Techniques for Testing IT General Controls

Stephen E. Coury, CISA
Chief Information Security Officer
City & County of Denver

Mountain and Plains Intergovernmental Audit Forum
August 23, 2013

DENVER TECHNOLOGY SERVICES

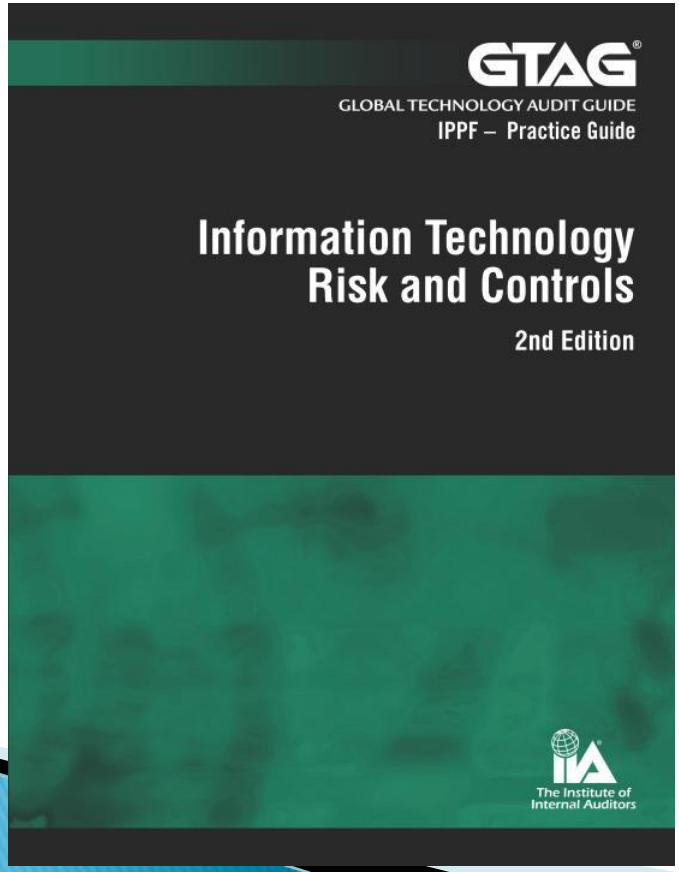
Session Objectives

- Overview of ITGCs
- Standards
- Frameworks
- Resources
- Case Studies
- Evaluation of your ITGC review capability

DENVER
TECHNOLOGY SERVICES

Overview of ITGCs

- Definition of Information Technology General Controls (ITGCs)



ITGC defined, GTAG 1, p. 4

IT controls provide for assurance related to the reliability of information and information services. IT controls help mitigate the risks associated with an organization's use of technology. They range from corporate policies to their physical implementation within coded instructions; from physical access protection through the ability to trace actions and transactions to responsible individuals; and from automatic edits to reasonability analyses for large bodies of data.

DENVER TECHNOLOGY SERVICES

ITGCs in Simpler Terms

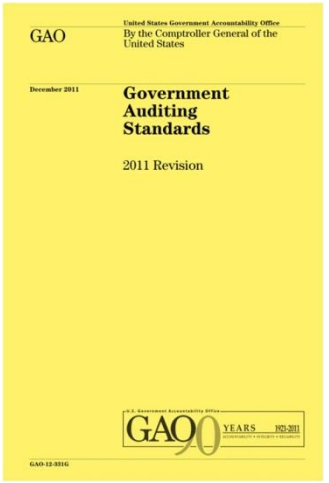
Information Technology (IT) general controls are those "behind the scenes" processes and procedures, both manual and automated, that serve as a foundation for the proper operation and security of information systems. General controls are implemented at the policy, physical, and technical levels. An example of a policy control is requiring all persons to be accountable for their access to systems. This is implemented through a physical control that restricts and logs access to the data center by way of a card reader. A technical control supporting accountability is the use of user IDs and passwords to gain access to systems.

General controls are also implemented through processes and procedures, such as one called provisioning, which includes the assignment of user accounts, the granting of access permissions, and the removal of access when personnel transfer or terminate their employment with the City. Other general controls include the physical security of the data center and its backup and recovery procedures.

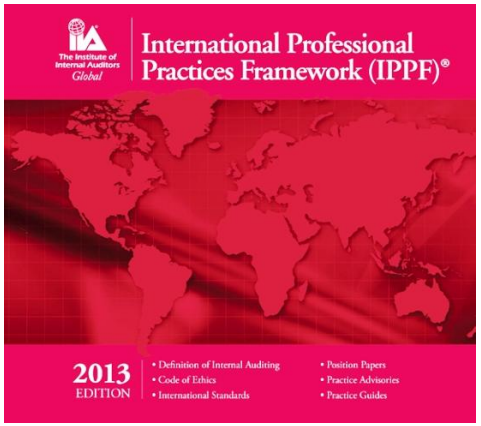
Differing Views of ITGCs

- Narrower Views of ITGCs
  - SOX (impact on financials, heavy on change control, not CoB)
  - PCI (impact on SSI, not backup)
  - CJIS (impact on CJI, not backup)

Standards



- Professional
- Formal
  - Generally Accepted Government Audit Standards (GAGAS)
  - International Professional Practices Framework (IPPF)
- Informal
- No standards



DENVER TECHNOLOGY SERVICES

Formal Adoption of Standards

Denver, Colorado, Code of Ordinances >> TITLE I - HOME RULE >> PART 2. - POWERS AND DUTIES >>

PART 2. - POWERS AND DUTIES

§ 5.2.1 - General powers and duties of Auditor.

(A) *Internal Auditing.* The Auditor shall conduct financial and performance audits of the City and County and its departments and agencies in accordance with generally accepted governmental auditing standards promulgated by the United States Comptroller General. The Auditor shall conduct audits of individual financial transactions, contracts and franchises of the City and County; and shall generally audit the financial and accounting systems and procedures administered by the Manager of Finance and other departments and agencies of the City and County, including records systems, revenue identification and accounting, and payment practices, for compliance with generally accepted accounting principles, best financial management practices, and any applicable laws and regulations governing the financial practices of the City and County. The results of any audit shall be reported by the Auditor to the Audit Committee as provided in Section 5.2.2

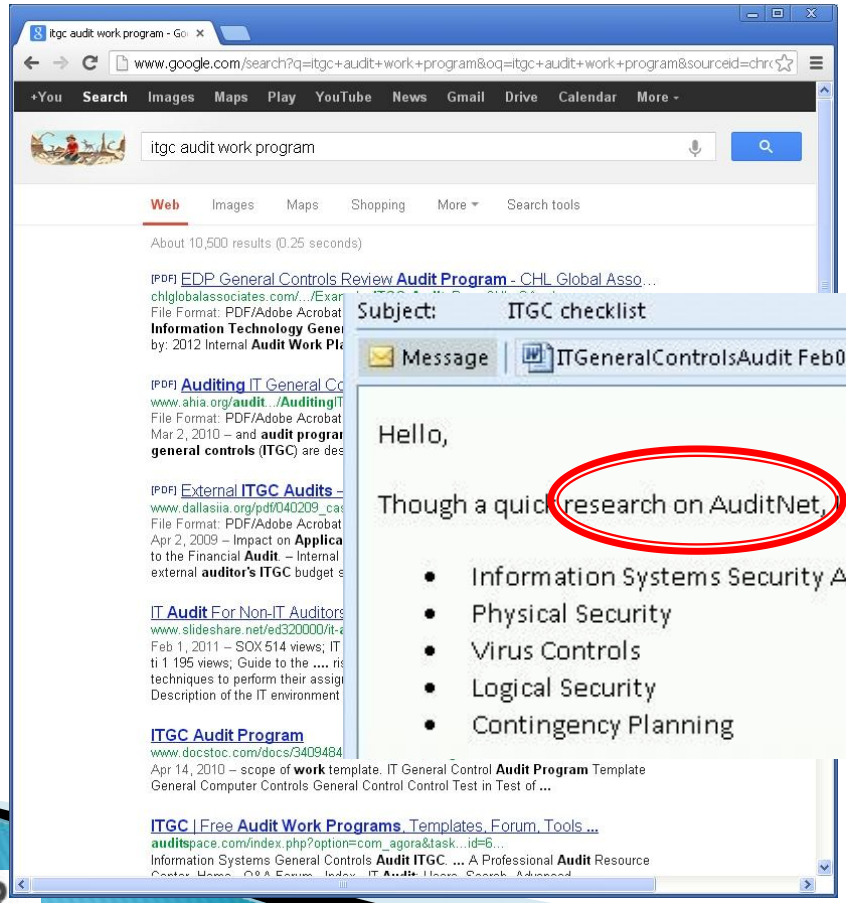
DENVER TECHNOLOGY SERVICES

Frameworks

- Federal Information Systems Control Audit Manual (FISCAM)
- Guide to Assessment of IT Risk (GAIT)
- Industry specific
  - Criminal Justice Information Services (CJIS)
  - Federal Financial Institutions Examination Council (FFIEC)
  - Payment Card Industry Data Security Standard (PCI/DSS)

Many Resources are Available

- Google and others will bring you a bunch



Be Careful!

303. Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.

Results:

_____

_____

_____

DENVER TECHNOLOGY SERVICES

Reputable Sources

- Steps will have criteria defined in framework (FISCAM)

General Controls				
Access Controls				
Critical element and control activity	**Control techniques**	**Audit procedures**	**Entitywide level conclusion/ reference**	**Sy co re**
AC-3.1. User accounts are appropriately controlled.	AC-3.1.8. Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters; review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.		

DENVER TECHNOLOGY SERVICES

Reputable Resources

Audit procedures based on clearly defined criteria

- Global Technology Audit Guides (GTAG)
- FISCAM Tables for Summarizing Work Performed in Evaluation and Testing General and Business Process Application Controls (Appendix II or TLTBS)

GTAGs can be found on IIA's site
https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx
FISCAM & Appendices can be found on GAO's site:
http://www.gao.gov/special.pubs/fiscam.html

DENVER TECHNOLOGY SERVICES

Case Studies

- Application Backup
- User Administration
- Equipment Inventories

DENVER
TECHNOLOGY SERVICES

Application Backup Case Study Backup Analysis Steps

- Gain an understanding of how backups run and how results are recorded
- Acquire data for analysis
- Analyze the data
- Summarize and present the results
- Confirm / Vet the conclusions

DENVER TECHNOLOGY SERVICES

User Administration Case Study Same Analysis Steps

- Gain an understanding of how users are provisioned (added and removed)
- Acquire data for analysis
- Analyze the data
- Summarize and present the results
- Confirm / Vet the conclusions

DENVER TECHNOLOGY SERVICES

Inventory Case Study

- Network equipment tested “book to floor” and “floor to book”
- Found 71% discrepancy rate
- Audit Committee asked what % would be expected or acceptable

DENVER TECHNOLOGY SERVICES