Preview of Key Points

- The Basic components of the IT environment
- Understanding the IT Control Structure
- General Control concerns
- Business process Application Controls
- Network basic risks and controls

Notes:
## The IT Control Structure

<table>
<thead>
<tr>
<th>Application Controls</th>
<th>General Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibility of:</strong></td>
<td><strong>Responsibility of:</strong></td>
</tr>
<tr>
<td><em>Business Process Owners</em></td>
<td><em>IT Management</em></td>
</tr>
<tr>
<td><strong>Focus Is On Transactions:</strong></td>
<td><strong>Focus Is On Managing:</strong></td>
</tr>
<tr>
<td>- Input</td>
<td>- Hardware</td>
</tr>
<tr>
<td>- Process</td>
<td>- Software</td>
</tr>
<tr>
<td>- Output</td>
<td>- Data</td>
</tr>
<tr>
<td>- Networks</td>
<td></td>
</tr>
<tr>
<td><strong>Control/Audit Objectives Are:</strong></td>
<td><strong>Control/Audit Objectives Are:</strong></td>
</tr>
<tr>
<td>- Accuracy</td>
<td>- Availability</td>
</tr>
<tr>
<td>- Completeness</td>
<td>- Reliability</td>
</tr>
<tr>
<td>- Authorization</td>
<td>- Confidentiality</td>
</tr>
<tr>
<td>- Compliance</td>
<td>- Compliance</td>
</tr>
</tbody>
</table>

Notes:

Big 12 Internal Audit Conference, May 2010

Slide 3

Richard Tarr, CIA, CISA
Role of IT within the Organization

- Information technology (IT) enables companies to provide service more efficiently, with greater accuracy, and on a timely basis.
- As dependence on IT systems increases, the need to do this more effectively increases;
- The supporting infrastructure becomes more critical.

Consider: “Information“ is “your business”.
  - IT systems support “Information”, hence
  - IT systems support “the business”.
- In many cases today, without IT there is no business!

Notes:
Role of IT within the Organization

- IT systems are the glue that connects the organization.
- Frequently, IT is the “primary process”, a critical component of all business processes.
- The IT infrastructure:
  - Provides the a primary control point for business activities.
    - Records transactions and stores the business information
  - Enables management to controls processes through monitoring.
    - Notification about activities that outside the norm.
  - Connects lines of business to support units, and customers to trading partners.
Management Risks in an Automated Environment

- As the interconnection among business units, partners, allies, suppliers, and others increases, the ability to rely on the system can be compromised.
- The risks occasioned by such use, along with potential threats from increasing use of the Internet instead of private networks, mean that the organization needs a method to understand and “control” them.
- That’s why auditors need to an understanding of IT because the technology is only increasing in importance.
- The risks listed next are not new, but ....

Notes:
Management Risks in an Automated Environment

- the **significance** of IT risks has increased; these risks include:
  - Improper reliance on the automated system
  - No audit trails
  - Inaccurate reporting
  - Loss of competitive edge
  - Loss of user confidence in the process
  - Lost business
Management Risks in an Automated Environment

- Loss of privacy, confidentiality
- Inadequate protection of assets
- Interruption of the business cycle
- Loss of productivity
- Loss of revenue
- Lack of data integrity
- Violation of regulatory or legal requirements
- Loss of the organization

Notes:
Security Risks in an Automated Environment

- Many of the potential problems related to IT can be traced to one word: **Security**
- Auditors need to gain an understanding of IT security risks and related possible controls.
- Key security risks include:
  - Physical and logical computer security
  - Physical and logical network security
  - Application logical security
  - Controls over input and distribution of output
  - Selecting and managing security technology
Managing Risks

How does an organization manage risks?  
---- By implementing a  

“System of Internal Controls”

- Internal controls can help an organization achieve its basic business objectives:
  - Achieve performance levels and objectives/goals
  - Prevent loss of resources/assets
  - Help ensure reliable financial reporting
  - Help ensure compliance with laws and regulations

Notes:
IT Audit Controls Reviews

- When auditing IT system hardware and/or software:
  - An application is subject to an “Application Controls Review” (ACR)
    - Often just called an “Application Review” (AR)
  - Everything else – software and hardware – is subject to a “General Controls Review” (GCR).
  - You CAN NOT certify an application without also certifying the General Controls on the underlying platforms(s) on which it executes!
- Controls reviews are conducted following one of the audit strategies discussed earlier.
Risk Categories and Controls Categories

- A common approach to identifying risks is to identify Risk Categories.
- IT controls can also be grouped into a collection of IT Controls Categories.
- Here is a simple mapping from Risk Categories to Control Categories.
  - The categories shown next are not the only possible grouping of topics. Each organization may define categories differently, but in the end they are essentially equivalent.
Mapping Risk and Controls Categories

Risk Categories
- Regulatory Issues
- Operations
- Data Integrity
- Security and privacy
- BC / DR
- Development methodology

IT Controls Categories
- IT Governance
- Operation Controls
- Network Controls
- Environmental Controls
- Change Management
- Database Administration
- Input, Process, Output controls
- Logical Security
- Physical Security
- BC / DR
- System Development

Notes:
IT Controls Categories and Reviews

- Some IT Controls Categories include topics
  - only related to applications, hence only included in Application Reviews. OR
  - only related to system hardware/software, hence only included in General Controls Reviews. OR
  - related to all aspects of an IT system, hence included in both types of Reviews.

- The chart on the next page indicates the relationship of IT Control Categories to Application Reviews and General Controls Reviews.
  - The line dividing Database Administration indicates separate topics in the same category
IT Controls Categories

Application Controls
- Input Controls
- Process Controls
- Output Controls

General Controls
- IT Governance
- Logical Security
- Change Management
- Business Continuity & Disaster Recovery
- System Development Methodology
- Database Administration

Operation Controls
- Physical Security
- Environmental Controls
- Network Controls

Notes:
Managing Risks

- However, effective internal controls can only help an organization achieve its objectives. They can not:
  - change a poor manager into a good one
  - make up for bad management decisions
  - overcome a bad economy
  - anticipate or overcome competitors actions
- The “control environment” is the tone or perspective of the organization about controls.
- Some say the majority of problems that occur in IT systems are due to the poor “control consciousness” of system users.

Notes:
Relative IT Control Effectiveness

Examples of Common IT Controls

- **Manual Detective**: report of user accounts not required to have a password
- **Manual Preventive**: published password policy
- **Automated Detective**: intrusion detection system with alerts
- **Automated Preventive**: failed login attempt limit with automated account lockout
About That Word – Control

- There are two views about what that word \textit{control} means:
  - The IT view
  - The business/audit view
- They are distinctly different.
- Language is important.
  - To help develop a required “control consciousness”, we need to speak the same language – the words mean the same things.
  - IT often doesn’t share the auditor’s language.
What is a Control?

- The IT view of a Control:
  - A control is “how something works”.
  - Controls allow or facilitate.
    - Access Control Software
    - ActiveX Control
    - Media Access Control (MAC)
    - Transmission Control Protocol (TCP)
What is a Control?

- The business/audit view of a **Control**:
  - A control is “how do you know something is working”?
  - Controls **limit**, **restrict**, or **assure**.
    - Policies, practices, and procedures used to assure that systems (and people who run it and use it) only work “as expected”.

Notes:
What is a Control?

- Two different views:
  - IT: How something \textit{works}.
  - Audit: How do you know something \textit{is working}?
  - No wonder IT and Audit often can’t communicate!
- It is assumed you are familiar with the audit view.
- When you talk with IT personnel you should not assume they understand your use of the word “control”.
Internal Control Definition (COSO) Objectives

Internal control is 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
- Safeguarding assets

*Source: Internal Control—Integrated Framework, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, 1992*
Internal Control Definition (COSO)

- Internal control is:
  - A process - a means to an end, not an end in itself.
  - Effected by people (not just policies and procedures) at all levels of the organization.
  - Provides reasonable assurance, NOT absolute assurance.
  - Influenced by the “Tone at the Top”.

Notes:
# Governance VS Control

<table>
<thead>
<tr>
<th>Governance</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level</td>
<td>Low level</td>
</tr>
<tr>
<td>Overview</td>
<td>Details</td>
</tr>
<tr>
<td>Enterprise wide</td>
<td>Specific</td>
</tr>
<tr>
<td>Tone at the Top</td>
<td>Individual</td>
</tr>
<tr>
<td>Strategic</td>
<td>Tactical</td>
</tr>
<tr>
<td>COSO</td>
<td>CobiT®</td>
</tr>
</tbody>
</table>

**Notes:**
General Controls in IT

- Apply to large mainframe data centers and client/server environments, although the types and depth of controls will vary
- Provide the business and its functions with a set of common controls that are shared by business units and functional units
- Support underlying functions that one or more applications depend on
- Ensure control and stability of business infrastructure
Relationship Between General and Application Controls

- In general, you cannot rely on application controls without general controls, such as program security, which helps prevent unauthorized changes to application programs, or data security which helps protect application data.

- To fully assess an organization’s IT controls requires a review of IT general controls and application control audits of high risk/impact applications.
IT Governance: Standards and Policies

During a review the auditor is testing whether there are policies and procedures that implement good practices based on accepted models/standards:

- Are properly documented and current
- Address management’s business/operating objectives
- Are reviewed periodically for:
  - Effectiveness
  - Conformity with business objectives and regulations
- Promote proper segregation, security, and safety of personnel

Notes:
IT Controls Categories

General Controls
- IT Governance
- Logical Security
- Change Management
- Business Continuity & Disaster Recovery
- System Development Methodology
- Database Administration
- Operation Controls
- Physical Security
- Environmental Controls
- Network Controls

Application Controls
- Input Controls
- Process Controls
- Output Controls

Notes:
General Control Standards

- COBIT\textsuperscript{\textregistered}: Control Objectives for Information and Related Technology
- ISO 27002 Security Standard
- NIST 800 series standards
- GAO Government Accountability Office
- ITIL IT Infrastructure Library
- IIA GTAG Global Technology Audit Guides

Notes:
Most Critical IT General Controls

- Access Security
  - Authentication
  - Authorization
- Change/configuration control
- System acquisition/development
- File backup and recovery
- Disaster recovery

Notes:
Application Controls

- Business applications consist of many transactions that perform specific functions.
- The set of all such transactions, taken as an entity, performs the business objectives of the application.
- A primary objective of application audits:
  - Ensure appropriate controls are in place to prevent, detect and correct errors and omissions in the processing of application transactions.
  - In other words: ensure that transactions are –
    - Accurate
    - Complete
    - Authorized
Application Control Standards

- There are none for Transactions!
Application Controls Categories

Input Controls

Process Controls

Output Controls

IT Governance

Logical Security

Change Management

Business Continuity & Disaster Recovery

System Development Methodology

Database

Notes:
Transaction Life Cycle

Each box in the process flow diagram represents a “Transaction Component”

Control Points

Notes:
Completeness and Accuracy of Input

- Ensure transactions are:
  - Input into the computer.
  - Accepted by the computer.
  - Processed only once.

- Errors are:
  - Identified.
  - Segregated from valid transactions.
  - Corrected in a timely and accurate manner.
  - Returned to mainstream processing.
Completeness and Accuracy of Input

Examples of controls include:

- Character checking – blank, alpha, numeric, etc.
- Field checking
  - Sequence check
  - Reasonableness, limit/range check
  - Check digit – existence and validity
  - Consistency, validity check
  - Completeness check – no missing fields
  - Logical relationship check
- Batch or level checking
  - Control totals and record counts
  - Hash totals (especially on time-separated entries)
- Key verification/duplicate entry
Completeness and Accuracy of Processing

- Processing controls help ensure that authorized transactions are:
  - Accepted by the application system.
  - Accurately processed with valid business rules.
  - Processed completely and available for authorized users in accordance with business requirements.
Completeness and Accuracy of Processing

- Risks from inadequate processing controls include:
  - Fraud.
  - Erroneous financial or management reporting.
  - Statutory sanction or legal action.
  - Business interruption.
  - Loss of competitive advantage.
Examples of controls include:

- Programmed procedures, programmed edit checks.
- Programmed balancing controls (run-to-run or process-to-process control totals).
- Anticipation controls
- Manual recalculation
- Reasonableness verification
- Limits for system calculations
- File reconciliations
- Exception reporting

Notes:
Output Controls

- A transaction output may be a single data item up to a multi-page document set.

- Ensure output data is:
  - Reported in the correct manner.
  - Viewable or made available to only authorized personnel.
  - Appropriately retained or destroyed.
  - Subject to necessary processing audit trails.
  - If erroneous, segregated from valid records, corrected and reentered into mainstream processing.
Output Controls

- Examples of controls include:
  - Balancing/reconciliation – does it match?
  - Controls over sensitive documents
    - before printing – blank negotiable documents
    - after printing – distribution to only authorized personnel
  - Destruction of sensitive data
    - retention requirements?
    - Waste disposal procedures

Notes:
Network Controls

- Organizations have built systems and applications that rely on interconnecting almost all of the computers in the organization.
  - In doing so they have greatly increased their reliance on telecommunications and networking for daily business communications.

- This extensive use of telecommunications and the Internet have introduced additional security and control risks.
  - Chief among these is:
    - Unauthorized access to applications and data.
Networks & Client/Server Processing

- The predominant distributed systems environment is **Client/Server** processing:
  - the total processing task is divided among two or more processes executing on two or more hardware platforms.
  - **client** – a **process** that requests a service
  - **server** – a **process** that provides that **service**

Note: the distinction between Client and Server is based on the nature of the **process**, NOT on the type of computer on which the process is executing.

Network Controls are all about controlling access to services.

Notes:
Network Audits

- These audits will determine if there are documented procedures in place that address the following key risk areas:
  - Network access security (most important)
  - Availability
  - Reliability
Network Security: User Authentication

- Authentication mechanisms can be grouped into three functional categories (factors):

  Something I *know*
  - Password
  - PIN

  Something I *have*
  - Smart card
  - Token

  Something I *am*
  - Signature
  - Thumb print

- Best method? Combination of the above! (Called multi-factor authentication.)
Network Security: Authorization

- Once a user is authenticated, they are granted certain access rights based on their user profiles.
- Need to differentiate access needs among users based on least privilege and “need to know” basis.
- Authorizations provide the basis for separation of duties.
- Data owners or management need to authorize access to specific systems, transactions and information.
- Access granted/limited to create, update, delete, display, execute ... or a combination of these depending on access required.
Question?

Thank You

Have a great day.