Trends in Information Technology (IT) Auditing

Padma Kumar
Audit Officer

May 21, 2015

Discussion Topics

- Common and Emerging IT Risks
- Trends in IT Auditing
- IT Audit Frameworks & Standards
- IT Audit Plan

Common and Emerging IT Risks

- Cyber Security
- Third Party Risks
- Insider Threat (malicious intent, errors, inappropriate use)
- IT Asset Management
- Business Continuity/IT Resiliency
- Information Security
- Data Management (Security, Availability, Quality, Compliance)
- Newer Technologies (Cloud, Internet of Things, Robotics, 3D-P)
- Mobile Computing
- Application Development
- Regulatory Compliance

Trends in IT Auditing

- Reviews of Key Risks
  - Cyber Security
  - Third Party Risks
  - Insider Threat
  - Business Continuity
  - Newer Technologies
  - Change Activities (project reviews)

- Talent Management
  - Ensuring appropriate skill sets
  - Talent retention, succession planning, cross-training (demand > supply worldwide)
  - Leveraging expertise from within the organization & outside

- Stakeholder Engagement
  - Co-ordination with other assurance providers
  - Increased interaction with business owners & non-IT stakeholders

- Enterprise Risk Management
  - Enterprise view versus siloed view of IT Risks
  - Linking IT Risks to organizational objectives
  - End to End Risk Assessment Approach
  - Increased engagement with the Board of Directors on IT Risks

- Audit Tools & Approaches
  - Ongoing Risk Assessments (dynamic vs static)
  - Continuous Auditing and Monitoring
  - Data Analytics

IT Audit Frameworks and Standards

Some of the frameworks and standards that auditors and risk management professionals use to guide their assessments;

- Control Objectives for Information & Related Technology (COBIT)
- Information Technology Infrastructure Library (ITIL)
- Committee of Sponsoring Organizations (COSO)
- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- Other National and Local Guidelines

These help with understanding the environment, identifying the key controls, evaluating design, testing effectiveness and reporting findings

IT Audit Frameworks & Standards - COBIT

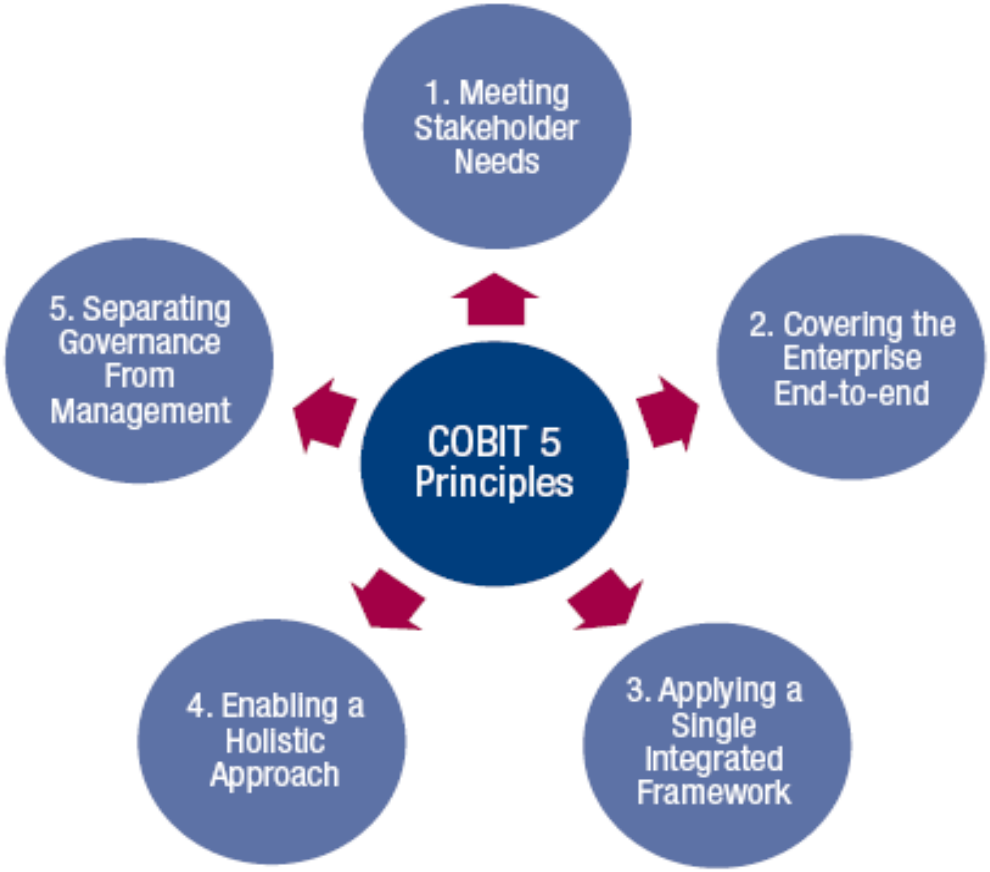
- Was developed by ISACA, which was previously known as Information Systems Audit & Control Association, but now only goes by the acronym ISACA to reflect the broad range of IT governance professionals it serves

- COBIT 5 was released in April 2012 and links together the prior version (4.0) with other ISACA standards such as Risk IT (IT risk management) and Val IT (IT value delivery), as well as other major standards and frameworks in the market place such as ITIL and ISO

- COBIT 5 provides a comprehensive framework, a set of generally accepted IT control objectives, that assists enterprises to achieve goals and deliver value through effective governance and risk management

- ISACA has created a Cyber Security Nexus (CSX) as a knowledge platform for cyber security related topics

COBIT 5 Principles At a Glance



Source: ISACA

Recent ISACA Publications - Sample Listing

- COBIT 5 for Information Security
- COBIT 5 for Risk
- Vendor Management using COBIT 5
- Transforming Cybersecurity (CSX publication)
- Implementing NIST Cybersecurity Framework (CXS Publication)
- Managing APTs (CXS Publication)

These publications are available for free download, or at a discounted price, for members on ISACA's website.

IT Audit Frameworks & Standards - ITIL

- Information Technology Infrastructure Library (ITIL) framework is a set of concepts and practices for managing IT services and provides best practices which organizations can adopt to improve overall IT service management and;
  - Help align IT services with current and future needs of the business
  - Improve the quality of IT services
  - Reduce the cost of providing the IT service
- The current version is ITIL 2011 edition and it comprises of the following processes; Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement
- The “library” is a series of documents, developed by the United Kingdom government’s Office of Government Commerce (OGC), that can be used to aid the implementation

IT Audit Frameworks & Standards – COSO

- COSO stands for the "Committee Of Sponsoring Organizations of the Treadway Commission," a nonprofit commission that in 1992 established a common definition of internal control and created a framework for evaluating the effectiveness of internal controls; COSO framework defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws and regulations
- COSO divides internal controls into five components; Control Environment, Risk Assessment, Control Activities, Information & Communication and Monitoring
- In 2004 COSO published the "Enterprise Risk Management – Integrated Framework" that expands on internal control and provides a broader enterprise wide focus
- COSO updated its 1992 framework and issued it in May 2013; the framework called "Internal Control – Integrated Framework:2013", includes seventeen (17) principles representing fundamental concepts associated with the five (5) components of internal control
- In January 2015 COSO published a document titled "COSO in the Cyber Age" to help explain how the 2013 framework can help organizations evaluate manage cyber risks

IT Audit Frameworks & Standards – COSO

The 17 principles are listed below and grouped according to the applicable COSO component

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: COSO

IT Audit Frameworks & Standards – ISO & NIST

- ISO publishes technical reports and specifications that can be used as a guide by organizations to implement control processes
    - ISO 27002 is a widely used framework for Information Security Management and an updated edition was published in 2013
    - ISO 27032 was published in July 2012 as a framework for cyber security

- NIST is a United States federal agency that develops and promotes measurement, standards, and technology
    - NIST 800-53 is a widely used framework for Information Security Management
    - In February 2014 NIST introduced a framework for improving cyber security and has since engaged with stakeholders in the public and private sectors to discuss and disseminate guidelines and practice advisories

IT Audit Frameworks & Standards – Other Guidelines

- In the United States, legislation relating to cyber security assessments and cyber threat sharing have either already been passed or are undergoing debate in the U.S Congress

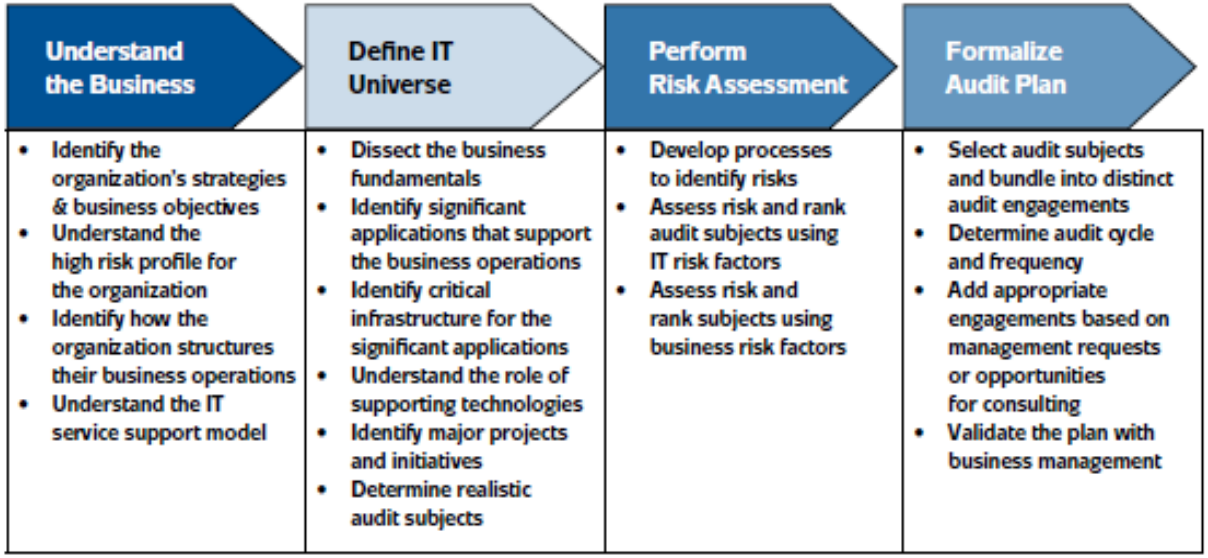
- In the United States, federal and state regulatory bodies have also released standards and guidelines relating to cyber security, third party risk management, data privacy, and business resiliency and more are expected

- European Parliament passed a Cyber Security Directive in 2014 with the aim to improve cyber security in the European Union by establishing security standards

- Several other nations have also either passed legislation/guidelines relating to cyber security and other emerging risks or are in the process of doing so

Developing an IT Audit Plan

Per the Institute of Internal Auditors (IIA), defining an IT Audit Plan involves knowledge of the business and supporting IT processes and developing an understanding of how business operations and IT services support the organizational objectives



Source: Institute of Internal Auditors

IT Audit Plan at FRB – New York

- Our IT Audit Plan is based on a combination of IT Processes, IT Infrastructure Services and Organizational Units

- It was developed by identifying and understanding:

    - Organization strategies and business objectives
    - Key business processes
    - IT service support model
    - Applications and technology infrastructure
    - Change activities

- Work executed by IT Audit includes:

    - Performing IT Process & Infrastructure Audits
    - Participation in Integrated Audits of Business Processes
    - Project Reviews
    - Consulting on new initiatives
    - Ongoing liaison activities

Conclusion – Key Reminders

- Changes in technology and processes introduce new risks – and major technology changes are expected by 2020!
- The importance of technology should be viewed within the context of business objectives (“business speak” vs “IT speak”)
- Increased co-ordination among assurance providers to leverage risk and control assessments and increased involvement from business owners and non-IT stakeholders, including the Board of Directors
- IT Audit Plan should be flexible and updated as needed to adopt to changes and ideally based on internationally accepted frameworks to increase credibility and acceptance with clients
- Talent management has become critical with demand exceeding supply with respect to skills in IT audit, IT risk, and IT security worldwide