# El proceso de auditoría del sistema de información (IS) en un sistema bancario: estudios del caso

Jahangir Khan[1] y el Dr. Imran Amin[2]
SZABIST
Karachi, PaquistÆn

***Extracto: El Proceso de Auditoría del Sistema de información define el procedimiento total de la planificación; la conducción de auditorías de ELLO ambiente y ESTO proceso de negocio basado. La auditoría del sistema de información tiene pasos diferentes para cubrir el ciclo de auditoría entero tal que ES la Planificación de Auditoría, la conducción ES la auditoría sobre la base de fases de auditoría es decir definiendo el sujeto de auditoría, el objetivo de auditoría, el alcance de auditoría, planificación de Preauditoría, pruebas de auditoría y recopilación de datos, evaluando la prueba, la comunicación con la dirección auditee y la preparación del informe de auditoría [S. Anantha Sayana].***

*Para conducir un eficaz ES la auditoría, un ES el Auditor tiene que tener un entendimiento bueno de estÆndares de auditoría profesionales, políticas, procedimientos y pautas como el Objetivo de Control para la información & Tecnología relacionada (COBIT), Information Systems Audit & Control Association (ISACA), ESTO Instituto del Gobierno (ITGI), ISO 27001 etc. Estos estÆndares definen las medidas de control que deberían ser obedecidas por el negocio para prevenir su ESTO procesos de negocio basados de amenazas diferentes y actividades de delito ciber [Lance M. Turcato].*

***Palabras clave: auditoría del sistema de información (IS), estatuto de auditoría, comitØ de cuentas pæblicas del consejo, ES proceso de auditoría, ES fases de auditoria, mandos internos, ES mandos de auditoría***

## 1. INTRODUCCIÓN

Actualmente, las organizaciones son muy dependientes de la Tecnología de la información para su proceso de negocio cotidiano. Aproximadamente todas las transacciones comerciales son funcionan a travØs de medios digitales, que aumentan el riesgo comercial y financiero y organización muestran su mÆs preocupación para reducir y mitigar estas amenazas [David etal 2006].

Como otros sectores financieros, la banca es tambiØn muy dependientes en la operación de tecnología de la información. Por lo tanto es necesario para bancos tener un departamento de la tecnología de la información, que puede manejar eficazmente las actividades operacionales y financieras basadas en el medio digital. Actualmente, el sector bancario que provee diferente servicios en línea como operaciones del ATM, transferencia del fondo en Línea, banca móvil, crØdito & operaciones de la tarjeta de dØbito etc. Estas todas las actividades del dinero plÆsticas funcionan a travØs de recursos del sistema de información disponibles en el sector bancario y no hay participación del dinero efectivo físico. Por lo tanto, el banco ESTO el departamento debería asegurar que el sistema de información del banco pueda proteger y salvaguardar el interØs del banco [Tommie W. Singleton].

Para evaluación y evaluación de ESTO los procesos de negocio basados, los órganos reguladores así como los estÆndares profesionales, Ønfasis para desarrollar un departamento de auditoría interna dentro de la organización, que periódicamente examinan y la organización de culos ESTO proceso de negocio basado y sistema de aplicación que corre dentro de la organización. El departamento de auditoría interna entonces tiene que desarrollar su estatuto de auditoría interna para sus políticas, procedimientos y pautas para sus auditores internos. El Estatuto de auditoría define el papel, responsabilidades, alcance, autoridad y responsabilidad de la función de auditoría. Es por lo tanto, necesario para una organización establecer y poner en prÆctica su propio Estatuto de Auditoría, que describe el objetivo y la misión de la función de auditoría [Louis Braiotta, Hijo].

## 2. INFORMACIÓN PREVIA

### 2.1 Revisión

La revisión es un proceso para conducir, tasar y evaluar entidades comerciales. Revisar es el proceso a travØs del cual una entidad como organización, empresas, empleados, sistema, el proyecto, producto etc., puede ser evalœan y sobre la base de esta evaluación las discrepancias/irregularidades pueden ser observadas. El objetivo principal de conducir la auditoría es mejorar las actividades operacionales de la entidad de auditoría y levantar las escapatorias contenidas en el proceso de negocio de ese sistema [Gerald Vinten].

### 2.2 Clasificación de revisión

La revisión puede ser clasificada en partes diferentes, que estÆ basado en la esfera de la entidad de auditoría y que Æreas ser cubierto en la revisión. Por lo tanto, el Auditor puede planear el

auditoría segœn su categoría [ISACA, Manual de CISA Review]:

Hay categorías diferentes de la revisión estÆn disponibles tal como Financiero Revisión, Operacional Revisión, Revisión de la dirección / Revisión Administrativa, ES Auditoría, Integrada Auditoría, auditoría especializada & auditoría forense [ISACA, CISA Examine el manual].

**3. REVISIÓN DEL SISTEMA DE INFORMACIÓN (IS)**

Los culos de Auditoría del sistema de información las Æreas bajo la esfera de Tecnología de la información es decir aguantan la Infraestructura de la Red & el Sistema de información de una organización son bastante capaces a salvaguardias la información y activos comerciales y proporcionan la seguridad del sistema de la información confiable, teniendo la provisión de la integridad de datos y proporcionan el aseguramiento de la disponibilidad de información por el funcionamiento liso del proceso de negocio [David etal].

El objetivo de ES la Auditoría, especialmente realizada por los auditores internos, debe definir las escapatorias, que pueden se hace la causa de cualquier actividad fraudulenta a travØs de recursos del ordenador, por tanto el ES Auditores debería conducir auditoría para mejora de tales mandos [S. Anantha Sayana].

Sistema de información profesional diferente Revisión el estÆndar ha sido desarrollado, que proporcionan pautas a travØs de las cuales los mandos principales de la actividad económica pueden ser observados, como Auditoría de Sistemas de información & Control Asociación (ISACA), proporciona el estÆndar, que trata con las políticas, marco, mandos y calidad de Æreas comerciales en tØrmino de ELLO marco. Por lo tanto, es necesario para un ES el auditor, para tener un conocimiento cuidadoso de estos estÆndares y analizan una auditoría en tØrminos de tiempo estas políticas, marco, los mandos de auditoría son correctamente describen y puesto en prÆctica dentro de la organización para evitar cualquier anormalidad [ISACA, Manual de CISA Review].

**4. ES TAREA DE AUDITOR˝A**

Lo siguiente ES la tarea de Auditoría debería ser seguido de la dirección de Auditoría [David L. Cannon, Timothy S. Bergmann, Brady Pamplin] [ISACA, Manual de CISA Review]:

Conforme a los estÆndares de auditoría, pautas y procedimientos; una estrategia de auditoría basada en el riesgo debería ser desarrollan y ponen en prÆctica para el Banco.

Para el aseguramiento razonable, que ESTO y el negocio/activo financiero de un Banco son salvan y bien protegido, un plan de auditoría debería ser se desarrollan.

Para encontrar el plan de auditoría, la conducta ES la Auditoría de varias entidades de un Banco, conforme al ES estÆndares de auditoría, pautas y procedimientos.

Siempre comuníquese con accionistas clave del negocio y comunique cuestiones próximas, riesgo posible y revise resultados.

La gestión del riesgo y la estrategia del control de riesgo deberían ser desarrollan y ponen en prÆctica dentro del Banco.

**5. DECLARACIÓN DE CONOCIMIENTO DE ES AUDITOR˝A**

UN ES el Auditor debería tener el conocimiento siguiente para el entendimiento de masa para rebozar del ES Æreas de proceso de auditoría [David L. Cannon, Timothy S. Bergmann y Brady Pamplin]:

UN ES el auditor debería tener el conocimiento de EST` relacionado control y objetivo de control p.ej. COBIT.

UN ES el auditor debería saber las tØcnicas de recopilación de información y debería saber cómo conservar pruebas.

UN ES el auditor debería tener el conocimiento de ES estÆndares de auditoría, pautas, procedimiento y políticas.

UN ES el auditor debería tener el conocimiento de revisa tØcnicas y revisa prÆcticas.

UN ES el auditor debería tener el conocimiento de la evaluación de riesgos de auditoría.

UN ES el auditor debería saber que el procedimiento junta pruebas, que apoyarÆn la observación del auditor.

UN ES el auditor debería saber, cómo planear y manejar tØcnicas de auditoría y auditoría.

UN ES el auditor debería saber las tØcnicas de comunicación y reportaje.

## 6. CAPACIDAD DE ES AUDITORES

UN ES el auditor debería tener un conocimiento de los œltimos instrumentos de Auditoría y tØcnicas y debería tener la formación apropiada de utilizar estos instrumentos y recursos. La dirección de alto nivel debería proporcionar las instalaciones a sus auditores internos en cuanto al acceso y la realización de nuevas tØcnicas de auditoría y los auditores internos deberían tener un ambiente de prueba comercial relacionado, de modo que los auditores puedan usar estos recursos de averiguar las escapatorias en la existencia ESTO el sistema de una organización [ISACA, Manual de CISA Review].

UN ES el auditor debería tener el entendimiento de, cómo conducir y planear un ES la auditoría dentro del período de tiempo estipulado y debería tener la idea cómo cubrir la esfera total de la entidad de Auditoría. El entendimiento bueno del relacionado ES estÆndares de Auditoría, pautas, procedimiento y política p.ej. ISACA, COBIT etc., tambiØn son necesarios de un ES Auditores [Lance M. Turcato].

**7. ESTATUTO DE AUDITOR˝A**

El Estatuto de auditoría define el papel, responsabilidades, alcance, autoridad y responsabilidad de la función de auditoría. Es por lo tanto, necesario para una organización establecer y poner en prÆctica su propio Estatuto de Auditoría, que describe el objetivo y la misión de la función de auditoría. El estatuto de auditoría del Sistema de información normalmente se desarrollaba ya que la parte del estatuto de auditoría interna por lo tanto revisa el estatuto define el papel y las responsabilidades de todas las entidades de auditoría es decir auditoría interna y auditoría del sistema de información [Louis Braiotta, Hijo].

Detalladamente, la responsabilidad de la función de auditoría cubre la esfera grande del ES la Auditoría; por ejemplo la responsabilidad de la dirección incluye la declaración de la misión, el objetivo, el alcance y el objetivo, la independencia, la asociación con auditor externo, factor de Øxito, indicadores de rendimiento clave (KPIs) etc. [David L. Cannon, Timothy S. Bergmann, Brady Pamplin].

**8. ES PLANIFICACIÓN DE AUDITOR˝A**

**8.1. Corto plazo ES planificación de auditoría**

En la planificación de auditoría a corto plazo, una dirección de auditoría interna organizativa tiene que desarrollar un plan de auditoría propuesto al principio del aæo, que describen esto que cuestiones serÆn cubiertas durante el aæo. La selección de la asignación de auditoría para el aæo debería estar basada en las Æreas del riesgo principales, que pueden afectar seriamente las operaciones comerciales. TambiØn pueden dar la prioridad con las Æreas, que no ha sido la auditoría hasta ahora o período de auditoría pasado exceden mÆs de dos aæos [Sandra Senft, Frederick Gallegos].

**8.2. Largo plazo ES planificación de auditoría**

El plan de auditoría a largo plazo debería estar basado en la futura estrategia de la organización sobre la base de ELLO la infraestructura. El ES la dirección de Auditoría debería tener la información sobre los cambios principales que pueden ser puestos en prÆctica dentro de la organización ESTO infraestructura [Frederick Gallegos, Sandra Senft].

**8.3. Planificación de auditoría individual**

Al lado de la planificación de auditoría corta y a largo plazo, un equipo de auditoría del Sistema de información (IS) tambiØn tendría que planear la auditoría, asignada a ellos. En primer lugar, el ES el equipo de auditoría debería conseguir un entendimiento profundo de los procesos de negocio de la entidad de auditoría. Por ejemplo, si el equipo de auditoría que conduce la auditoría del sistema de información de un sistema de aplicación financiero, entonces tienen que tener el mejor entendimiento de que actividad económica ha estado realizando a travØs de este sistema [ISACA, Manual de CISA Review].

**9. FASE DE AUDITOR˝A DEL SISTEMA DE INFORMACIÓN (IS)**

La revisión del sistema de información (IS) tiene fases diferentes que tienen que ser cubiertas. Aquí, voy a describir Østos dividen en fases con dos estudios del caso realizados durante la preparación de este informe. La auditoría del sistema de información de dos centros de datos diferentes, Lahore & Karachi, de un banco comercial ha sido conducida durante 22

nd a 27 th Febrero de 2010 & 15th a 20 th Marzo de 2010, respectivamente. Por tanto cada fase tiene sido descrito aquí con los ejemplos de estudios del caso:

**9.1 Sujeto de auditoría**

La entidad que tiene que ser revisada. Cada organización tiene Æreas operacionales diferentes que pueden ser revisadas segœn la esfera comercial. El sujeto de auditoría define las Æreas que deberían ser la tapa durante el curso de auditoría [Andrew Hawker] [S. Anantha Sayana].

**Estudio del caso 1:**

Sujeto de auditoría: auditoría del sistema de información (IS) de centro de datos regional Lahore

**Estudio del caso 2:**

Sujeto de auditoría: auditoría del sistema de información (IS) de centro de datos regional Karachi

**9.2 Objetivo de auditoría**

El Objetivo de la Auditoría es conseguir el objetivo particular e identificar Æreas que tienen que ser mejoradas. El objetivo principal de la auditoría es reducir la posibilidad del riesgo comercial y analizar todas las Æreas comerciales sensibles. DespuØs de la identificación de las Æreas del riesgo principales, el auditor tiene que comprobar que el tiempo hizo falta que los mandos hayan sido colocados y seguidos correctamente o no. Si el control requerido no ha sido puesto en prÆctica o puesto en prÆctica, pero no seguido puede ser el resultado de cualquier anormalidad y el auditor tiene al mencionado este riesgo en el informe de auditoría tan ellos la irregularidad puede ser rectificada y las posibilidades de la actividad fraudulenta pueden ser minimizan [a Sandra Senft, Frederick Gallegos].

**Case Study 1:**
**Audit Objective**

The Primary Objective of this audit assignment is to access and minimize the IT/business risk associated with the implementation of technology in the banking operations and to establish IT governance, best practices and ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of the information and technology employed by the bank. The audit team will specifically check the compliance of following areas during the audit period.

Provision for the creation of the user IDs with respective rights for branches

Management of Dormant User IDs of branches and RDC
Trouble shooting management of the RDC for branches
Support provided to region for generating different MIS reports

Server room maintenance and security controls features i.e humidity controls etc

Segregation of duties, Leave record maintenance, Effectiveness of Dispatch of Statement of Accounts

BCP /DRP, Effectiveness of Communication Channels Utilization and security features

Compliance of SBP guidelines on ATM operations

ATM downtime management

TNA and training of the staff, Maintenance of office discipline

Review of system values, Application level security and administrator controls

Management of Hardware / old IT equipments, Management of Antivirus.

**Case Study 2:**
**Audit Objective (Same as case study 1)**

**9.3 Audit Scope**

Audit scope define the period as well as the domain of the audit entity that should be cover during the course of audit and if the subject audit integrated with other operational areas then that areas can also partly covered. Although, auditors has the authority to review any sort of operational areas at any time, but it is recommended that the auditor should not go beyond the audit scope. The scope of the audit i.e period and domain, will also help for the auditorto make him secure such if any fraud commented before or after the audit period or the fraud not relates to the domain of audit area [S. Anantha Sayana].

**Case Study 1:**
**Audit Scope**

The period of audit will range from the **last audit date to 20th Feb 2010** and will cover all the operational area of data centre and support provided to branches,comes under data centre jurisdiction.

**Case Study 2:**
**Audit Objective**

The period of audit will range from the **last audit date to 13th April 2010** and will cover all the operational area of data centre and support provided to branches comes under data centre jurisdiction.

**9.4 Pre-Audit Planning**

In a Pre-Audit planning, the audit team has to discuss the operational and technical areas of the entity that has to be audited, before starting audit. To cover the technical aspect of any system the auditor has to again the complete knowledge of business process of that area. On the basis of discussion between audit team, pre-inspection data should be developed and requested from the auditee management [ISACA, CISA Review Manual].

**Case Study 1:**
**Pre-Audit Planning**

Audit Period: 22nd to 27th February 2010
Pre-Audit Meeting between Audit Team Members: 17th February 2010
(Discuss different operational Areas of Regional Data Centre such as online branches operational activities, offline branches operational activities, ATM operations, Server Machine Security Controls, Physical Access Control etc)
Requirement of Pre-Inspection Data from Data Centre

**Case Study 2:**
**Audit Objective**

Audit Period: 15th to 20th March 2010
Pre-Audit Meeting between Audit Team Members: 10th March 2010
(Discuss different operational Areas of Regional Data Centre such as online branches operational activities, offline branches operational activities, ATM operations, Server Machine Security Controls, Physical Access Control etc)

Requirement of Pre-Inspection Data from Data Centre

**9.5 Audit Evidence & data gathering procedures**

The pre-Inspection data required from the auditee management should include all related documentations, policies, operational & technical manuals and guidelines.

Through these resources the auditor is able to assess, whether the operational activities are performing on the basis of policies, procedures and guidelines. If any deviation between the operational activity and available documentation, then the auditor mentions this irregularity in its report and these documents should be use for the purpose of evidence [Sandra Senft, Frederick Gallegos].

**Case Study 1:**

This phase defines the 1st part of audit, where auditors have to collect all the information mentioned in the pre-inspection data.

**Audit data gathering:**

Gather all the policy document such a user/operational manual, Organizational chart of data centre, job description of data centre employees etc

Collect a copy of all MIS reports generated by the data centre such as ATM down time report, Audit log reports, system values, user list etc

Data centre physical access security

Server Room Physical Access Security

Detail of IT equipment

Detail of all software applications supported by Data Centre Lahore.

List of employees who have left the Data Centre during the last two years.

Details of Training provided to the staff during last two years.

Detailed of all user IDs / Profiles for logging on to server machine.

Maintenance of log and fault reporting procedure followed in case of Computer Hardware and Software.

Backup/ Contingency procedures & policies being followed at Data Centre Lahore.

Backup tape movement log and its review procedure / evidence.

Steps taken by the RDC to physical secure Data tapes/storage media.

Procedure to be adopted in case of backup restoration or backup tapes testing procedure.

Network Diagrams including Internal network of Data Centre, External links to other Data Centers, Head Office, online branches, ATMs etc.

Different security policy related to Anti Virus, Network Security etc.

Last year Internal IS Audit Report of the Data Centre.

External Audit Report of the RDC during last 5 years, if any.

A photocopy of approved Mandatory leave plan for 2009/2010.

Detail of Fraud / Enquiry (if any) during last two years.

List of all Projects / Software (Implemented, Partially Implemented, Pilot & Pipelined) in 2009/2010 Documents related to Email IDs i-e request to create, enable, disable or delete, amend accordingly from branches / controlling offices.

File maintained for User Change/Amendments Requests from end users for changing / amendments in different applications / software.

Details of Internet connection (if any) at RDC.

**Case Study 2:**

**Audit data gathering: (Same As Case Study 1)**

**9.6 Procedures for evaluating test/review result**

The auditor should also review its observation and test conduct during the course of audit and should ensure that the proper evidence is available for the support of your observations [Frederick Gallegos, Sandra Senft].

**Case Study 1:**

**Procedures for evaluating test/review result**

On the basis of data and information collected in data gathering phase, from data centre Lahore, the audit team members raise the following issues:

Unapproved Organizational Chart

Weak physical security of data centre

Non-wearing of ID cards by staff

Non-Avaiblity of digital lock in server room

Non-availability of humidity and temperature controller

Non-availbility of smoke detector

segregation of duties

training not provided to staff

Non availability of IDS/IPS

Non availability of encryptors

Sharing of Administrative Password

Sharing of primary partition

Non availability of security policy

No availability of disaster recovery & contingency plan

No availability of Backup policy

**Case Study 2:**

Approximately same irregularities has been observed, while conducting the IS audit of data centre Karachi.

**9.7 Procedures for communication**

During the course of the audit the auditor should also present its findings/observations to the auditee management for their comments and response. This procedure will also helpful for the auditors to ensure that his/her observation is fine and there is no contradiction between auditors and auditee managements. Normally, the findings that has been raised by the auditors, discussed with the auditee management to know the management response against that observations [S. Anantha Sayana].

**Case Study 1:**
**Procedures for communication**

A meeting has been conducted with the auditee management of data center Lahore at the 5th day of audit period and all major irregularities has been presented and discussed with the auditee management. The auditee management tried to clear their position against observation raised by the auditors. Some of the observations are omitted after the satisfactory clarification of auditee management.

**Case Study 2:**
**Procedures for communication**

The same meeting has been arranged with the auditee management on the last day of the audit period and major finding has been discussed with auditee management. Auditee management accept all the finding raise by the auditors.

**9.8 Audit report preparation**

The auditor should also prepare its report during the course of audit and present to the auditee management. The draft audit report should also discuss with the auditee management at the end of audit and if possible, take management comment on the audit observations. It is recommended that the draft audit report should be submitted and discussed with auditee management at the end of audit but if it is not possible, then the draft report can be submitted to auditee management after some days as well [S. Anantha Sayana].

**Case Study 1:**
**Audit report preparation**

During the course of the information system audit of regional data centre the auditors prepared a Draft IS Audit Report comprising all finding observed during course of audit. At the end of the audit assignment the draft audit report has been presented to the auditee management for their comments against each observations at the same time, but the auditee management requested that they will furnish the management comment within three days.

An exit meeting letter has also been presented by the auditors to the auditee management about the final discussion and then duly signed by the auditee management members and audit team members.

**Case Study 2:**
**Audit report preparation**

In regional data centre Karachi, the draft audit report has been submitted on the last day of the audit and the same report has been discussed with auditee management. The auditee management provide their comments against each observation. A copy of draft audit report comprising management comment has also taken by the auditors for their record.

**10. Internal Controls**

Internal controls are strategy, develop and implemented by the organization, to reduce major risk. The main objective of internal control is to safeguard the organization's business interest by implementation of preventive, detective and corrective control measures. Internal control provides reasonable assurance to the high level management that the organizational business process comply the policies and guidelines provided by the regulatory body and professional standards [Sandra Senft, Frederick Gallegos].

Information System (IS) Internal Controls can be classified into three major categories:

IS Preventive Controls
IS Detective Controls
IS Corrective Controls

**11. IS Audit Controls**

An Information System (IS) auditor needs to cover different areas during the course of IS audit assignments. This is also the responsibility of an IS auditor to review and analyze the general as well as physical controls when performing an IS Audit. Although, these general & physical controls having no issues of IT but these controls can be directly affect the operation of information systems and can be the cause of any illegalactivity. The followi

are major control areas that need to be covered during the course of information system auditing [Frederick Gallegos, Sandra Senft]:

General control
Organizational control
Continuity of Operations
Operating Systems Platform security
Network Security
Application Level Security & Controls

**12. Conclusion & Discussion**

The information system audit process is the evaluation and assessment of the IT based business processes, the regulatory bodies as well as professional standards, emphasis to develop an internal audit department within the which organization, periodically review and asses organization's IT based business process and application system running within the organization [S. Anantha Sayana].

Furthermore, for more effective review of IS internal control, organization need to conduct external audit from independent audit firm. At the end of audit, the audit team present and discuss draft audit report with the auditee management, which contain the information related to audit entity and audit findings/observation. The audit management then explain their concern about the finding raised during the audit assignment and these management comments will then incorporated in the audit report [Sandra Senft, Frederick Gallegos].

During the completion of this report, I have conducted the information system audit of two data centers Lahore & Karachi of a leading commercial bank. The duration of audit assignment was one week for each data centre.

Complete life cycle, which I have mentioned in my report has been carried out during the course of auditing the regional data centre Lahore and Karachi. Phases of information system auditing has also described according to case studies.

**13. References**


[1] David L. Cannon, Timothy S. Bergmann, Brady Pamplin "CISA-Certified Information Systems Auditor ™ Study Guide", 2006

[2] Gerald Vinten, "Current Issues in External and Internal Auditing", 2004

[3] Alan Calder, Steve Watkins "IT GOVERNANCE - A MANAGER'S GUIDE TO DATA SECURITY AND BS 7799/ISO 17799 3rd Edition", 2005

[4] Andrew Hawker, "Security in Information Systems : A Guide for Business & Accounting", 2000

[5] Christopher L. T. Brown, "Computer Evidence: Collection and Preservation", 2005

[6] Ken Doughty, "Best Practices, Volume 15: Business Continuity Planning: Protecting Your Organization's Life", 2000

[7] Louis Braiotta, JR., "THE AUDIT COMMITTEE HANDBOOK Fourth Edition", 2004

[8] ISACA, Certified Information System Auditors (CISA) Review Manual – 2008

[9] Sandra Senft, Frederick Gallegos, "Information Technology Control and Audit" 3rd Ed – 2009

[10] Frederick Gallegos, Sandra Senft "Information technology control and audit" 2nd Edition – 2004

[11] Lance M. Turcato, "Integrating COBIT® into the IT Audit Process" (Planning, Scope Development, Practices) – 2006

[12] IT Audit Monograph Series # 1 "Information Technology Audit", General Principles

[13] Fred Gallegos, "IT Audit Independence: What Does It Mean?", Volume 6, 2003

[14] S. Anantha Sayana, CISA, CIA, "The IS Audit Process" Information Systems Control Journal, Volume 1, 2002

[15] Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, "What Every IT Auditor Should Know About Scoping an IT Audit" Volume 4, 2009

[16] Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, "IT and Privacy Audits" Volume 5, 2009

[17] S. Anantha Sayana, "Approach to Auditing Network Security", Volume 5, 2003