ITG General Controls / IT Risk Assessment – Taking it to the Next Level

June 7, 2016

John A. Gatto, CISA, CRISC
President
JAG Associates
Port Charlotte, FL

Agenda

1. Audit Structure

2. IT General Overview

3. IT General Controls

4. IT Risk Assessment & Audit Planning
Core Principles of IA 2016

For an internal audit function to be effective, all Principles should be present and operating effectively. How IA activity demonstrates this may be quite different from organization to organization, but failure to achieve any of the Principles would imply that an internal audit activity was not as effective as it could be in achieving internal audit’s mission.

- Demonstrates integrity
- Demonstrates competence and due professional care
- Is objective and free from undue influence (independent)
- Aligns with the strategies, objectives, and risks of the organization
- Is appropriately positioned and adequately resourced
- Demonstrates quality and continuous improvement
- Communicates effectively
- Provides risk-based assurance
- Is insightful, proactive, and future-focused
- Promotes organizational improvement

Background

Audit departments are still structured into Finance and IT

- Teams rely on their counterparts without understanding their scope
- Automation of common activities / tests isn’t always leveraged
- Teams don’t know what their counterparts are doing
- Teams don’t communicate well
- Teams blindly trust in some “controls”
- Teams don’t know what IT General Controls are protecting
Current State

**Financial Audit**
- Focuses on end-user and manual processes

**IT Audit**
- Focuses on application controls and general IT controls

**What’s Needed**
- Directing non-IT Auditors to ask questions that will improve scope
- Increasing the knowledge of IT controls
- Bridging the knowledge gaps to cover more risk

Improvements

Financial and operational controls now supported by IT systems and system generated reports.

**We need to:**
- Recognize what our systems can and cannot do
- Realize that some system controls can be overridden or circumvented
- Understand the separation of business/operational activities and IT
Finance and IT rely on reports to validate the effectiveness of controls

- Reports are generated based on query criteria or SQL; inaccuracies in filter criteria may exist
- Reports are pulled from various databases; the incorrect source of record may be used:
  - Where is data being reported from?
  - Are the queries used appropriate?
  - At what intervals is data being propagated?
- Review reconciliations between front-end and back-end systems
- Review account reconciliations to identify discrepant processes

**Agenda**

1. Audit Structure
2. IT General Overview
3. IT General Controls
4. IT Risk Assessment & Audit Planning
Keeping up with the ever evolving legislative and regulatory requirements is time consuming and expensive as IT must design and maintain systems to comply with these legislative and regulatory requirements.
Considerations for security, shared services, IT resource maximization and governance concerns have contributed to a growing focus on enterprise-based IT management and IT governance.

After many spectacular data breaches and losses, and enormous spending in state-of-the-art security technologies, organizations are finally realizing that information security is all about being able to manage it adequately.
DR and BCP

Business continuity management (BCM) proactively improves the enterprise’s resilience against operational disruptions and provides the capability to adequately react to these.

Challenges of Managing IT Risks

IT’s pervasiveness and ubiquity also bring about (sometimes inconspicuously) significant risks that, if realized, might jeopardize the viability and success of the enterprise.
Vulnerability Management

The process of vulnerability management allows enterprises to enhance the security of their systems as well as meet their regulatory requirements by assessing and mitigating vulnerabilities in their IT systems.

Continuous Process Improvement

Modern enterprises now recognize that “business processes are the business” and that enterprise success is dependent on establishing the capabilities and infrastructures to continually improve business processes and rapidly implement change.
**Advanced Persistent Threats (APTs)**

Increasingly sophisticated APTs target specific vulnerabilities in organizational networks (using techniques such as spear phishing) to install malware and exfiltrate organizational data.

Seventy percent of CISOs believe it is likely their organizations will be hit by an advanced attack in the near future.

Shortfalls in information security talent and inadequate detection and response processes exacerbate vulnerability to APTs.

---

**Insecure Employee Behaviors**

With information security breaches rising at an exponential rate, employee error and misconduct have been identified as the biggest root cause of control failures.

Last year, 48% of data breaches were caused by human error.

The increased “datafication” of the work environment, plus ineffective training and awareness programs, undermine the value of the employee security perimeter.

---

**Business-Led IT**

Businesses are reliant on increasingly powerful and often niche technology to increase productivity.

Business leaders are increasingly procuring their own IT solutions, but do not always follow central security standards.

Risk is heightened by IT’s limited visibility to these technologies and the 3rd party relationships often have little regard for the appropriate controls.
Businesses’ reliance on technology requires continuous innovation and up-to-date, increasingly advanced systems. However, 93% of organizations use older legacy systems, which are not designed to cope with today’s complex digital environment. These systems are often incompatible with up-to-date security programs and can be costly to maintain while hampering productivity.

Major IT Challenges
Control Frameworks
IT Auditor Competencies
Control Frameworks

COSO
Sarbanes-Oxley
NAIC / MAR
CobiT

COSO

Committee of Sponsoring Organizations of the Treadway Commission

- “Business Control Model”
- Originally formed to study causal factors of fraudulent financial reporting
Sarbanes-Oxley (SOX)

Protect investors from executive fraud

- Public Company Accounting Oversight Board (PCAOB)
- External Auditor independence rules
- Audit Committee independence requirements and oversight

NAIC MAR

- Similar to Sox but less stringent than Sox
- Issued by the National Association of Insurance Commissioners (NAIC)
- For non-publicly traded insurance companies
- Requires controls to be in place and tested ensuring financial reporting accuracy and integrity
- Requires assertion by Management

COSO Sarbanes-Oxley NAIC / MAR CobiT
COBIT 5 Principles

1. Meeting Stakeholder needs
2. Covering the Enterprise end to end
3. Applying a Single Integrated Framework
4. Establishing a Holistic Approach
5. Separating Governance from Management

Control Objectives for Information and Related Technologies

COBIT 5 Domains

Align, Plan and Organize
Build, Acquire and Implement
Deliver, Service and Support
Monitor, Evaluate and Assess
**Control Activities**

Ensure enterprise management and key stakeholders:
- Are informed by IT on the current technology environment, possible future trends and value opportunities for the business
- Discuss future business directions and enterprise goal

Ensure IT management contributes to:
- Business strategy planning and
- Identifies capabilities available to support enterprise goals

Align business imperatives and priorities with IT capabilities:
- To establish enterprise priorities
- Include them in the IT strategic plan

**IT General Overview**

- Major IT Challenges
- Control Frameworks
- IT Auditor Competencies
Competencies

- Common sense
- Knowledge of area to be audited
- Knowledge of Policies & Procedures
- Flowcharting techniques
- Core Audit Skills
- Project Management

Competencies

- Management concepts
- Auditing concepts
- Negotiating skills
- Communication skills
- Audit tools (CAATs)
- Sense of humor
**IT Competencies**

- Understanding of IT risks
- Corporate strategic / operational plan
- Information Technology operational plan
- IT Organizational charts
- Corporate Policies and Procedures
- IT Infrastructure
  - Hardware
  - Applications
  - Networks

**IT Risks**

- Information Security Breaches
- Data Leakage and Privacy Violations
- Outsourcing Exposures
- Human Resource Shortcomings
- Business Enablement Challenges
- Funding and IT Governance Deficiencies
- Regulatory Concerns
- Cybersecurity
- Lost productivity from IT downtime
- Inability to defend lawsuits due to poor record keeping
Agenda

1. Audit Structure
2. IT General Overview
3. IT General Controls
4. IT Risk Assessment & Audit Planning

IT Controls

- Definition of Internal Control
- Fundamental Concepts
- Components of Internal Control
- Control Classifications
Definition of Internal Control

According to COSO

A process affected by an organization’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievements of objectives in these categories:

- **Operations**: Efficiency and Effectiveness of Operations
- **Reporting**: Reliability of Financial Reporting
- **Compliance**: Compliance with Applicable Laws and Regulations

Safeguarding of assets

Understanding IT Controls

IT control is a process that provides assurance for information and information services, and helps to mitigate risks associated with use of technology.

- **Two components**
  - Automation of business controls
  - Control of IT
Importance of IT Controls

**IT controls are needed to:**
- monitor and control cost
- remain competitive
- protect information assets
- comply with laws and regulation

**Implementing effective IT controls will:**
- improve efficiency
- increase reliability
- provide flexibility
- increase availability of assurance evidence

Fundamental Concepts

A means to an end
Dynamic not static
Affected by people - not just policies and procedures
Impacts all levels of the Company

Internal Controls is a PROCESS
**IT General Controls**

**Fundamental Concepts**

Internal control provides *reasonable* assurance, not *absolute* assurance

- Achieving absolute assurance is not possible and costly
- Attempting to achieve absolute assurance is cost-prohibitive for most entities

**Components of Internal Control**

- **Control Environment**
- **Risk Assessment**
- **Control Activities**
- **Information and Communication**
- **Monitoring**
Employees at all levels use risk management. It applies to all departments and environments across the entire organization.

**Defined**

- Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with benefits.
- The total process of identifying, controlling, and minimizing information system related risks to a level commensurate with the value of the assets protected.

**Principles**

- Integrating risk management into planning, preparation, and execution.
- Making risk decisions at the appropriate level in the organization.
- Accepting no unnecessary risk.

---

**Risk Management**

---

**Risk Appetite**

In our dynamic world, risks are constantly changing...

- The existing level and distribution of risks across risk categories (e.g. financial, market, operational, reputation, etc.).
- The maximum risk an organization may bear and remain solvent.
- Acceptable levels of variation an organization is willing to accept around specific objectives.
- What is the desired risk/return level.

**Determination of Risk Appetite**

- Existing Risk Profile
- Risk Tolerance
- Desired Level of Risk
- Risk Capacity
Components of Internal Controls

Control Environment
- Tone of the organization
- Foundation of all other components of internal control
- Includes: integrity, ethics, role and involvement of Board of Directors

Risk Assessment
- Identify and analyze relevant risks to achieve objectives
- Basis for how the risks are managed
- Includes: Annual risk assessment, mid-year updates, ongoing risk monitoring

Information and Communication
- Systems supporting the exchange of information
- Form and timeframe enabling people to carry out their responsibilities
- Includes regular reporting, Policies & Procedures, Intranet sites

Control Activities
- Ensure management directives are carried out
- Approvals, Authorizations, Reconciliation, Security, Segregation of Duties

Monitoring
- Feedback on strengths and weaknesses in system of internal control
- Includes: Performance measured to detect problems early
- Management ensures that internal controls are effective and efficient

Controls Life Cycle
- Design
- Implementation
- Operational Effectiveness
- Monitoring
Agenda

1. Audit Structure
2. IT General Overview
3. IT General Controls
4. IT Risk Assessment & Audit Planning

IT General Controls

IT General Controls
Policy Management

- Define elements of an IT control environment aligned with the enterprise’s management philosophy and operating style
- Develop and maintain a set of policies to support IT strategy - relevance confirmed and approved regularly
- Deploy and enforce IT policies to all staff so they become an integral part of enterprise operations
- Disseminate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise

Policy Life Cycle

- Plan
- Design
- Implement
- Operate
- Monitor
- Update
Establishes the foundation for a policy framework by covering the stakeholders and goals dimensions defined previously

Identifying gaps between the governance principles and current, valid policies helps to redesign and improve the policy framework in use

Define a logical structure of documentation that will support and clarify policy principles

The goal is to improve clarity of policy principles and support their implementation

Policy Life Cycle - Plan

Setup
- Identification of policies needed
- Risk-based approach is used that addresses policy principles
- Set deadlines and priorities for their creation
- Set deadlines for review and approval

Policy Structure Definition
- Draft: Identify individuals responsible for researching and writing policies
- Review: Identify individuals responsible for providing independent review of policies
- Procedures to obtain final policy approval from authorized individuals; determine policy communication and training strategy
- Define writing quality standards, including document format, font, language style, glossary and document structure

Policy Life Cycle - Design
IT General Controls

Policy Life Cycle – Implement / Operate

Implement

• Getting the policies active
• Enforcing them
• Defining the activities to assist the organization in transitioning from a noncompliant to a compliant state

Operate

• An effective policy should be part of the organization’s DNA
• Building an accountable culture and using policies in daily operations ensures that the organization’s goals are met
• Organizations should “walk the talk” of policy principles

Policy Life Cycle – Evaluate / Update

Evaluate / monitor

• Confirms that policy requirements are properly implemented
• The organization is operating effectively

Update / dispose

• Reviewed for updating or removal
• Adjusts the phases defined previously to maintain or improve the maturity of the policy framework
• Policies to be reviewed on a regular basis, typically every 12 months
Defining the role of IT

IT management (including goals and objectives)

Adequacy of policies and procedures

Compliance with policies and procedures

Policies defining levels of security and privacy required:
  - Rights of access to specific types of information (HIPAA regulations)
  - Ownership of information
  - Processes and procedures for employment in sensitive areas

Policy Management

Evergreen Process – timing and approvals

Cross referencing

Standards and procedures aligned with policy

Policy Review Board
A review of all Standards occurs at least once every 2 years or as needed by the Standards Owner (Director or above). Evidence of the review is documented and retained. A process exists to manage policies and standards. The Policy Management organization facilitates the review of all policies on a rotating, at least once every 2 years or as needed with the applicable process owners to ensure the policy's appropriateness. The Policy Owner (VP or above) approves the framework as changes occur.

1. Obtain the current policy manual and TOC
2. Obtain the exception process log and select 25 exceptions and:
   a. Ensure the submission was timely
   b. Ensure the justification was reasonable
   c. Validate that approvals were appropriate and timely

A review of all Standards occurs at least once every 2 years or as needed by the Standards Owner (Director or above). Evidence of the review is documented and retained.

1. Obtain the evergreen procedures and perform the following:
   a. Select 25 policies and determine when they were issued and last revised
   b. Ensure the Policy Manual contains the latest version of the policy
   c. Ensure appropriate signatures were obtained and maintained
**IT Organization & Management**

**Why is the organization of the IT group so important?**

- Ensures alignment with the business
- Defines lines of reporting and responsibility
- Allows the implementation of control systems

---

**Business Alignment - WHY**

- A winning business strategy requires the assessment of market forces, competitive challenges, organizational strengths and weaknesses, and customer needs.
- IT capabilities are an important component of an organization's capabilities and business expectations for IT are rising.
- Business processes are enabled by computer systems, and there are no fall back paper processes.
- Process changes are virtually impossible without the corresponding technology changes.
- High levels of availability, reliability and security are needed for key business systems.