

# Corporate Governance

(Sarbanes-Oxley, PIPEDA, GLBA, OSFI)

**SCIENTON™**

The Information Risk and Security Modeling Company

[www.scienton.com](http://www.scienton.com)

ISO17799 User Group

[www.scienton.com/7799ug/](http://www.scienton.com/7799ug/)

[info@scienton.com](mailto:info@scienton.com)



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

**SCIENTON™**

## Topics

- Corporate Governance
  - (Sarbanes-Oxley, PIPEDA, GLBA, OSFI)
- Governance, Management System, Audit Framework
- Mapping Exercise



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

**SCIENTON™**

# Drivers for Governance and Management Conundrum

COSO or COCO ?  
WHAT IS IT  
AGAIN?

ISOXXX or some other  
number, what is it that we  
can do...

Auditor external, internal first  
party or what kind of auditors?

Management System do we have it, we do have business  
process, but it is adhoc

Business  
process map for  
governance?  
Why?

CONTROLS,  
those just slow  
business  
process and  
prevent  
creativity!!!

We do all this and it costs  
arm and leg. Can we do  
something about it...

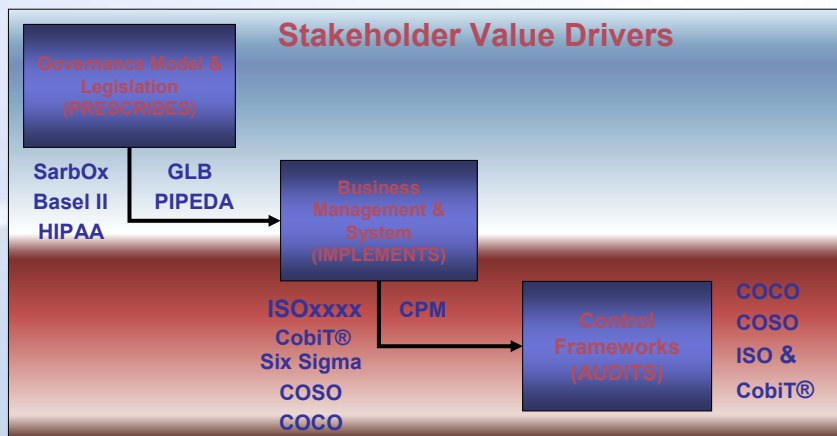
ES&S World Association of Consultants



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

# Organization Modelling Approach



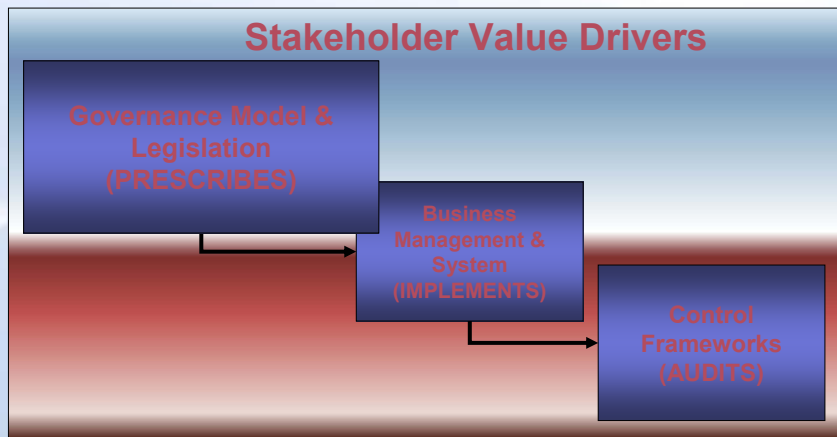
ES&S World Association of Consultants



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

# Corporate Governance



# Corporate Governance

## ■ Legislations

- Sarbanes-Oxley
- GLB, Basel Accord
- HIPAA, FIPPA, PIPEDA

## ■ Different guidelines

- Canada – Dey Report, CICA Guidelines, OSFI Guidelines
- USA – SEC Guidelines (Sarbanes-Oxley)
- UK – Turnbull Report (The Combined Code)

## ■ Prescribed Responsibilities

- Internal audits and controls
- Board and corporate management
- Risk management

# OSFI Guideline & Sarbanes-Oxley

## ■ OSFI

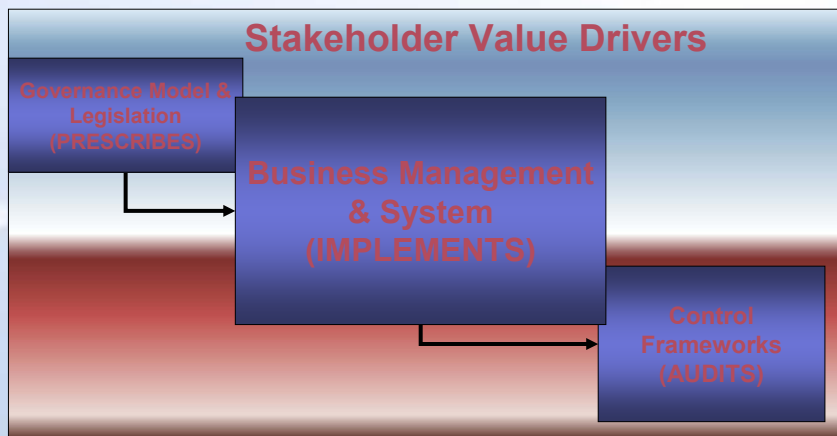
- Board independence & responsibility
- Internal controls
- Risk management – OSFI guidelines
- Board effectiveness
- Independent assessment
- OSFI assessment and recommendations

## ■ Sarbanes-Oxley

- Board independence & oversight responsibility (Title I)
- Independent external audit with registered audit firms (Title II)
- Independent internal audit (Title III)
- Quarterly reports – CEO, CFO responsibility (Title III)
- Governance dictates risk identification & business decision justification (Title IV, VII)
- Penalties & imprisonment

- Separation of management and management system implementation from audit and control framework measurement

# Management Systems



# Management System Definition

## What is a Management System?

- A management system is a system to establish policy and objectives and to achieve those objectives. Management systems are used by organizations to develop their policies and to put these into effect via objectives and targets using:
  - Organizational structure
  - Systematic processes and associated resources
  - Measurement and evaluation methodology
  - Review process to ensure problems are corrected and opportunities for improvement are recognized and implemented when justified

What gets monitored gets measured, what gets measured gets managed.



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

# Management System Implementation

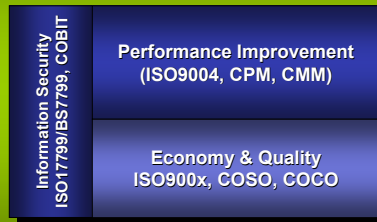


CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

# Complete Management System

## Business Management System Improvement



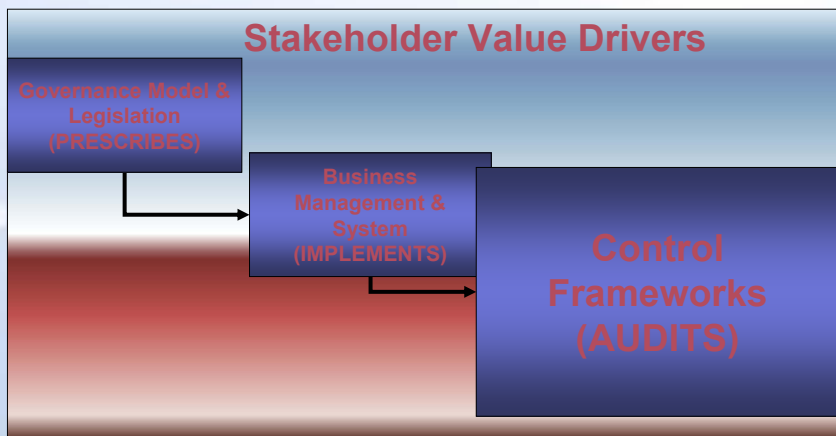
CONFIDENTIAL - Copyright

Technologies Inc. © 2003-2004

SCIENTON™

# Control Frameworks & Audit

## Stakeholder Value Drivers



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

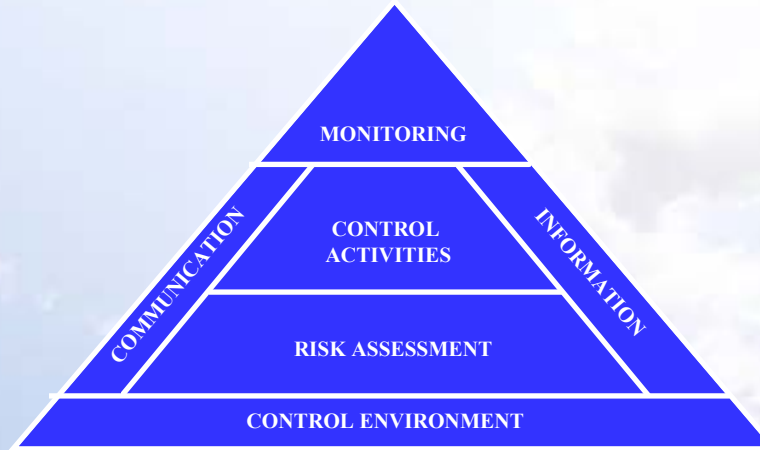
# Control Frameworks and Control

- **CONTROL** – Set of policies, procedures, practices and organization structures for the management system to provide the reasonable assurance that business process and objectives will be optimized and achieved, and that with reasonable assurance undesired events will be prevented, detected and corrected using defined management system.

# Governance Control Frameworks

- 1992 Committee of Sponsoring Organization of the Treadway Commission – Internal Control Integrated Framework
  - COSO – USA (AICPA, IIA)
  - COCO – Canada (Criteria of Control Principles)
- Other International quality management
  - ISOxxxxx, Six Sigma, ISO17799
- Information frameworks
  - CobiT®, ITIL
- **ALL FRAMEWORKS** – Strict separation of implementation and audit

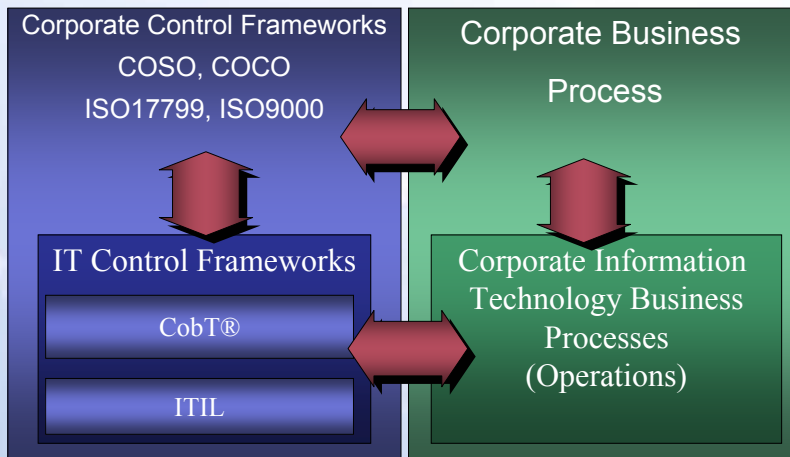
# CONTROL FRAMEWORKS - COSO



# CONTROL FRAMEWORKS - CoCo



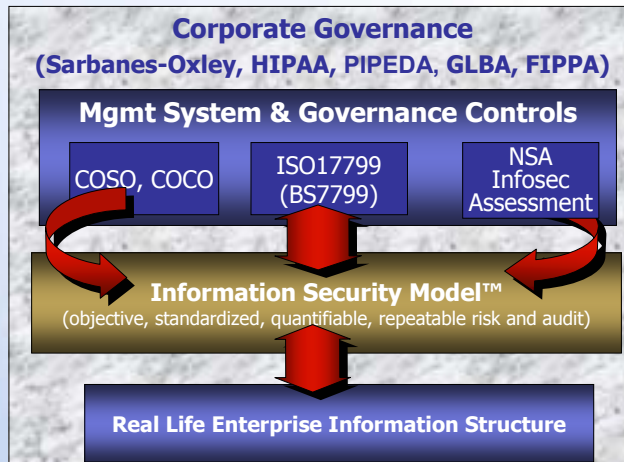
## Control Frameworks Position



## Organization Goals

- Should build the ability to implement governance top-down
- Understanding of corporate and information governance
  - Governance requirements should be used for management system implementations
  - Develop parallels between management systems (ISOxxxxx & COSO)
  - Ability to map business solutions across SarbOx, PIPEDA, GLBA, HIPAA
- Leverage Management Systems across departments within the organization

# Scienton Governance & Information Strategy Advantage



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™

## Questions?

- Basis for the new shareholders trust:
  - Corporate Governance
  - Management System
  - Control Framework
- A view on Sarbanes-Oxley - Alan W.

CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004



CONFIDENTIAL - Copyright Scienton Technologies Inc. © 2003-2004

SCIENTON™