INTRODUCTION
Danny M. Goldberg

- Founder, GOLDSRD (www.goldsrd.com)
- Former Director of Corporate Audit/SOX at Dr Pepper Snapple Group
- Former CAE - Tyler Technologies
- Published Author (Book/Articles)
- Texas A&M University – 97/98
- Chairman of the Leadership Council of the American Lung Association - North Texas – Calendar Year 2012
- Served on the Audit Committee of the Dallas Independent School District (CY 2008)
- Current Dallas and Fort Worth IIA Programs Co-Chair
- Fort Worth IIA Board Member
- IIA North America Learning Committee Member (2014-15)

Certifications:
- CPA – Since 2000
- CIA – Since 2008
- CISA – Since 2008
- CGEIT - Since 2009
- CRISC - Since 2011
- CRMA – Since 2011
- CCSA – Since 2007
- CGMA – Since 2012

Danny M. Goldberg

- Highly-Rated, Internationally Recognized Speaker
  - 3rd Rated Speaker, 2015 IIA All-Star Conference
  - One of the Top Rated Sessions, 2015 GAM Conference
  - 8th Rated Speaker, 2015 MISTI AuditWorld
  - 10th Rated Speaker, 2015 ISACA CACS
  - One of the Top Rated Speakers, 2014 IIA All-Star Conference
  - 7th Rated Speaker, 2014 ISACA ISRM Conference
  - One of the Top Rated Speakers, 2014 IIA Mid-Atlantic Conference
  - 3rd Rated Speaker, 2014 ISACA CACS
  - One of the Top Rated Speakers, 2014 IIA Gaming Conference
People-Centric Skills

- Added to IIA and ISACA Bookstores, Summer 2015
- Published August 2014 (Wiley Publications)
- Over 2,000 copies sold - Amazon Rating
- Coauthored with Manny Rosenfeld
  - Chief Audit Executive with four global F500 Cos. and a global Financial Services organization.
- First book specific to internal audit communications and personal interactions
- This is not a reference book!
  - Story book format
  - Character development
  - Fictional Internal Audit Department
  - Fictional Professional Coach/Trainer
  - Situational

GoldSRD Snapshot

Staff Augmentation:
- Market leader in locating cost-effective, recognized resources in accounting, finance, audit and IT
- All requests filled within 72 hours

Professional Development:
- Nationally-Recognized Leader in Audit and People-Centric® Skills Training
- Institute of Internal Auditors ("IIA") Recognized CPE Provider (only 6 firms in North America!)
- Over 170 Full-Day Courses on Audit, IT Audit, Accounting, Finance, Personal Development and People-Centric® Skills
- Registered with NASBA to offer CPE’s for all courses in course catalog (Live and Web-Based)
- Interactive and Educational Courses for all levels

Executive Recruiting:
- Unique approach to filling positions, including personality assessment for candidate and organization
- Expansive network of qualified candidates actively looking
Bi-Monthly Webinar Series

- Each two-hour webinar will be on the first Monday of EVERY OTHER month (beginning in February), starting promptly at Noon CST (minimum of ten attendees to hold the class or it will be rescheduled/ refunded). Each webinar can be purchased for $50.00 or an annual subscription can be purchased at a 20% discount at $240.00.
- Group discounts can drive individual pricing down to $20/hour and, based on group size, down to $13.50/hour! All webinars are NASBA-Certified!

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 6th</td>
<td>Audit Interviewing</td>
</tr>
<tr>
<td>April 3rd</td>
<td>Assessing Corporate Culture</td>
</tr>
<tr>
<td>June 5th</td>
<td>Audit2020: Evolving IA</td>
</tr>
<tr>
<td>August 7th</td>
<td>Project Management for IA</td>
</tr>
<tr>
<td>October 9th</td>
<td>Conflict Management/Negotiation Skills</td>
</tr>
<tr>
<td>December 4th</td>
<td>Business Etiquette for the Modern Auditor</td>
</tr>
</tbody>
</table>
IA’s Obligation in Regards to IT

Straw Poll

• What is an internal auditor’s responsibility in regards to knowledge of IT risks and controls?
IIA Standards and IT Auditing

- **1210.A3 – Proficiency**
  - Internal auditors must have *sufficient knowledge* of *key information technology risks and controls* and available technology-based audit techniques to perform their assigned work.
  - However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

GOLD NUGGET #1

- **GTAG – Global Technology Audit Guide**
- Prepared by The IIA, GTAG is written in straightforward business language to address timely issues related to information technology (IT) management, risk, control, and security
- **Here’s the kicker** – IIA members access GTAG’s **FREE!**
GTAG I – Categories of IT Knowledge

- Defines three categories of IT knowledge for auditors:
  - **Category I**: Knowledge of IT needed by all professional auditors, from new recruits up through the CAE
  - **Category II**: Knowledge of IT needed by audit supervisors
  - **Category III**: Knowledge of IT needed by IT Audit Specialists

---

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing Application Controls (Previously GTAG 8)</td>
<td>January 2009</td>
</tr>
<tr>
<td>Auditing IT Governance (Previously GTAG 17)</td>
<td>July 2012</td>
</tr>
<tr>
<td>Auditing IT Projects (Previously GTAG 12)</td>
<td>March 2009</td>
</tr>
<tr>
<td>NEW! Auditing Smart Devices: An Internal Auditor’s Guide to Understanding and Auditing Smart Devices</td>
<td>August 2016</td>
</tr>
<tr>
<td>Auditing User-developed Applications (Previously GTAG 14)</td>
<td>June 2010</td>
</tr>
<tr>
<td>Business Continuity Management (Previously GTAG 16)</td>
<td>January 2009</td>
</tr>
<tr>
<td>Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition (Previously GTAG 2)</td>
<td>March 2012</td>
</tr>
<tr>
<td>Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition (Previously GTAG 3)</td>
<td>January 2009</td>
</tr>
<tr>
<td>Data Analysis Technologies (Previously GTAG 16)</td>
<td>August 2011</td>
</tr>
<tr>
<td>Developing the IT Audit Plan (Previously GTAG 11)</td>
<td>January 2008</td>
</tr>
<tr>
<td>Fraud Prevention and Detection in an Automated World (Previously GTAG 13)</td>
<td>December 2009</td>
</tr>
<tr>
<td>Identity and Access Management (Previously GTAG 9)</td>
<td>January 2009</td>
</tr>
<tr>
<td>Information Security Governance (Previously GTAG 15)</td>
<td>June 2010</td>
</tr>
<tr>
<td>Information Technology Outsourcing, 2nd Edition (Previously GTAG 7)</td>
<td>June 2012</td>
</tr>
<tr>
<td>Management of IT Auditing, 2nd Edition (Previously GTAG 4)</td>
<td>January 2013</td>
</tr>
</tbody>
</table>
Category I Knowledge

- Understanding concepts such as applications, operating systems and systems software, and networks
- IT security and control components such as perimeter defenses, intrusion detection, authentication, and application system controls
- Understanding how business controls and assurance objectives can be impacted by vulnerabilities in business operations and the related and supporting systems, networks, and data components
- Understanding IT risks without necessarily possessing significant technical knowledge

Straw Poll

- How many of you can confidently raise your hand (not half-way but a full hand raise) and agree that you have Category I knowledge?
SIMILARITIES/DIFFERENCES BETWEEN INTERNAL AUDIT AND IT AUDIT

Type of Audit Objectives

**Financial/Operational**
- Completeness
- Accuracy
- Validity
- Authorization
- Rights & Obligations
- Presentation & Disclosure
- Efficiency
- Effectiveness

**IT Objectives**
- Security
- Availability
- Confidentiality
- Integrity
- Scalability
- Reliability
- Effectiveness
- Efficiency
Type of Audit Objectives

<table>
<thead>
<tr>
<th>Financial/Operational</th>
<th>IT Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>Security</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Availability</td>
</tr>
<tr>
<td>Validity</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Authorization</td>
<td>Integrity</td>
</tr>
<tr>
<td>Rights &amp; Obligations</td>
<td>Scalability</td>
</tr>
<tr>
<td>Presentation &amp; Disclosure</td>
<td>Reliability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Effectiveness</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>Efficiency</td>
</tr>
</tbody>
</table>
Control Frameworks

- Internal Controls
  - COSO Internal Control – Integrated Framework (Most Popular)
- General Computer Controls
  - COBIT (Most Popular)
    - Control Objectives for Information and Related Technology
    - Generally applicable and accepted standard for good IT security and control practices that provides a reference framework for management, users, and audit practitioners
    - Developed by the IT Governance Institute
  - ITGI Control Objectives For Sarbanes Oxley
  - ITIL (IT Infrastructure Library)

WHAT IS COBIT®?

Control Objectives for Information & related Technology
**COBIT®**

- Designed to be used by auditors and business process owners
  - Uses a set of 34 high-level control objectives that cover 210 control objectives grouped into four domains:
    - Plan and Organize
    - Acquire and Implement
    - Deliver and Support
    - Monitor and Evaluate
- Provides guidance for executive management to govern IT within the enterprise
  - More effective tools for IT to support business goals
  - More transparent and predictable full-life-cycle IT costs
  - More timely and reliable information from IT
  - Higher quality IT services and more successful projects
  - More effective management of IT-related risks
- Looks at fiduciary, quality and security needs of enterprises, providing seven information criteria that can be used to generically define what the business requires from IT
  - Effectiveness
  - Efficiency
  - Availability
  - Integrity
  - Confidentiality
  - Reliability
  - Compliance

**IT Risk Framework Benefits**

- Aligned with **business risk** – focus on what is important to the business
- Valuable input to the IT and business strategy, as well as the IT Audit plan
- Linked to maturity assessment to provide roadmap for process improvement
- Addresses risk factors affecting each aspect of the IT environment:
  - IT Governance, IT Processes, IT Applications and Infrastructure
- Compatible with other IT frameworks including COBIT, PMI, ITIL, ISO, etc
- End-to-End (comprehensive) view of all IT processes, such as development, support, help desk, security, etc.
- Addresses all critical “layers” of the IT environment, i.e. applications and infrastructure such as network, OS, DB
## How Should IT Success Be Judged?

### Control Types

- **Dual Controls** (Partially Automated and Manual)
  - People enabled controls
  - People rely on information from IT systems for the control to function

- **Manual**
  - People enable control
  - Fully independent of IT systems

- **Automated**
  - Programmed controls
  - Strong in nature
  - Lack human error
  - Repetitive, same functioning
  - Test of 1 vs. Many
IT Controls Overview

- Classification
  - General Controls
  - Application Controls
- Classification
  - Preventative
  - Detective
  - Corrective
- Classification
  - Governance controls
  - Management controls
  - Technical controls
Types of IT Controls

- Preventive controls prevent errors, omissions, or security incidents from occurring
  - EXP: data-entry edits, access controls, antivirus software, firewalls, intrusion prevention systems
- Detective controls detect errors or incidents that elude preventative controls
  - EXP: monitoring accounts or transactions to identify unauthorized or fraudulent activity
- Corrective controls correct errors, omissions, or incidents once they have been detected
  - EXP: correction of data-entry errors, recovery from incidents, disruptions or disasters
Group Exercise

In groups, think of a simple metaphor to define in layman’s terms what general controls are.

The House Analogy

Inside of the House: Application Controls

Foundation of the House: General Controls
House Metaphor

Foundation
• Without a strong foundation, all of the “insides” are irrelevant – they will be destroyed if the foundation does not work well.

Furniture, Electronics, Hardwood Floors
• Beautiful furnishings and eccentric artwork will become severely damaged if the foundation cracks a sinkhole swallows the insides!

IT General Controls (ITGC’s)
Major Categories
1. Access to Programs and Data
2. Program Changes
3. Program Development
4. Computer Operations
ITGC #1: Access to Programs & Data

**RISK:** Unauthorized access to program and data may result in improper changes to data or destruction of data

**OBJECTIVES:** Access to program and data is properly restricted to authorized individuals only

**COMPONENT CONSIDERATIONS:**
- Policies & procedures
- User access provisioning & de-provisioning
- Periodic access reviews
- Password requirements
- Privileged user accounts
- Physical access
- Appropriateness of access/segregation of duties
- Encryption
- System authentication
- Audit logs
- Network security

INFORMATION SECURITY

Designing, implementing, and maintaining information security, including both physical and logical security over all access paths to programs and data. Accessing and prioritizing relevant security risks. Defining data owners, classifying data as to necessary security, and selecting and implementing security tools and techniques.

**Control Objectives**

- Tools and techniques restrict access to programs, data, and other information resources
- Restricts access to programs and information
- Physical access restrictions are implemented and administered to restrict access to information
- All information resources subject to appropriate physical and logical security

**Value Add Areas**

- Virus Protection
- Software is used in accordance with licensing agreements and management’s authorization
- Information is protected against environmental hazards and related damage

**Covers**

- Security policies
- Security standards
- Data ownership
- Information security architecture
- Security administration
- Logical access
- Security logging & monitoring
- Physical access
- Environmental
Information Security – Coverage Areas

- Defining Data Owners – Identifying owners is key; is it the business or IT?
- Data Classification – Confidential, Private, Highly Sensitive Customer Corporate and Customer Data, Sensitive Internal Data, Public
- User Provisioning/De-provisioning – Covered in next section
Access Controls – Leading Practices

• No matter what method is chosen to scope the review of application controls, the module’s or application’s logical access controls need to be reviewed periodically.

• In most cases, the user and administrative access rights (e.g., read, write, and delete) are built using the inherent security platform and tools within the application.

• The strategies employed to determine which logical access rights will be assigned to users vary from a need-to-know basis to a need-to-withhold basis.

• Access rights should be granted based on the user’s job function and responsibilities.

How logical access rights are created vary from package to package. In some cases, the logical access rights are granted based on a transaction code or a screen name or number, while others, such as SAP R/3, use more complex object based security protocols. When a review of an application’s logical access controls is performed, it is important to ensure that the general application security controls are reviewed as well, including:

• Length of the user name or user identification
• Password’s length
• Password character combinations
• Password aging (e.g., users must change their password every 90 days)
• Password rotation (e.g., users cannot use any of their last eight passwords)
• User account lockout after six unsuccessful login attempts
• Session timeout (e.g., the application automatically logs out a user if the user has not interacted with the application within 15 minutes)
User Access Administration

- Common control concerns:
  - Informal, decentralized or fragmented process
  - User roles not formally defined
  - Inadequate user access request methods:
    - Forms too general
    - Requests and approvals not documented
    - Audit trail not maintained
  - User termination notification processes not effective
  - User removal processes not comprehensive
  - Periodic reviews not performed
  - No intuitive access report available for management review
User Provisioning

- Who is responsible for user provisioning?
- When should user access be cut-off once they notify/are notified they are leaving a company?
- How quickly should access be cut-off once this notification occurs?
- Does Active Directory alleviate all concerns?

WHAT IS ACTIVE DIRECTORY/SINGLE SIGN-ON? IF ACTIVE DIRECTORY IS SHUT-OFF, CAN USER ACCESS THE NETWORK?
### ITGC's #2 & 3: Program Changes/Development

#### Program Changes

- **Risk:** Inappropriate changes to systems or programs may result in inaccurate data.

- **Objectives:** All changes to existing systems are properly authorized, tested, approved, implemented and documented.

#### Program Development

- **Risk:** Inappropriate system or program development or implementation may result in inaccurate data.

- **Objectives:** New systems/applications being developed or implemented are properly authorized, tested, approved, implemented and documented.

#### Component Considerations:

- Change management procedures and system development methodology
- Authorization, development, implementation, testing, approval, and documentation
- Migration to the production environment (Separation of Duties (SOD))
- Configuration changes
- Emergency changes
- Data migration and version controls
- Post change/implementation testing and reviews

### Application Sys Implementation & Maintenance

#### Selecting or developing, implementing, and maintaining application systems

**Critical Areas**

- New application systems are implemented appropriately and function as expected
- When new application systems are implemented, existing data that is appropriately converted
- All necessary modifications to existing application systems are implemented timely
- Modifications to existing systems are properly implemented and function as expected

**Value Add Areas**

- New application systems are acquired or developed consistent as expected
- Application systems are maintainable and supportable

**Control Objectives**

- Project planning & management
- Project prioritization
- Project budgeting
- Systems development methodologies
  - Design Specifications
  - Programming standards
  - Programmer access
  - Modifications to purchased software
  - Testing
  - Change control
  - Program documentation
  - User documentation

**Covers**
App Sys Implementation & Maintenance – Coverage Areas

- Superuser/Admin Access
- Off the Shelf Software – What are modifications? Why are they important?
- SDLC/Change Control

Change Control

- Types of changes:
  - Program code changes, software updates, system patches, new software implementations
- Change controls should include:
  - Monitoring and logging of all changes
  - Steps to detect unauthorized changes
  - Confirmation of testing
  - Authorization for moving changes to production
  - Tracking movement of hardware and other infrastructure components
  - Periodic review of logs
  - Back out plans
  - User training
- Specific procedures should be defined and followed for emergency changes
Managing the data architecture and maintenance in terms of defining and maintaining the structure of master file data, transaction data, and organization data. Maintaining the database management system (or its equivalent).

### Critical Areas
- The data structure is appropriately implemented and functions consistent with management’s intentions
- All necessary modifications to the data structure are implemented timely and with proper approval (SDLC)
- Modifications to the data structure are appropriately implemented and the modified data structure functions consistent with management’s intentions

### Control Objectives
- Data architecture
- Database implementation
- Database administration & monitoring
- Database maintenance & modifications

### Topics Covered

#### Gold Nugget #2
- Master Files
  - Customer
  - Employee
  - Vendor
- Why is protection of the master file important?
**Network Support**

Designing, installing and operating networks and communication software and protocols. This includes defining the structure and interrelationships between components of the network, configuring the physical locations of files and equipment, and planning the operating capacity and capabilities to meet current network needs.

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>Topics Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical Areas</strong></td>
<td>Network &amp; communication software:</td>
</tr>
<tr>
<td>• New network and communication software is appropriately implemented and functions properly and implemented in a timely manner.</td>
<td>• Acquisition &amp; approval</td>
</tr>
<tr>
<td>• Modifications to existing network and communications software are properly implemented and function as expected</td>
<td>• Implementation &amp; testing</td>
</tr>
<tr>
<td><strong>Value Add Areas</strong></td>
<td>• Support</td>
</tr>
<tr>
<td>• New network and communication software is acquired consistent with management’s intentions</td>
<td>• Maintenance</td>
</tr>
<tr>
<td>• Network and communication software is maintainable and supportable</td>
<td>• Performance monitoring</td>
</tr>
<tr>
<td></td>
<td>• Documentation</td>
</tr>
</tbody>
</table>

**System Software Support**

Selecting, implementing, and maintaining necessary systems software, including the parameters that configure and control such software. Implementing and monitoring system software changes, including vendor upgrades.

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>Topics Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical Areas</strong></td>
<td>Operating system acquisition</td>
</tr>
<tr>
<td>• New system software is appropriately implemented and functions properly</td>
<td>• Installation, configuration and updates/patches</td>
</tr>
<tr>
<td>• All necessary modifications to system software are implemented timely</td>
<td>• Maintenance</td>
</tr>
<tr>
<td>• Modifications to system software are properly implemented and function as intended</td>
<td>• Performance monitoring</td>
</tr>
<tr>
<td><strong>Value Add Areas</strong></td>
<td>• Documentation</td>
</tr>
<tr>
<td>• New system software is acquired consistent with management’s intentions</td>
<td></td>
</tr>
<tr>
<td>• System software is maintainable and supportable</td>
<td></td>
</tr>
</tbody>
</table>
ITGC’s #4: Computer Operations

**Risk:** Systems or programs may not be available for users or may not be processing accurately

**Objectives:** Systems and programs are available and processing accurately

**Component Considerations:**
- Batch job processing
- Monitoring of jobs (success/failure)
- Backup and recovery procedures
- Incident handling and problem management
- Changes to the batch job schedules
- Environmental controls
- Disaster Recovery Plan (DRP) and Business Continuity Plan (DRP)
- Patch management

**Information Systems Operations**

Supervising and maintaining computer systems operations. Providing scheduled, monitored, and secure computer operations. Satisfying end-user requirements for computer processing support and problem resolution.

**Control Objectives**
- Job scheduling
- Processing control
- Output control
- Problem logging, tracking & reporting
- Problem escalation & resolution
- Capacity planning
- Performance monitoring
- Facilities management
- Help desk procedures
- Backup & Recovery
- Business Continuity/Disaster Recovery

**Critical Areas**
- Production to process batch and on-line transactions and prepare related reports are executed timely and completely
- Only valid production programs are executed

**Value Add Areas**
- Data is retained in accordance with laws, regulations, and company policy
- Computer processing environment service levels meet or exceed management’s expectations
- Users receive appropriate systems training in the use of application systems
- Users receive appropriate support to ensure that application systems function as intended
Backup and Recovery Controls

- Requirements should be defined for backup of critical data (type and frequency)
- Periodic inventory of backup files should be performed
- Procedures should be in place to periodically validate recovery process
- Procedures should exist to destroy old backup media
- Physical controls should be in place at onsite and offsite storage locations

Backups - Control

Backups are performed on a periodic basis as per automated schedule. These could be tape backups or replication to disk. Data is stored offsite either on tape or replication to other facility.
Business Continuity/Disaster Recovery

- Disaster recovery plan should be documented, updated and tested
- Management should identify, analyze, and prioritize mission-critical functions based on: Criticality
- Scope and consequences of disruption
- Survivability (time-sensitivity)
- Coordination requirements with other units or external partners
- Facilities, infrastructure, and IT support requirements.

Top Mistakes Companies Make in DR

- Inadequate planning: Have you identified all critical systems, and do you have detailed plans to recover them to the current day?
- Failure to bring the business into the planning and testing of your recovery efforts
- Failure to gain support from senior-level managers. The largest problems here are:
  - Not demonstrating the level of effort required for full recovery
  - Not conducting a business impact analysis and addressing all gaps in your recovery model
  - Not building adequate recovery plans that outline your recovery time objective, critical systems and applications, vital documents needed by the business, and business functions by building plans for operational activities to be continued after a disaster
  - Not having proper funding that will allow for a minimum of semiannual testing
Initial Business Process Owner Interview

- You are interviewing the business process owner in a process that you audit every two years. You can ask **up Yes/No questions** to the process owner to get a preliminary determination of risk – make a list of those questions.
Questions

- Significant change to people/process/systems?
- Do you periodically review access to your systems?
- Have you experienced significant downtime?
- Are there any known issues for the system?
- Any other audits that have occurred and results?
- Change in integration/flow of data?
- Has the system demand change?
- Do you policies/procedures and are they updated?
- Do you receive/review/understand SOC reports?
- Do you have any systems/databases not managed by IT?
- Penetration Testing
- DR/BCP Tested?

- Is the system of record off the shelf or internally developed?
- If off the shelf, has the system been customized?
- If off the shelf, is the system currently in regards to updates and upgrades?
- When you run a report from the system, are you confident in the accuracy of the report?
- Has the audit log been turned off for any key systems?
- Any changes in external environment? What have you done?
- Change in third parties/vendors
- Are there ways (in your opinion) to utilize the system to make the process more efficient/effective?
- Is there a risk assessment of the system of record performed?
- Have there been any data breaches over the period under review?
- Any pending litigation?

Who Owns General Controls?

- Business Management
- Information Technology
- Both
Segregation of Duties

Group Discussion

Are SoD’s an IT or Business Control?
What is Segregation of Duties (SOD)?

- Control activity where different portions of a transaction or set of transactions are divided among several people to reduce risk of unintentional errors and intentional fraud (i.e. misappropriation of assets, identity theft, etc.)

- Proper segregation of duties reduces the risk of fraud if users assigned access consistent with job responsibilities

- Segregation of duties is “preventative” in nature

General Categories of Duties

- Four general categories of duties are examined for segregation of duties:
  - **Authorization** (approval of a transaction)
  - **Custody** (physical or logical ownership/access to an asset or transaction)
  - **Record keeping** (accounting for)
  - **Reconciliation and monitoring** (detective review of a transaction)
Understand Segregation of Duties

• In an ideal environment, different employees would perform each of the four major functions. No one person should control two or more of these responsibilities.

• The more negotiable the asset, the greater the need for proper segregation of duties, especially when dealing with cash, negotiable checks and inventories.

• The need for segregation of duties applies to both systematic and manual process environments.

**GROUP EXERCISE**

**WHAT IS THE DIFFERENCE BETWEEN ROLE-BASED AND INDIVIDUAL SECURITY MODELS?**
Security Models: Role-Based

- Roles are created for various job functions
- Permissions to perform certain operations are assigned to specific roles
- Employees are assigned roles and acquire computer permissions to perform particular system functions through those roles
- Since users are not assigned permissions directly, management of individual user rights becomes a matter of simply assigning appropriate roles to the user’s account

Three primary rules are defined:

1. **Role assignment**: Subject can exercise a permission only if the subject has selected or been assigned a role.
2. **Role authorization**: Subject’s active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
3. **Permission authorization**: Subject can exercise a permission only if the permission is authorized for the subject’s active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

Security Models: Individualized

- Roles are **NOT** created for various job functions
- Permissions to perform certain operations are **NOT** assigned to specific roles but assigned to users that need them/ad hoc
- Users **are** assigned permissions directly so management of individual user rights is time-consuming
Mitigating and Compensating Controls

- If duties cannot be fully segregated, mitigating or compensating controls must be established.
- Mitigating or compensating controls are additional procedures designed to reduce the risk of errors or irregularities (fraud):
  - For instance, if the record keeper also performs a reconciliation process, a detailed review of the reconciliation could be performed and documented by a supervisor to provide additional control over the assignment of incompatible functions.
The Most Efficient Way to Test SoD?

Testing SoD

• Make sure the provisioning/de-provisioning process is sound
• System Software (Add-ons)
• Access review
  – Establishment of access from onset
  – User Reports have to be readable
  – Users have to “own” this responsibility
• Screen-prints/Attempts to use access
AUDITING APPLICATION SYSTEMS

GROUP DISCUSSION
ARE SOD’S AN IT OR BUSINESS CONTROL?
Application Controls – Layman’s Terms

- Do not think of Application Controls as something “IT”
- Application controls, at their core, have nothing to do with IT
- Business Rules set up in a system
- Most likely would exist in some form regardless if a system is used

Defining Application Controls

- Application controls are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting.
- Objective of application controls is to ensure that:
  - Input data is accurate, complete, authorized, and correct.
  - Data is processed as intended in an acceptable time period.
  - Data stored is accurate and complete.
  - Outputs are accurate and complete.
  - A record is maintained to track the process of data from input to storage and to the eventual output
Benefits of Application Controls

- Reliability
  - Reduces likelihood of errors due to manual intervention
- Benchmarking
  - Reliance on IT general controls can lead to concluding the application controls are effective year to year without re-testing
- Time and cost savings
  - Typically application controls take less time to test and only require testing once as long as the IT general controls are effective

SOURCE: IIA GTAG 8 Auditing Application Controls

Types of Application Controls

- Input Controls – These controls are used mainly to check the integrity of data entered into a business application, whether the data is entered directly by staff, remotely by a business partner, or through a Web-enabled application or interface. Data input is checked to ensure that it remains within specified parameters.
- Processing Controls – These controls provide an automated means to ensure processing is complete, accurate, and authorized.
- Output Controls – These controls address what is done with the data and should compare output results with the intended result by checking the output against the input.
- Integrity Controls – These controls monitor data being processed and in storage to ensure it remains consistent and correct.
- Management Trail – Processing history controls, often referred to as an audit trail, enables management to identify the transactions and events they record by tracking transactions from their source to their output and by tracing backward. These controls also monitor the effectiveness of other controls and identify errors as close as possible to their sources.

SOURCE: IIA GTAG 8 Auditing Application Controls
### Common Application Controls

Application controls are commonly grouped into five categories:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Checks (Input)</td>
<td>Limit risk of inappropriate input, processing or output of data due to field format</td>
<td>• Required fields&lt;br&gt;• Specific data format on input</td>
</tr>
<tr>
<td>Validations (Input)</td>
<td>Limit risk of inappropriate input, processing, or output of data due to the confirmation of a test.</td>
<td>• Three-way match&lt;br&gt;• Tolerance limits</td>
</tr>
<tr>
<td>Calculations (Processing)</td>
<td>Ensure that a computation is occurring accurately.</td>
<td>• Accounts receivable aging&lt;br&gt;• Pricing Calculations</td>
</tr>
<tr>
<td>Interface Balancing (Processing)</td>
<td>Limit risk of inappropriate input, processing or output of data being exchanged from one application to another.</td>
<td>• Transfer of data between systems&lt;br&gt;• Error reporting during batch run</td>
</tr>
<tr>
<td>Authorizations</td>
<td>Limit the risk of inappropriate input, processing or output of key financial data due to unauthorized access to key financial functions or data. Includes:&lt;br&gt;• Segregation of incompatible duties&lt;br&gt;• Authorization checks, limits and hierarchies</td>
<td>• Approval to post journal entries&lt;br&gt;• Two approvals for check printing</td>
</tr>
</tbody>
</table>

### Application Control Activities – Common Examples

- Determining whether sales orders are processed within the parameters of customer credit limits
- Making sure goods and services are only procured with an approved purchase order
- Monitoring for segregation of duties based on defined job responsibilities
- Identifying that received goods are accrued upon receipt
- Ensuring fixed-asset depreciation is recorded accurately in the appropriate accounting period
- Determining whether there is a three-way match among the purchase order, receiver, and vendor invoice
Input Controls

- Designed to provide reasonable assurance that data received for computer processing is appropriately authorized and converted into a machine-sensible form and that data is not lost, suppressed, added, duplicated, or improperly changed.
- Include data checks and validation procedures such as check digits, record counts, hash totals, and batch financial totals.
- Computerized edit routines — which are designed to detect data errors — include valid character tests, missing data tests, sequence tests, and limit or reasonableness tests.

Input Controls - Examples

- Input data validation checks
  - Limit test: test of reasonableness
  - Validity test: comparison against master files
  - Self-checking number: check for accuracy
- Batch integrity of online or database systems
- Input controls for batch processing
  - Item count – check for completeness
  - Control total – check for accuracy
  - Hash total – can be a sum of all order numbers
- Error reporting and handling
Processing Controls

- Designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting.
- Many processing controls are the same as the input controls, particularly for online or real-time processing systems, but are used during the processing phases.
- Examples:
  - Run-to-Run Totals
  - Control-Total Reports
  - File and Operator Controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests.

Output Controls

- Designed to provide reasonable assurance that processing results are accurate and distributed to authorized personnel only.
- Control totals produced as output during processing should be compared and reconciled to input and run-to-run control totals produced during processing.
- Computer-generated change reports for master files should be compared to original source documents to assure information is correct.
GROUP EXERCISE

Discuss and determine what is the most efficient & effective approach to testing an application control (ex. depreciation expense calculation of fixed assets)
Auditing Application Systems Approach

- Meet with business process owners to:
  - Understand business function that application supports
  - Identify responsible personnel (owner, superusers, application administrators, security administrators)
  - Map out process (if appropriate)
  - Identify application inputs, outputs, interfaces
  - Identify application controls and manual controls
  - Identify existing documentation
  - Highlight any issues or concerns
- Identify key risks and test key controls
  - All key controls should be driven by risk
- Same approach to auditing in general

Testing Application Controls

- Are application controls working?
- Substantive testing
- Information technology general controls review
- Ways to test:
  - Inspection of system configurations
  - Inspection or re-performance of reconciliations with supporting details
  - Re-Performance of the control activity using system data
  - Inspection of user access listings
  - Re-Performance of the control activity in a test environment
Benchmarking

- If it has not changed, do we need to retest annually?
- Defined through SOX testing (PCAOB)
- Factors to consider:
  1. Effectiveness of the controls over the IT control environment i.e. the controls over application changes, application purchases and overall computer operations.
  2. In case of changes in softwares/applications during the period of audit, how well does the auditor understand the changes to the applications and the resulting comfort factor.
  3. The nature and timing of other related tests for application and business related controls.
  4. Last but not the least, in case there are errors relating to the application controls that were benchmarked, what are the resulting consequences of errors.

Benchmarking Questions to Ask

- Have there been changes in the risk level associated with the business process and the application control from when it was originally benchmarked (i.e., does the business process provide substantially greater risk to financial, operational, or regulatory compliance than when the application control was originally benchmarked)?
- Are ITGCs operating effectively, including logical access, change management, systems development, acquisition, and computer operation controls?
- Can the auditor gain a complete understanding of the effects of changes, if any, on the applications, databases, or supporting technology that contain the application controls?
- Were changes implemented to the business process relying on the application control that could impact the design of the control or its effectiveness?
Nature, Timing, & Extent of Testing

• Nature of Testing will depend on if the control is embedded or configurable
• Configurable application control:
  – Inspect configuration of each significant transaction type (can be performed via walkthrough also)
  – Consider override capability
    • Other menu and record level functionality
  – Generally can be viewed within a configuration screen or via a system generated report
• Embedded application control:
  – Walkthrough of each significant transaction type
  – Consider override capability
  – Positive and negative aspects of control
• Identify any dependencies on other controls
Electronic Audit Evidence (EAE)

- Data generated by or processed through an application, spreadsheet and/or end user computing solution, be it in electronic or printed form, used to support audit procedures
  - Data used for analytical and data analysis procedures
  - Data supporting the performance of internal controls, including key performance indicators
  - Data that represents substantive audit evidence to support assertions for significant accounts
    - Aging list of accounts receivable
    - Spreadsheet specifying hedging transactions
    - List of gains and losses from sales of marketable securities

EAE Reliance

- Establishing a basis for relying on electronic data includes:
  - Determining the source of the electronic data (which application produces the data)
  - Determining, through identification and evaluation of internal controls or through substantive procedures, whether the electronic data is complete and accurate
Testing Report Logic

- Evaluate to what extent the logic of the report or query guarantees that the report is **complete** and **accurate**
- Test procedures are determined based on risk assessment:
  - What is the origin of the software?
  - Is the report used frequently by the client?
  - Can the client influence the content of the report?
  - Can the client edit the output of the report?
  - Are we sure the data in the underlying database is complete and accurate?
- Test procedures are based on controls testing or substantive testing

Data Integrity/Validation

- How do we verify the completeness of a report?
  - Run the report ourselves
  - Walkthrough
  - Observation
- What type of questions should we ask?
- What is the true source of information?
- How does change management factor in?
Walkthrough Questions

• It is not the first question, it is usually the next question
  – Interfaces
  – Reports
  – When discussing controls, make sure to ask if the control:
    • Is in the system?
    • If it is manual, could it be done in the system?
  – Include SME with Process Owner in interviews?
GOLD NUGGET - ITFNITA

- Understanding the Basics of IT Auditing make a general auditor much more capable of handling understanding a multitude of risks
- Cannot wholly audit an area without considering IT risks
- Understand how general controls and application controls work together/play off each other
- Application controls are not IT – they are business rules established in the system