Agenda

- Introductions
- What are “General Computer Controls”? 
- Auditing IT processes controls
- Understanding and evaluating application controls
- Addressing IT Governance and Entity Level concerns
- IT Process and Control Frameworks
- When to involve an IT Specialist in your audits
“Auditing IT processes and activities within the organization is among the highest priorities for today’s Internal Audit Departments, particularly given IT’s purpose as a critical enabler of virtually all business functions.”

- Protiviti's 2010 IA Capabilities & Needs Survey
What are “General Computer Controls”?
What are General Computer Controls?

By definition, **General Computer Controls** are control activities performed within the IT Organization or the technology that they support that can be applied to every system that the organization relies upon;
Why are IT General Controls Important?

Systems support many of a company’s business processes, such as those below…

- Accounts Receivable
- Accounts Payable
- Inventory
- Treasury (ex. Integra-T)
- Payroll (ex. ADP)

General Ledger

Financial Consolidation

Ex. SAP, PeopleSoft, JDEdwards, Oracle, Peachtree, Quickbooks, AccPac, Baan, Macola, Lawson, ManMan

Hyperion, TM1
Why are IT General Controls Important?

• Systems hardware and software applications support the critical business processes of almost every company;

• General control concepts can be applied regardless of industry, business line, or size and complexity of the systems processing environment.

• **Without effective** General Computing Controls, **reliance** on IT systems may **not be possible**
A more complete view of GCCs

IT Process Controls

Application Controls  IT Governance & Entity Level Controls

TECHNOLOGY  PROCESS  ORGANIZATION
Auditing Application Controls
Application Controls Defined

Application controls are manual or automated control procedures that typically operate at a detailed business process (cycle or transaction) level and are designed to ensure the integrity of the accounting records.
The Objective of Application Controls

The objective of internal controls over application systems is to ensure that:

– All input data is accurate, complete, authorized and correct
– All data is processed as intended
– All data stored is accurate and complete
– All output is accurate and complete
– A record is maintained to track the process of data from input to storage, and to the eventual output
– Access to data is limited based on business need
– Incompatible duties within an application are systematically prevented
Application Control Examples

**Input Controls**
These controls are used mainly to check the integrity of data entered into a business application. For example…

- Users are limited to selecting a values in a pre-populated dropdown box
- The system validates that a valid number is entered into a field where a dollar amount is expected.

**Processing Controls**
These controls provide automated means to ensure processing is complete, accurate, and authorized. For example…

- Transactions exceeding a specific dollar amount must be approved by an executive before being applied in the system.
Application Control Examples (Continued)

**Output Controls**

These controls address what is done with the data. They should compare results with the intended result and check them against the input. For example…

– Reports are complete and accurate

**Integrity Controls**

These controls can monitor data in process and/or in storage to ensure that data remains consistent and correct. For example…

– Systematically checking for duplicated data before adding information to the application
– Control totals & record counts are included on all reports
– Users are limited to selecting a values in a pre-populated dropdown box
– Data rollback procedures
Application Control Examples
(Continued)

Audit Trail

Processing history controls enables management to track transactions from the source to the ultimate result and to trace backward from results to identify the transactions and events they record. For example….

– An audit log is maintained listing all changes made to a record within the system, including the date of the change and the user making the change.

Limitation of Access

Users are assigned the fewest application privileges consistent with their assigned duties and functions. For example….

– Users are restricted from accessing (viewing or updating) information within the application that is not related to their job function.
Segregation of Duties

Separation of the management or execution of certain duties or of areas of responsibility is required in order to prevent and reduce opportunities for unauthorized modification or misuse of data or service. For example:

– Users with the ability to create a vendor are systematically restricted from paying that (or other) vendors.
How do I test Application Controls?
Auditing IT Process Controls

IT Process Controls

Application Controls

IT Governance & Entity Level Controls
Protiviti’s Technology Risk Model℠
IT Process Risk & Control Examples

Define IT Strategy and Organization

**Risk:** Information Security is not managed within the company.

**Control:** All information security functions are managed by a third party vendor.

Manage Security and Privacy

**Risk:** Access to the network is not adequately protected or restricted.

**Control:** A system account request form must be completed and approved by one or more authorized individuals prior to the creation/modification of a user account within the applicable environments. Required approvals are defined in the associated procedures and are dependent upon the type of access being requested.
IT Process Risk & Control Examples (Continued)

Manage IT Infrastructure

Risk: Systems may be unavailable resulting in loss of revenue and operational inefficiencies.

Control: Server downtime is monitored, recorded, and resolved within a reasonable amount of time.

Ensure Continuity

Risk: Loss of customer base if unable to recover critical processes within stated objectives; inability to satisfy contractual obligations results in fines or lost contracts.

Control: The development of a Business Continuity Plan will allow the company to recover quickly and efficiently with causing a limited amount of damage.
IT Process Risk & Control Examples
(Continued)

Manage IT Assets

**Risk:** The organization is unaware of what information technology assets it owns or where each asset can be presently located.

**Control:** An inventory of material IT assets owned or leased by the organization exists in a central repository and is updated on a regular basis.

Support Users

**Risk:** The lack of adequate user problem reporting and analysis may impair informed decision-making by IT management and continuous improvement of IT services to key users and business processes.

**Control:** A formal problem review process exists and User Support management understands how it works, who attends and how often it occurs.
IT Process Risk & Control Examples (Continued)

**Deploy and Maintain Solution**

**Risk:** Incomplete, inaccurate, or unauthorized changes are introduced into the production environment for server operating systems, applications, and supporting databases.

**Control:** All changes migrated to production are formally approved by the appropriate IT representative, business owner, and process owner, prior to migration. This approval is retained for audit purposes.
How do I test IT Process Controls?
Auditing IT Governance & Entity Level Controls

IT Process Controls

Technology

Process

Organization

Application Controls

IT Governance & Entity Level Controls
What is IT Governance?

- The Institute of Internal Auditors (IIA) and the IT Governance Institute (ITGI) define IT Governance as the ability for the enterprise’s IT to sustain and extend the organization’s strategies and objectives.

- IT Governance is facilitated through the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership</td>
<td>Recognition of the relationship between IT objectives and the current/strategic needs of the business by IT management, and the ability to effectively communicate this message to both IT and business personnel.</td>
</tr>
<tr>
<td>Organizational Structures</td>
<td>The enablement of dialogue and accountability between business and IT personnel through the current organizational structure. This should include the existence of necessary roles and reporting relationships to allow IT to adequately meet the needs of the business.</td>
</tr>
<tr>
<td>Processes</td>
<td>The formalization of efficient process activities, integrating key control activities, to meet the needs of the business while providing the necessary assurance over financial statements.</td>
</tr>
</tbody>
</table>

- Effective IT Governance is the responsibility of all of the organization’s executives and the board of directors.
What is IT Governance?

• IT governance has the ability to significantly impact the organization as a whole, including the:
  – Relationship between the business and IT
  – Balancing of Demand and Service capabilities
  – Visibility into IT management’s ability to achieve its objectives
  – Adaptability of IT to a changing business environment
  – Management of risks and identify continuous improvement opportunities for business and IT outcomes

• In fact, recent research from the MIT Sloan Center for Information Research found that “firms with superior IT governance have (on average) 20% higher profits”
The Five Elements of IT Governance

- The **Five Elements of IT Governance** as defined by the IT Governance Institute is used by the project team to identify the specific governance practices and goals to be reviewed during the audit.
- This industry standard framework consists of the five components listed in the graphic above.
The Five Elements of IT Governance

**Objective:**
Determine if a relationship exists between IT and business objectives and if this relationship has been established through participation between both IT and business management.

**Example Review Documents:**
- IT Strategic Plan
- Third Party service provider agreements and RFP process

**Typical Areas to Assess:**
- Is IT management aware of the overall business strategy?
- What is IT’s involvement in defining the business strategy?
- Do current IT initiatives relate to one or more of the organization’s strategic objectives?
- Is there a clear line of communication between IT and business management?
- How do 3rd party service providers support business objectives?
- What IT archetype is necessary to support the business objectives?
The Five Elements of IT Governance

Objective:
Determine if activities are conducted relating to the identification and analysis of risks impacting the achievement of business objectives and the preparation of financial statements.

Example Review Documents:
- Business Continuity and Disaster Recovery Plans and Test Results
- IT Risk Assessment
- 3rd Party Service Provider Agreements and Request For Proposal Policies and Procedures

Typical Areas to Assess:
- Is a process in place to assess, address, and communicate IT risks to key stakeholders and executive management during the project, change, and release management processes?
- How does IT select and manage third party vendor relationships?
- Does a business continuity and disaster recovery plan exist and is it tested on a periodic basis?
- Does a risk management plan exist and are risk management activities incorporated into project, change, and release management process?
The Five Elements of IT Governance

Objective:
Determine if the effectiveness of IT systems, processes, and personnel, internal and external, are being monitored for alignment with business needs.

Example Review Documents:
- Performance metrics for services, projects, processes, and systems
- Reports of IT’s performance against defined metrics to key stakeholders and executive management
- 3rd Party Service Level Agreements
- Cost Allocation Policies and Procedures

Typical Areas to Assess:
- Does the IT organization report performance metrics to key stakeholders?
- Do performance management activities consider both internal and 3rd party IT activities?
- Is IT performance reported in IT or Business terms? Are the metrics operational, strategic, or both?
- Is a process in place to establish performance metrics based on changing business needs?
Objective:

Determine if adequate activities are being performed to align the use of resources (applications, information, infrastructure, people) to meet the needs of the business.

Example Review Documents:

• IT Organization Chart
• IT Job Descriptions
• Sourcing Strategy for IT projects

Typical Areas to Assess:

• Has an IT sourcing strategy been established that align with business objectives?
• Do IT resource dedicate more time to operational or strategic objectives?
• Does the IT department have processes in place to facilitate knowledge sharing within the department and with the business?
• Have formal job descriptions and reporting relationships been created and communicated for all IT positions?
The Five Elements of IT Governance

**Objective:**
Determine if IT is effectively managing costs as they relate to meeting business objectives and communicating this management to the appropriate individuals.

**Example Review Documents:**
- IT Steering Committee Meeting Minutes
- Policies and Procedures for the Development and Management of IT projects
- IT Budget

**Typical Areas to Assess:**
- Is there a clear relationship between IT project performance indicators and business objectives?
- Has the IT budget been communicated to business leadership? Does business leadership understand the investments that have been made in IT?
- Does IT actively communicate the expected and realized value of IT projects?
- Does the business rely on the integrity and accuracy of data captured and reported by IT systems?
- Do IT and business leaders meet on a periodic basis to review the current and upcoming IT initiatives to reassess alignment with business objectives?
How do I test IT Governance & Entity Controls?
Building your IT knowledge through Industry Frameworks
About the IIA’s GTAG Series

• The Global Technology Audit Guides (GTAGs) are IIA publications that are intended to communicate issues related to IT management, control, and security in relatable business terms.

• The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

• There 15 books within the GTAG series covering a variety of topics, including:
  – Information Technology Controls
  – Change and Patch Management Controls: Critical for Organizational Success
  – Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
  – Management of IT Auditing
  – Managing and Auditing Privacy Risks
  – Managing and Auditing IT Vulnerabilities
  – Auditing Application Controls
  – Identity and Access Management
  – Business Continuity Management
  – Auditing IT Projects
  – Fraud Prevention and Detection in an Automated World
  – Auditing User-developed Applications
  – Information Security Governance
  – Developing the IT Audit Plan
  – Information Technology Outsourcing
COBIT™ Framework
COBIT™ Framework

**By the numbers…**
- 4 Domains
- 6 Maturity Levels
- 10 Publications
- 34 IT Processes
- 318 Control Objectives
- ∞ Control Practices

CobiT’s overall theme is **execution**:
- Are we doing things the right way, and are we getting them done well?
- More focused on **what** the results **ought** to be like
- Less focused on **how** to build it
An Introduction to ITIL

What is ITIL?

• ITIL stands for the IT Infrastructure Library guideline which was originally developed by the OGC (Office of Governance Commerce), a branch of the British government.

• ITIL outlines a highly scalable framework of best practices designed to provide guidance on developing a systematic approach to the provisioning and management of IT services.

• ITIL does not define a set of activities or implementation steps.

• ITIL provides terminology and a common language for communication within the IT department and with the business.

• ITIL is complimentary to other frameworks such as CobiT and ISO/IEC 27000. You do not have to choose just one framework.

• There are currently two accepted versions of ITIL
An Introduction to ITIL

Terminology

- **IT Service Management (ITSM):** The implementation and management of quality IT Services that meet the needs of the business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, processes and technology. ITSM is made up of Service Delivery, and Service Support.

- **Service Delivery:** Covers the processes required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of IT services delivered.

- **Service Support:** Describes the processes related to the day-to-day support and maintenance activities associated with the provisioning of IT services.
  
  - Service Desk
  - Incident Management
  - Problem Management
  - Change Management
  - Release Management
  - Configuration Management
An Introduction to ITIL

Service Management
The ISO 27001 Standard

- Information Security Management Standard
- Examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts
- Requires the organization to design and implement a coherent and comprehensive suite of information security controls
- Brings information security under explicit management control
ISO 27001 Domains

Security Governance

Operational

System Development and Maintenance

Communications and Operations Management

Business Continuity Management

Incident Management

Physical and Environmental Security

Human Resources Security

Compliance

Asset Management

Access Control

Organizational Security

Security Policy

CONFIDENTIAL: This document is for your company's internal use only and may not be copied nor distributed to any third party.
So, what’s the right framework?

**Proscriptive:** Describe how processes should work

**Focus:** Effectiveness, Efficiency

**Descriptive:** Describe what objectives processes ought to achieve

**Focus:** Effectiveness, Alignment

- Answer: **All** of them…they’re not mutually exclusive (example: (CobiT) Controls describe how (ITIL) processes work)
- IT management generally gets more value out of proscriptive frameworks
- Audit and control practitioners “speak” control language
When should you involve an IT Specialist?
For additional information on conducting IT Audits or to receive a copy of this slide deck, please contact the presentation team:
Powerful Insights. Proven Delivery.™