Outsourced Information Technology Environment Audit

GIAC (GSNA) Gold Certification

Author: Navaratnasingam Arunanthy, arun.navaratnasingam@gmail.com
Advisor: David Shinberg

Accepted: March 11, 2010

Abstract

The outsourcing of IT services provides the organization with flexibility that enables the organization to focus on its core business by transferring the services, infrastructure or applications processing to a service provider. Outsourcing IT resources probably increases the information asset risks associated with the IT environments. In any event, outsourcing IT increases the complexity and scope of an IT Audit. This paper provides guidance on performing an audit of an outsourced IT environment following the industry standard frameworks.

1. Introduction

Outsourcing was hyped in the mid 90's as one way to reduce IT cost, as well as to gain expertise for better business operations. Today some or many of the information technology activities in many organizations are outsourced.

"IT outsourcing occurs when an organization contracts a service provider to perform an IT function instead of performing the function itself. The service provider could be a third party or another division or subsidiary of a single corporate entity. Increasingly, organizations are looking offshore for the means to minimize IT service costs and related taxes."(CICA, 2003)

Outsourced environments are complex and highly integrated with organizations and operations. As complexity increases managing relationships with service providers becomes challenging.

"A survey performed by the IT Governance Institute indicates that problems with outsourcers increased on year 2007 from 74 Compound Problem Index (CPI) on year 2005 to 127 CPI. The CPI is the result of multiplying the outcomes from the several questions about the IT-related problems experienced by the749 respondents."(ITGI, 2008)

Fundamental to outsourcing is accepting that, while service delivery is transferred, organizations retain the responsibility for the work being done by the service provider; and therefore must ensure that the risks are identified and managed. The outsourced IT environment audit not only influences a successful partnership but also avoids significant problems by providing,

- Trend analysis related to relationship incidents and identifies root-causes to avoid a significant problem that could impact the organization's operations;
- Assurances over secure software development practices and adequately controlled change management process to avoid software backdoors and insider attacks;
- Assurance over secure data management to avoid data leakage and information fraud;

- Assurance related to logical and physical security to avoid malicious attacks, robbery, and frauds and
- Assurance related to compliance requirements, legal and regulatory requirements and contractual requirements to avoid significant penalties and/or legal sanctions for violations.

This paper will focus on how to perform an outsourced IT environment audit to ensure that the key areas of risks are identified and reviewed. The two key areas addressed in this paper are performing an audit within the organization and with the service provider.

2. Getting Started

Organizations decide to outsource their IT functions for numerous reasons, including reducing costs, enabling the organization to focus on its core business and improving the quality of service. Whatever the justification is, it is important to not only focus on achieving the objectives, but also evaluate the possibilities of running a successful business while outsourcing. As a result, it is critical to carry out an IT audit for outsourcing that identifies the appropriate key risks.

The outsourcing contract is a legal document that establishes the requirements, scope, terms, conditions, legal liabilities, responsibilities and controls between the organization and the service provider. This explicit and comprehensive detailed descriptions of key provisions are essential to a successful relationship between the organization and the service provider.

Evaluation of the IT outsourcing process within the organization and evaluation of the outsourced service execution by the service provider are the primary areas of the audit. The IT outsourcing processes in an organization varies depending on the type of outsourcing arrangement, but should include:

- Enterprise-wide policies and procedures to govern the outsourcing process;
- Process to define the requirements;
- Risk assessment and due diligence process in selecting a service provider;

- Offshore risk evaluation;
- Contract negotiation process; and
- Ongoing monitoring.

Evaluation of the service provider needs to be customized according to the type of outsourcing arrangement, but normally includes evaluation of:

- Software development and acquisition;
- System and software change management;
- Logical access;
- Data management;
- Personnel Security;
- Physical and environmental protection and
- Business continuity.

This paper will focus on providing information and direction for the practice of IT audit to ensure that the key areas of risk are identified and evaluated. Methodologies mentioned in this paper may not be the "right" solution for every organization depending on the outsourcing arrangement and relationship with the service provider. However, each organization should perform a risk assessment considering the risk tolerance of shareholders and produce a customized audit program developed for the organization.

"The risk assessment is necessary to evaluate where audit resources should be focused. In most enterprises, audit resources are not available for all processes. The risk-based approach ensures utilization of audit resources in the most effective manner." (Norm, Kelson, 2009)

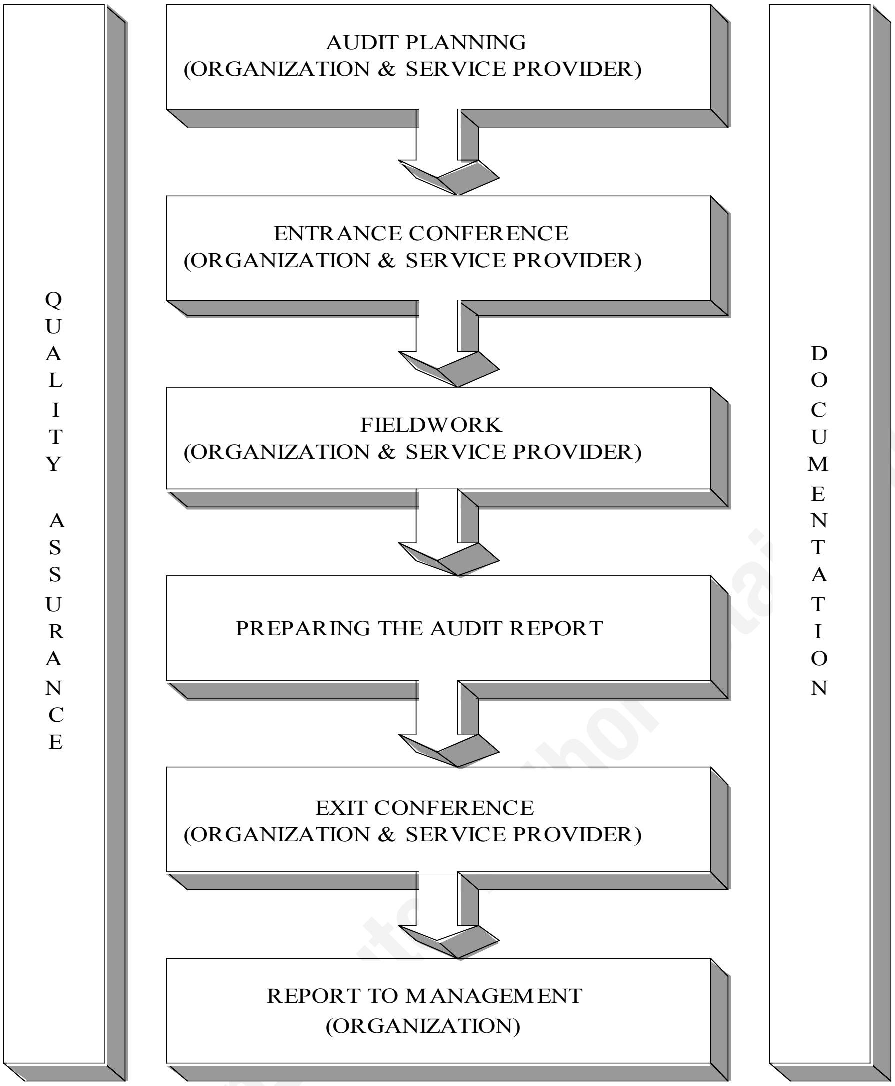
AUDIT PLANNING
(ORGANIZATION & SERVICE PROVIDER)
ENTRANCE CONFERENCE
(ORGANIZATION & SERVICE PROVIDER)
FIELDWORK
(ORGANIZATION & SERVICE PROVIDER)
PREPARING THE AUDIT REPORT
EXIT CONFERENCE
(ORGANIZATION & SERVICE PROVIDER)
REPORT TO MANAGEMENT
(ORGANIZATION)
QUALITY ASSURANCE
DOCUMENTATION

Figure 1: Primary Audit Steps

The primary audit steps (Figure 1) are audit planning, entrance conference, fieldwork, preparing the audit report, exit conference and report to management. Documentation and quality assurance are the supporting functions that should be integrated with the process from the beginning. The primary audit steps of the audit and the testing fundamentals remain the same. However, outsourcing does introduce certain elements such as communication and escalation protocols with service provider. Also, concerns with activities performed at non organization sites need to be taken into consideration. The audit of the service provider requires significantly more planning and coordination than the internal evaluation related to organization's process. The following

(Figure 2) highlights some challenges related to service provider audit and the approaches an auditor can take. However, the most experienced auditors recognize there is more than one way to approach a challenge.

Challenges	Approach
Traveling service provider sites	Identify the service provider sites in early planning stage and plan accordingly to accommodate the cost and time.
Accessing the service provider sites	Identify the protocols to access the service provider sites in advance to avoid unnecessary delays.
Scheduling meetings with the service provider personal	Identify the appropriate personal for the meeting in advance utilizing resources like organization chart to avoid meeting reschedules.
Working from the service provider sites	Verify and request an appropriate working area in advance, to ensure a suitable area to work with confidential information and data.
Limited access to audit evidences and information	Provide a requirement list or deliverable list in advance, to ensure the sufficient time for evidence collection.
Data provided is difficult to analysis (e.g. paper evidence and scanned documents)	Clarify that the advantages of data analysis such as trends and pattern. Request the data that can be analysis where possible in advance.
Contradicting audit evidences or statements	Clarify with appropriate upper management, to identify the correct evidence or statement. Do the necessary notification and escalation where needed.
Handling the Intellectual Property Right data and information	Identify the Intellectual Property Right data and information utilizing resources like contract.

Figure 2: Challenges and Approach

3. Audit Planning

Adequate planning is a necessary first step to develop an audit plan in performing an effective outsourcing audit. The auditor should develop an audit plan that can be used as a guide to successful audit. When planning an outsourced IT environment audit, the auditor must have an understanding of the environment to be audited. That includes the organization that outsourced and the service provider. This should include a general understanding of the various business operations and the functions relating to the audit scope, as well as the types of information systems, organization's information architecture and technological direction, technology supporting the business and legal and regulatory requirements. An IT auditor could take following steps (Figure 3) to gain an understanding of the business.

Step	Benefit
Reading background material including industry publications	Understand the industry standards
Annual reports and independent financial analysis reports	Understand the financial position
Reviewing long-term strategic plans	Understand the long-term goals
Interviewing key stakeholders	Understand the business issues
Reviewing prior audit / IT-related reports	Understand the control issues
Identifying specific regulations applicable to the organization	Understand the regulatory requirements

Figure 3: Steps and Benefits

Understanding key elements of outsourcing, identifying business impact and key risks, understanding of roles and responsibilities and identifying key stakeholders in the relationship are the primary planning steps. Other planning steps are defining objectives, scope, overall audit approach, audit schedule, team and deliverables.

Another primary step of the planning is scheduling of available audit resources to each task defined in the audit plan. The IT auditor who prepares the plan should consider the requirements of the audit assignment, staffing resources and other impacting factors. The key deliverables in the audit planning stage are objective, risk matrix, scope, deliverables definition, available resources and schedule, audit strategy and procedures and entrance conference memorandum.

3.1. Key Elements of Outsourcing

The key elements of outsourcing are enterprise-wide policies and procedures to govern the outsourcing process, process to define the requirements, risk assessment and due diligence process in selecting a service provider, off-shore risk evaluation, contract negotiation process and ongoing monitoring. Understanding the key steps of outsourcing is essential to identify the business impact and risks associated to business.

Organizations that commit to an IT outsourcing partnership without the enterprise-wide policies and procedures do not have the means to properly manage the outsourced activity. *"An effective outsourcing oversight program should provide the framework for management to identify, measure, monitor, and control the risks associated with outsourcing." (FFIEC, 2004)*

Defining requirements is a critical step in the outsourcing. Appropriate stakeholders should be engaged in the requirements definition stage to ensure detailed requirements are appropriately documented. *"The definition of business requirements sets the stage for all outsourcing actions and forms the basis for subsequent management of the outsourced activity. The requirements are developed through a process that identifies the functions or activities to be outsourced, assesses the risk of outsourcing those functions or activities, and establishes a baseline from which appropriate control measures can be identified." (FFIEC, 2004)*

The risk associated with an outsourced IT service is subject to the service outsourced, the relationship with service provider, and the technology used by the service provider. *"Selecting the right service provider is crucial, so it is important to develop a thorough understanding of the provider's financial and operating conditions. It is vital to undertake a due diligence review of the service provider's processes before entering into a binding agreement. This review should examine the service provider's operational and financial ability to meet the organization's needs and objectives, and can include a review of audited financial statements, audit reports on internal control, insurance coverage (fire, liability, data losses, etc.) and meetings with management, as well as an on-site visit." (CICA, 2003)*

The off shore outsourcing raises country, compliance, contractual, reputation, operational and strategic issues in addition to those presented by the use of a domestic service provider. The level of risk associated with offshore outsourcing should be measured and managed by the organization's management.

The contract is a legal document that defines all the requirements and characteristics of an outsourcing arrangement. *"A comprehensive contract should be documented. Legal counsel is always advisable. The organization should seek the services of a lawyer who specializes in such contracts." (CICA, 2003)*

The organization should have an ongoing monitoring process to ensure service provider's performances are aligned with the outsourcing contract. "*The organization should establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions." (Norm, Kelson, 2009)*

3.2. Business Impact and Key Risk

The services provided by the service provider may have a varying impact on the organization's business processes depending on the outsourced services, quantity, and magnitude. However there are two primary elements that should be considered during risk assessment.

3.2.1. Organizational Capability Level

Failure of the organization to implement appropriate controls, assurance and ongoing monitoring related to the outsourcing process may result in:

- Incorrect solution or significant missing requirements
- Costly solution or solution failing to meet business requirements and not performing as required
- Questionable service delivery, Service Level Agreement (SLA) and Operational Level Agreements (OLA) issues
- Unclear responsibilities and accountabilities for controls and processes may result in missing service delivery and non compliance to a standard
- Solution / service not integrating with strategic IT plan, information architecture and technology direction

- Violation of the organization's obligations, added costs and/or business disruption and/or total loss of the organization
- Inability to satisfy external client auditors and requirement of regulator that can subject the organization to legal sanctions
- Poor knowledge about international laws and regulation can subject the organization to legal sanctions
- Overcharges and inaccurate billings
- Cost of operations, operations efficiency and reputation of the organization, or a business unit

3.2.2. Service Provider Level

If the service provider fails to implement appropriate controls, assurance and ongoing monitoring related to the outsourced service may result in:

- Poor service quality with unacceptable number of failures and/or errors
- Service disruption and failure to meet the organization's client obligations
- Privacy and confidentiality issues
- Contractual discrepancies between the organization expectations and service provider's process
- Reduced system availability, questionable integrity of information and compromised security and confidentiality
- Insufficient allocation of resources and inability to meet the industry benchmark
- Service provider's technology and system architecture issues related to scalability, capacity, and performance
- Failing to meet the organization and/or business unit requirements as defined or not performing as expected
- Inability to maintain appropriate internal operational and IT controls and meet regulatory requirements such as PCI, HIPAA, SOX and GLB
- Poor disaster recovery and business continuity capabilities of the service provider

- Cost and resources required to find an alternative service provider or to bring the out sourced service in-house

3.3. Roles and Responsibilities

Understanding roles and responsibilities provides clear accountability and critical for effective audit execution. Listed below (Figure 4) is a list of roles and responsibilities related to outsourcing audit.

Roles	Responsibilities
Audit Manager	Oversees audit as per audit plan and provides guidance to auditor in-charge and audit team
Auditor In-charge	Responsible for developing audit scope, audit procedures, and preparing audit reports reflecting the results of the work performed
Audit Team	Responsible for reviewing and evaluating information processing systems, related process as per audit procedures
Executive Sponsor	Oversees global Master Service Agreement (MSA) and schedules and ensures communication about the contract
Program Manager	Work closely with the service provider to ensure services are delivers as per the contract
Engagement Manager	Work closely with organization to ensure services are delivers as per the contract

Figure 4: Roles and Responsibilities

3.4. Scope

The scope of the audit will address adequacy of controls designed to manage internal and external risks relating outsourcing of the services to the organization and the service provider environment in a steady state. The scope will include the following:

- Achievement of business and IT requirements
- Compliance with contract
- Relationship management
- Functionality and controls of provided services
- Service provider's internal controls

- Fulfillment of assurance charter and compliance requirements

The scope excludes the initial justification, decision, billing process and terms and conditions considered relating to the outsourcing process.

3.5. Objective

Audit objective is critical to set the stage and should align with the scope. In addition, objective will determine the level of audit test details that need to perform during the audit. The objectives of the IT outsourcing audit are to provide management with an independent assessment of:

- The controls relating the organization's IT outsourcing process such as enterprise-wide policies and procedures to govern the outsourcing process, process to define the requirements, risk assessment and due diligence process in selecting a service provider, offshore risk evaluation, contract negotiation process and ongoing monitoring.
- The controls relating service providers' environment such as software development and acquisition, system and software change management, logical access, data management, personnel security, physical and environmental protection and business continuity.

3.6. Deliverables

A Detailed audit report and report to management are the primary deliverables at the conclusion of the audit. Audit report has to be clear and easy to understand and report has to be written so that it is:

- Easy to follow, so that readers can simply refer to sections that apply to their roles and responsibilities;
- In a tone that elicit cooperation rather than alienation from those audited and
- In a tone that reflects the importance of recommendations.

The detailed audit report will include at a minimum executive summary, background/introduction, objectives, scope, audit methodology, results, conclusions, recommendations and action plans, references, acknowledgements and appendix. An executive summary will help draw the reader's attention to important issues. The suggestions and recommendations should be as to how the service could be improved.

The Report to Management should be based on the executive summary that wrote in correlation with the detailed audit report. It should include the audit purpose, audit scope and conclusion. In addition, it should have a section for every bullet point in executive summary. It's a good idea to include some notes to point out highlights or to explain why they are important.

3.7. Available Resources and Schedule

A schedule should be developed with target completion dates according to the available resources. Date of entrance conference, fieldwork starting, fieldwork completion, draft audit report delivery, exit conference, and final audit report / report to management are the key milestones dates. Please consider that auditor will likely need to coordinate with the service provider to travel to service provider sites.

3.8. Audit Strategy and Procedures

Identifying appropriate risks associated with the outsourcing arrangement is important to the success of the audit. The auditor should develop an audit plan that based on the objectives of the organization, related to the outsourced services and associated risks. The auditor should also consider the applicable laws, regulations and standards. The IT outsourcing audit should include these key aspects however not be limited to the following aspects of the outsourcing:

3.8.1. Enterprise-wide Outsourcing Policies and Procedures

The enterprise-wide policies and procedures used to govern the outsourcing process are critical to ensure outsourcing decisions are aliened with the organization's strategic plans.

"The board and senior management should develop and implement enterprise-wide policies to govern the outsourcing process consistently. These policies should address outsourced relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the outsourced relationship." (FFIEC, 2004)

The auditor should verify and evaluate the policies and procedures related to outsourcing.

3.8.2. Process to Define the Requirements

The requirement definition is an essential step in the outsourcing process. Appropriate stakeholders should be engaged in the requirements definition stage to ensure detailed requirements are documented and signed-off. The auditor should verify and evaluate the requirement definition process to ensure that the appropriate parties were involved and signed-off.

3.8.3. Risk assessment and Due-diligence in Selecting a Service Provider

The risk assessment and due diligence process in selecting a service provider are critical steps to ensure that the right service provider is selected. The outsourced IT services can contribute to operational risks and reputation risks. Operational risks may arise from inaccuracy, or the inability to deliver products and or services. Reputation risks may arise from the inability to manage information appropriately.

When responses to outsourcing service requests have been received, the appropriate teams should begin to analyze the service provider's information against the pre-defined due diligence framework. Action items to be completed include:

- *"Client reference checks during the final due diligence stage. The project team must evaluate the vendor's project management competency, success rate, the quality and standard of work, adherence to contract terms, and communication process.*
- *Country-specific risks and information, including availability of skills, costs, political environment and stability, cultural compatibility, and accessibility.*
- *Site visits to evaluate the service provider's capabilities, operations, infrastructure, and local culture." (IIA, 2007)*

The auditor should verify and evaluate the pre-defined risk assessment and the due-diligence process to determine if the controls are working as intended.

3.8.4. Offshore Risk Evaluation

The use of offshore service providers is a common business practice that can be an inexpensive alternative to in-house processing and domestic service providers. The use of offshore outsourcing as a mechanism for increasing productivity and providing enhanced services to customers of organizations has been increasing significantly in recent years. Increasingly, organizations need guidance with issues they may consider when contemplating an offshore relationship.

The offshore outsourcing raises country, compliance, contractual, reputation, operational and strategic issues in addition to those presented by the use of a domestic service provider. The level of risk associated with offshore outsourcing should be measured and managed by the organization's management. The following are key risk factors in addition to those presented by the use of a domestic service provider:

- Reputation risk
- Corporate, culture and language differences
- Significant time-zone differences and geographic distance
- Currency difference and challenges of quantifying total costs
- Compliance requirements to ensure continued adherence with laws and regulations of the organization's choice
- Legal jurisdiction and governing law for the contract
- Consideration of political and economic insecurity
- Disaster recovery/business continuity resources and options

The auditor should verify and evaluate to ensure that the key elements of off-shore outsourcing are considered and addressed as necessary.

3.8.5. Contract Negotiation Process

The contract is a legal document that defines all characteristics of an outsourcing arrangement. A written contract should be present in all outsourcing relationships. After selecting a service provider, the organization should negotiate a contract that fits their needs and requirements. The explicit and comprehensive descriptions of key provisions are essential to a successful relationship between the organization and the service provider. The auditor should verify that the key provisions are addressed in the contract. The provisions in the contracts vary depending on the type of outsourcing arrangement, but all contracts should include these key points:

- *"Ownership or lease of hardware, software licenses, etc;*
- *Employee transfer (where data center is conveyed);*
- *Applications licensed;*
- *Intellectual property terms;*
- *Rights to audit the environment and third-party assurance of controls;*
- *Billing;*
- *Recourse and remediation of unsatisfactory performance;*
- *Renewal or termination of services and*
- *Legal breach of data liability." (Norm, Kelson, 2009)*

Listed below are the key requirements to enforce the contract:

- The accuracy of the description of the outsourcing relationship in the contract. In addition the contract is clearly documented and contains sufficient detail to define the rights and responsibilities of each party comprehensively.
- Scope of contract and Out-of-scope services: Descriptions of required services, timeframes for the implementation, and assignment of responsibilities; Obligations of, and services to be performed by, the service provider including support and maintenance, training of employees, or customer service and obligations of the organization; The contracting parties' rights in modifying existing services performed under the contract; Process for adding or removing services and for contract renegotiation and The process of proposing and executing out-of-scope services and the responsibilities of both parties.

- Controls: Operational controls required by the organization; Compliance with applicable laws and regulatory requirements; The organization's records management requirements required by the organization; Communication requirements such as material changes to services, systems and key relationship personal and Technical controls required by the organization.
- Service level agreements and Reporting procedures: Performance standards that define minimum service level requirements and remedies for failure to meet standards; Percent system uptime; Deadlines for completing jobs; Percent of processing errors; The frequency and type of reports the institution will receive (e.g., performance reports, audit reports, financial statements, security, and disaster recovery/business continuity testing reports) and The process and fees for obtaining custom reports.
- Ownership and Location of Records: Ownership of all assets (Data, hardware and software, system documentation or intellectual property) related to the outsourcing arrangement; Service provider's right to use the assets related to the outsourcing arrangement and Legislation requirements for location of records.
- Assignment and Sub-contracting: Prohibit assignment of the contract to a third party without the organization's formal sign-off and The notification requirements for any changes to material subcontractors.
- Insurance: Insurance coverage required to maintain by the service provider and Communication requirements about significant changes in insurance coverage and disclose general terms and conditions of the insurance coverage.
- Penalties for non-performance and Termination: Penalties for non-performance are adequate and enforceable, if service provider failure to perform its obligations and The notification and timeframe requirements and provide for the timely return of the organization's data and resources in a machine readable format upon termination.

- Disaster Recovery/Business Continuity Plans: The service provider's responsibility for backup and record protection, including hardware, software and data files, and maintenance of disaster recovery and business continuity plans; The service provider's responsibility to test the plans regularly and provide the results to the organization.
- Security and Nondisclosure: Security requirements and responsibilities are clearly defined and in alignment with the organization's policy; The both parties responsibility for physical and logical security of the organization's resources and Nondisclosure agreement requirements.
- Right-to-audit and Regulatory Compliance: The types of audit reports it is entitled to receive (e.g., SAS70, internal control, and security reviews); The audit frequency, any charges for obtaining the audits, as well as the rights of the organization and its regulatory agencies to obtain the results of the audits in a timely manner; Rights to obtain documentation of the resolution of any deficiencies and to inspect the site facilities and operating practices of the service provider; Applicable regulatory guidance and requirements and The agreement to provide accurate information and timely access to the appropriate regulatory agencies based on the type and level of service it provides to the organization.
- Offshore outsourcing: The legal and regulatory requirement of the cross border jurisdiction, if outsourcing arrangement results in services being provided in a cross border jurisdiction.

3.8.6. Ongoing Monitoring

The organization should have an ongoing monitoring process to ensure service provider's performances are aligned with the outsourcing contract. The auditor should verify and evaluate that pre-defined ongoing monitoring process is in place and effective. The monitoring processes should but not limited to followings:

- *"Define and document criteria to monitor service suppliers' performance;*

- *Ensure that the supplier regularly reports on agreed-upon performance criteria;*
- *Invite users to provide feedback for assessment of supplier performance and quality of service;*
- *Evaluate the costs and market conditions for the service levels by benchmarking against alternative suppliers, and identify potential for improvement and*
- *Define arbitration procedures to consult an arbitration committee before bringing an action." (Norm, Kelson, 2009)*

3.8.7. Software Development and Acquisition

An enterprise software development and acquisition process is essential to reduce acquisition and implementation risks. *"Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organizations to properly support business operations with the correct automated applications." (COBIT, 2007)*

Service providers should follow the industry's best practices throughout the software development life cycle for all new application developments and major acquisitions. Auditor should verify and evaluate the software development and acquisition process followed by the service provider.

3.8.8. System and Software Change Management

Appropriate system controls should exist to make sure all changes are properly made. The auditor should verify and evaluate the controls such as assessments of changes, authorizations of change requests, reviews, approvals, documentation, testing and implementation. Also the changes that could impact the organization's information and/or data (e.g. direct data changes) requires sign-off or approval from the organization.

3.8.9. Logical Access

Necessary logical access is very important and essential to prevent unauthorized access from locations where sensitive data is processed or stored. The auditor should carefully verify and evaluate the logical controls in such high risk locations. Before the logical access testing, the auditor should verify that no test will violate any specific law of local or national statute. As well, the auditor should consider obtaining a signed "authorization form" from the service provider agreeing to the deployment of testing tools and methods where applicable. Key logical access considerations include:

- *"Verifying that security requirements specified in the contract are implemented, such as regulatory specifications.*
- *Reporting security breaches regularly, such as invalid access attempts.*
- *Using independent tests to check that security levels cannot be breached, such as conducting penetration tests of IT networks and Web sites.*
- *Restricting access to sensitive data or particular transactions to key staff.*
- *Auditing the technology and processes used to prevent unauthorized access to the client's records in situations where a supplier provides IT operation services to several customers. This may require specialist assistance.*" *(IIA,2007)*

3.8.10. Data Management

Safeguarding substantial amounts of sensitive and confidential data, personal information, intellectual property and trade secrets from malicious attacks and accidental loss is one of the biggest challenges for IT management. *"Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data."(COBIT, 2007)*

The auditor should verify and evaluate that the appropriate controls are in place to mange the organizations data.

3.8.11. Personnel Security

The personal security is essential to make sure all personnel who have access to sensitive information or a particular location have the required authority and approvals.

The auditor should verify and evaluate the controls related to personal security including but not limited to the following:

- *"Detailed background checks of potential employees that identify previous employer reference checks, criminal record checks, and educational qualifications. The background check also could verify other aspects, such as a person's social background. Although most organizations prefer to conduct employee reference checks in-house, they may be outsourced to a specialized local agency.*
- *Mandatory confidentiality agreements for all employees. Most outsourcing partners have a standard non-disclosure agreement, which states the penalties for a breach of contract, including termination of services."(IIA, 2007)*

3.8.12. Physical and Environmental Protection

Depending on the type of outsourced arrangement, the auditor should ensure that the service provider's documents, systems, and infrastructure are secured properly.

"Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel."(COBIT, 2007)

3.8.13. Business Continuity

The business continuity is a critical element of any business process and the auditor should ensure that business continuity plan is comprehensively addressed by all the key elements.

"A Business Continuity Plan (BCP) may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements."(NIST, 2002)

The Audit Work Program should be consistent with industry-accepted standards and best practices as defined, for example, by ISACA and IAA.

Audit requires two sources of baselines. *The corporate standards defined in policy and procedure documentation establish the corporate expectations. At minimum, corporate standards should be implemented. The second source, a good-practice reference, establishes industry standards. Enhancements should be proposed to address gaps between the two (Norm, Kelson, 2009)*.

A sample work program (Appendix 1) is provided utilizing IIA and ISACA frameworks.

3.9. Entrance Conference Memorandum

An entrance conference memorandum should be prepared and sent to the attendees prior to the entrance conference. The preparatory documentations, a summary of the topics to be discussed at the entrance conference, the date of the conference, and attendees (Name and Title) should be documented in the memorandum. The following is a sample list (Figure 5) of preparatory documents.

Preparatory documentations	Rational
Initial and recent business case analysis for outsourced arrangement	A Detailed business case is important to document the objectives and scope of the outsourcing arrangement.
Initial and recent risk assessments of outsourced arrangement	An updated risk assessment is essential to assess the risks factors affecting the services provided.
Initial contract with service provider and amendments	The contract is a key legal document detailing the relationship between the organization and service provider and the amendments are contract adjustments.
Billing and adjustments details	Billings and adjustments are evidence of services charged or paid.
Service provider dashboard reports	Service provider dashboard reports are evidence of monitoring
Service provider resources plan	Service provider resources plan is an evidence of monitoring
Steering committee outsourcing dashboard reports	Steering committee outsourcing dashboard reports are evidence of monitoring

Preparatory documentations	Rational
Organization's issue management process document	Organization's issue management process document is an evidence of monitoring
Incident record tracking (with severity) reports	Incident record tracking (with severity) reports are evidence of monitoring
Problem record tracking reports	Problem record tracking reports are evidence of monitoring
Change record tracking reports	Change record tracking reports are evidence of monitoring
SLA compliance reports	SLA compliance reports are evidence of monitoring
Critical physical access reviews performed by service provider	Physical access reviews performed by service provider are the evidence of physical security.
Privileged access reviews performed by service provider SAS 70s and/or ISO 27001s provided by service provider	Privileged access reviews performed by service provider are the evidence of logical access management. SAS 70s and/or ISO 27001s provided by service provider are the evidence of reviews from a third-party.
Previous and recent audit reports within the scope	Audit reports are the evidence of reviews from an auditor.
Status of high risk issues identified from recent audit reports	Status of high risk issues are the evidence of monitoring.
Service provider's disaster recovery / business continuity plan.	The disaster recovery / business continuity plan is an essential document for business continuity.

Figure 5: Preparatory Documents

4. Entrance Conference

The entrance conference is conducted in preparation for the audit and to communicate information with everyone who needs to know about the audit. The auditor in charge conducts the entrance conference to communicate the nature of the audit, timing and extent of the audit. Key individuals attending the entrance conference include the audit manager, auditor in charge, audit team, auditee management, the designated auditee contact person and any other personnel that the auditee feels would be appropriate to the meeting including service providers' contact. The following key points should be discussed during an entrance conference:

- Planned audit objectives and scope of work

- Estimated time schedule of fieldwork and report issuance
- Team members assigned to the audit engagement and their contact details
- Communication process during the audit engagement, including the methods, time frames, and individuals who will be responsible
- Organization conditions and operations of the activity being examined, including recent changes in management or major systems, if and when appropriate
- The procedures for conducting engagements, including how, when, and to whom the engagement results will be communicated
- Questions, concerns or any requests from auditor and auditee

5. Fieldwork

In fieldwork, auditors obtain and analyze the data and information provided to determine if the identified controls are working as intended. This is accomplished by completing the audit steps identified in the Audit Program. Audit steps may include interviewing key stakeholders and managers, reviewing documents (e.g. contracts, status reports, dashboards and meeting minutes), gathering statistical data, database searches and analysis of independent third-party data sources and industry surveys. The audit fields work objective is to develop an audit report.

6. Preparing the Audit Report

The audit report is the output of the field work and to assure that the facts and findings have been clearly stated. This report will be issued to the management during the exit conference requesting a written response from management to any audit findings, recommendations and corrections of errors or misrepresentations.

7. Exit Conference

The purpose of the exit conference is to communicate the results of field work and any findings that will be presented in the audit report; as well, obtain management's feedback on potential findings and recommendations before the audit report is finalized.

The findings presented at the exit conference may have been previously communicated with the responsible management. Management's comments on the findings and recommendations are important to ensure that the audit results are fairly presented and that recommendations are reasonable and free of any errors or misrepresentations. After the exit conference, management will be asked to respond to the findings and recommendations in writing.

Key individuals attending the exit conference include the audit manager, auditor in charge, audit team, auditee management, the designated auditee contact person and any other personnel that the auditee feels can contribute to the meeting. If the auditee has disagreements regarding the results of the field work and/or findings and recommendations, these issues should be discussed during the exit conference; so that the auditor and auditee clearly understand each other's position, prior to the report being finalized.

Exit conference can be scheduled separately with the organization and service provider if appropriate and depending on the outsourced arrangement. These decisions should be planned and scheduled during audit planning.

8. Report to Management

This report should be consolidated and based on the details of an audit report finalized after an exit conference. It should include the audit purpose, audit scope and audit goals. If applicable, provide the rationale or explanation related with financial numbers (Dollar value) why the findings are important to the organization and/or the service provider.

9. Conclusion

Conducting outsourced IT environments audit can be successfully completed by understanding the organization's objectives, detailed planning and support and coordination from appropriate management from the organization and service provider. Utilizing industry standards like COBIT, Institute of Internal Auditors Global Technology Audit Guide, Center for Internet Security and National Institute of Standards and Technology will ensure that a detailed audit test is performed. Using a detailed requirement list and scheduling meetings in advance with the appropriate personnel will result in successful and efficient auditing. Communicating with the appropriate managements within the organization and service providers will provide a great deal of support to complete the audit on schedule. The responsible managements from the organization and the service provider should be continuously involved in the audit findings to address corrective or remediation actions accordingly. Documentation and quality assurance should be integrated within the audit from the beginning to provide a quality audit report.

10. References

Federal Financial Institutions Examination Council. (2004). *Outsourcing Technology Services, IT Examination Handbook*. USA.

IT Governance Institute. (2008). *IT Governance Global Status Report*. Rolling Meadows, Illinois, USA.

Mayurakshi, Ray, & Parthasarathy, Ramaswamy. (2007). *Global Technology Audit Guide, Information Technology Outsourcing*. Altamonte Springs, FL, USA: IIA.

National Institute of Standards and Technology. (2002). *Contingency Planning Guide for Information Technology Systems.* USA.

Norm, Kelson. (2009). *Outsourced IT Environments Audit/Assurance Program*. Rolling Meadows, Illinois, USA: ISACA.

The Canadian Institute of Chartered Accountants. (2003). *Information Technology Outsourcing.* Toronto, Ontario, Canada.

Information Systems Audit and Control Association. (2007). *Control Objectives for Information and related Technology (COBIT)*. Rolling Meadows, Illinois: ISACA

Appendix 1 - Sample Work Program

Control Objective 1: Determine that board and senior management developed and implemented enterprise-wide policies to govern the outsourcing process.

Ref #	High Level Test	Detailed Test
1.1	Determine that enterprise-wide policies and procedures addressing the risk to the institution from outsourcing relationships.	Inquire of appropriate management members likely involved in the outsourcing process. Verify that policies and procedures address outsourced relationships from an end-to-end perspective, including: ▪ Establishing servicing requirements and strategies ▪ Selecting a provider ▪ Negotiating the contract ▪ Monitoring, changing, and discontinuing the outsourced relationship

Control Objective 2: Determine that adequate process and controls in place to define the requirements.

Ref #	High Level Test	Detailed Test
2.1	Determine that an enterprise-wide process is in place to ensure detailed requirements are documented and signed-off.	Inquire of appropriate management members likely involved in the outsourcing process. On the existence of process, verify that process are adequate and require: ▪ Appropriate evolvement from business and IT ▪ Necessary sign-offs from management

Control Objective 3: Determine that the process in place requires a risk assessment and due diligence prior to outsourcing.

Ref #	High Level Test	Detailed Test
3.1	Determine that a risk assessment relating to the outsourcing was performed initially, and is updated.	Inquire of appropriate management members likely involved in the outsourcing process. On the existence of process, obtain and review the initial and most reasoned outsourcing risk assessment and verify that: Risk assessment address the risks pertaining to the function outsourced, risks pertaining to the service provider and risks pertaining to the technology used include: ▪ Any risks identified in the initial risk assessment have resulted in significant losses ▪ High-risk issues identified in the risk assessment have been lessened through new process or insurance ▪ The updated risk assessment reflects the current business and risk environment ▪ The current risk assessment results are within the current risk tolerance ▪ The senior management provides appropriate governance and oversight over risk assessment

Control Objective 3: Determine that the process in place requires a risk assessment and due diligence prior to outsourcing.

Ref #	High Level Test	Detailed Test
3.2	Determine that a due diligence was performed to evaluate service provider's capabilities.	Inquire of appropriate management members likely involved in the outsourcing process. On the existence of process, verify that due diligence

Control Objective 4: Determine that adequate process and controls in place to address off-shore outsourcing risks.

Ref #	High Level Test	Detailed Test
4.1	Determine that enterprise-wide process in place to ensure key off-shore outsourcing risks are addressed.	Inquire of appropriate management members likely involved in the outsourcing process. On the existence of process, verify that process are adequate and address: ▪ History and reputation of the service provider ▪ Corporate, culture and language differences ▪ Time-zone differences and geographic distance ▪ Currency difference and challenges of quantifying total costs ▪ Compliance requirements to ensure continued adherence with laws and regulations of the organization's choice ▪ Legal jurisdiction and governing law for the contract ▪ Privacy, data-protection and security breach laws. ▪ Legal validity of electronic communications and signatures ▪ Intellectual property rights ▪ Consideration of political and economic instability ▪ Infrastructure issues (e.g. Telecommunications, utilities and transportation) ▪ Knowledge transfer ▪ Disaster recovery/business continuity resources and options

Control Objective 5: Determine that the contract with service provider was developed, documented, and executed comprehensively.

Ref #	High Level Test	Detailed Test
5.1	Determine that procedures are in place to manage the outsourcing contracts.	Obtain and review the contract procedures for following: ▪ The legal department and the IT outsource executive sponsors are required to involve in the contract process ▪ Sign-off from IT Outsource executive sponsors and appropriate business executives are required ▪ Any amendment or additions to the contract required appropriate

Control Objective 5: Determine that the contract with service provider was developed, documented, and executed comprehensively.		
Ref #	**High Level Test**	**Detailed Test**
5.2	Determine that the contract provisions address the key requirements to enforce the contract.	Obtain and review the contract in-effect for key requirements. (Refer section 3.8.5.Contract Negotiation Process, for details)
5.3	Determine that the contract has been executed according to law required, and has been amended appropriately to reflect changes in the service provider/client relationship.	Obtain and review the contract, amendments and latest revisions and verify that: ▪ The contract has been executed with the appropriate signatures ▪ The amendments to the contract have been initiated and executed ▪ The amendments have been properly executed according to the provisions of the initial contract ▪ The contracts reflect the current business and operating environment

Control Objective 6: Determine that adequate monitoring process in place to address outsourcing relationship and issues.		
Ref #	**High Level Test**	**Detailed Test**
6.1	Verify that service level agreements (SLA) and operational level agreements (OLA) are clearly established.	Inquire of appropriate management members likely involved in the SLAs that process in place to develop, manage, review and adjust according to business requirement. Verify that the SLAs established in the service provider contract are; ▪ Current and reflect the business requirement ▪ Measurable for quality and quantity of the services outsourced ▪ Exclusions, commercial arrangements and OLAs ▪ Appropriate approval and sign-offs
6.2	Determine that the delivery performance using SLAs are monitored on a regular basis and performance issues are addressed by the organization management.	Verify that processes exist to measure and report the SLA performance. Inquire of appropriate management members likely involved in SLA review meetings On the existence and frequency of SLA review meetings, inquire the objective of these meetings. Sampling: Based on the frequency of these meetings, determine the appropriate sample size to be tested. Obtain minutes of these meetings for the selected sample dates and review them for evidence of: ▪ Appropriate management involved ▪ Underperforming SLAs are evaluated ▪ Remediation process between the organization and the service provider are discussed ▪ Actions summaries are recoded and accomplished

Control Objective 6: Determine that adequate monitoring process in place to address outsourcing relationship and issues.		
Ref #	**High Level Test**	**Detailed Test**
6.3	Determine that an incident management system is utilized to track problems encountered during operations.	Inquire of appropriate management members likely involved in the issue management: On the existence, determine if the activities of the service provider are recorded in the incident management system.
6.4	Incident management system is utilized to ensure that non-standard operational events (e.g. incidents, problems and errors) are recorded, analyzed, resolved and escalated in a timely manner.	Verify that the issue management tool and confirm by review that: ▪ It is used for logging problem events of all types ▪ It allows defining severity levels to the incident log, which trigger the calculation of the number of days for resolution. It is expected that the system will be tied to the management defined service levels ▪ It allows defining level of impact and/or severity ▪ Notification procedures are defined with appropriate management following the severity rating to the problem ticket Obtain a list of incidents / issues related to service provider. Sampling: Based on the population, determine the appropriate sample size to be tested. For the selected sample of incident or issue tickets review them for evidence of: ▪ Issues are evaluated based on severity ▪ Action plans are established, with milestone dates and deliverables ▪ The milestone dates are tracked, closure dates are recorded and open, and late action items reported ▪ The recourse when action items are late ▪ Issues reported are monitored and closed on a timely basis. For items that are late, determine actions taken to address performance issues ▪ Billing adjustments were initiated based upon delayed issue remediation ▪ There are established criteria for escalating issues to management ▪ The escalation communications are documented ▪ Determine if billing adjustments were initiated based on issues ▪ Root course was identified for re-occurring incidents

Control Objective 6: Determine that adequate monitoring process in place to address outsourcing relationship and issues.		
Ref #	**High Level Test**	**Detailed Test**
6.5	Verify that the internal management conducts reviews at regular intervals to discuss service provider performance, issue management and the status of the service provider relationship.	Inquire of appropriate management members likely involved in the relationship management: ▪ The reviews conducted at regular intervals to discuss service provider performance, issue management and the status of the service provider relationship ▪ The appropriate organization representatives, is at a senior level in the organization, with relationship personal involved in the review and addresses the significant issues between the organization and the service provider ▪ Evaluates the achievement of business requirements / objectives, and the satisfactory execution of service provider promises and requirements ▪ Identifies issues for escalation with service provider management
6.6	Verify that the members of the organization and service provider management conduct a status review of the contract and the service provider's performance at regular intervals.	Inquire of appropriate management members likely involved in the relationship management: ▪ Includes the appropriate representatives, is at a senior level in both enterprises, and addresses the significant issues between the organization and the service provider ▪ Evaluates the achievement of business requirements / objectives and the satisfactory execution of service provider promises and requirements ▪ Identifies issues for escalation with service provider management ▪ An action plan is initiated for remediation ▪ Organization analyzes where the relationship between the enterprises has deteriorated to a point where additional attention or intervention is necessary

Control Objective 7: Determine that a formal software development and acquisition process is utilized for all new application development and major acquisitions.

Ref #	High Level Test	Detailed Test
7.1	Determine that a formal software development and acquisition process, with specific checkpoints, is utilized for all new application development and any major acquisitions.	Inquire of appropriate management members likely involved in the software development and acquisition. On the existence of process, obtain and review for a sample of major IT software implementations, inspect documentation evidencing compliance with the defined process. Inspect a sample of implementations to determine that appropriate parties are involved at various stages of the development as necessary, including design and testing.

Control Objective 8: Determine that a change management processes in place for new programs, program changes, system changes, and maintenance.

Ref #	High Level Test	Detailed Test
8.1	Determine that an enterprise-wide change management processes in place for new programs, program changes, system changes, and maintenance with appropriate check points.	Inquire of appropriate management members likely involved in the change management process. On the existence of process, inspect a sample of change requests to verify that appropriate approval was obtained.

8.2	Determine that necessary tests are developed and executed for all changes appropriately.	Inspect a sample of changes, and determine that the standard test steps had been conducted, based on the type of change, as appropriate:
		Unit Testing;
		Integration Testing;
		System Testing;
		System Integration Testing;
		Regression Testing and
		Acceptance testing.
		Verify that appropriate sign-off had been obtained after test execution and prior to the final implementation.

Control Objective 9: Determine that the logical access controls in place for operating systems, databases, applications and network devices.

Ref #	High Level Test	Detailed Test
9.1	Determine that a process in place for all logical access request including operating systems, databases, applications and network devices.	Inquire of appropriate management members likely involved in the service desk or operations center process. On the existence of process, obtain and review the sample of access requests determine that standard processes were used with appropriate management approvals.
9.2	Determine that the access to operating systems, databases, applications, and network devices requires a unique user account and password.	Inspect a sample of operating systems, databases, applications and network devices, and verify: ▪ Standard users require an individual user account and a password to login. ▪ Generic user accounts were approved by management and their use was restricted to key staff. ▪ Privileged accounts were approved by management and their use was restricted to appropriate staff. ▪ All the standard, generic and privileged accounts were reviewed periodically and preceded accordingly.
9.3	Determine that a process in place for all logical access removals including operating systems, databases, applications and network devices.	Inquire of appropriate management members likely involved in the service desk or operations center process. On the existence of process, obtain and review the sample of access removals determine that standard processes were used with appropriate management approvals.
9.4	Determine that firewalls protection with access rules and restrictions for internal network.	Inquire of appropriate management members likely involved in the network management. On the existence of firewalls, inspect the current network infrastructure and determine that firewalls were implemented at all external network connections. For selected firewalls, inspect the system security configurations to determine that they provide adequate protection.

Control Objective 10: Determine that the logical access controls in place for operating systems, databases, applications and network devices.

Ref #	High Level Test	Detailed Test
10.5	Determine that antivirus software is implemented on all systems.	Inspect, for a sample of systems, to determine that anti-virus software was installed, configured to receive virus signature updates on a daily basis and scans are scheduled to run on a real time basis.

Control Objective 11: Determine that the data management process in place for all data classification.		
Ref #	**High Level Test**	**Detailed Test**
11.1	Determine that all data is classified and managed accordingly.	Inquire of management as to the security policies and procedures specifically addressing data classification and management. On the existence of policies and procedures, inspect the evidence of data classification, and corresponding physical and logical security levels assigned, throughout the data lifecycle. For the same sample of data categories, inspect the classification and determine that they were assigned adequate security levels throughout their lifecycle.

Control Objective 12: Determine that detailed business continuity plan in place for all services in scope.		
Ref #	**High Level Test**	**Detailed Test**
12.1	Determine that comprehensive business continuity panning exist with key components.	Inquire of appropriate management members likely involved in the business continuity panning. On the existence, review them for evidence of following components: ▪ Risk analysis was performed considering criticality of the outsourced service ▪ Recovery objective(s) are clearly documented ▪ Plans are considered with outsourcing relationship ▪ Testing requirements are explicitly documented ▪ Event management plans are clearly documented ▪ Governance structure documented with sufficient details ▪ Insurance coverage requirements are documented

Personnel security, physical and environmental protection controls should be verified and assessed by the auditor according to the outsourcing arrangement as discussed at the section 3.8.11.and 3.8.12.