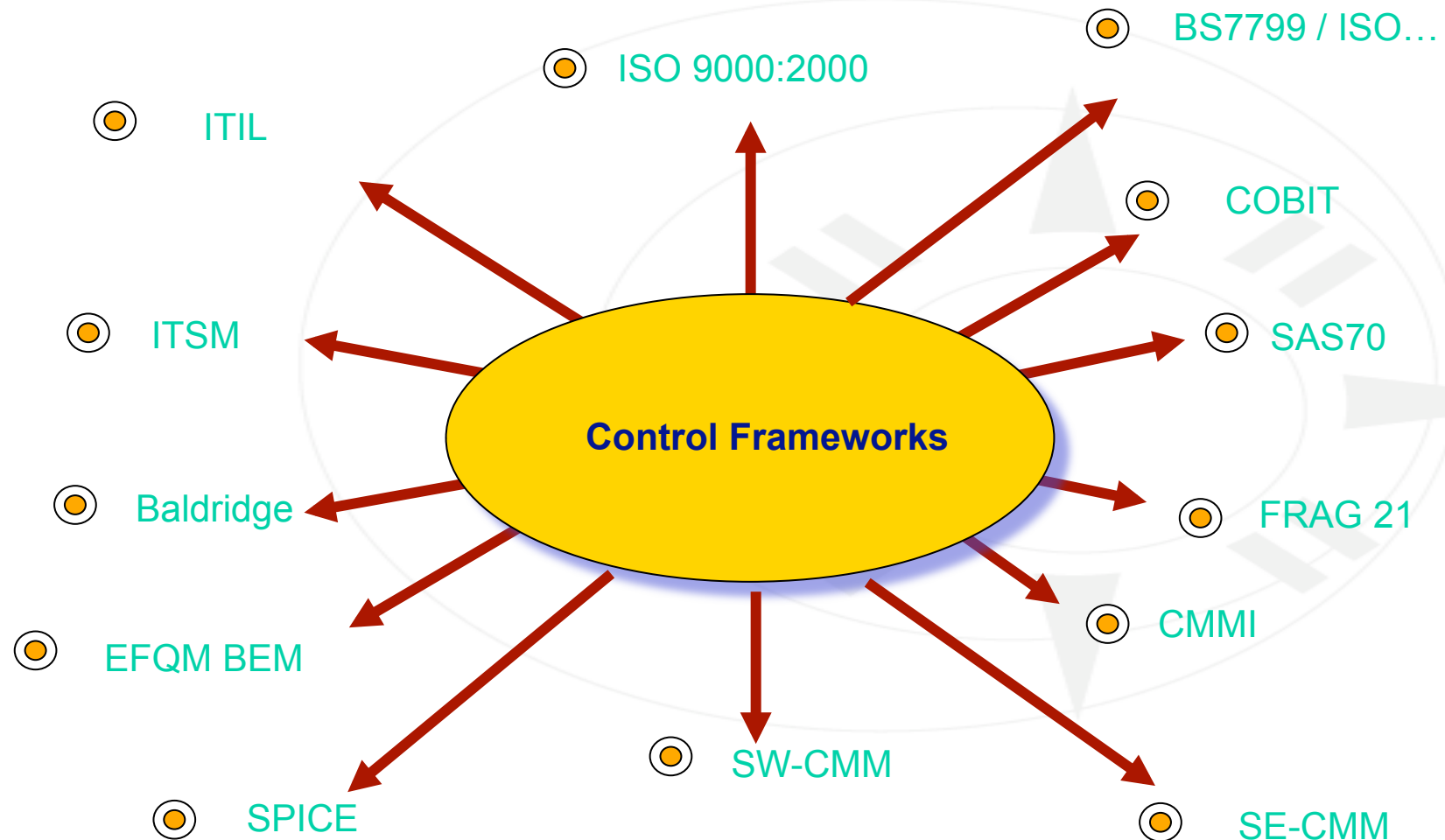
Difficult to evaluate – look to maturity models



# Addressing the Problem

How to demonstrate control?

# Control Frameworks – What is Available?





# Strengths of CMMI

- Integrated Model
- Directly involves Senior Management
- Improvement Model
- Customise Approach to fit Organisation Need
  - E.g. Staged or Continuous Representation
- Appraisal Methods

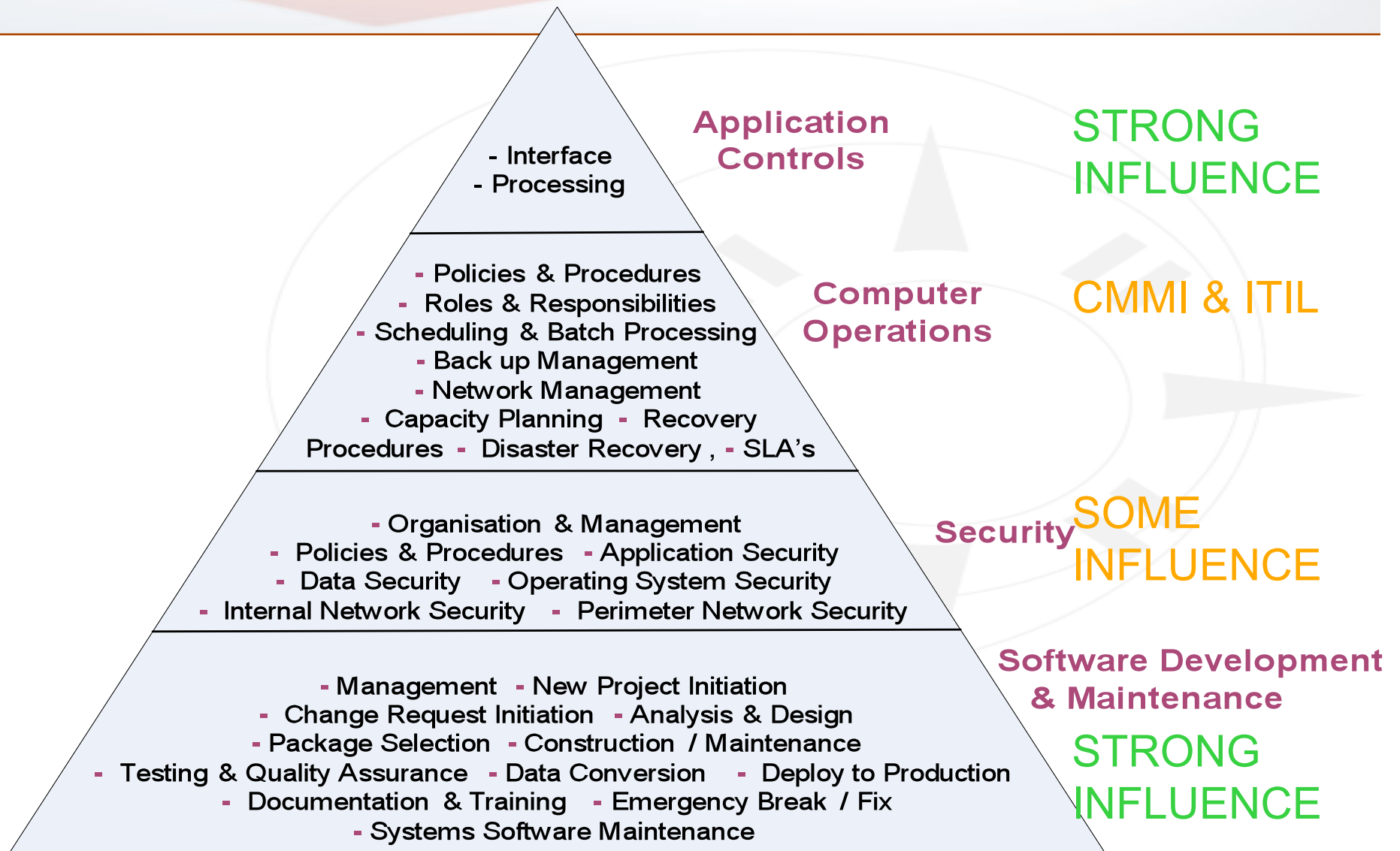


## Remember

A model is not a process.

The model shows what to do, NOT how to do it or who does it.

# How Can CMMI Help?



# Software Development & Maintenance

MATURITY LEVEL	PROCESS AREAS							
5- OPTIMISING	Organisational Innovation & Deployment	Causal Analysis & Resolution						
4- QUANTITATIVELY MANAGED	Organisational Process Performance	Quantitative Project Management						
3- DEFINED	Organisational Process Focus	Organisation Process Definition	Organisational Training	Organisational Environment For Integration	Integrated Teaming	Decision Analysis & Resolution	Integrated Supplier Management	
	Requirements Development	Technical Solution	Product Integration	Verification	Validation	Risk Management	Integrated Project Management	
2- MANAGED	Requirements Management	Project Planning	Project Monitoring & Control	Supplier Agreement Management	Measurement & Analysis	Process & Product Quality Assurance	Configuration Management	

# CMMI Continuous Representation

CATEGORY	PROCESS AREAS							
PROJECT MANAGEMENT	Project Planning	Project Monitoring & Control	Supplier Agreement Management	Risk Management	Integrated Teaming	Integrated Project Management	Quantitative Project Management	Integrated Supplier Management
ENGINEERING	Requirements Management	Requirements Development	Technical Solution	Validation	Verification	Product Integration		
SUPPORT	Configuration Management	Measurement & Analysis	Process & Product Quality Assurance	Decision Analysis & Resolution	Casual Analysis & Resolution	Organisational Environment for Integration		
PROCESS MANAGEMENT	Organisational Process Focus	Organisation Process Definition	Organisational Training	Organisational Innovation & Deployment	Organisational Process Performance			

**CAPABILITY LEVELS**

- 5- OPTIMISING
- 4- QUANTITATIVELY MANAGED
- 3- DEFINED
- 2- MANAGED
- 1- PERFORMED
- 0- INCOMPLETE

# Institutionalisation – The Generic Practices

**GP 2.1: Establish an Organisational Policy**

**GP 2.2: Plan the Process**

**GP 2.3: Provide Resources**

**GP 2.4: Assign Responsibility**

**GP 2.5: Train People**

**GP 2.6: Manage Configurations**

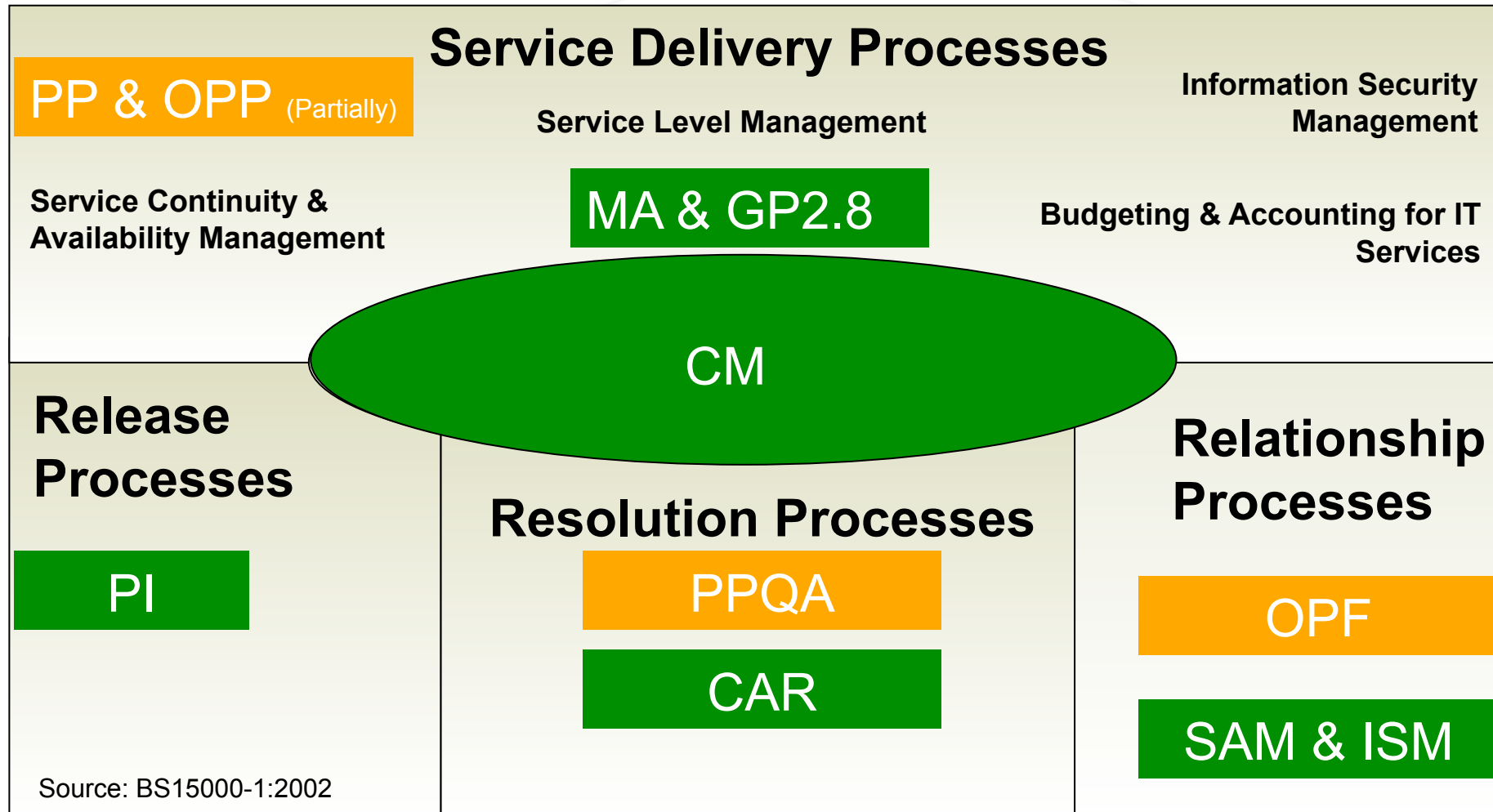
**GP 2.7: Identify and Involve Relevant Stakeholders**

**GP 2.8: Monitor and Control the Process**

**GP 2.9: Objectively Evaluate Adherence**

**GP 2.10: Review Status with Higher Level Management**

# SOX – CMMI & ITIL





# **CMMI Based Appraisals - Giving Confidence**



# CMMI Appraisal Method Classes

<b>Characteristics</b>	<b>Class A</b>	<b>Class B</b>	<b>Class C</b>
Amount of Objective Evidence Gathered (relative)	High	Medium	Low
Ratings Generated	Yes	No	No
Resource Needs (relative)	High	Medium	Low
Team Size (relative)	Large	Medium	Small
Appraisal Team Leader Requirements	Lead appraiser	Lead appraiser or person trained and experienced	Person trained and experienced

Extracted from Appraisal Requirements for CMMI, Version 1.1 (ARC) (CMU/SEI-2001-TR-034)

# Features of SCAMPI Appraisals

- Team approach
  - Internal & External Team Members
- Rigorous Method
  - Repeatable
  - Objective Evidence Based (PIIDs)  
Direct, Indirect & Affirmation
- Generates Specific Data for Process Improvement
- Rigor + Part of PI Effort = Organisation Establishing Control



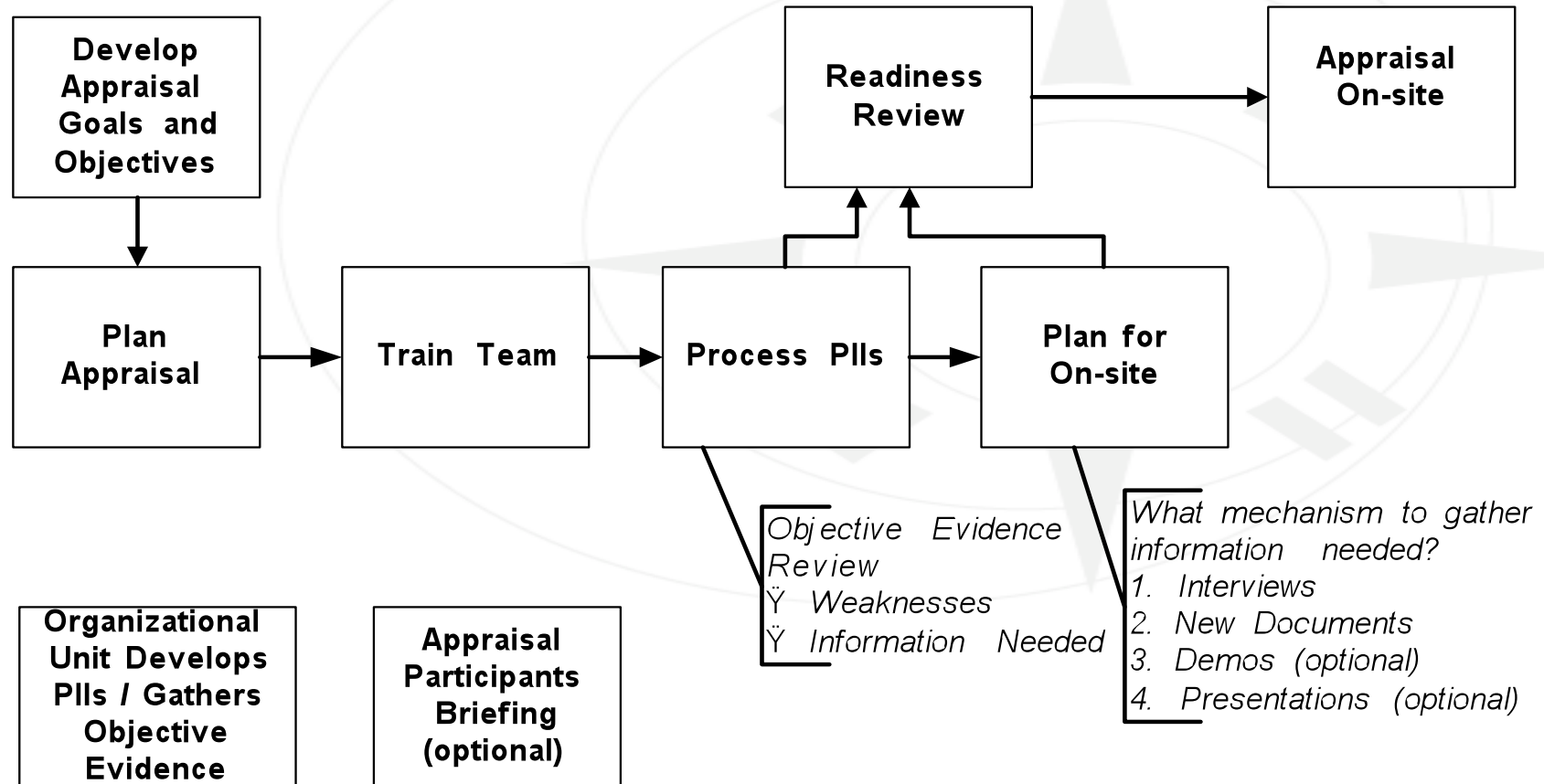
# Summary

- Sarbanes Oxley brings new Requirements for Organisations to demonstrate control of their processes
- CMMI is one vehicle that can be used to demonstrate this compliance
- CMMI's advantages:
  - Integrated Model
  - Process Areas & Practices provide tangible steps
  - Appraisal process – provides confidence and evidence of way forward

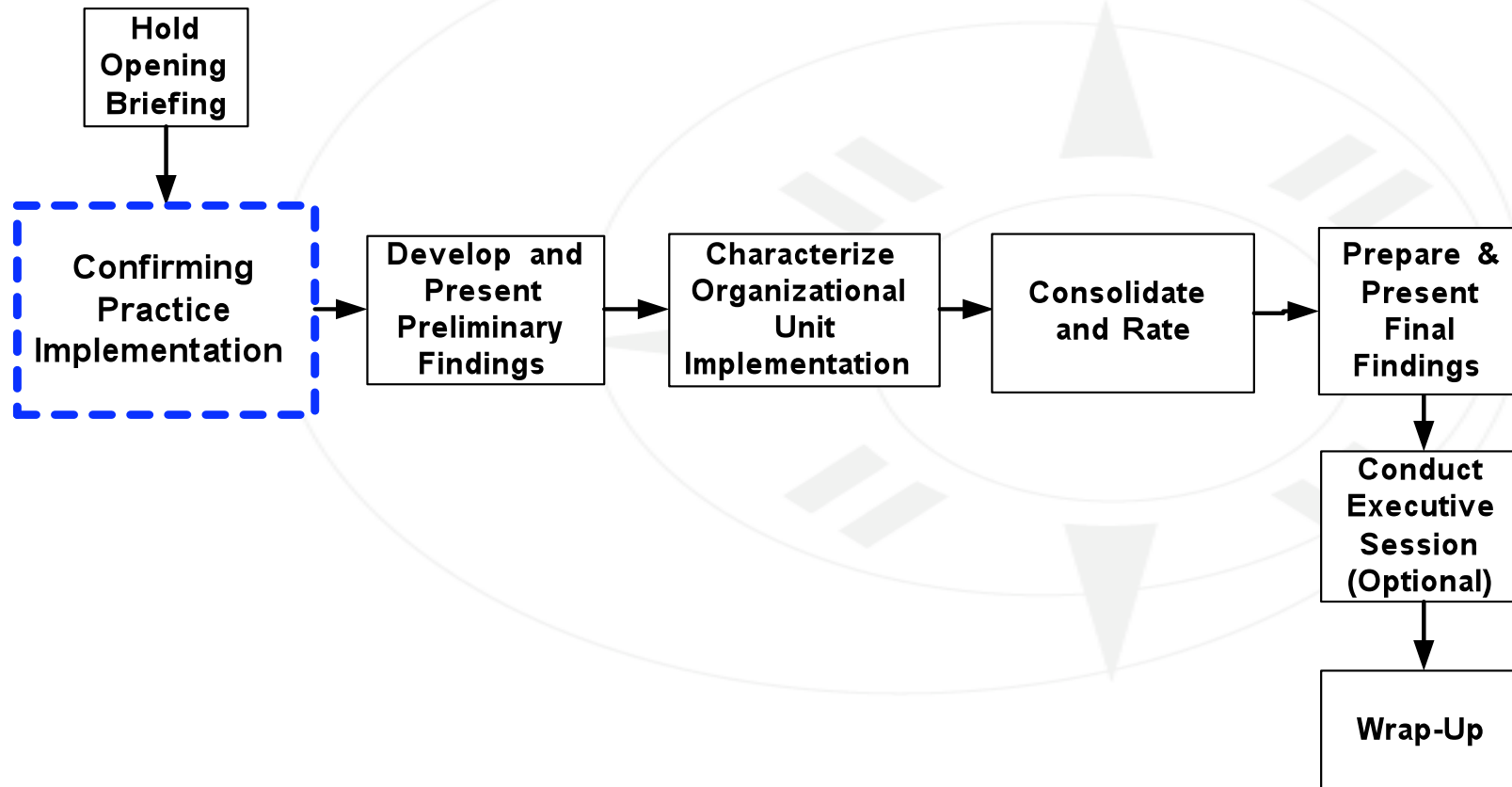


Questions ?

# SCAMPI Class A Pre On-site Activities



# SCAMPI Class A On-site Activities



*Note: The Report Results phase is included in this graphic*

# Characterizing Practice Implementation

<b>Fully Implemented (FI)</b>	<ul style="list-style-type: none"><li>• Direct artifacts present and appropriate</li><li>• Supported by indirect artifact and/or affirmation</li><li>• No substantial weaknesses noted</li></ul>
<b>Largely Implemented (LI)</b>	<ul style="list-style-type: none"><li>• Direct artifacts present and appropriate</li><li>• Supported by indirect artifact and/or affirmation</li><li>• One or more substantial weaknesses noted</li></ul>
<b>Partially Implemented (PI)</b>	<ul style="list-style-type: none"><li>• Direct artifacts absent or judged inadequate</li><li>• Artifacts or affirmations indicate some aspects of the practice are implemented</li><li>• One or more substantial weaknesses noted</li></ul>
<b>Not Implemented (NI)</b>	<ul style="list-style-type: none"><li>• Any situation not covered above</li></ul>