FOX | ITACS
Master of IT Auditing & Cyber-Security
Fox School of Business
TEMPLE UNIVERSITY

IT Audit Process

Prof. Liang Yao

Week Four – IT Controls

IT Controls

- Activities in place that can mitigate or reduce risks associated with technologies
- Two questions to ask:
  - For risk – So what?
  - For control – How do I know?
- IT Control description
- IT Control ownership

Type of IT Controls

- Preventive
  - Prevent “bad things” from happening
  - Automated in nature, manual possible
- Detective
  - Post modern
  - Confirm the occurrence of the adverse event
- Corrective
  - Take actions on top of ‘detection’
- Deterrent

Sample IT Controls

CISA Review Manual – pg. 43 Figure 1.5 Control Classifications

- IT Strategy and Governance
- Logical and Physical access
- SDLC and Change Management
- IT Operations
- Disaster Recovery and Business Continuity Plan
- Network and Communication
- Database Administration

Q: Do you think "Internal Audit" is a detective control?

Control Implementation

- Preventive or Detective or both
  - Already keep in mind of cost and benefit
  - Risk and exposure
  - Likelihood of happening
  - Impact
  - Layers of defense
- Q: discuss examples of different types of IT controls

Control Assessment

- Two step approach
  - Step 1: design adequacy
    - Is the control properly designed to mitigate the risk?
  - Step 2: operating effectiveness
    - Does the control work as expected?

Control Assessment

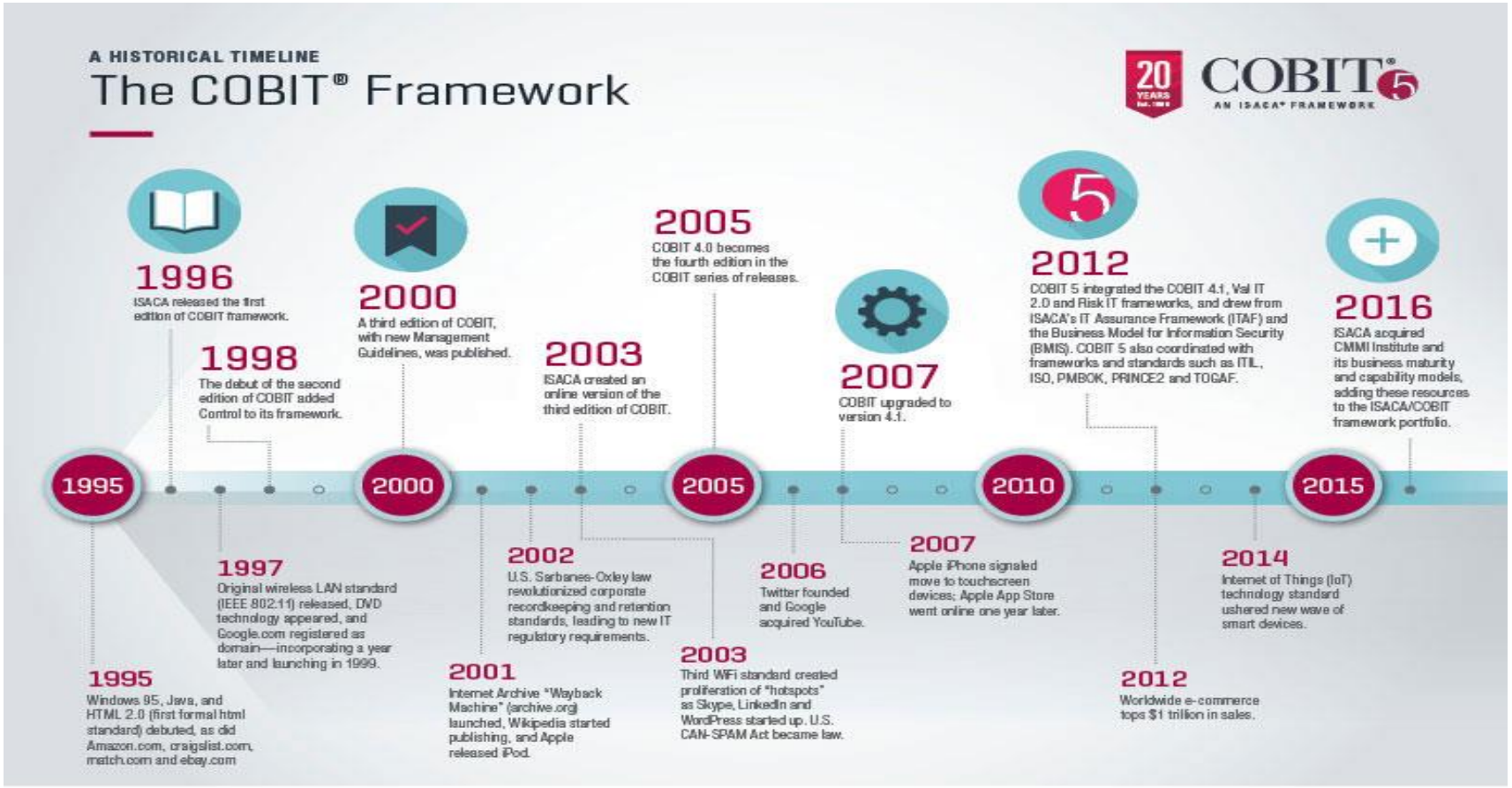
- Design adequacy assessment:
  - Starting with risk
  - Identifying controls: Does management have a control GAP?
  - Understanding the nature of control design (preventive/detective, etc.)
  - Understanding how controls can be evidenced

- Operating effectiveness assessment – only (a) no GAP (b) adequately designed (will cover in “Testing” section)

Control Assessment Practice

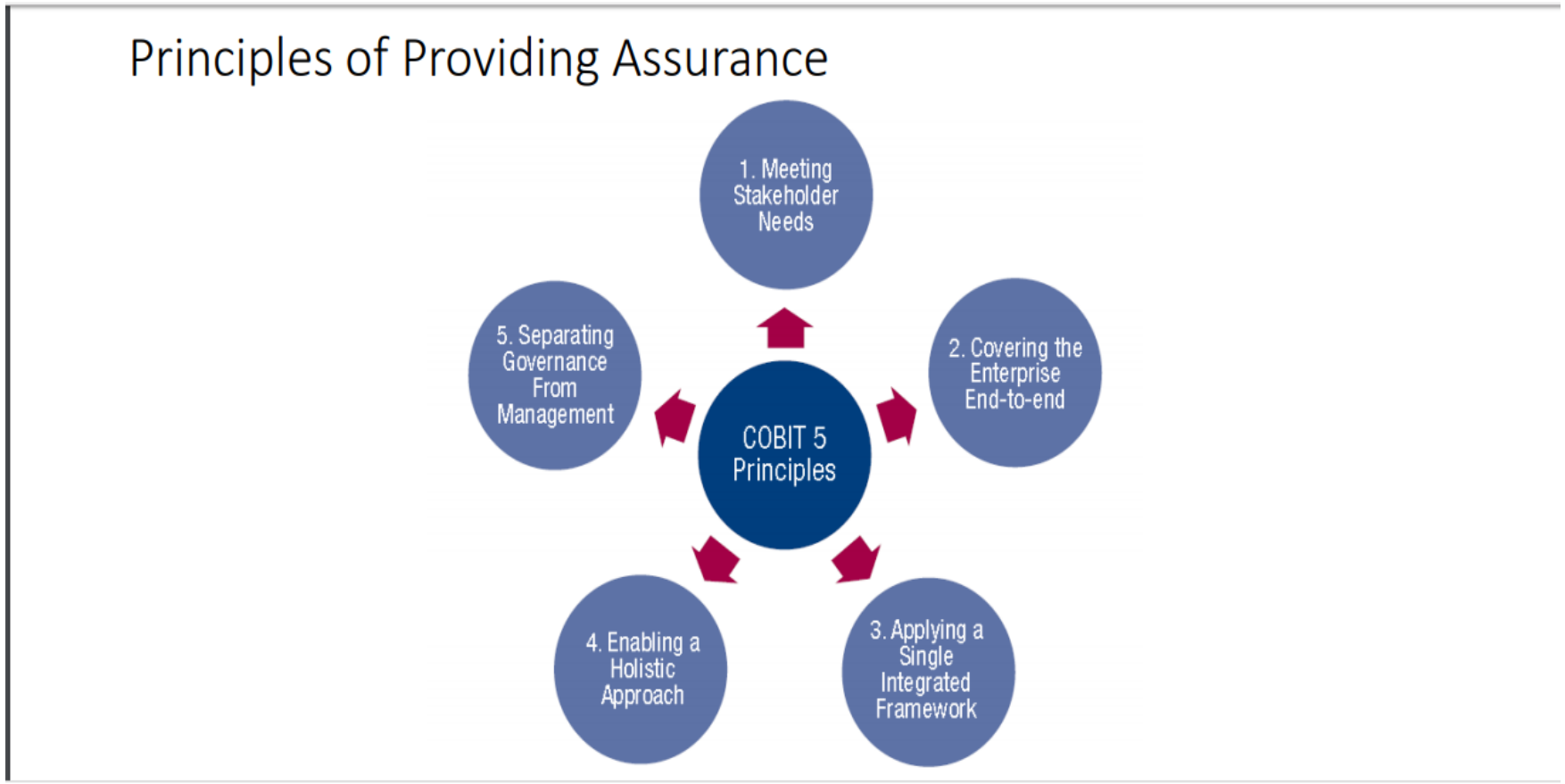
- Control Attributes
  - Nature of control
    - Automated vs. manual
    - Primary vs. secondly
  - Control frequency (daily, weekly, monthly, quarterly, annual, etc.)
  - Who performs the control?
  - How to evidence?
- Assessing control design adequacy
- Assessing control operating effectiveness

COBIT History



http://www.isaca.org/COBIT/PublishingImages/20th/COBIT-Timeline-lg.jpg

COBIT 5


Principles of Providing Assurance
1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

COBIT 5

- Principle One: Meeting Stake Holder Needs
- Principle Two: Covering the Enterprise End-to-End
- Principle Three: Applying a single, integrated framework
- Principle Four: Enabling a Holistic Approach
  - Principle, policies and framework
  - Processes
  - Organizational structure
  - Culture, Ethics, and Behavior
  - Information
  - Services, Infrastructure and Application
  - People, Skills and Competencies

COBIT 5

- Principle Five: Separating Governance from Management
  - Governance:
    - Steering the company's direction
    - Responsible party – The Board of Directors; committees and subcommittees; e.g. Cyber security
  - Management:
    - Execution
    - Responsible party - CEO