Technical Guide on
IT Migration Audit

Committee on Information Technology
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Technical Guide
on
IT Migration Audit

Committee on Information Technology
The Institute of Chartered Accountants of India
(Setup by an Act of Parliament)
New Delhi

Edition	:	January, 2010
Committee/ Department	:	Committee on Information Technology
E-mail	:	cit@icai.org
Website	:	www.icai.org, http://cit.icai.org
Price	:	Rs. 70/-
ISBN	:	978-81-8441-299-4
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002.
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra 282 003. January / 2010/1,000 Copies

FOREWORD

Information Technology is the prime business driver for enterprises encompassing all facets of its operations. It is impossible today to visualize an organization without any element of Information Technology initiatives. As organizations evolve and grow, it is imperative that IT also keeps pace with the evolution and growth of the organization by migrating to more efficient and effective IT systems considering increasing requirements and technology evolution. The oft repeated phrase today is – "Successful organizations manage their IT successfully".

Managing IT successfully is a challenge not just from organizational change perspective, but also from the change that happens within IT itself. A wide array of IT resources such as software, hardware resources, IT facilities and so on are used by organizations. These need to be updated to keep in tune with emerging requirements and technological innovations to service increasing informational requirements. Also, new vulnerabilities and threats develop on existing IT infrastructure and hence the need for updates or enhancements is essential from a security point of view also.

Organizations therefore, periodically transit from one IT environment to another either from an efficiency or security point of view. This transition or in other words migration, is a part and parcel of any IT management function today.

IS Auditors -D.I.S.A. (ICAI), are the guardians of controls in IT Infrastructure and have an important role in ensuring the effectiveness, security, availability and reliability of such infrastructure. The role of IS Auditors becomes very critical in IT migration projects and there is an emerging need need to be updated in this area.

The Committee on Information Technology of the Institute has brought out this Technical Guide on IT Migration Audit to provide detailed guidance on the scope and coverage of an IT Migration Audit. I am sure that this guide will address the professional expectations and requirements of IS Auditors involved in migration audits.

I believe that this publication is a laudable effort and a necessary step in the right direction as it attempts to provide guidance on IT migration audit related issues to

the members and various stakeholders to such an exercise. I am confident that this guide would be well received by the profession and the industry.

I complement the Committee on Information Technology and its Chairman, CA. K.Raghu and Committee members for doing valuable work in bringing out this technical guide and the Committee Secretariat in promptly coming releasing the same.

CA. Uttam Prakash Agarwal
President

January 21, 2010
New Delhi

PREFACE

IT migration has become a very critical function in IT management today. The risks that arise from such migration exercises and the controls that should be implemented during such an exercise are very important and should be clearly understood, to ensure that the migration activity is in line with expected deliverables.

The Committee on Information Technology has been at the forefront in equipping Institute members on the latest developments and best audit practices. An IT migration exercise is a key milestone event in any IT management process, and this technical guide makes an earnest effort to brings forth the critical areas that need to be checked by auditors during migration audits.

This guide covers major migration events such as data center migration, database migration, ERP migration, application migration, OS migration, server migration etc apart from the detailing the controls to be adhered in pre migration and post migration exercise.

While the primary audience of this guide is our member fraternity, I would also request our members to discuss this guide with CIO/CTO's so that organizations undergoing migration can ensure compliance to control requirements.

I hope this guide will not only enhance the professional knowledge of members in undertaking migration audits, but also attempts to provide the IT management and governance functions considering the compliance expectation of migration process.

I am indeed very thankful to CA. Uttam Prakash Agarwal, President and CA. Amarjit Chopra, Vice President for the guidance and support in coming out with this Technical Guide. I would like to record my deep appreciation for the guidance and support of the members of the Committee on Information Technology in coming out with this guide. I appreciate the efforts put in by Mr. Ravi K. Arora, Jt. Director and the officials of the Committee Secretariat for their contribution in timely releasing this Technical Guide

I place on record my sincere thanks to CA B Mahesh Balan, CA V Vijayakumar, CA N Swameshwar and CA Suresh Rangarajan for their inputs in preparing this technical guide. I am also thankful to CA N Venkatakrishnan Special Invitee of the Committee on Information Technology for his valuable contribution in

finalizing the Guide. I am also thankful to members of the Committee on Information Technology for their valuable contribution in finalizing the Guide.

CA. K. Raghu
Chairman
Committee on Information Technology

Place: New Delhi
Date: 21st January 2010

CONTENTS

1
Introduction

Information technology has been growing rapidly in recent years. This has led to a huge growth in data generation and storage for better information processing. Newer technologies are being introduced in the Information Technology spectrum for businesses to arrive at better informed decisions. Organizations are constantly revamping their information technology architecture to take advantage of these new developments. This includes introducing new ERP applications, moving to state of the art data centers, implementing better and more secure operating systems, and installing faster storage devices and servers. There could also be other business reasons for a data migration like mergers and acquisitions of new businesses. This means migration of existing data in legacy or disparate applications, operating system, storage devices, etc to a new environment.

Definition of IT Migration

According to the Webster dictionary migration means “to move into or come to live in a region or community especially as part of a large-scale and continuing movement of population”.

Extending this meaning, IT Migration can be defined as a “process of movement of any one or a group of IT Assets from one state of existence to another”.

It is important to understand what constitutes IT Assets, before understanding IT Migration. IT Assets comprise hardware, software, data, people and related infrastructure. A successful migration project requires business impact analysis to mitigate risks, detailed planning and excellent project management skills.

Types of Migration Events

With rapid technological innovations, migration events happen in every touch-point in an IS environment. The major migration events are of six types:

A. Application Migration (ERP, Email, CRM, Web Applications)

This involves migration from a legacy application to new-breed applications, from one vendor application to another vendor application or from an application written in an old programming language to a new one.

B. Operating System Migration

OS migration involves migration from one vendor OS to another vendor OS or an upgrade from an old version of OS to another version of the same OS.

C. Database Migration

This includes migrating from one vendor database to another vendor database, from one version of a database to another version of the same database, or consolidation of different databases into one database.

D. Hardware Migration

Hardware migration includes migration from one server to another server, consolidation of servers, migration from one storage device to another device, and migration from one network device to another device.

E. Datacenter Migration

Data center migration includes migration of existing information processing facilities to third party data centers and consolidation of multiple data centers.

F. Service Provider Migration

With new technologies like SaaS (Software as a Service) and cloud computing, almost all the IT activities can be outsourced. In such a scenario, migrating from in-house IT processing facility to a third party or moving from one third party to another third party can be categorized under service provider migration.

This technical guide gives the IS auditor an overview of the IS migration lifecycle and the activities to be performed in the pre- and post-migration audits. It also deals with procedures for audit of each type of migration event.

2
Migration Lifecycle

The major activities in a typical migration project are scoping, planning, pre-migration audit, actual migration event and post-migration audit. Each of these activities is briefly explained below.

1. Scoping and Planning

A preliminary analysis of the current environment is undertaken to determine the scope of the migration and its requirements. The following details are gathered in this phase:

i. Type of migration event

ii. Quantity of data to be migrated

iii. Details of existing applications, OS, and hardware that are being migrated

iv. Estimated downtime for Application/IT infrastructure downtime that is proposed to be migrated

v. Performance Impact

vi. If available, a working plan from a similar migration event.

Based on the above, a detailed plan with migration design and timelines is prepared, which details the following:

i. Migration type

ii. Details of the current hardware, data center, applications, data, etc

iii. Details of the new environment

iv. Tools to be used for the migration

v. Testing methodologies to be followed

vi. Resource plan and detailed timelines

vii. Vendor support documentation and co-ordination

Risk assessment of the migration project is done in this phase to find out what can go wrong, how to prevent it and how to mitigate the impact of a failed migration.

In the planning phase, migration scripts are developed if the migration is planned to be automated using scripts for upload of data into the new hardware / database. Load tests are conducted to test the migration process as well as the capacity of the new environment to take in data as per the planned migration throughput rates.

2. In the planning phase, a detailed business continuity plan is also designed to overcome a situation of failed or delayed migration. This plan has to be tested before the migration event. Pre-migration audit

Before the actual migration event happens, it is advisable for organizations to conduct a pre-migration audit. The Information System Auditor should be engaged for the purpose. For this, the auditor will have to check the following:

i. Infrastructure review

ii. Audit of migration scripts

iii. Load tests review

iv. Compatibility Checks

v. Business Continuity Plan review

vi. Legal compliance and checks

The above activities are explained in detail in the chapter “Pre-migration Audit”.

Though it is desirable to conduct a pre-migration audit in every migration exercise, it is generally done for large scale events such as data center migration and ERP migration.

3. Actual migration event

Migration event, which is carried out as per the plan, involves the following activities:

i. Backup of data being migrated is taken and tested.

ii. If the migration is a data migration, then data is cleansed for duplication, deterioration, errors and missing fields.

iii. Data throughput rates are monitored to find out any deviation of actual throughput rates from the estimated throughput rates. If any deviations are noticed, the migration methodology and plan are modified to achieve a successful migration.

iv. Data integrity checks are conducted by the migration team to check for completeness and accuracy of data.

v. Sign-off is obtained from the end users for the completion of the migration process.

vi. Decommissioning of the original source of data.

4. Post-migration audit

Information systems auditors are also involved in this final phase of the migration audit. The auditor performs the following audit checks to confirm that the migration has been successfully accomplished.

i. Data integrity checks

ii. Log Analysis for errors and mitigation

iii. Performance review

The above activities are explained in detail in the chapter “Audit of Actual Migration Event”.

3
Objectives of Migration Audit

Like any other audit, migration audit too has its objectives. The audit should be planned and executed to realize these objectives, which should be in line with the expectations from the migration event. The major objectives that each migration audit should cover are:

i. Integrity

The first and foremost objective of a migration audit is to ensure that the data in the new migrated environment qualifies the integrity and reliability tests. This applies to all types of migration events. If any errors or mistakes are identified, suitable counter measures should be recommended to mitigate their impact.

ii. Control adequacy

Auditors should verify that adequate control framework has been established for migration. This can be in terms of project documentation, project team definition, backup plans, vendor support, test documentation, etc. IS auditors should assure the management that migration plan and controls have been adhered to.

iii. Business Continuity

The Information systems auditor should ensure that the migration team has taken adequate security measures for the migration event so that major business disruptions do not happen during the process of migration.

iv. Effectiveness

As part of the migration audit, the IS auditor should review the migration processes and methodology, to ensure compliance of the original budget and schedule and identify deviations and (inefficiencies or deficiencies). He also needs to find out whether appropriate migration tools and software were used for the migration. For this he may obtain end-user feedback and suggest opportunities for improvement.

4
Pre-Migration Audit

Before the commencement of the actual migration event, the management of the enterprise should carry out a pre-migration audit by qualified IS auditors.

A pre-migration audit is warranted in case of large scale migration events such as Data Center migration or ERP migration. Relatively simpler migration events do not generally require this audit.

The pre-migration audit may involve all or any of the following activities, depending upon the particular migration event type:

i. Infrastructure review

Infrastructure review is a must for datacenter migration. Before moving the equipment, it is necessary to ensure that the new data centre is completely ready for occupation. It should be complete in all respects with the required infrastructure: power, HVAC (Heating, Ventilating and Air Conditioning) systems, proper electrical and network connectivity. Core infrastructure is the backbone for all applications; its non-availability in the production environment adversely impacts a significant number of operations. It is also essential to carry out final inspections to identify any apparent or likely problems that might crop up after moving into the new location. A walkthrough of the entire program to identify possible barriers to the migration should also be done.

ii. Audit of Scripts

Scripts are used in database migrations and application migrations. These convert the old database structure to a different structure that fits the parameters of the new application or database and may also assist in populating the data into the new databases. The IS auditor should review these scripts before their actual deployment in the course of the migration event. The review can be done by using a black box or a white box approach.

In the black box approach, the scripts are run on a set of old data. The migration results are then compared with the old data set to find out any discrepancies. The IS auditor should ensure that he selects an appropriate sample size. . This approach is also used where third party tools are used for migration.

In the white box approach, the auditor does a code review of the scripts that are used for the migration activity. For this, the IS auditor should have programming knowledge of the language that has been used to write the scripts.

iii. Load / Stress Tests

Load tests are used for database migration, hardware migration, and OS migration. Load / stress tests may also be relevant to applications that check whether the programming has been done efficiently. This type of testing is carried out to ensure that hardware is capable of meeting the desired performance levels for a given workload. The factors that should be tested are whether the new IT environment can (a) handle not only the current load requirements but also the projected requirements, (b) handle peak level processing requirements, (c) take in huge individual data sets for processing, and (d) process the most complex programming requirements of the enterprise. Tools are available for conducting load / stress tests on databases and networks. In some cases, manual stress tests will have to be conducted on the test environment. The IS Auditor may perform stress tests or review the results of the load / stress tests done by the migration team to satisfy himself that the capacity and capability of the new IT environment is up to the mark.

iv. Compatibility Checks

While choosing new hardware, operating systems, applications or databases, the IT organization should check inter-compatibility and intra-compatibility of the new systems. The following compatibility checks should be done before the migration event:

- New applications should be compatible with the OS and databases
- New database should be compatible with the OS and application
- New OS should be compatible with the existing hardware

The IS auditor should insist on vendor product documentation to satisfy himself that the various migration objects pass the compatibility checks. Where adequate documentation is not available, the IS auditor should insist on test runs.

v. Business Continuity Plan Review

Any enterprise which plans a migration should conduct a risk assessment of the migration activity:

a. to identify the risks associated with the migration

b. to analyze the business impact in case of delayed or failed migration

c. to prepare the business continuity / backout plan in case of delayed or failed migration

The IS auditor should review the Risk Assessment documents and Business Continuity Plans. BCP should cover all possible failure actions and plans to face and mitigate risks arising from such failures.

vi. Legal compliance and Checks

Legal compliance and checks are required in the case of data center migrations. If data centers are located in an overseas location or away from the current location, they should comply with the local laws. In case of application and database migrations, the IS auditor should check whether the required licenses have been obtained. If applications are to be certified / tested before implementation by governing bodies, the auditor should check whether pre-implementation audits have been conducted prior to the migration event.

5
Post-Migration Audit

It is highly recommended to engage a qualified information systems auditor to conduct a post-migration audit. It should focus on comparing the post-migration results to the original business. The deviations should be identified and measured to determine errors. Feedback should be taken from the key stakeholders and team members. The lessons learned from the migration project can be used to leverage process improvements to enhance future projects. The major post-migration audit steps are discussed below. The appropriateness and scope of these checks may vary from one migration event type to another. .

A. Data integrity checks

Pre-migration and post-migration data sets should be compared for data non-integrity issues. Data integrity checks should check the following data parameters:

i. Raw data integrity

ii. Business rules / configuration rules

iii. Data relations

Data integrity may be checked by using tools or manually by using various techniques like check digits, batch input totals, etc.

B. Log Analysis for errors and mitigation

The Information Systems auditor should review the migration logs from data upload / transfer tools to check for errors in data migration. The logs should be verified for successful completion of the data migration as well as for any error messages like data sets getting corrupted or omitted, etc. Configuration and user setting logs should be extracted and compared with those of the earlier systems / applications. If any errors had been noticed by the migration team, the auditor should ask for the action taken report to find out whether the errors were rectified, and also check the mitigation steps taken to minimize the impact of such errors.

C. Performance review

Post-migration audit should review the performance of the new environment. The performance of the database, servers, applications, operating system, etc should be compared with the migration objectives as well as the pre-migration environment. Such an analysis assures the management that the migration objectives have been achieved.

6
Audit Procedures– Migration Events

6.1 Data Centre Migration

Background

Many organizations underutilize their existing infrastructure assets and hence consider the option of consolidation to better leverage all resources. Data centre consolidation and migration can help in streamlining the information infrastructure and realize cost, energy and service delivery benefits.

There could be numerous reasons for relocation of data centers. But the major ones are:

a. Inadequate infrastructure and cost considerations

The datacenter may lack power facilities needed to upgrade to high density server and storage systems. Adequate HVAC system may not be available economically. The increasing need for more power and cooling has made the traditional data centers expensive and difficult to maintain. Moreover, if the data center is operating on a leased facility, the lease terms may have reached the end of its useful life. The facility owner may be unwilling or unable to upgrade the facility to meet “state of the art” requirements for high density data centers.

b. Business-driven reasons

The corporate world is taking to business reorganizations in a big way. Data centers get moved and consolidated for a variety of business-driven reasons, such as mergers, acquisitions, or divestitures. Expanding business may render the existing data centre’s capacity inadequate to support the same. Or business acquisitions may result in the organisation having several data centers that need to be consolidated into a single data centre.

Audit Objectives

Since data center migration is a major IT event in an organization, the role of the Information Systems Auditor becomes particularly important. He needs to identify the audit objectives or premises on which to audit the data center migration. An illustrative set of audit objectives is given below:

a. Business continuity will not be impacted by the data center migration event

b. Application interdependencies are not impacted

c. Procurement and logistics are not impacted

d. Complexity of the data center migration has been properly estimated

e. Vendor reliance is manageable

f. Management objectives like cost and infrastructure efficiencies have been achieved

Audit Procedure

Audit of pre-migration activities

A data center migration project, especially of a large data-centre, is massive in its scale of operations. It is complex, time-consuming and costly. It touches and impacts every aspect and function of the organization. . The risks arising from the improper planning and execution of data center migration projects are quite heavy. . A poorly handled data center migration can result in disruption of operations, data losses and, in worst cases, loss of customer support resulting in loss to business and its reputation.

a. Check whether the business case has been reviewed and analyzed

This section contains the reasons for initiating the project. Information to be included in the formal business case includes the project background, critical success factors, expected costs and benefits, ROI projections, a gap analysis, and expected risks and potential obstacles.

b. Verify whether a budget has been developed for the data center migration activity

Budgeting is a crucial task as a project budget ensures that all the internal stakeholders have been consulted, adequate and timely resources made available, and all the project related costs duly approved and accounted for. A data center migration is generally a very expensive project. The benefits of the project should therefore exceed the costs involved. The data center migration budget must adequately cover new construction, renovation, site closure, equipment, staff, tools, and outside expertise from vendors and specialists. Provision should also be made for cost escalation.

c. Verify whether key stakeholders and migration team members have been identified

Several organizations maintain an inventory called Application Portfolio management, which maintains application profile and key contact information of stakeholders. These include executive sponsors, business unit leaders, major application owners, and IT operations management.

A well-rounded team should include a mix of people and skills. The team should consist of process experts, end-user representatives, technical people from the organisation and the vendors from whom the organisation has purchased hardware and software. The team will require a dedicated project manager, who is closely aligned with the IT organization, to lead and coordinate all activities during the planning phase, and through the migration. The project leader has to also identify and implement the newly defined processes and procedures post migration.

d. Verify whether an impact analysis of the migration project on the existing infrastructure has been done

Assessing and documenting the impact of the project on inventories, equipment, infrastructure (assets), technical and business resources, applications, key business processes and external factors (customers, suppliers, government, stakeholders) pertaining to the organisation. Preparing a detailed list of inventory of data centre equipments that has to be relocated acts as a good starting point to document and track assets and contracts associated with those assets prior to the actual data centre move. The impact assessment should be multifaceted, i.e., which includes holistically the physical and logical relationships of the assets belonging to the data centre.

e. Check whether an application interdependencies documentation has been done

A business application architecture interfaces with a large number of other business applications. In a data center migration project, this calls for a thorough assessment of the impact of moving the application on the interfacing applications. This analysis would first assist in understanding the existing interdependencies and then evolving appropriate 'Move Bundles' – a simple and detailed list of all the systems and their dependent components and applications belonging to a particular domain. Many critical interfaces may require that the dependent applications be grouped together for the purpose of migration.

f. Check the new data center facility design document

A detailed design development of the new data centre should be carried out in the light of functional, technical and financial considerations. Wherever new process improvements are to be made, these should be identified and documented. Care should also be taken to maintain the environmental conditions prescribed for equipment maintenance. Planning and designing of the physical environment in terms of space layout, rack layout, heating, ventilation, air –conditioning, power and network connectivity should be done to take care of future growth in IT Infrastructure.

g. Check whether a detailed project plan has been drawn up

The order in which the equipment is to be moved to the new location is to be planned. Besides the company should engage skilled logistics professionals who take care of the entire movement of the equipment: from its unracking, packing, transportation, unpacking and re-installation at the new site. Insuring the equipment is also important. The plan should also address issues relating to back-up operations during the move, installation and testing and ongoing operations, specific equipment relocation process (i.e. where the equipment should be placed in each rack, how the racks will be positioned on the raised floor, how network and electrical cables are to be arranged, etc). The plan should also include a complete plan of how the work has to be carried out. .

Clear project goals help to define the project deliverables, i.e., tangible and intangible objects produced as the desired end result of the project. These deliverables in turn can be broken down into actual work requirements. The

greater the definition of the actual work requirements, the better it is. Once this is done, the scheduling part is started where time and the necessary resources are allocated.

h. Check whether a Risk Assessment has been carried out before the data center migration

The IS Auditor should verify whether an exhaustive risk assessment has been carried out before the data center migration. Along with this, mitigation strategies should also have been identified for each of the risks assessed. Some of the possible risks and their mitigation strategies are:

Risk	Mitigation Strategy
There may be an issue of availability due to interdependencies between software applications and hardware. This may result in an availability risk.	The interdependencies between software application s and hardware should be studied. Steps should be taken to remove dependencies or to move the dependency to another software application or hardware.
New hardware or software may not support legacy application running on old hardware/ software.	The application may be rewritten / redesigned to host the same on the new hardware/software. The legacy OS may be virtualized until the application is redesigned.
Budgetary constraints, consistently, drive changes in the scope of the migration program.	Divide the program scope into multiple phases based on priorities to prevent from losing focus.

i. Check whether appropriate information security measures have been planned

A data centre migration is all about movement of hardware, software and data. When everything is in movement there is a possibility that an asset may get lost because of an unintentional or malicious act. This necessitates the need to develop an effective security plan which ensures that data is kept safe, unauthorized activities are kept out and the business remains un-compromised in all aspects: technical, competitive and financial.

j. Check whether a BCP and DR plan has been defined and adopted

Last but definitely not the least is the contingency planning. Despite planning for weeks, it could be that the plan does not work to the expected optimum level due to very many reasons. If this happens then the operations get disrupted leading to financial losses. Contingency planning consists of two components: Business Continuity Planning which is proactive and aims at avoiding or mitigating risk; Disaster Recovery Planning which is reactive and aims at restoring business to its normalcy after a disaster has occurred. The BCP and DR plans should clearly state the following two aspects:

- Recovery Time Objective: The maximum amount of time that an IT-based business process can be unavailable before the organization starts suffering significant material losses.
- Recovery Point Objective: The maximum amount of data an IT-based business process is willing to lose in case of non availability of systems.

k. Verify whether the source data that will be migrated has been backed up and tested for restoration

Backup is a copy of the application, data and configuration settings so that these can be recovered in the event of a disaster. Recovery is the process of reverting to the backed up copy of the application, data and configuration settings to resume normal business. The organization should effectively plan the movement of these storage assets and ensure proper backing during the in-between time lag. This could be a challenging task especially for companies handling petabytes worth data.

l. Check whether pilot applications testing has been conducted

A group of applications should be selected for this exercise. Using this pilot build, testing should have been done to ensure that

i. Implementation plan is flawless

ii. All internal and external dependencies have been taken care of

iii. Business services are not hampered

iv. Hardware & software in the new location is compatible

Lessons from this pilot implementation may help in designing alternative strategies to improve the implementation plan for successful build and test activities.

m. Verify whether a proper logistics plan has been developed for movement of hardware

As stated earlier, equipment movement involves insuring, un-racking, packing, transportation, un-packing, and re-installation of expensive computer equipment by I.T. logistics professionals. The move group plan should contain specific information on when each system has been re-racked, booted up and brought online.

Audit of post-migration activities

a) Check whether proper technical testing of the migration event has been conducted

Several tests described below should have been carried out to ensure that the data migration project goals have been met:

i. **Unit testing**

Every individual component of hardware should be tested to ensure that it functions as expected.

ii. **Stress testing**

This type of testing is carried out to ensure that hardware is capable of meeting desired performance levels for a given workload.

iii. **Integration testing**

It is the testing of combinations of components or modules to verify that they are working properly and returning proper output.

iv. **Shared infrastructure testing**

It involves testing whether interfaces to shared services environment are performing successfully; for example, in applications that require use of shared databases. Stress testing of shared infrastructure tests its capacity and scalability.

b) Verify whether the old data center has been properly decommissioned after the migration event

Once the new data centre becomes fully operational it is necessary to decommission or close the old data centre. It ensures the optimization of the IT infrastructure maintenance costs and meets the environmental and

security requirements. Where an old application is to be scrapped, all the concerned stakeholders should be informed about the decommissioning plans. Necessary data should be backed up for meeting regulatory compliances. The procedures laid down for disposing off the old hardware as per the ISMS guidelines of the organisation should be duly followed. Asset registers should be updated to provide details of assets acquired and disposed.

6.2 Database Migration

Background

Database Migration means moving the data from one database vendor/version to another, as from Oracle to MySQL or upgrading the version of database software used, as from SQL server 2003 to SQL Server 2008. Database migration can also occur if there is an integration of two databases into a single one, like integration during mergers.

Database constitutes a fundamental and crucial element in an organization's information systems. It is essential for both an ERP system and simple computing software. Because of this, databases are to be sensitively handled and carefully managed.

Audit Objectives

The Information Systems Auditor should look for the following for auditing the database migration event:

- Reduced data corruption
- Reduced errors and database crashes
- Maintaining data integrity and accuracy
- High levels of performance with improved response time
- Data security
- Adequate business continuity / a fall back plan

Audit Procedure

a) Check whether a proper database migration plan has been drawn up

The IS Auditor should ensure that a proper database migration plan has

been drawn with the following elements:

- Identification of the migration tasks to be performed
- Identification of the required hardware, software and human resources
- Infrastructure sustenance plans
- Identification of training requirements
- Determining the network connectivity requirement for both the source and target environment
- Plan for archiving historical data to reduce the amount of data to be migrated
- Testing strategies to be adopted
- Deciding on the test cases and documenting the expected results
- Determining details of integration with other systems
- Testing the migration scenario
- Developing plans for security, business continuity and disaster recovery, performance monitoring, change management, incident management, stress testing and vulnerability assessment

b) Check whether risk assessment exercise has been done

Risk assessment done prior to database migration should cover the following:

i. **Operating System readiness assessment**

Verify the compatibility of the operating system and patches with the version of database server to be used

ii. **Database readiness assessment**

Verify the compatibility of the database in the new environment. Identify possible migration issues and special cases where major re-working may be necessary

c) Check whether proper data profiling and data mapping techniques have been deployed

Data profiling or extracting database metadata involves studying the source

data thoroughly to understand its content, structure, quality and integrity. Modeling tools and reverse engineering can help in capturing all details of the schema. Once the data has been profiled, it can help in developing an accurate set of mapping specifications. This process is called data mapping, and constitutes a major part of the schema migration process.

All database objects in the source database need to be converted to the equivalent objects in the target system. These include data types, tables, columns, views, indexes, stored procedures, triggers, packages, sequences, authorities, functions etc. Factors such as data type, scale, precision, length and default values for table columns, functions, and stored procedures, null values etc. should also be considered.

d) Verify whether appropriate query conversion process has been carried out

Even though the basic SQL commands are the same in almost all databases, SQLs differs from engine to engine. SQL translation requires good expertise and knowledge of both the source and target systems. This helps in making sure that there are no performance issues. The IS Auditor should ensure that the migration team has adequate skills in this area of query conversion, which is the penultimate step in a database migration. After query conversion the converted objects are implemented by building a database structure on the target platform through scripts or facilities provided in the target system.

e) Verify whether appropriate data integrity checks have been done

The IS auditor should ensure that data integrity has been tested by using tools like batch totals, check digit totals, number of records and other value parameters.

6.3 ERP Migration

Background

ERP migration involves migrating from the legacy systems to ERP systems. Enterprise resource planning (ERP) is a company-wide computer software system used to manage and coordinate all the resources, information, and functions of a business from shared data sources. ERP delivers a single database that contains all data for the software modules, which include

manufacturing, supply chain management, financials, project management, human resources management, customer relationship management. Prior to ERP, software was developed to fit the processes of an individual business. Due to the complexities of most ERP systems and the negative consequences of a failed ERP implementation, most vendors have included "Best Practices" into their software. These "Best Practices" are what the Vendor deems the most efficient way to carry out a particular business process in an Integrated Enterprise-Wide system. These practices are incorporated into most ERP vendor's software packages. When implementing an ERP system, organizations can choose between customizing the software or modifying their business processes to the "best practice" function delivered in the "out-of-the-box" version of the software. The use of best practices can make complying with requirements such as IFRS, Sarbanes-Oxley or Basel II easier.

Audit Objectives

ERP migration audit should consider the following:

i. Adoption of improved and better business processes

ii. Better employee productivity

iii. Planned return on investment in the new ERP application through reduced inventory holding, higher sales, efficient procurement, etc

iv. Quicker make-to-sell life cycle

Audit Procedure

Audit of pre-migration activities

The IS Auditor should prepare a checklist of audit steps on the pre-migration activities, which is similar to the one illustrated below.

a) Check whether a migration plan has been prepared

To ensure that the project is progressing in the correct direction, it is important that a project quality plan or method document is produced. This document explains to both the supplier and the customer the principles of the approach and how they will be implemented across the project. Along with this, it is essential to develop a detailed project plan stating the project phases, milestones and dependencies as well as the responsibilities for each activity.

Implementing ERP software is generally too complex for "in-house" skill, so it is desirable to hire professionally trained outside consultants for three types of services - Consulting, Customization, Support. The length of time to implement an ERP system depends on the size of the business, the number of modules, the extent of customization, and the scope of the change and the willingness of the customer to take ownership of the project.

b) Verify the business blue print or business process mapping document

Identifying critical business processes is essential for business process mapping, which involves defining what activities the business entity performs, the people who are responsible for them, the standards to which the activities or the process should adhere to, and measuring the success of the business process. The specific assessment of the processes will obviously be dependent on the business sector and key drivers within the individual organisation. For example, the criteria to select critical business processes may include:

- What are the high volume business processes?
- What are the major revenue generating processes?
- What are the processes which have the greatest impact on customer satisfaction?
- What are the areas which generate high profits?

Once identified, these critical business processes can be used as metrics to measure progress.

c) Check whether a conference room pilot has been done

Conference Room Pilots are meant to progressively validate the design, configuration and customization activities. CRP can designed as

i. A project team presenting areas of the system to representatives from the business

ii. The business representatives actually performing job roles on the system, carrying out specific activities in a simulated environment

d) Check whether proper risk assessment exercise has been conducted

Effective risk management is fundamental to the success of any project. Risk registers created at the start of the project should be used throughout

the project life cycle and serve as a mechanism to avoid deviations from acceptable quality, costs, or timescale standards. Risks identified should be categorized in terms of their likelihood and their consequences.

Regular review meetings with managers and stakeholders where decisions can be made relating to the management of risks are pivotal for managing risks effectively.

The most common method for evaluating completeness of the configuration is to measure modules configured in each of the business areas (e.g., Customer Service, Operations and Finance) and report back on a weekly basis. Customization involves modifying the program code of the ERP system to gain a competitive advantage. Key differences between customization and configuration are :

- Customization is always optional, whereas some degree of configuration (setting up cost/profit centre structures, organizational trees, purchase approval rules, etc.) may be needed before the software can work
- Configuration is available to all customers, whereas customization allows individual customer to implement proprietary "market-beating" processes
- Configuration changes tend to be recorded as entries in vendor-supplied data tables, whereas customization usually requires some element of programming and/or changes to table structures or views
- The effect of configuration changes on the performance of the system is relatively predictable and is largely the responsibility of the ERP vendor. The effect of customization is unpredictable and may require time-consuming stress testing by the implementation team
- Configuration changes are almost always guaranteed to survive upgrades to new software versions. Some customizations (e.g., codes that use pre-defined "hooks" that are called before/after displaying data screens) will survive upgrades, though they will still need to be re-tested. More extensive customizations (e.g., those involving changes to fundamental data structures) will be overwritten during upgrades and must be re-implemented manually

f) Check the migration plan for migration of data relating to ERP

Data migration is one of the most important activities for determining the success of an ERP implementation. Since many decisions must be made before migration, a significant amount of planning has to be there. Unfortunately, because data migration is the last activity before the production phase of an ERP implementation, it receives minimal attention, mostly because of time constraint. The following steps of a data migration strategy can help with the success of an ERP implementation:

1. Identifying the data to be migrated
2. Determining the timing of data migration
3. Generating the data templates
4. Freezing the tools for data migration
5. Deciding on migration related setups
6. Deciding on data archiving

g) Check whether BCP or fall back plans have been developed

Whatever the size of an ERP project, a fallback or contingency plan is required to provide options, if any key component of the new solution is late or absent. The plan should first be developed on completion of the business process mapping and the high level design. At this point it will be clear where the key elements of the solution are located and what would be required at a high level for a successful launch should they not be available. The contingency plan should then be revisited after each CRP where input from the business will highlight or provide additional operational information regarding the importance of the various elements of the solution.

Audit of post-migration activities

a) Verify whether User Acceptance Testing has been carried out

The IS Auditor should review the user acceptance testing records. On completion of the ERP migration or implementation, the users are requested to test the configured ERP application. Based on the test results, the ERP application is fine tuned and further tests are conducted. The results of such user acceptance testing should be reviewed by the auditor to ensure that the

business blueprint requirements have been configured in the new ERP system and that the end users are committed to the new ERP application.

b) Check the new ERP configurations with the business blueprint requirements

The IS auditor should check whether the business requirements as per the business blueprint have been configured in the new ERP environment. For this the auditor should have reasonable knowledge of the ERP application. He may engage module specific functional consultants to carry out this task.

c) Verify whether the organization's DOA has been properly incorporated in the new system

ERP applications have robust user role and profile management functionalities. The IS auditor should check whether these configurations have been set as per the company's Delegation of Authority document. This can be checked by using various off-the-shelf tools or through a walk through of the application and its user configurations. The auditor should also check that these settings do not violate the segregation of duties concept.

d) Verify whether users have been provided adequate training

The IS Auditor should check the training documents to find out whether adequate end user training has been provided to the users. He should also ensure that user guides and system manuals have been provided by the ERP implementer.

e) Traditional GL balance checks and master data checks to be carried out

The IS auditor should also compare the GL data from the migrated ERP application with the data available in the old GL. He should also look into the control accounts in each of the modules and verify whether they tally with the control accounts balances in the GL. Similarly, the auditor should look at the cut-off documents in the old system and the new ERP environment to take care of such cut-offs.

A separate case study on SAP migration has been provided in another chapter.

Application Migration

Background

In a complex business environment, organizations have to keep up with technological advancements. Businesses are constantly upgrading or moving to new state of the art applications written in latest programming languages. Applications may consist of databases, languages and different systems. A seamless migration into the new application environment calls for effective planning and professional support.

Audit Objectives

A business enterprise carries out an application migration with the objectives that are mentioned below. The IS auditor should take into account these objectives while carrying out an application migration audit:

- Reduction in overall cost
- Increased agility
- Faster processing
- Increased productivity
- Minimum disruption of business continuity
- Easily adaptable system
- Chance to explore new opportunities
- Increased security

Audit Procedure

The IS auditor should consider the following checks for the pre- and post-migration activities:

a) Verify whether a case for migration to the new application has been defined and documented with reasons and expected results

b) Check whether experts with adequate technical migration knowledge are engaged in the migration activity

c) Check whether a proper migration plan has been prepared and key migration points have been identified. The plan should also include BCP and DR plans

d) Check whether the security requirements are met in the new application

e) Check whether all configurations in the old application have been implemented in the new application

f) Verify whether backup of all the data in the previous application has been created and tested for restoration

g) Verify whether the application has been tested and user acceptance has been received before the actual migration event

h) Check whether the existing hardware is compatible with the new applications, and if not whether suitable procurement plans have been made

i) Check whether the vendor of the new application has provided the company with adequate user and system documentation

j) Check whether data integrity checks have been carried out

6.4 E-Mail Migration

Background

Email migration means moving emails from one system to another efficient system. It involves many tasks, such as data migration, training, change management, hardware purchases, and licensing. Projects involving migration of the organization's entire mailbox content from one platform to another are time-sensitive, and require migrating email accounts, preferences, rules, folders, email messages, distribution lists, etc.

Audit Objectives

The key audit objectives that the IS auditor should focus on during an email migration are:

- New email environment should take care of the medium and long term future capacity requirements of the organization
- Technical support should be available for end users during the early part I the post-migration period

- Email migration should meet the business objectives like speed and better archival and retrieval facilities

Audit Procedure

The following checks need to be performed by the IS auditor during the course of the email migration audit:

a. Verify whether an inventory of email data has been prepared

When email systems are migrated, there is a significant amount of user data that the migration connector either cannot or will not transfer. It is therefore essential to get a complete understanding of the existing data. Major categories of email data include server side emails, client side emails, server side personal address books, client side personal address books, corporate address books, web server contacts, contacts and emails on PDAs, appointments and calendar data, and user accounts.

b. Verify whether the right migration tool has been selected

Selection of appropriate software is crucial for stable migration. The client side migration software should automatically configure itself for the workstation on which it is run to allow fully automated deployment. Some factors which should have been considered for the selection of the migration tool are:

- Is the migration tool client side usable?
- Should the software be installed or can it be run without installing it?
- Can the software be pre-configured so that it can be run non-interactively?
- Can the software locate the files automatically or the location of the files has to be manually mentioned?

c. Verify whether message conversion has been tested

The IS Auditor should check whether a small sample mailbox has been converted into the new environment and the following factors have been evaluated:

a. Did all the folders convert?

b. Does each folder contain the correct number of messages?

c. Did the subject of each message come though properly?

d. Are the dates correct? (Received, Created, Sent, etc.)

e. Are the unread messages appropriately marked?

f. Did the attachments come through? (Try opening a few of them.)

g. Are the embedded pictures converted properly?

h. Are the items from the old application's "Sent" folder put in the new application's "Sent" folder? (Same for Inbox.)

i. Can you reply a migrated message and get the correct email address?

d. Verify whether a stress test has been conducted

The IS auditor should check whether a stress test has been conducted during the email migration. A large mailbox has to be converted into the new environment and the following factors should have been tested:

- Did all the folders convert, even nested folders several levels down?
- Did the software complete the migration without any incident?
- Were very large messages migrated successfully?

e. Verify whether the contact conversion has been tested

The following checks should have been tested for proper contact conversion:

- Were all the address books converted?
- Can a contact be opened?
- Were contacts from the old default address book correctly placed in the default contacts folder/address book in the destination application?
- Are all the relevant fields migrating correctly? (For example, many migration applications don't convert fields like birthday, spouse, and comments.)
- Can a name from the default address book be used to create an email?
- Were the secondary email addresses copied correctly?
- Were the distribution lists converted?

f. Verify whether a pilot email migration has been done and feedback has been obtained

Pilot testing is essential to ensure that no last minute problems crop up. Samples for testing are drawn from both extensive users and beginners and the testing is done exactly to see how the final deployment is executed. User feedback should also be taken up during and after the pilot project. This helps to identify various problems faced by the users and develop suitable solutions.

g. Hardening and Implementing Security in the Email Server

The email server and security settings should be set in accordance with the security policy of the organisation.

6.5 Server Hardware Migration

Background

Hardware migrations are common occurrences in the system administration activities of most organizations. Frequent drive failures, controller failures and communication failures are signs of an ageing server and call for hardware replacement. Hardware migration encompasses migration of servers, networking equipments, storage devices, printers, etc.

The three primary reasons behind hardware migration are:

- The company is growing and cannot work effectively with the existing infrastructure
- The company is in the process of equipment consolidation
- Hardware has reached the end of its useful life and requires replacement

Audit Objectives

Server hardware migration audit should focus on the following audit objectives:

- The new server hardware should fit into the capacity planning of the IT infrastructure of the organisation
- The new server should result in consolidation and better system administration

- Migration should result in faster processing and enhanced employee productivity
- Server migration should result in the planned ROI

Audit Procedure

a. When an existing server is upgraded, say for instance from windows server 2003 to windows server 2008, it is essential to conduct the following checks:

   i. Verify that hardware and software are compatible

   ii. Obsolete users and local groups have been identified and cleansed

   iii. Disabled accounts and accounts that have not accessed the server for a period of time have been removed

   iv. Local groups without members or local groups that do not have access to folders or shares have been removed

   v. Unknown accounts and SIDs in local groups and files, folders and share ACLs have been identified and removed

b. If the migration involves server consolidation, duplicate user names and duplicate local group names from the servers that will be combined should be identified and removed.

c. Other technical considerations that should be verified are:

   - On the target server verify that the 'Local Password Policy' is equal to or less restrictive than the source server's password policy
   - Check whether password migration registry requirements are automatically set
   - Check whether the following settings have been enabled:
     - NetBios browsing should have been enabled to resolve computer names)
     - NetBIOS over IP should have been enabled in the source and target servers' TCP/IP Advanced Network Card Properties.
     - 'Enable lmhost Lookup' should have been enabled in the source and target servers.

- 'lmhosts' file with built-in LMHCreator should have been created after the migration.
- Remote Registry Services and RPC Services should be running on both the source and target servers.
- Account that is being used as the service account should have 'Logon as a Service' and 'Logon Locally' rights on the source and target servers.

- Verify that EFS is disabled on both the source and target servers

6.6 Operating System Migration

Background

Operating system migration can be conducted by adopting various methods. These include: (i) in-place upgrade or basic system upgrade of the new operating system, (ii) side-by-side computer replacement and (iii) clean installation. To determine which migration method to be adopted the following two factors should be considered:

- Whether the migration is from one hardware to another or within the same hardware?
- Whether the users' personality settings should be restored or captured and transferred?

Basic System Upgrade (In-place upgrade): This kind of migration is usually adopted in a home or small business environment. In a basic system upgrade the system engineer will physically carry out the upgrade in the end user's system. In this kind of migration, there may be participation from the end user who may like to have his preferential personalized settings. This is not an efficient way to manage large numbers of users or to create a consistent standard installation across the enterprise for easy manageability in the future. In-place migration usually leaves behind old operating system files, outdated applications and data in the machine.

Side-by-Side Migration: In this type of migration, user's data in the source machine is transferred a new target computer. In this kind of migration, a support lab and staging area are in place. This method is used for transferring user settings. Tools such as LDAP Directory may also be used to transfer user settings and data. Such tools help in making the migration activities remote and

centralized. This migration type results in too much administration overhead for the migration team.

Clean Installation: In this kind of migration, a standard installation on a new target machine is created. A baseline operating environment is created. This will include the standard operating system features, standard drivers and other standard utilities. A clean installation migration is useful for centralized and standardized deployment of operating system across an enterprise. This is the most efficient migration method in terms of cost, time and administrative efforts.

Audit Objectives

Audit of operating system migration should consider the following management objectives:

- Incorporation of enhanced features
- Providing better manageability
- Enhancement of productivity and performance
- Provision of increased application support
- Provision of greater security and reliability

Audit Procedure

A checklist for conducting the operating system migration audit is provided below:

1. **Backup**

   Make a backup of the entire existing operating system settings before migrating. In case of OS Upgradation, ensure that all the files, applications and system settings are captured as an image (using disc imaging feature). This avoids the need to individually transfer them for use on the new operating system.

2. **Hardware requirements**

   Ensure that adequate hardware as per OS requirement specifications is made available. Some OS vendors have come up with downloadable tools which can be run to find out if the system requirements are sufficient to install various versions of the OS (for e.g. Windows Vista Upgrade Advisor from Microsoft).

3. **Application compatibility**

Ensure that all the crucial business supporting applications are supported by the new operating system.

4. Migration Plan

Ensure that a proper migration plan with time schedules for migrating and assigned responsibilities has been prepared. The migration plan should also contain BCP or fallback plans.

5. Testing

Regression testing and stress testing have been planned and performed. The results of these tests should be made available to the auditor. In case of any adverse results, the auditor should look into the action taken report.

7
Case Studies

A Migration In A Bank

Migration from a non-core banking system to a core banking system software

Background

This case study provides an overview of migration activities involved in migrating data from existing non-CBS (Non Core Banking Software) to CBS, including details of planning and finalizing the approach for migration. The major application related migration checks (black box approach) which the information system auditor should undertake are also discussed. It should be noted that this discussion deals only with the activities relating to data migration involved in this kind of application migration. Other activities relating to the CBS migration like hardware upgradation, data center migration are not dealt with here.

Migration Activities

The activities relating to the migration of a legacy banking application to CBS software can be broadly classified as (i) pre-migration activities, (ii) migration activities and (iii) post-migration activities.

i. Pre-migration Activities

Prior to migration of data from the bank's existing legacy banking system into CBS, certain activities need to be completed as pre-requisites for setting up organization-wide data for CBS and cleaning up the existing data. These activities are:

a) Planning

A detailed plan of the various migration activities is drawn up. The plan also includes the responsibility matrix of the migration team members for the various migration activities. A business continuity plan is also a critical component of this activity.

b) Data Mapping and Preparation

This activity identifies mapping of fields from existing legacy banking system of the bank to fields in the new CBS, primarily for automatic conversion of data. This is also done to decide on the scope and the extent of manual data conversion

In the course of migration, banks use automatic migration tools. For the migration tools to work, organization data, module data and product data are set up.

While preparing the data for migration the bank prepares a migration guideline on the following lines:

- Date fields and percentages will be provided as per CBS format.
- If the balance in amount field is negative, the first character should be '-'sign or Dr/Cr as required by the new system.
- All closed accounts will not be migrated
- Only Cutover Date Balances will be migrated except for loan accounts. In case of loan accounts transaction history will be migrated.
- Interest accrual figure & last accrual date will be uploaded, so that new system can take care of interest calculation after migration by considering the accrual amount and date
- Codes like Country code, City code etc. in current system needs to be mapped with the new CBS system codes.
- If data is currently not available for certain fields in the new CBS, such fields will populated with some pre-defined default values by the bank.
- Account numbers in the old system should be migrated to the new CBS system with one to one mapping with respect to old system of numbering.
- The data upload file should contain all the records for the table line by line. Within the record in a line, the various fields would have to be provided in the format as required and mentioned in the data mapping document.

- All dates to be as per CBS specified format. The value of the field must not exceed the maximum length as specified in the data mapping document.
- The data type of the values provided in the file must match with the data type of the corresponding field values in the data-mapping document.
- There could be some fields that are not directly available in the source database, however if these fields are under the definition of mandatory fields in the new CBS software, the upload file should be structured by the migration team to take care of this issue. These fields may be assigned default values after considering impact of such data set-up in terms of operations in CBS system which needs to be ratified by banks' personnel.

c) Data Cleansing

In this stage, missing or incorrect data is rectified before conversion. The new CBS software may require certain unique keys (set of fields that make a record unique) to be set for each table. The bank will have to ensure that there are no duplicates on these keys. Pilot migration runs would indicate possible data cleansing that needs to be taken up before actual migration.

ii. Actual Migration Activity

The actual migration event will comprise the following activities:

a) Data Backup

Data in the existing legacy banking application as on the cut-off date for migration is backed up for compliance and business continuity purposes.

b) Data Extraction and Loading

Migration team culls out the data from the existing legacy banking application and builds it into a format required by the new CBS application. Extracted and formatted data is then loaded into the new CBS application by using data uploader tools.

c) Log analysis

When the migration of the data is completed, the migration team extracts logs of data moved and checks for any errors. The team then decides on the steps needed for rectifying those errors and transferring the missing data either manually or through automatic conversion route. Action taken report on such errors in the logs is prepared by the migration team and made available to the IS auditor at the time of post-migration audit.

The data that could not be migrated due to unavailability in the extraction file or erroneous source values needs to be manually maintained as a post-migration activity. The data which is defaulted by the migration programs due to non-availability in the old system might also need to be enriched and modified later for any corrections.

iii. Post-migration Activity

The major post-migration activity is data validation or post-migration audit by a qualified Information Systems Auditor. Data validation is an important component of data migration and adequate safeguards have to be built in to ensure that the exact status of the system before and after the migration is captured. This can be accomplished by using reports to compare the data migrated.

Validation methodologies, which can be used, are:

- The bank will identify the critical data elements for each module. After the Upload in the new system, the data will be extracted in the required format from the system. Data in the same format is extracted from the existing system and compared with the data extracted in the new system.
- The critical data from the earlier system is compared procedurally using the new system standards.

Apart from data validation, the IS auditor also checks whether adequate precautionary steps were taken prior to migration, as detailed in the Pre-migration activities section of this case study. A sample post-migration audit checklist is given below.

Sample Post-Migration Audit Checklist

The IS auditor undertaking a post-migration data consistency audit will use the post-migration audit checklist given below as a reference document and customize a detailed audit checklist based on the banking environment.

General Ledger

- Verify the balances from the Trial Balance in old GL on the date of migration to the Trial Balance from the migrated system. The balances may be verified at the GL level and adjusted for regroupings as required.
- General Ledger balances in the existing system should balance at the Branch Level. This means that at the branch level, the total Debits and Credits for real and contingent accounts should match separately.

Customer Information

- Verify Customer Information file (CIF) for generating new account numbers with old numbers
- Verify whether the mapping of the new customer number with the old number is maintained in the new CBS system for future reference
- Verify whether multiple CIF exists for a single customer
- Check whether CIFs have been created for all the joint account holders
- Check whether address and all-important data have been input in the system or else kept blank
- Check for mandatory parameters in customer masters that are blank

Data Mapping

- Check whether existing products have been mapped in the new system properly.
- A cross-reference of the GLs in the Old and the new systems should have been maintained at the extraction side as a mapping. This includes the product wise break-up of any GL balance. This will be helpful for the verification and reconciliation of balances GL-wise in both systems at the end of the conversion activity.

Balance Carryover

- Verify whether account-wise balances for all products (SB, CA, Loans, TD) in the old system have been carried forward to the new system
- Verify whether accounts with frozen status have been migrated with the same status
- Check SB Interest for accrual and carry over on the date of conversion
- Verify that the break up between principal and interest, progress period interest, charges, holiday period in loans (and term deposit) have been correctly retained along with special category (Like NPA etc)
- Check whether active limits and drawing power have been migrated properly
- Check whether lien marked details have been migrated with the same status
- Verify whether security details and loan documents have been migrated properly
- Ensure that the date of last date of interest credit / accrual has been correctly entered in the new system
- Verify the carry over of individual entries in suspense debtors (others) in the new system
- Verify for carry over of individual festival advance / suspense debtors (staff accounts) etc
- Verify for the carry over of locker caution deposit of all the lockers account-wise. Check whether reconciliation is in place for the account
- Verify whether outstanding OBC's have been carried over to the new system
- Verify whether DD/pay orders payable account of all the outstanding pay orders have been carried over to the new system
- Verify whether the pay orders payable account was reconciled on the day of conversion
- Check whether all the outward clearing outstanding cheques have been uploaded. Outstanding means deposited but not realized till the date of migration
- Check whether all the cheques accepted as a part of the cutover date's inward clearing have been reflected as debits in the customers' account

- Verify whether guarantees, open LC and bills have been correctly carried over to the new system
- Check for ATM suspense entries and their carry forward to the new system
- Check for ATM Switch receivable / payable account and reconciliation of such accounts post migration
- Verify whether the Bank has sent customer statement generated from the old system on the date of stopping the operations and obtained confirmation

Instructions

- Verify carry over of Standing Instructions
- Verify stop payment instructions in SB, Current, CCOD
- Verify whether stop payment of drafts has been carried over to the new system accurately
- Check whether special notes with regard to Lien, Deceased A/c, Stop Payment of cheques, attachment order, Garnishee order etc., have been carried over accurately in the new system

Log Analysis

- Verify the exception reports (errors/integrity error reports) generated during data migration procedure
- Ensure that all the exceptions have been rectified and necessary sign off has been obtained

Other Master Data

- Check whether Interest rates for Deposit Accounts / Loan Accounts have been correctly carried over
- Check whether account status in products such as inactive, dormant, overdue have been correctly carried over
- Verify whether cheque books issued to the account holders have been carried over to the new system
- Evaluate controls over migrating signatures of customers to the new system

Backup

- Check whether the entire Backup of Database up to the date of conversion has been taken. This is required for legal compliance and business continuity purposes.

B Sap Migration

Migration from disparate legacy business applications to Enterprise-wide Resource Planning (ERP) application

Investment in enterprise resource applications (ERP) and enterprise applications in general remains the top IT spending priority for most large organizations. A major driver for many large companies is regulatory compliance initiatives such as Sarbanes-Oxley for public companies or Basel II in the banking industry.

Other business drivers behind the decision to purchase and implement ERP applications like SAP include:

- Standardizing enterprise business applications to support and unify business processes that are changing and evolving
- Providing accountability through operational transparency
- Upgrading or consolidating existing SAP systems due to new functionality or a company merger or acquisition
- Creating a single view of the customer to cut order costs and increase customer satisfaction

Major phases in SAP implementation

ERP applications like SAP have a considerable impact on business processes. Therefore, the decision to purchase and implement them is approached with considerable diligence.

a) Vendor Selection

While the vendor selection and implementation decision (gets much of the spotlight change this by stating why this spotlight), the success of a SAP implementation hinges on critical project phases.

b) Business Process Re-engineering

Software that touches and drives processes across the enterprise cannot simply be installed and turned on. Current “as is” processes must be understood and methodically mapped to the new SAP system and it’s “to be” capabilities. Invariably, gaps are uncovered during business process reengineering which must be planned for.

c) Change management

SAP implementations cannot rely on an "if we build it, they will come" approach. The success of a new business application is ultimately measured by its adoption by business users. Careful consideration must be given to executive sponsorship and to business and technical user training.

d) Data Migration

While business processes evolve and are enhanced during these aforementioned project phases, no data is migrated directly from one system to another during these phases. Data migration is the only phase during which data is actually moved from legacy applications to SAP. Effective data migration directly affects business user adoption rates. Data migration is therefore a critical component of a SAP implementation.

One of the major reasons for organizations to implement SAP is that it helps to centralize business processes and data within a consistent application. With the mature and growing list of mySAP business applications, SAP boasts more than 30,000 interrelated tables driving business across more than 25 industry verticals. While the SAP application platform provides mature interfaces to upload data into SAP, these application program interfaces (APIs) typically require the data in a specific format to be properly validated and accepted by the SAP application layer. Data typically is not loaded directly into the database layer of any SAP system, but instead has to t pass through strict validation checks based on SAP business rules within the application layer.

SAP Interface and Loading Techniques

The Information System Auditor should know what kind of interface and loading techniques are available in SAP for data migration to judge the adequacy and effectiveness of the controls that are inherently available in these techniques. The various interface and loading techniques available for SAP data migration are given below.

i. Data Migration Interface (DMI)

   a. DMI is a SAP certified interface tailored for SAP data migration

   b. DMI includes SAP delivered programs for the most common master and transactional data need in any SAP data migration project

c. DMI requires data to be in a valid flat file

d. DMI supports a combination of batch and direct input of data into SAP

ii. Batch Input Processing

e. Batch input processing is a more common method of migrating data into SAP

f. Batch Input Processing automates and mimics processing data in the same fields and screens as an online user would step through the entire SAP transaction logic

iii. Direct Input Processing

g. Under Direct Input Processing method, data is directly written to the database layer of an SAP system

h. Direct input processing method does not go through the complete SAP transaction logic

i. This method takes into consideration the SAP application validation checks

j. This kind of migration may be used if throughput from batch input is not much.

iv. Intermediate Document (IDOC)

k. IDOC is a Standard SAP data structure for common business objects such as material master, customer master, GL accounts or purchase order

l. IDOC supports integration of both transaction and master data

m. Advantage of IDOC is it can carry out near real time data movement as well as larger batches of data

v. Business Application Programming Interface (BAPI)

n. BAPI is a library of standard SAP interfaces that are Remote Function Call (RFC) enabled

o. BAPI has the capability of migrating data both ways - into and out of SAP

p. This data migration method may be used to do pre-validation or lookups of legacy data against the SAP application

vi. Computer Aided Testing Tool (CATT)

   q. CATT supports the testing of a SAP business process

   r. Though this tool is designed for recording and automating QA tests, it can be used for migration of data into production environment

vii. Legacy System Migration Workbench (LSMW)

   s. MSMW orchestrates various data migration processes and thereby facilitates easy migration of data. Strictly, this is not a migration method but a combination of different migration methods.

   t. Under this migration technique, BAPI, IDOC or DMI processes are scheduled and run by LSMW to migrate data

   u. This technique supports both direct input and batch input processing techniques

Data validations available in SAP

During the course of data migration in SAP, if parts of the data being loaded into SAP doe not pass the SAP validation, the entire record will be rejected by the system. The following are the various types of data validation checks performed by SAP:

- Syntactical – Validity of the field length and the data type of the data that is being migrated is checked
- Semantic – This is a contextual verification of data. Whether the piece of data represents a customer or material item or vendor is an instance of semantic validation.
- Structural – Under this validation, the parent – child relationships are checked. Eg: Header and line items of invoices.
- Dependency – Under this validation, data is validated against other master records or dependant transaction detail.

Sample audit procedure for SAP migration audit

SAP data migration is not just about moving the data into SAP; it is about making the data work within SAP. This means that the data in the SAP application must be accurate and trustworthy for business users to readily transition from their legacy applications to SAP applications. Information Systems Auditor who has

been engaged by the organization carrying out the SAP migration should consider the following aspects during the course of audit to give an effective management assurance report.

Pre-migration Checks

a) Check for migration plans

Research has shown that software implementations are put at risk when data migration is not thoroughly considered and planned. According to recent research, more than 80 percent of software implementation projects fail or overrun their budgets and schedules. Of the projects that are overrun, half exceed timescales by 75 percent and two-thirds exceed the overall project budgets. The successful implementation of mission-critical SAP enterprise applications requires a mission critical approach to data migration. The migration plan should be meticulously planned. It should include migration timelines, methodologies, tools to be used, responsibilities of the migration team and tests to be carried out by the migration team. The plan should also include back-out plans in case of delay or failure in the execution of the migration plan. The IS auditor should check that such migration plans do exist.

b) Check whether source data has been identified and analyzed

Most teams tasked with migrating data into SAP to have experience with the legacy systems. But these teams are often new to SAP and the requirements corresponding to migrating data into SAP. Data migration project teams often may not give sufficient attention to the identification and analysis of the source data to be required by SAP.

IS Auditor should verify whether the migration team has considered the following while analyzing the data:

- Whether all data sources spread across mainframes, proprietary legacy applications and other packaged applications have been considered?
- Whether data residing with a business partner or remote data center have been considered for migration?
- Whether the existing data will fit the new system?
- How will XML/hierarchical data structures or non-relational database (NRDB) data formats be reconciled in SAP?

- Whether existing data is of good quality? Without proper data analysis, how can the data migration team be sure?
- Does the SAP project team include the business and technical experts who understand the legacy data and business rules?
- Is the migration / implementation documentation complete? Is it reliable? Does documentation even exist?

c) Check whether appropriate migration tools, techniques and resources have been deployed

While extracting data from legacy applications, requisite skill sets and resources with legacy application knowledge should be available. The key considerations while migrating from legacy applications are identification of sources, method of data extraction, staff involved in migration and tools to be deployed. These tools and techniques must be provide accurate data migration within the planned timeframes.

As mentioned earlier, the IS auditor should also look into the techniques being used for data migration for him to judge the adequacy and effectiveness of the controls that have been exercised in the course of data migration.

Post-migration Checks

a) Blueprint verification

SAP configurations in the various SAP modules like FI, CO, GL, MM, SD, AM, HR, PP, PS etc should be cross checked with the business blue-print document prepared by the SAP implementation team and vetted by the management of the organization. This review provides considerable assurance to the management on the quality of the SAP implementation.

b) Data Consistency Checks

The IS Auditor should verify that the data that has been migrated into the SAP systems are consistent with the data as on the cutoff date for migration in the legacy systems. Establishing master controls like checking of GL level balances, number of item masters, number of employees, number of product lines, number of business units, etc help the IS auditor in checking data consistency, in addition to various advance data consistency checks like bit level checks. Also SAP provides with numerous reports in each module for

verification and reconciliation with other modules and other applications. The IS auditor should familiarize himself with these reports before undertaking data consistency checks.

c) User / Profile and SOD Review

The IS Auditor should perform the following user / profile and segregation of duties review by using the current Delegation of Authorities (DOA) document:

- The IS auditor should validate roles, profiles and rights assigned in SAP with the functional roles performed by the users and identify any discrepancies between them
- The IS auditor should identify users with access to company codes / business divisions outside their area of activity
- Critical violation of segregation of duties controls should be identified

d) User Training

For successful migration from legacy applications to SAP, the end users using the SAP application should be retrained on the new SAP environment. All users should be involved in end user training and proper sign-off should be received from them for satisfactory completion of user training.

e) Documentation

During the course of SAP implementation, many documents need to be created. The IS auditor should ensure that such documents have been created with version controls. These documents include (i) User Requirement Document (ii) Business BluePrint (iii) Testing Documentation (iv) System / Technical documentation (v) Post-migration test document. All these documents should be signed off by appropriate persons like end users, core team users and management staff.

Annexure 1

Bank Branch Level CBS Migration Audit – Sample Checklist

Sl.No	Control Question	Auditors Comments
1.	Verify the balances from the Trial Balance in Branch GL on the date of migration to the Trial Balance from CBS. The balances may be verified at the GL level and adjusted for regroupings as required.	
2.	Verify Customer Information file (CIF), generation of new account number with old numbers. Whether multiple CIF exists for a single customer? If so whether cleansing has been done prior to migration? Whether CIF's have been created for all the joint account holders? Whether address and all-important data have been input in the system or else kept blank?	
3.	Verify the exception reports (errors/integrity error reports) generated during data migration procedure. Ensure that all the exceptions have been rectified and necessary sign off has been obtained.	
4.	Verify whether the pre-migraion and post-migration reports (Trial Balances / General Ledger Balances etc,) have been approved / signed off by the Branch Manager and Officer, along with the personnel from conversion team.	

Sl.No	Control Question	Auditors Comments
	Whether these Conversion Reports are preserved after authentication as a permanent record for future reference?	
5.	Select a few balances for all products in CBS (the sample for which audit is being conducted may be used for testing the migration also) and verify the closing balance in the earlier system and ensure that the same has been carried forward to CBS.	
6.	Verify that the break up between principal and interest and the fields like term deposit and category has been correctly retained. In respect of sample selected, ensure that the date of last date of interest credit / accrual has been correctly entered in CBS, and confirm the same by manually computing interest for the same.	
7.	Verify for carry over of individual festival advance / suspense debtors(staff accounts)etc.,	
8.	Verify for the carry over of locker caution deposit of all the lockers account wise. Check whether Reconciliation is in place for the account.	
9.	Whether outstanding OBC's are carried over to CBS system.	
10.	Verify 'Pay orders payable account' of all the outstanding pay orders have been carried over to the new system. Whether the Pay orders Payable account has been reconciled on the day of conversion? If No, whether the A/C is now balanced? What are the plans of the branch / data center for this account into an automatic reconciliation type, to facilitating control on open entries.	

Sl.No	Control Question	Auditors Comments
	Also verify whether the Pay Orders Payable reconciliation, are done monthly after post conversion.	
11.	Verify carry over of Standing Instructions	
12.	Veriy whether Stop payment Instructions for SB, Current, CCOD accounts have been migrated to the new CBS	
13.	Whether Interest rates for Deposit Accounts / Loan Accounts have been verified?	
14.	Whether cheque books issued to the account holders are carried over to the system? Also check for Cheque Book records maintained by the Branch prior to conversion.	
15.	Whether the entire Backup of Database upto the data of conversion is taken?	
16.	Whether a certificate is available at the Branch for having checked and authenticated all the Account balances under each Head of Account.	
17.	Whether stop payment instructions for Drafts have been carried over to new system accurately.	
18.	Whether special notes with regard to Lien, Deceased A/c, Stop Payment of cheques, attachment order, Garnishee order etc., have been carried over accurately in the new system.	
19.	Have signatures been scanned for all SB,CDCC accounts? Report the number of accounts for which signature has not been scanned.	

Annexure 2

Database Migration Audit – Sample Checklist

Sl.No	Control Question	Auditors Comments
A.	**Pre-Migration Activities**	
1.	Whether appropriate data migration technology has been considered and frozen?	
2.	Has the time frame for the data migration been arrived at?	
3.	Is the migration team adequately staffed and have appropriate experience in migration?	
4.	Have the roles and responsibilities of the migration team members been defined?	
5.	Has a risk assessment or business impact analysis of the data migration project been done?	
6.	Is there a detailed data migration plan in place?	
7.	Does the data migration plan incorporate backout or BCP plan?	
8.	If any third party vendors are involved in the data migration, have they been adequately briefed about the migration activity?	
9.	Whether data mapping has been done between the source and target data?	
10.	Have data migration tools been identified and tested?	
11.	Is there a data quality specification document to which the final migration results should adhere to?	

Sl.No	Control Question	Auditors Comments
12.	Have service level agreements been defined for the migration team members as well as for third party vendors?	
13.	Has the migration been tested in a test environment before the actual migration? Have the results of such tests been recorded?	
14.	Have appropriate data validation techniques been identified?	
15.	Is there a proper plan to decommission the legacy data and legacy hardware?	
B.	**Post Migration Activities**	
16.	Has the change management procedure of the organization been followed for the data migration?	
17.	Have logs of the migration activity been captured and analysed for errors? If any errors were found, has an action taken report been prepared?	
18.	Has the performance of the new database been clocked and compared with the migration objectives?	
19.	Are there signoffs from the business teams for successful migration and decommissioning of the legacy data	
20.	Check whether the database security parameters of the legacy system been transported to the new database.	

Annexure 3

Useful Website Links for IT Migration Audit

Some useful website links on various migration events, migration strategies and open source data migration tools are provided below:

www.datamamgmtguide.computerworld.com

www.erp.ittoolbox.com

www.microsoft.com/midsizebusiness/businessvalue/erp-strategy.mspx

www.databasejournal.com

www.technet.microsoft.com

www-03.ibm.com/systems/migratetoibm/reasonstomigrate/

www.sun.com/datacenter/migration/

www.itsmwatch.com/itil/article.php/3758781

www.datacenterjournal.com/content/view/3068/40/

www.talend.com - For open source data migration and integration tools