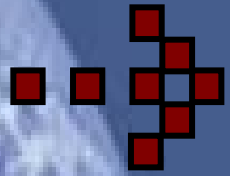


# International Institute of Management

**Executive Education Seminar**

Mr. Med Yones

**IIM Open Courseware Project**



Здравствуйते

こんにちは

سلام

*Howdy*

你好

नमस्ते

Ciao

*Hola*

您好



여보세요

*Hallo*

*Guten Tag*

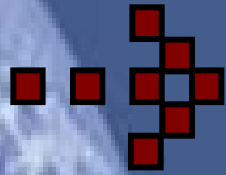
مرحباً

וּלְהָ!

*Salut*

Obrigado

Xin chào



# IIM Open Courseware (OCW)

Copyright International Institute of Management ([www.iim-edu.org](http://www.iim-edu.org))

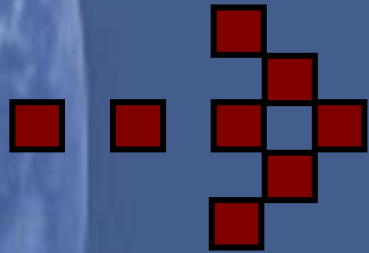
This work is the intellectual property of the authors. Permission is granted for this material to be shared for educational or commercial purposes. IIM also grants the rights to disseminate otherwise or to republish in full or in part, provided that this copyright statement appears on the reproduced materials.

As courtesy, please provide us with a notice of use.

## IIM Open Courseware

International Institute of Management  
10161 Park Run Dr. #100  
Las Vegas, NV 89145  
USA

Email: [contact\\_us\(at\)iim-edu.org](mailto:contact_us@iim-edu.org)



# *Governance*



*CIO,  
Corporate Governance  
& The Sarbanes Oxley Act*

*(SOA) . (SOX)*

Med Yones

# Sarbanes-Oxley (SOX) Compliance Project Discovery. Assessment. Remediation. Testing.

## Section 302:

Disclosure Certification by  
CEO & CFO

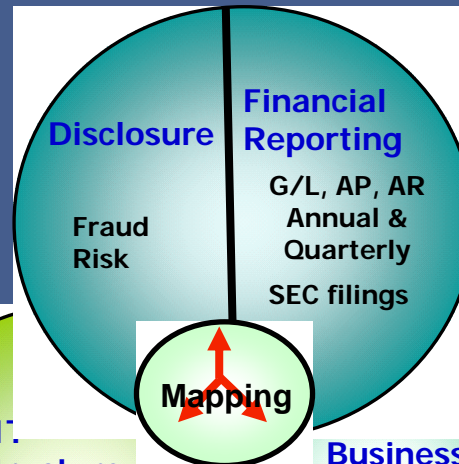
Accuracy and completeness  
of all statements in SEC 10K,  
and 10Q filings

Fair representation of financial  
position and result of  
operations

Evaluation of  
effectiveness of  
Disclosure Controls

Disclosure of  
significant events  
related to financial  
reporting and  
business  
operations

## Accounting & Auditing Team



IT Team

Biz Team

## Section 404:

Management Assessment of  
Internal Controls

Annual assertion by the CEO &  
CFO regarding internal controls  
in 10K

Responsibility for  
establishing and  
maintaining internal  
control structure and  
procedures  
Assessment of  
effectiveness of internal  
control structures and  
procedures  
Attestation/Test by the  
external auditor

Disclosure of  
deficiencies in internal  
control to Audit  
Committee and  
external stakeholders



# Best Practices: COSO, COBIT and GCC

- SOX recommends the use of COSO (The Committee of Sponsoring Organizations of the Treadway Commission) as the framework for auditing financial systems.
- The Information Systems Audit and Control Association (ISACA) has prepared an industry accepted “mapping” of CoBIT (Control Objectives of Information and Its related Technology) to the COSO internal control model and the SOX information system internal control requirements.
- The development of the support systems, processes, procedures, and controls identified under the GCC (General Computing Controls). GCC includes controls for:
  - Software (Systems) Development Lifecycle (SDLC)
  - Change Management
  - Production Operations
  - Operations Security (Access and Vulnerability Management)
  - Systems Backup and Recovery



# Typical Project Methodology & Timeline

## Phase 1 Discovery

- Business Scope Identification, Project Plan and Client Training 3-4 Weeks
- IT Scope Identification, Project Plan and Client Training 3-4 Weeks

## Phase 2 Assessment

- Enterprise Business Controls Gap Assessment 6-8 weeks
- Enterprise IT & Applications Controls Gap Assessment 6-8 Weeks
- Business Controls to IT Controls Mapping 4-6 Weeks

## Phase 3: Remediation

- Business Process Remediation 4-6 Weeks
- IT Process Remediation 4-6 Weeks

## Phase 4: Internal Testing

- Business Internal Testing 4-6 Weeks
- IT Internal Testing 4-6 Weeks

## Phase 5: Certification

- SAS 70 Compliance 4-6 Weeks
- External Auditor Testing 4-6 Weeks
- Signoff and Certification



# What are SOX Project Deliverables?

## Phase 1 Discovery

- Project Definition Document
- Project Plan With Resources, Dates and Milestone
- Executive and Managers Training Material
- Business Compliance and Reporting Templates
- IT Compliance Reporting Templates

## Phase 2 Assessment

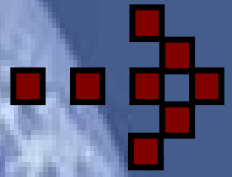
- Business Transactions Control Process Flow Diagrams
- List of Mapping of GL Accounts to Process Flows
- List of Business Controls & Risks for Each Business Cycle
- IT Transactions/Process Flow Diagram
- List of IT and Applications & Risks Controls
- Mapping Biz and IT Controls (in collaboration with business managers)

## Phase 3: Remediation

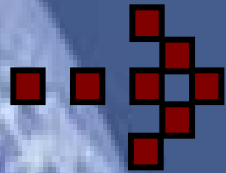
- Business Remediation Recommendation
- IT and Applications Remediation Recommendation

## Phase 3: Testing

- Internal Testing Biz Controls Results
- Internal Testing IT Controls Results



# Questions?



Спасибо

*Gracias*

Grazie

متشكراً

ありがとう  
ございます

धन्यवाद

*Merci*

**See You Next Time!**

*Danke*

谢谢

**For More Information  
You Can Visit**

너를 감사하십시오

*Howdy*

[www.iim-usa.org](http://www.iim-usa.org)

*Thank you*

謝謝  
شكراً

אנא בדוק האם המלה

Cảm ơn