Integrated Approach to Financial and IT Audit

This article emphasises the need for an Integrated approach to audit i.e., inclusion of IT audit procedures as part of Financial Audit in order to address the risk of material misstatement. It attempts to answer the question "What are the IT audit procedures that need to be carried out in order to provide increased assurance that Financial Statements present True and Fair View and Internal Controls are adequate to support assertions in Financial Statements?" It provides a brief framework for and scope of examination and audit of the IT systems. Read on to know more….

Introduction

Information Technology is an essential part of any business and with the greater focus of Government of India on promoting digital transactions in the economy, importance and use of information technology has increased manifold.

CA. Ashish Agarwal

(The author is a member of the Institute. He can be reached at ashishagarwal26@gmail.com.)

It is imperative that auditors must obtain sufficient and appropriate audit evidence to form an adequate basis for expressing Statutory Audit Opinion and for communicating issues in Internal Audit Reports. It is important to note that as per para IG 4.3 of the Guidance Note on Internal Financial Control issued by ICAI, auditor's understanding of IT's role in the entity's processes is important to the identification and assessment of risks of material misstatement and for planning further substantive procedures.

In order to obtain sufficient and appropriate audit evidence, relevant audit procedures must be performed by auditors. As a material amount of evidence is generated, stored or maintained by

pnb Housing Finance Limited

Ghar Ki Baat

LET'S JOIN HANDS FOR GROWTH.

Calling Financial Consultants. Come and Join hands.

Welcome to PNB Housing Finance Limited, the fastest growing Housing Finance Company.

Avail our services of Home Loans / Non Home Loans and Fixed Deposits.

For more information, please send us an email at: **businesspartners@pnbhousing.com** or give us a missed call at **09223108020.**

Please mention the following details in your mail:

- Complete Name
- Address and Contact Details
- Brief write up about your Profile, Work Experience etc.

Our team will get in touch with you within 2 working days.

Visit: www.pnbhousing.com

As per the code of ethics, chartered accounts in practice are not permitted to receive, or agree to receive any part of profits from a non member

CIN:L65922DL1988PLC033856

IT systems and applications and in order to place reliance on such evidence, it is necessary to include audit of IT systems and applications (IT Audit) in the scope of audit. Therefore, financial auditors must obtain a minimum level of confidence on IT systems and applications used by the organisation. If in addition to the financial or internal audit, there is a separate IT Audit being carried out by an independent IT auditor, the statutory or internal auditors must obtain the report of an IT Audit and use it in a manner appropriate for their audit purpose. Assurance on IT systems and applications assumes more importance in case of audits of banking and financial sector given the increased focus on online and digital banking. However, the objectives of financial audit are not different in an IT environment, but the scope of financial audit becomes much wider and requires use of sophisticated tools and techniques.

Scope of and steps to carry out an IT Audit

Usually, all the guidance on IT Audit recommends an understanding of the accounting and internal control systems as a first step for preparing the audit plan and carrying out the audit. This understanding can be obtained based on previous audit reports, discussions with senior management and own past experience.

A more effective approach to prepare the audit plan can be to base the audit plan on the results of High Level Testing carried out on important areas under audit. High level testing is different from detailed risk assessment. High level testing should mainly include compliance testing for key controls and substantive testing for a small sample of transactions in the important areas under audit. High level testing can provide quantitative background to the use of auditor's judgment and experience. High level testing should be designed to uncover potentially risky areas for carrying out detailed audit review. Based on the results of high level testing, detailed audit planning and review can be carried out. Audit activities can be focused on processes where results of high level testing are not within the acceptable limits.

Assurance on IT systems and applications assumes more importance in case of audits of banking and financial sector given the increased focus on online and digital banking.

In addition to carrying out high level testing, potentially risky areas under audit can also be identified based on inherent risk, business risk, criticality, previous and third party audit reports, common industry issues, senior management requirements, audit committee directions etc.

During the audit review both compliance and substantive testing should be carried out. Compliance testing for adequacy of controls should be carried out at Application, Database and Network level. Substantive testing can be carried out in areas where high risk is identified based on compliance testing or in other areas where the inherent and perceived risk is higher.

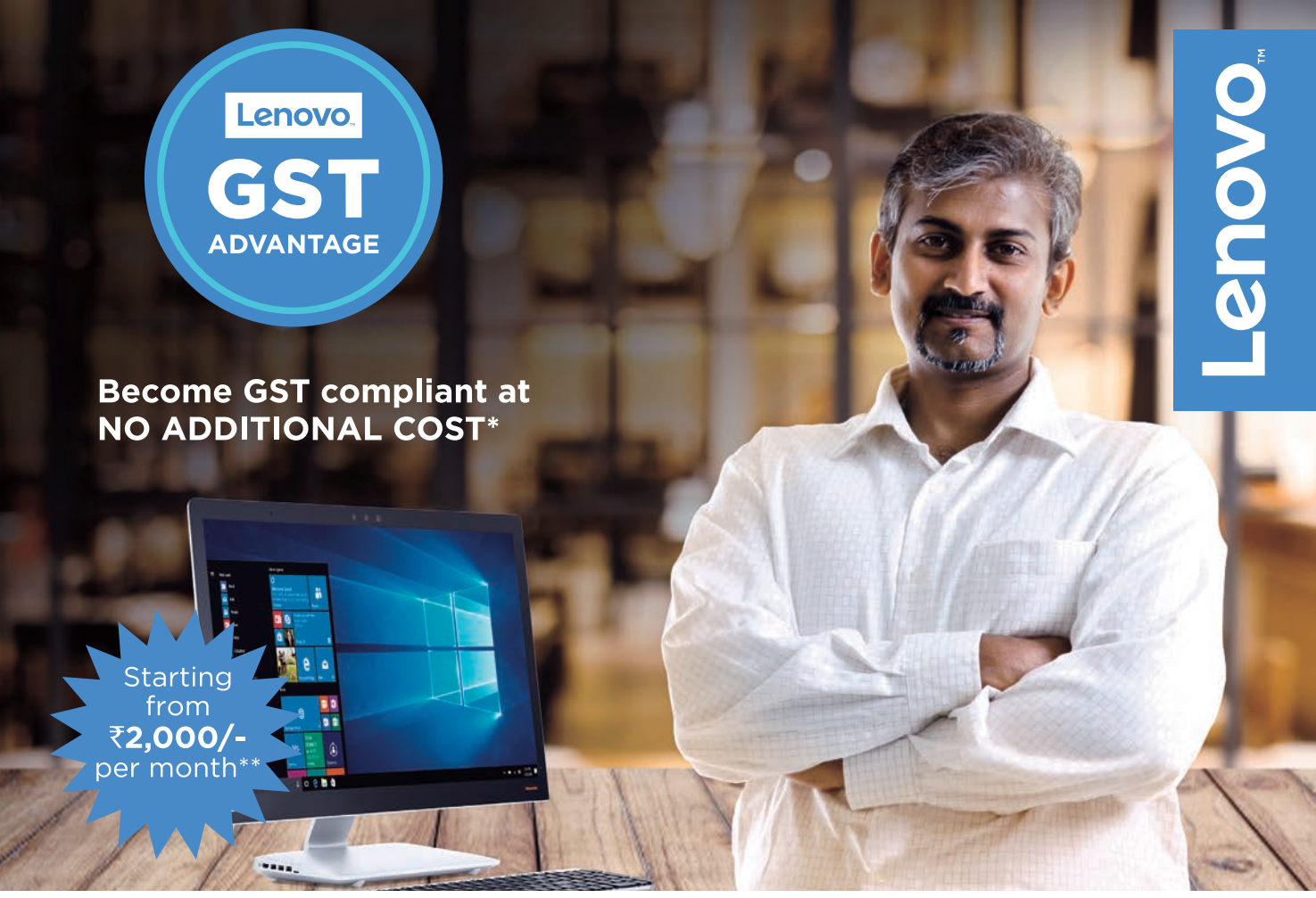
Compliance Testing

It should be carried out for controls at:-

- Application level
- Database level
- Network level

Each of the above audit areas including Application, Network, and Database Controls are discussed in the table below:-

Areas	Key objective	Audit checklist of Questions to be asked	Risk / Impact of vulnerabilities
Application Level Control	• Application access control, Controls over application source code, object code and key documentation of the application. • Maintain Integrity of Accounting Data. • Auditable trail of data.	• Are the passwords issued securely? If there is a choice of passwords, correct validation of password and secure storage of password? • Are there adequate controls over data processing like existence of control totals? • Is there a data field along with audit trail?	• Risk of unauthorised access and manipulation. • Risk of inaccuracy and integrity of processing. • Risk that transactions output may not show the correct account balances. • Risk that a transaction may not be auditable from input to output in absence of Audit Trail, thus leading to lack of audit evidence.



Buy any Lenovo PC

Choose the GST package that suits your business best

Available in-store, GST compliant ERP & accounting software package

Awarded as India's BEST ERP for SMEs and MSMEs by Dataquest 2016

*MRP ~~₹12,600/-~~ now **Free** for 6 months

GSP Invoice upload package for filing GST returns

In-built tax preparation and tax return filing solutions

*MRP ~~₹2,500/-~~ now **Free** till 30th September 2017

Simple web based GST ready accounting package

First cloud accounting and compliance software in India

*MRP ~~₹3,000/-~~ now **₹900/-** for 12 months

AtomicAds

Turn GST into an Advantage

AIO 910
Powered by
Intel® Core™ i7 processor.
Intel Inside®.
Extraordinary Performance Outside.

To know more:
Visit - http://www3.lenovo.com/gst
Email - corpsales@lenovo.com
Call - 1800 3000 9991

Found at www.lenovo.com

*Terms & Conditions apply. For detailed Terms & Conditions, log on to https://buyalenovo.com/rest/service/gettc/127
**Avail 3x9 EMI scheme to pay ₹6,000/- as down payment and enjoy No Cost EMIs of ₹2,000/- for next 6 months. Offer valid on select products only.

Areas	Key objective	Audit checklist of Questions to be asked	Risk / Impact of vulnerabilities
Database Level Controls	• Controlled access to database. • Maintaining the Database integrity and controls over Database through segregation of duties i.e., user, administrator, security. • Database operations including storage space, performance management.	• Is there a list of roles, responsibilities and accesses allowed to database personnel based on need to know basis? • Is there clear partition between live and historical transactions database storage area? • Have there been any incidents in the past where Database performance has resulted in downtime? What is the performance statistics of the Database?	• Risk of breach of database integrity and irreversible data changes. • Risk of deletion of historical transactions data which is a very critical risk. • Risk of low performance of database and eventual processing failure. • Risk of deletion of audit trail and absence of data control totals.
Network Level Controls Management	• Configuration of Network devices should be controlled. • Public key infrastructure must use approved security controls, standards and certificates. • Firewalls, Intrusion detection and prevention systems should be in place. • Routers and switches should be protected by hardware and software firewalls. • Incidents of Network intrusion, cyber attacks, and phishing attacks should be documented and resolution reported and recorded.	• Is there a policy defining Network configuration and is it implemented? • Is the configuration of Network devices standardised or customised? • Is Penetration Testing or Vulnerability Assessment carried out prior to production implementation? • Are the servers, databases and web servers protected through firewall and IDS? • Are antivirus patches applied from time to time on network servers and devices? • Have there been any network intrusion attempts in the period of audit.	• Risk of critical financial, customer information being vulnerable. • Risk of internet website being hacked. • Risk of successful cyber attack. • Risk of account and financial information being leaked to cyber criminals. • Risk of virus coming in through external network and causing havoc inside the organisations' servers and IT systems.

Substantive testing

It is the detailed testing of areas identified for audit. The results of the preliminary testing can be used to plan the detailed substantive audit. Based on the preliminary testing a categorisation of business areas can be made into High Risk, Medium Risk and Low Risk. Auditors should categorise the control risk as high unless relevant controls are:

- Identified,
- Effective and
- Tested and Operating appropriately

Detailed substantive audit can be carried out for areas under high and medium risk. For low risk areas an adequate sample based testing can be carried out. Also the area of medium and low risk can be covered only on rotation basis in case the audit is quarterly or several times in a year. Time and resources can be dedicated to areas of high and medium risk. There are many benefits of using this audit approach. A risk focused approach shall provide efficient utilisation of costly resources and time while still maintaining the quality of audit reporting. A risk focused approach shall also reduce detection risk and provide adequate coverage of all important business risks, thus increasing the assurance provided in the audit reports. This method of doing audit is also part of Risk Based Audit approach.

Key steps in substantive audit for each of the broad areas of Application Controls, Database Controls, and Network Management are given below :–

- Substantive Audit of Application Controls –
  1. Adequate segregation of duties – the person updating accounting and financial data and the person authorising should be different to ensure effective control over data input.

A risk focused approach shall provide efficient utilisation of costly resources and time while still maintaining the quality of audit reporting. A risk focused approach shall also reduce detection risk and provide adequate coverage of all important business risks, thus increasing the assurance provided in the audit reports.

NSDL
Technology, Trust & Reach

NSDL e-Governance Infrastructure Limited

NSDLgst

Your trusted GST partner

File GST returns (GSTR1 , GSTR2 , GSTR3 etc.) seamlessly through NSDLgst

NSDLgst exclusive features:

- Special module for Chartered Accountants /Tax Consultants to service their clients
- Reconciliation & Ledgers
- Comprehensive Dashboards and MIS reports
- Securely store uploaded data for multiple years
- eSign facility
- Helpdesk for Dealers / Tax Consultants and Chartered Accountants

When it comes to GST... Trust the experienced

Visit www.nsdlgsp.co.in

(020) 2567 8300

gstinfo@nsdl.co.in

Also there should be segregation of duties with respect to custody, authorisation, recording and reconciliation of data in order to maintain data integrity within the application.

2. Determining how the accounting and financial data received from other applications or systems is validated for completeness and accuracy prior to processing in the application.
3. Application automated checks for, check digits on all identification keys, checks for missing data, checks for extraneous data, record mismatches, out of sequence conditions, existence checks on all key fields.
4. Controls over processing include end-user reconciliation procedures that facilitate completeness and accuracy of processing. Also verify if special reconciliation procedures need to be applied to month-end, fiscal year, etc.
5. For error-reporting, is there an exception report generated for long-outstanding error transactions, with an aging analysis?
6. Financial and accounting output reports should ensure output data is viewable only to authorised personnel and carry adequate identifying information including time and date stamps.

- Substantive Audit of Database controls –
  1. Database access control list should assign all users specially database administrators separately. The list should be approved by management.
  2. Details of financial and accounting jobs run including batch jobs run should be maintained and monitored by database administrator. Any exceptions should be duly monitored.
  3. Direct read and write access of financial and accounting data for database users should not be allowed even to senior management or approved users. If allowed under exceptional circumstances, it should be duly pre-approved and for a limited time frame only and for specific purpose.
  4. Reference tables and static data tables such as heads of accounts and consolidation, grouping lists should be password protected in order to restrict and track any changes, if any. Similarly, the fields containing audit trail should have read only access including to the database administrator.
  5. Deletion of financial and accounting records, especially historical records in database should be only with written approval of senior management and Information Security Administrator. Historical records may be required to be maintained under various legal and regulatory requirements for a defined time period.

- Substantive Audit of Network controls –
  1. Network controls are important to protect information assets of the organisation. Such information includes financial and accounting information and confidential data.
  2. Configuration of network devices must be checked so that there is no known vulnerability. This is especially important in case of multilocation organisation and audit.
  3. External interfaces to the network should be evaluated specially at end points or nodes. Any transmission of data through the network should be encrypted. Any use of public email ids or public network for transmission of confidential information should be evaluated. This specially holds good for organisations storing or processing bank or payments related information.
  4. In case services of a third party service provider are used for network connectivity, contract with the third party services provider should be evaluated to examine information security during data transmission.
  5. Records of log into server connected on network should be available for audit examination. Any abnormal logging in activity from a remote location must be investigated further.

An important overall check is to examine the existence of audit trail from input till output. In case audit trail is missing or broken, risk assessment should be carried out for the same and further audit procedures including analytical procedures, reconciliations, compliance and substantive testing must be carried out.

- Avail complete solution for GST Filing, GST Compliant Invoicing and Purchase Reconciliation.
- Package available for both existing as well as new customers.

DCB 24-Hour Customer Care

Call Toll Free: 1800 209 5363

Email: customercare@dcbbank.com

Web: www.dcbbank.com

DCB BANK

Terms and conditions apply. The GST filing and accounting services are enabled by an Application Service Provider (ASP), a third party and DCB Bank Limited shall not be liable and responsible for the ASP services mentioned herein.

Applicable Standards and Guidance

In carrying out the above audit procedures, Standards and Guidelines on IS Audit provided by Information Systems Audit and Control Association (ISACA) are useful. A key summary of standards and guidelines is given below –

Standard/Guidance	Key points to be kept in mind by Auditor
1202 Risk Assessment in Planning	• Analyse the risks related to system availability, data integrity and business information confidentiality and plan the audit based on assessed risk. • Carry out risk assessment at least once in a year and seek approval of risk assessment from the audit and other key stakeholders.
1205 Audit Evidence	• Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both. • Some key points regarding audit evidence in IT environment are – ▪ Evidence obtained through observation is limited to point in time at which observation took place. ▪ Electronic evidence should be time stamped and have clear trail or source. ▪ Voluminous data can be analysed to obtain trends or inconsistencies. Using CAATs in such cases can be highly useful. ▪ Source (internal, third party, management) and Form (oral, written, representation) of evidence must be evaluated to understand the reliability of evidence.
2208 Audit Sampling	• Sampling can be used when volume of information requires very high time to examine. Sample should represent the entire population. • In assessing whether sample represents the entire population both quantitative and qualitative aspects must be taken into account. Qualitative aspects must be aligned to audit objectives.
2401 Audit Reporting	• Statutory Audit Report – In case the overall assessed and tested level of IT controls risk is very high and information obtained by Statutory Auditor is inadequate to support True and Fair view, a qualified report should be issued. A high level of IT control risk can impair the financial data integrity and thus reliability on information obtained cannot be placed by the auditor. An example is, passing entries even after the book closing because of weaknesses in authorisation and application level controls, especially in IT environments where transactions and entries are passed at multiple levels.
1402 Follow-up Activities	• IT auditor should carry out adequate and timely follow on audit procedures to evaluate the actions taken by management on audit report observations.

In addition to the above, relevant standards issued by ICAI are listed below -

- **Standard on Auditing SA 315**- Identifying and Assessing the Risk of Material Misstatement through understanding the entity and its environment. This standard deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the entity's internal control.
- **Standard on Assurance Engagements SAE 3402**- Assurance reports on Controls at a Service Organisation-Applicable to Audit of Service Organisations. In cases where the IT function is outsourced, this audit standard can be used to provide guidance.

External Risk Assessment –

In addition to internal risk assessment and audit carried out through the Compliance and Substantive Testing and Procedures, an assessment of external risks should be carried out by the organisation.

Any organisation that is exposed to World Wide Web is susceptible to cyber-attacks. An auditor must evaluate the vulnerabilities present in the IT applications, database and network of the auditee organisation. A financial or internal auditor may not be having the required skills

20+ NATIONALISE BANKS

25+ PRIVATE BANKS

44+ FOREIGN BANKS

50+ NBFC

100+ CO-OPERATIVE BANKS

Why go to various Institution for your fund requirement ?

Just4uloan
Educate - Empower - Enhance - Engage

shall cater to your funds by selecting the Financial Institution best suited for you which has :

- Speedy Approval.
- Lowest Processing Fees.
- Fast Disbursement
- Quick Processing.
- Lowest Rate of Interest.
- Higher Eligibility.

Do You Know ?

- Working Capital loan is available at approx 8.5% - 9.00% p.a.*
- Loan is available against plot of NA Land.*
- Loan to Builders & developers (Rera Compliant) Within 20-25 working days.*
- Unsecured loan between 11-13 % p.a.*
- Startups can avail loan upto ₹ One Crore without collateral under government sponsored schemes.
- Eligibility of Housing loan can be increased by considering projected income.*
- Loan is available upto 90% of the property value.*
- Small business can avail working capital loan upto ₹ 10 Lacs without collateral under government sponsored scheme.*
- Loan is available for educational Institute against discounting of future fees.*

*Terms & Conditions Apply

Contact Now:

Just4uloan
Educate - Empower - Enhance - Engage

- Reduce your interest cost without reducing your loan.
- Enhance your eligibility.
- Loan at your Door Steps.

enquiry@just4uloan.com | www.just4uloan.com

Call Now: 022 - 28615154/ 28615150

Address - 601-606, Rainbow Chambers, Near MTNL Exchange, SV Road, Kandivali West, Mumbai 400067

and competence to carry out an assessment and testing of vulnerabilities to external threats, but the Auditor should be able to evaluate and use the work of an expert IT auditor carrying out vulnerability testing.

Some vulnerabilities and risks that auditor must consider while evaluating the organisation's IT system are as follows:–

Type of Attack	Type of Vulnerabilities	Risk
Denial of Services Attack (DoS)	Network	Organisation network may become unavailable. Due to network unavailability financial transactions done online or ledger maintained online using an enterprise resource application, may result in differences, errors and omissions in transactions. In case a procedure exists where manual recording of transactions is carried out, adequate reconciliation, approval, and adequate compensatory controls must be present for the manual processing.
Ping Attack	Database server	This type of attack may lead to data being stolen from database.
SQL Injection – Passing unintended SQL code into an application without proper validation	Database driven website	This can lead to unauthorised access to database connected to website. The data in the database can be exposed outside the organisation and can be stolen as well. Therefore, there is a risk to data confidentiality especially in case of public companies.
Viruses, Worms and Spyware	Network, Database, Application	Viruses, Worms and Spyware can lead to temporary shutdown of the IT application and database, which means unavailability of the IT application. If the application is online with multiple access points, it can cause operational problems.
Unauthorised access through the internet of World Wide Web	Database, Network	It can lead to data theft specially financial and accounting data. In case of public company due to announce the results, it can be a higher risk if financial and accounting data is leaked before formal announcement.
Malicious codes (Trojans)	Network, Application	Similar to Viruses. Trojans are most common. They can damage the computer data and storage on desktop machines.

Even though the above tabulated threats may be external to an organisation they can impact financial and accounting systems and therefore, should be included in scope of statutory and internal audit.

Conclusion

An integrated approach to statutory and internal audit including IT Audit must be adopted in order to reduce the risk of material misstatement. As part of IT audit, internal and external IT risk assessment should be carried out by the financial auditor in order to obtain evidence in order to support the assurance provided. IT audit procedures should be based on applicable guidelines and audit standards. ■