IT Audit Process

Prof. Mike Romeu

September 2, 2015
Corporate Governance

“The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.” (ISACA Glossary).

Corporate governance helps to:
- Set Strategic Direction
- Ensures goals and objectives are achievable
- Risks are properly addressed
- Resources (People, Time, Monies) are properly utilized
Governance

Shareholders

- External Director
- CFO
- CEO
- Legal Counsel
- External Director

Internal Directors

- Human Resources
- Operations
- Sales and Marketing
- Information Technology
- Finance
Audit Charter

• **GS 1001 Audit Charter**
  1001.1 The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.
  1001.2 The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.

• **GG 2001 Audit Charter**
  The Audit Charter communicates:
  • Purpose of the audit function (Scope) (2.2.2)
  • Responsibility of the audit function (2.2.3)
  • Authority of the audit function (2.2.4)
  • Accountability of the audit function (2.2.5)
Organizational Independence

• **GS 1002 Organizational Independence**
  1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.

• **GG 2002 Organizational Independence**
  • Conceptual Framework that requires professional Judgement
  • Reporting Structure
  • Consultation
  • Impairment and non-audit services
  • Reporting – full disclosure
Professional Independence

• **GS 1003 Professional Independence**
  1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

• **GG 2003 Professional Independence**
  • Conceptual Framework that requires professional Judgement
  • Reporting Structure
  • Consultation
  • Impairment and non-audit services
  • Reporting – full disclosure
Due Professional Care

• Diligence that a person, who possesses a special skill, would exercise under a given set of circumstances.

• GS 1005 Due Professional Care
  • Standards Statement 1005.1 – “IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagement.”

• GG 2005 Due Professional Care
  • Professional Skepticism and Competence
  • Professional Character
  • Reasonable assurance
  • Reasonable expectations
The Foundations of Due Professional Care
by Frederick Gallegos

• Peer Review
• Technical Competence – Training/Shadowing
• Auditor Conduct - “Gotcha” mentality, Independence, Observations AND recommendations
• Judgment – Experience driven
• Business Knowledge
  • Knowing your clients environment
  • Negotiation and communication skills
• Certifications and Standards

Bottom Line: Clients receive a high-quality review
✓ Poor Service
✓ Data Leakage
✓ Inadequate Support
✓ Lack of Assurance

✓ Non-compliance with regulations
✓ Non-compliance with software licenses

✓ Unsupported applications
✓ Critical system failures
✓ Unable to handle load
✓ Configuration issues

✓ Damage to servers
✓ Inflexible IT architecture
✓ Theft
✓Obsolete technology

✓ Disclosure of sensitive data
✓ Corruption of data
✓ Unauthorized access
✓ Failure to mine information

✓ Operator errors during backup or maintenance
✓ Breakdown of operational processes

✓ Budget overruns
✓ Significant delays
✓ Poor quality of deliverables
✓ Ineffective change control

✓ Intrusion of malware
✓ Virus attacks
✓ Web site attacks
✓ Poor patch management

✓ Utilities Failures
✓ Natural Disasters
✓ Labor Strikes
✓ Environmental Sanctions

✓ Loss of key IT resources
✓ Inability to recruit IT staff
✓ Skills mismatch
✓ Lack of business knowledge