IT AUDITING FOR NON-IT AUDITORS

Danny M. Goldberg, Founder

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

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

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

### All GTAG’s:

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing Application Controls (Previously GTAG 4)</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><em>NEW</em> 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 10)</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 2009</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>Information Technology Risk and Controls, 2nd Edition (Previously GTAG 1)</td>
<td>March 2012</td>
</tr>
<tr>
<td>Management of IT Auditing, 2nd Edition (Previously GTAG 4)</td>
<td>January 2013</td>
</tr>
</tbody>
</table>
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

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?
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
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)
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
IT Controls Overview

General Computer Controls

Governance Controls
Management Controls
Technical Controls

Source: IA GIAG-1
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**

- **Critical Areas**
  - 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

Group Discussion

DE-PROVISIONING: WHO SHOULD BE ULTIMATELY ACCOUNTABLE?

Human Resources
Information Technology
Hiring Manager
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?

Group Discussion

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

**Control Objectives**
- **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.

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

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

DATABASE IMPLEMENTATION & SUPPORT

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).

**Control Objectives**

**Topics Covered**

**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

- Data architecture
- Database implementation
- Database administration & monitoring
- Database maintenance & modifications
**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.

**Control Objectives**

- New network and communication software is appropriately implemented and functions properly and implemented in a timely manner.
- Modifications to existing network and communications software are properly implemented and function as expected.

**Value Add Areas**

- New network and communication software is acquired consistent with management’s intentions.
- Network and communication software is maintainable and supportable.

**Topics Covered**

- Network & communication software:
  - Acquisition & approval
  - Implementation & testing
  - Support
  - Maintenance
  - Performance monitoring
  - Documentation
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></td>
</tr>
<tr>
<td>• All necessary modifications to system software are implemented timely</td>
<td></td>
</tr>
<tr>
<td>• Modifications to system software are properly implemented and function as intended</td>
<td></td>
</tr>
<tr>
<td><strong>Value Add Areas</strong></td>
<td>• Installation, configuration and updates/patches</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
Informations 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

- 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

Critical Areas

- 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

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Job</th>
<th>Retention</th>
<th>Time</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>BHMSGL</td>
<td>Monthly</td>
<td>3:00AM</td>
<td>2</td>
</tr>
<tr>
<td>Backup</td>
<td>BHMSGL</td>
<td>Weekly</td>
<td>5:00AM</td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>BHMSGL</td>
<td>Daily</td>
<td>3:00AM</td>
<td>SubMoTuWeTh</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSGL</td>
<td>Monthly</td>
<td>6:00PM</td>
<td>1</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSGL</td>
<td>Weekly</td>
<td>6:00PM</td>
<td>Fr</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSGL</td>
<td>Daily</td>
<td>6:00PM</td>
<td>SubMoTuWeTh</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSYS</td>
<td>Monthly</td>
<td>8:00PM</td>
<td>1</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSYS</td>
<td>Weekly</td>
<td>8:00PM</td>
<td>Fr</td>
</tr>
<tr>
<td>Backup</td>
<td>ATLSYS</td>
<td>Daily</td>
<td>8:00PM</td>
<td>SubMoTuWeTh</td>
</tr>
<tr>
<td>Backup</td>
<td>BM_system</td>
<td>Daily</td>
<td>6:00AM</td>
<td>MoTuWeTh</td>
</tr>
<tr>
<td>Backup</td>
<td>BM_system</td>
<td>Weekly</td>
<td>6:00AM</td>
<td>Fr</td>
</tr>
<tr>
<td>Backup</td>
<td>BM_system</td>
<td>Monthly</td>
<td>8:00AM</td>
<td>1</td>
</tr>
</tbody>
</table>
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?
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.

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

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