Information Technology (IT) General Controls Discussion

Technical Overview and Practical Audit Approach

December 14, 2015

Agenda

• Why focus on IT Internal Controls?
• What are the components of IT General Controls?
• What has changed?
• Where to go next.

Why Focus on Internal Controls?

• IT Security consists of the policies, procedures, controls and actions leading to the protection of an organization’s Information System assets and data.

• Techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization.1

---

1 Webopedia.com.
Why Focus on Internal Controls?

- IT Controls involve multiple “pieces” of IT architecture. A subset of those items includes the following:
  - Computer hardware and how its configured
  - Computer network software
  - Training of employees in proper use of technology
  - “Operating” software (Excel, Financials, Interfaces)
  - Monitoring

What are the Components of IT General Controls?

- Major Categories Include:
  - General Overview and Entity Level
  - Computer Operations
  - Logical Access
  - Backup and Recovery
  - Vendor Compliance
  - Physical & Environmental Security
  - Vulnerability Management

What are the Components of IT General Controls?

IT Controls can be broken into the following sub-categories

- General (General)
- Internal Compliance (General)
- Authentication (Logical Access)
- Business Continuity (Backup & Recovery)
- Firewalls, Routers and Servers (Computer Operations)
- Intrusion Detection System (“IDS”) (Vulnerability Management)
- Networks (Computer Operations)
- Penetration Testing (Vulnerability Management)
- Remote access (Logical Access)
- Security Program (Computer Operations/General)
- Vendor Oversight (Vendor Compliance)
- Virus Protection (Vulnerability Management)
- Wireless Networks (Computer Operations)
- Physical Security (Physical & Environmental Security)
- Environmental Security (Physical & Environmental Security)
What are the Components of IT General Controls?

- **General** – this area covers the governance policies and procedures the organization has in place for administering IT Security.

- **Authentication** – this area covers the mechanisms in place for users of technology to gain access and the levels of access granted to them.

- **Internal Compliance (Audit)** - a high-level assessment or evaluation of the organization's IT components, controls, operations or program compliance.
What are the Components of IT General Controls?

- Business Continuity – assessments in this area cover the organization’s plans and readiness for handling interruptions to its operations.

- Firewalls, Routers and Servers – this area covers the major hardware components of any organization’s network for proper setup and configuration.

- Intrusion Detection Systems – these components incorporate the prevention and determination of how vulnerable your network is to third-party hackers.
**What are the Components of IT General Controls?**

- **Networks** – this area encompasses the examination of the software components of the organization’s information technology systems and whether they are configured properly.

- **Penetration Testing** – these evaluations are designed to purposely “hack” into the organization’s information technology systems.

- **Remote Access** – this area examines how the organization has designed its information technology systems to permit employees to access the systems when away from the office.
What are the Components of IT General Controls?

- Security Program – this is an area that is general in nature. It covers the components of your IT security environment and how they are managed.

  IT security says...

- Vendor Oversight – audits of vendors typically encompass the largest providers of services to your organization and focus on the administration of internal controls in the vendor’s operations.

- Virus Protection – for an organization to prevent and detect unwanted disruptions to its computing environment, assessments in this area concentrate on the management of the organization’s systems to protect itself from malicious external threats.
Wireless Networks – these components make up a portion of the configuration and location of untethered connections in your information technology system.

Physical Security – this area is concerned with your office and data center’s protection from unauthorized personnel.

Environmental Security – these evaluations focus on the safeguards in place to protect your IT hardware.
What has Changed?

- Change Management – traditional methods of developing software and applications has changed dramatically in the last five years.

What has Changed?

- Backup and Recovery – historical methods of maintaining data have almost disappeared. With “real-time” capabilities, back-ups don’t have to be retrieved.

What has Changed?

- Third Party Vendors – the use of third-party organizations has proliferated and evaluations of these vendors needs to be part of any evaluation.
Where to go Next?

- What do you do now?
  - Schedule a meeting with your IT Director and ask what types of audits have been performed in the past and what issues were raised and how were they managed.
  - Ask a lot of questions – the organization may look different now than even 6 months ago.
  - Align the answers from bullet #1 with the risks you and your auditors have identified are the most critical to the organization.
  - Revisit the alignment and risks from bullet #2 in 6-9 months to determine their relevancy.

Information Technology General Controls Discussion

Torpey White, CPA/CITP, CISA, CGEIT, CGMA
Partner, Risk Advisory Services
Wipfli LLP
twhite@wipfli.com
(610) 368-7337

Thank You