

COSO Risk Assessment



Committee Of Sponsoring Organizations (COSO) was formed to develop **Risk Management and Mitigation Guidelines** throughout the industry.

Designed to **protect Stakeholders** from uncertainty and associated risk that could erode value.

A **Risk Assessment** in accordance with the COSO Enterprise Risk Management Framework, consists of (see www.erm.coso.org for details):

- **Internal Environment Review,**
- **Objective Setting,**
- **Event Identification,**
- **Risk Assessment,**
- **Risk Response,**
- **Control Activities,**
- **Information and Communication,**
- **Monitoring and Reporting.**

Creation of **Organizational Structure**, Personnel Job Descriptions and Functional Responsibilities, Workflows, Personnel Evaluation and Career Path Definition, Human Resource Management.

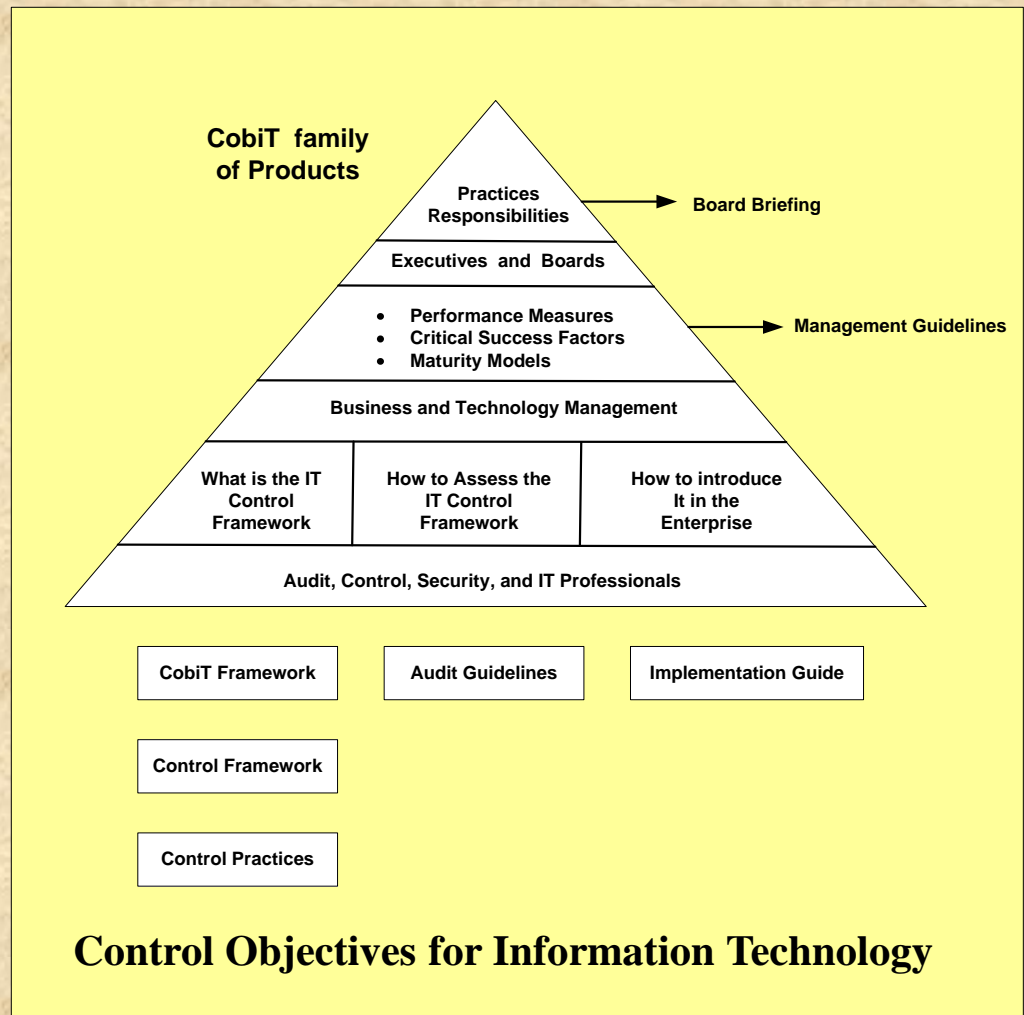
Implementation of **Standards and Procedures** guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.

CobiT Family of Products

Integrating CobiT

- The Board receives Briefings;
- Management receives Guidelines;
- The remaining staff receives:
 - CobiT Framework;
 - Control Framework;
 - Control Practices;
 - Audit Guidelines; and an
 - Implementation Guide.



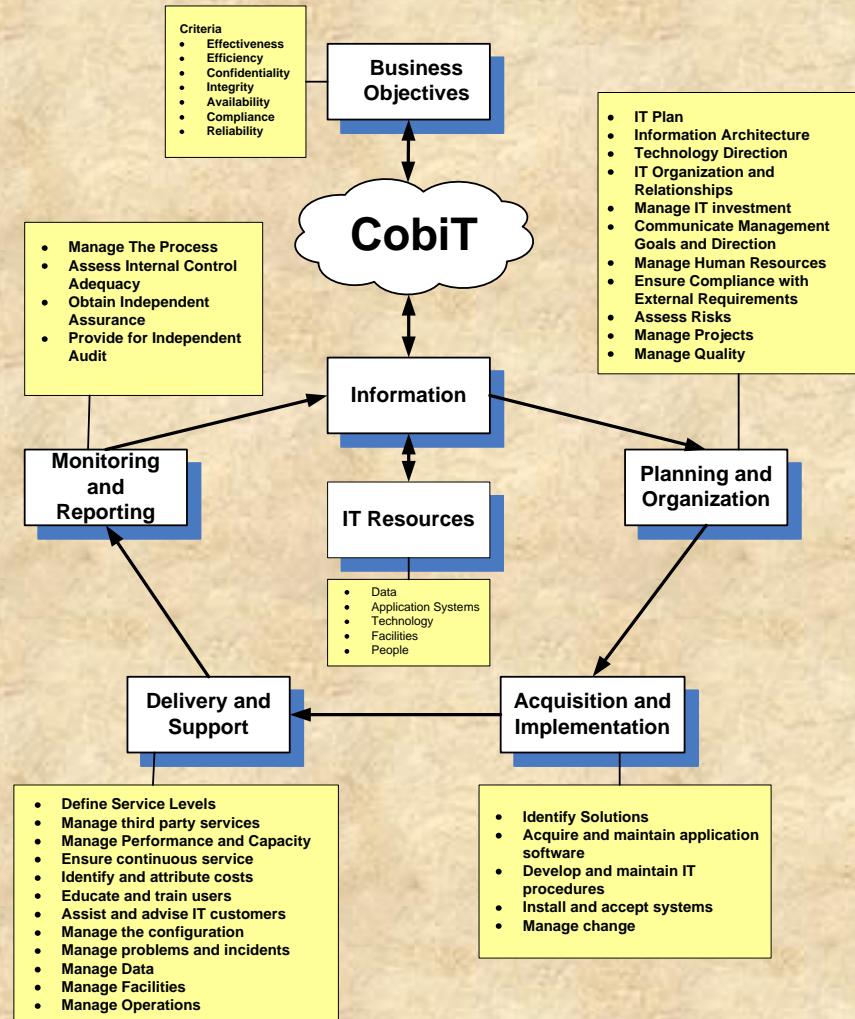
CobiT Framework

Control Objectives for Information Technology (CobiT)

Is designed to extend COSO controls over the IT environment by:

- Providing guidelines for Planning and integrating new products and services into the IT Organization
- Integrating new acquisitions;
- Delivering new acquisitions and supporting them going forward;
- Monitoring IT activity, capacity, and performance; so that
- Management can meet Business Objectives, while protecting Information and IT Resources.

CobiT Framework and Functionality



ITIL Framework

Information Technology Infrastructure Library (ITIL) Structure

