IT Service Delivery and Support - Week Two
Frameworks, Standards and Regulations

IT Auditing and Cyber Security

Fall 2016
Instructor: Liang Yao
Committee of Sponsoring Organization of the Treadway Commission (COSO)
Control Objectives for Information and Related Technology (COBIT)
IT Infrastructure Library (ITIL)
ISO 27001
National Security Agency INFOSEC Assessment Methodology
Frameworks and Standard Trends
Initiated in 1985
Internal control and framework formed in 1992
Key Categories:
- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
The only framework for Internal Controls used by SEC, PCAOB
Internal Control Key Concepts

- Internal control is a process
- Internal control is affected by people
- Internal control can only provide “reasonable assurance”
- Internal control is geared to the achievement of objectives in one or more separate by overlapping categories
COSO Cube

- Control Environment – Tone from the top
- Risk Assessment – Identification and Analysis Risks
- Control Activities – Policies and procedures
- Information and Communication – Enable managers and staff to carry out responsibilities
- Monitoring – Assess the quality of the performance
- Each components are NOT isolated
Enterprise Risk Management

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring
The COSO Enterprise Risk Management Framework
COSO’s Effect on IT Controls

- General Computer Controls
  - IT Governance and Management
  - IT Infrastructure
  - Security Management
  - HW and SW Acquisition and Development
  - Services Delivery and Support, etc.

- Application Controls
  - SDLC
  - SOD
  - Access Control, etc.
COBIT* Framework

- First published in April 1996
- Control Objective Domains
  - Plan and organize
  - Acquisition and implementation
  - Delivery and support
  - Monitor and evaluation

- Control Objectives for Information and Related Technology
COBIT Framework (continue)

- Seven Qualities of Information
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability
- Control Objectives and Control Activities
COBIT Framework (continue)

- Standards for good practice of IT controls
- Technology platform independent
- Management and process owner-oriented
- A de facto standard for IT governance
IT Governance

- Complexity of IT environment
- Fragmented or poorly performing IT infrastructure
- Enterprise vs. ad hoc solution
- IT cost
- Reactive vs. proactive IT management
- Communication gaps between IT and Business management
- IT’s role in business strategies
IT Governance (continue)

* Compliance with laws and regulations
* Scarcity of skilled staff
* Application ownership
* Competing IT resources/priorities among business units
* Flexibility and nimbleness
* Risk exposure
* External environment change
Developed by the U.K government in mid 80s
Provides best practices describing how to plan, design and implement effective service management capabilities

Information Technology Infrastructure Library
ISO 27001

- International Organization for Standards (ISO)
- ISO 27001, 17799, BS 7799 – Information Security Practice
- 1333 security controls in 11 areas
  - Security policy
  - Information security organization
  - Asset management
  - Human resource security
  - Physical and environment security
  - Communication and operations management
  - Access control
  - Information system acquisition, development and maintenance
  - Security incident management
  - BCP
  - Compliance
Regulations

* The Sarbanes-Oxley Act of 2002
* The Gramm-Leach-Bliley Act (GLBA)
* State level privacy regulations, e.g. California SB 1386
* The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
* EU Commission and Basel II
* Payment Card Industry Data Security Standard (PCI)
Regulations

- Regulatory Impact on IT Audit
- IIA and ISACA Guidelines for establishing IT control and audit processes
Response from the corporate scandals:
- Enron/Arthur Anderson
- Tyco, Aderphia, Worldcom, HealthSouth...

Focus on Internal Control Over Financial Reporting

Impact on Public Corporations
- Executives to attest to the adequacy and effectiveness of ICOFR
- Controls must be audited externally
- CEOs & CFOs are held accountable for (reports generated by systems and applications)
SOX (continue)

* **Section 101**
  * Establishing of PCAOB as the governance agency to regulate accounting firms such as Big 4

* **Section 302**
  * CEOs & CFOs are responsible for all internal controls

* **Section 404**
  * Attestation that IC are in place, documented and effective

* **Section 409**
  * Disclosure for significant changes
SOX (continue)

* IT specific controls required for SOX compliance
  * Access control
    * Authentication and authorization
    * Physical and Logical access
    * Re-certification, etc.
  * Change control
    * Request/review/approval
    * Back-out plan/schedule
  * Data management
    * Data transfer
    * Database structure
    * Data element consistency
    * Physical control of data
    * Data backup
  * IT operations
  * Network operations
  * Asset management
GLBA

- Financial Institutions
- How FIs’ customer information may be shared
- Customer privacy provisions
- Section 501B
  - Ensuring the confidentiality of customer information
  - Protecting against anticipate threats to customer records
  - Protecting against unauthorized access to customer information that could result in substantial impact to the customer
Interagency Guidance

- Office of Currency Comptroller (OCC)
- Federal Reserve (FRB)
- Federal Deposit Insurance Corporation (FDIC)

Control Requirements
GLBA (continue)

- Written Information Security Program
- Risk Assessment and Management
- Access Control for Customer Information Systems
- Physical Access Control for areas containing customer information
- Encryption (data at rest, data in transition, data in use)
- Change control
- Dual control/SOD/employee background check
- Security Monitoring
- Incident response and notification
- Disposal customer information
∗ Passed in 1996 by Congress
∗ Protect patient information
∗ IT relevant – prescribe a standard methodology for security; standardize the format for health-related information
∗ HIPAA Privacy and Security Rules
  ∗ HIPAA Privacy Rules
  ∗ HIPAA Security Rules
HIPAA (continue)

* HIPAA Privacy Rules
  * Administration controls designed to protect patient information
  * Effective April 2003

* HIPAA Security Rules
  * Technical controls: network perimeter protection, encryption, and workstation security
  * Ref. to page 432, Table 17-1 HIPAA Rule Requirements
PCI Data Security Standard

- Payment Card Industry Data Security Standard
- Not a law
- Mandatory compliance for participants in the card payment-processing industry
- Not only adopt, but also validate the compliance of the standard
- PCI compliance doesn’t mean your firm is secure – Target example
Level 1/High Risk Merchant
- Quarterly internal and external scan
- Independent validation of compliance by a QSA
- ROC

Others
- Self-evaluation (SAQ)

Common Adopted data security standards and practices

Not a panacea – Recent Target Data Breach
Other Privacy Regulations

* California SB 1386 – the most visible state laws dealing with breaches of security that cause private information to be breached: disclosure
* EU Directive on the Protection of Personal Data
* Canada PIPEDA