सत्यमेव जयते

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

PursuIT e-Journal

International Center for Information Systems and Audit

of

COMPTROLLER AND AUDITOR GENERAL OF INDIA

PursuIT

December 2020 issue

Auditing in ERP Environment

About the Journal

The e-Journal “PursuIT" is a platform for sharing of experience and inculcating professional excellence in the emerging areas in the domain of Information Technology. The e-Journal aims at having features on emerging areas of Information Technology viz. cybersecurity, Data Security, e-Governance etc. The e-Journal also looks into the technological developments, future of technology, national policies and standards, as well as articles on IT Audit conducted in various SAI’s.

Editorial Board

Feedback/Suggestions

We strive for constant improvement and encourage our readers to provide their valuable feedback/suggestions to make the endeavor successful. Send us your suggestions, comments, and questions about the e-Journal to icisa@cag.gov.in.

Submission of Articles

To support this initiative of e-Journal, we welcome you to contribute electronic submission of articles from emerging areas in the domain of Information Technology. The article should be relevant to the theme of the upcoming e-Journal and should be in the range of 1000 to 3000 words. All submissions should be accompanied by a short profile of the author. The article is to be sent to icisa@cag.gov.in.

Disclaimer

Facts and opinions in articles of the e-Journal are solely the personal statements of respective authors and they do not in any way represent the official position of Indian Audit and Accounts Department. This e-Journal is for internal circulation within Indian Audit and Accounts Department only. The contents of this e-Journal are meant for information purpose only. ***i****CISA disclaims all liability for actions taken or failed to be taken based on any content of this e-Journal.*

Director General’s Message

PursuIT -the e-Journal of iCISA in its journey exploring new dimensions in Information Technology Auditing is presenting the fifth issue. The main aim is to disseminate knowledge and share experiences among the officers and staff of IA&AD. I am hopeful that this issue will add value to the reader.

In this issue, the focus is on auditing in Enterprise Resource Planning (ERP) environment. The articles on Waste Management in Indian Cities using GIS and Smart Technologies, Data Security in Cloud Environment and Risk Management of e-Governance- ICT Based projects are also included. An article on implementation of software applications viz. Optimise Performance using Technology and Information & Management in Audit (OPTIMA) & Auditee Information Management System (AIMS) developed in-house in IAAD is an example of innovation in our field office.

Considerable effort has gone into bringing it in its present form and the efforts of the officers who have contributed is worth appreciating. I am glad to acknowledge the efforts of members of the Editorial Board and my distinguished predecessor for their efforts despite their busy schedule. Looking forward for your valuable suggestions to make this e-Journal better in future.

K. Srinivasan

Additional Chief Technology Officer & Director General, *i*CISA

Auditing in ERP Environment

- Mr. R . Jayaprakash

ABOUT THE AUTHOR

Mr. R Jayprakash is a retired Senior Audit Officer- Trained in ERP systems and have 5 years of audit experience in ERP systems of public and private telecom service providers in India. He also authored a book titled 'Handbook on Audit in PSU ERP' for Office of the Finance & communication, Delhi. He regularly contributes write ups on new trends in the field of accounting, auditing, management, governance, Information technology etc. He also handled workshops on ERP, Information Technology Audit, High Value Contracts, VAT etc within the department and in public sector.

Migration to integrated IT solutions called ERP (Enterprise Resource Planning) systems in public sector has posed new challenges to auditors. Though the scope and objectives of audit remain the same, in the absence of paper trails, auditors have to rely on the database in the ERP. Unlike the legacy IT solutions, ERP solutions integrate various modules of organizational functions with intercommunication abilities and sharing a common database. The system-based workflow and inbuilt controls are also different from that in a manual system. For effective audit, auditors need the skill and expertise to interact with the ERP system of the audited entity.

Many ERP solutions like, SAP (Systems Applications Products), Oracle ERP Cloud, Oracle NetSuite, Microsoft Dynamics 365, Sage Intacct etc. are available in market.

This article intends to familiarize the readers with certain audit related issues in ERP system with special focus on procurement audit, based on hands on experience in SAP system of a central Public Sector Undertaking (PSU).

SAP provides vital inputs for risk analysis, like, revenue and expenditure patterns across different Business Areas, Profit/Cost Centers for different reporting periods, which facilitates selection of audit units and focus areas for audit. Analysis of various drilldown reports on POs, Materials, Inventory, Assets, debit/credit details, cleared/open items etc. helps in selection of samples for detailed audit.

Auditors need a clear understanding on the following:

- The business process re-engineering done in connection with migration to SAP
- The Architecture of SAP and the Enterprise Structure
- The structure of accounts and the General Ledger accounts in SAP
- The organizational functions and process flow

Understand the Business Re-engineering

Migration to ERP system necessitates certain business re-engineering processes. The major re-engineering done in a central PSU were merger of all civil, electrical and store units with the district level Business Areas (BAs), centralization of payment system, consolidation of banking operations, rationalisation and reduction in the number of Heads of Account from 6100 to 3700 and renaming of organizational units in SAP.

The Architecture of SAP and the Enterprise Structure

SAP has a three layer architecture- Database, Application and Presentation. In central PSU, the database is maintained in Oracle RDBMS at Outstation Data Centre and the Disaster Recovery site elsewhere. SAP architecture is given in figure1.

The Structure of Accounts and the General Ledger accounts in SAP

All transactions in SAP are recorded in a General Ledger. SAP maintains three types of Chart of Accounts. These are:

- **Operating Chart of Accounts:** It contains all the General Ledger (GL) accounts that are used to meet the daily needs in a company.
- **Country Chart of Accounts:** It contains a list of all General Ledger accounts that are required to meet the operating country's legal requirements.

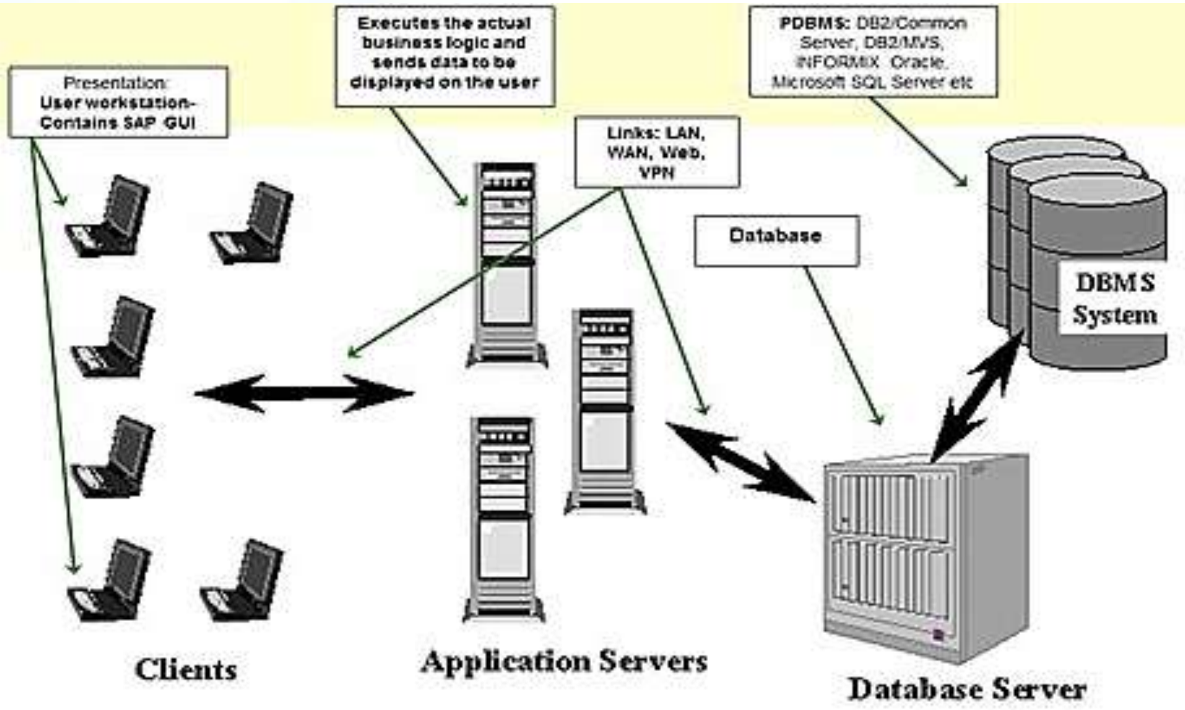

Presentation:
User workstation-
Contains SAP GUI
Executes the actual business logic and sends data to be displayed on the user
PDBMS: DB2/Common Server, DB2/MVS, INFORMIX Oracle, Microsoft SQL Server etc
Links: LAN, WAN, Web, VPN
Database
DBMS System
Clients
Application Servers
Database Server

Figure 1: Architecture of SAP

- **Group Chart of Accounts:** The group chart of accounts contains the GL accounts that are used by the entire corporate group. This allows the company to provide reports for the entire corporate group.

Since the central PSU is operating within India only, it has only one India specific Chart of Accounts in SAP.

General Ledger is the core component of SAP, which keeps all the transactions in a single database. The FICO Module (Financial and Control) manages the General Ledger and the other modules like HCM (Human Capital Management), Material Management, Sales & Distribution, Real Estate Management etc., share its database.

The Organizational structure and Workflow

SAP Enterprise structure is the organization as represented in SAP system. This is defined in the system for maintenance of data in an organized manner. At the top of the hierarchy there will be Company, which is the smallest organizational unit for which a complete set of financial statements can be drawn according to the applicable commercial laws. Under the Company, there will be different enterprise units like Business Areas, Business Segments, Functional Areas (HR, S&D, REM, and PM), Profit Centre, Cost Centre, Plant, Storage Location etc. The workflow in respect of every organizational procedure is also captured in SAP with relevant system-based controls.

Auditing in SAP- Requirements

- Creating Audit User ID by the IT wing of the audited entity.
- Setting up Audit workplace in laptop/desktop by installing SAP Graphic User Interface (GUI).
- Extensive authorizations within SAP Production system with read only access to all modules and features for effective conduct of audit.
- Installing Audit Information System (AIS) in SAP.
- Analysis tools like MS Excel, IDEA and KNIME.

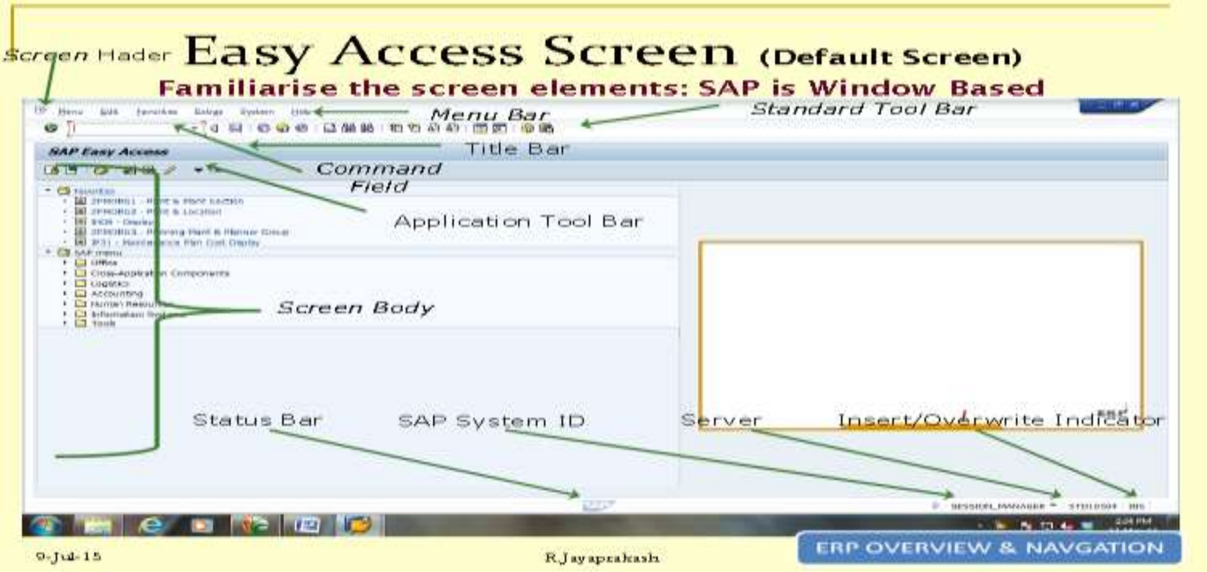


Figure 2: Screenshot of SAP Default Screen Elements

Auditors have the following options to access the data during an audit in SAP:

Audit Information System (AIS) is an Embedded Audit Module (EAM) for audit. It serves as a repository of reports, queries, and views. AIS enables auditors to monitor and analyze transactions in SAP. AIS can generate exception reports, which highlight data that are in some way anomalous or critical. Since AIS was not activated in the central PSU, audit was conducted through access privileges given to audit users.

Access Privilege

Auditors can log on to SAP, access the required data and obtain the details using the relevant Transaction Codes/Reports. The SAP menu folder 'Information System' contains Transaction Codes and Reports useful in audit. Reports are Advanced Business Application Programming (ABAP) whose function is to look up for information in the database and display it.

SAP Audit Management

SAP Audit Management is an end-to-end audit management solution, powered by High-Performance Analytic Appliance. It provides full coverage of the audit roadmap, including planning, preparation, execution, report, and follow-up.

Navigation in SAP

SAP GUI is menu driven with user friendly features. A screenshot showing the default screen elements in SAP Easy Access Screen is shown in figure 2.

Audit of Procurement in SAP

SAP is a 'Procure to Pay' (P2P) system which takes care of all procurement related activities like, requisitioning, purchasing, receiving, paying for, accounting for goods and services. The procurement functions are managed by the Material Management (MM) Module in SAP. The MM module consists of several components and sub-components. The most prominent and widely used are Material Master, Vendor Master, Purchasing and Inventory.

The Vendor Master contains all relevant details like vendor name, address, tax registration, bank accounts etc.

The Material Master contains relevant details of all the material procured by the organization etc.

The Procurement Process Flow in SAP

SAP follows the normal procurement process flow with necessary system-based controls (figure 3).

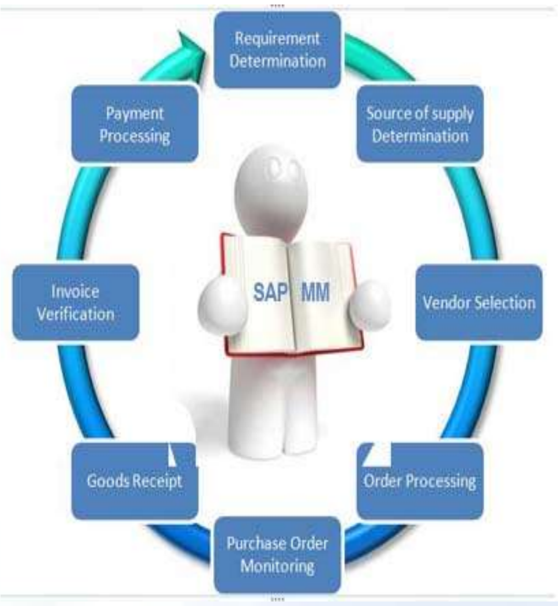


Figure 3: Procurement Process Flow

- Risk Ares in Procurement
- Audit of procurement in SAP environment
- should address the following risk areas.
- Unwanted/Excess Procurements
- Duplicate payments/Over Payments
- Violation of Payment terms
- Unauthorized or fraudulent transactions
- Missed discount opportunities
- Payment for damaged or defective goods.

SAP has system-based controls to prevent the above risks. Still, chances of frauds cannot be ruled out. One method of procurement fraud is creation of fake vendors in the Vendor Master with incomplete details (using transaction codes XK01, MK01, FK01). After the payment is made, the vendor is deleted from the Vendor master (tcode XK06). Another method is creation of a duplicate vendor with an abbreviated vendor name, but with the same details. The duplicate vendor is used for bid rigging or phantom bid. Sometimes the existing vendor master fields are temporarily modified to redirect the payment to a different bank account and reverting to the original details after the payment has been made. This method is called 'flipping vendor fraud'. A fake PO can be generated in the system to make a payment without the purchase occurring. These types of frauds can happen only if the system based controls are compromised or when there is collusion of many people.

An understanding of the Process Controls in SAP to mitigate the above risks will help the auditors in deciding the nature and extent of audit checks. A list of procurement related system-based controls is given in table 1

Table 1: Procurement related system-based controls in SAP

Sl. No	**Controls**	**Description**	**Examples**
1	Configurable Controls	Maintain the integrity of the Master Data	• Configuration of Vendor Master mandatory fields • Dual authorization for sensitive fields • Duplicate vendor checks- warning message and reporting
2	Manual Controls	Approvals by authorized individuals	• Decision making authority • Financial and administrative approvals • Segregation of Duties • Financial Powers etc.
3	General IT Controls	Computing controls to guard against unauthorized changes	• Input Controls • Process Controls • Output Controls
4	Process Controls	System process flow, authorization levels	• 2- or 3-way verification or matching of Invoice with POs and Goods Receipt
5	Detective Reports	Standard detective reports and customized reports	• Various reports in MM Module
6	Security Controls	Physical and logical access controls	• Physical access to the system • Logical access- username and passwords • Privileges to various functional areas in SAP based on segregation of duties
7	Policies & Procedures	Documented procurement policies and procedures which are to be mapped in to the system	• Procurement Policy document • Circulars, Guidelines and instructions on procurement

Procurement Related Audit Checks in SAP

SAP offers complete visibility to the auditors with the right type of access privileges. Auditors can cull out the required information from SAP using the relevant Transaction Code or Reports. The audit checks on procurement in SAP can be categorized as below:

General Checks on Purchase Requisitions, Stock Overview, Requests for Quotes

TCode/Report	Purpose
ME5A	Display a list of Purchase Requisitions
ME53N	Display a particular Purchase Requisition (PR)
MMBE	Display Stock Overview
ME48	Display Requests for Quotes (RFQs)
ZMMF_PC and ME49	Price Comparison of RFQs

PO Related Checks

TCode/Report	Purpose
ME2L	Display Vendor-wise Purchase Orders (POs)
ME2M	Display Material-wise Purchase Orders
ME2C	Display Material Group-wise Purchase Orders
ZFI172	Display Vendor Master
ME2N	Display PO by number
ME2W	Display PO by Supplying Plant

Vendor Related Checks

TCode/Report	Purpose
S_alr87012086	Display Vendor List
XK03	Display a Particular Vendor
RFKEPL00S_ALR_870012089	Display Changes in Vendor Master
RFKKVZ00 S_ALR_87012086	Display List of New Vendors
XK06	Display Vendor details
FBL1N	Display Vendor Line-Item Balances and Special GL Transaction with Vendors
FK10N	Display Vendor Account balance

Material Related Checks

TCode/Report	Purpose
MMBE	Display Stock Overview of a Material
MC.9	Display Material Stock
MC.A	Display Receipt and issue of Materials
MC.1	Display Plant Stock
MB52	Display Inventory Value
MB53	Display Plant Stock Availability

Audit Analysis

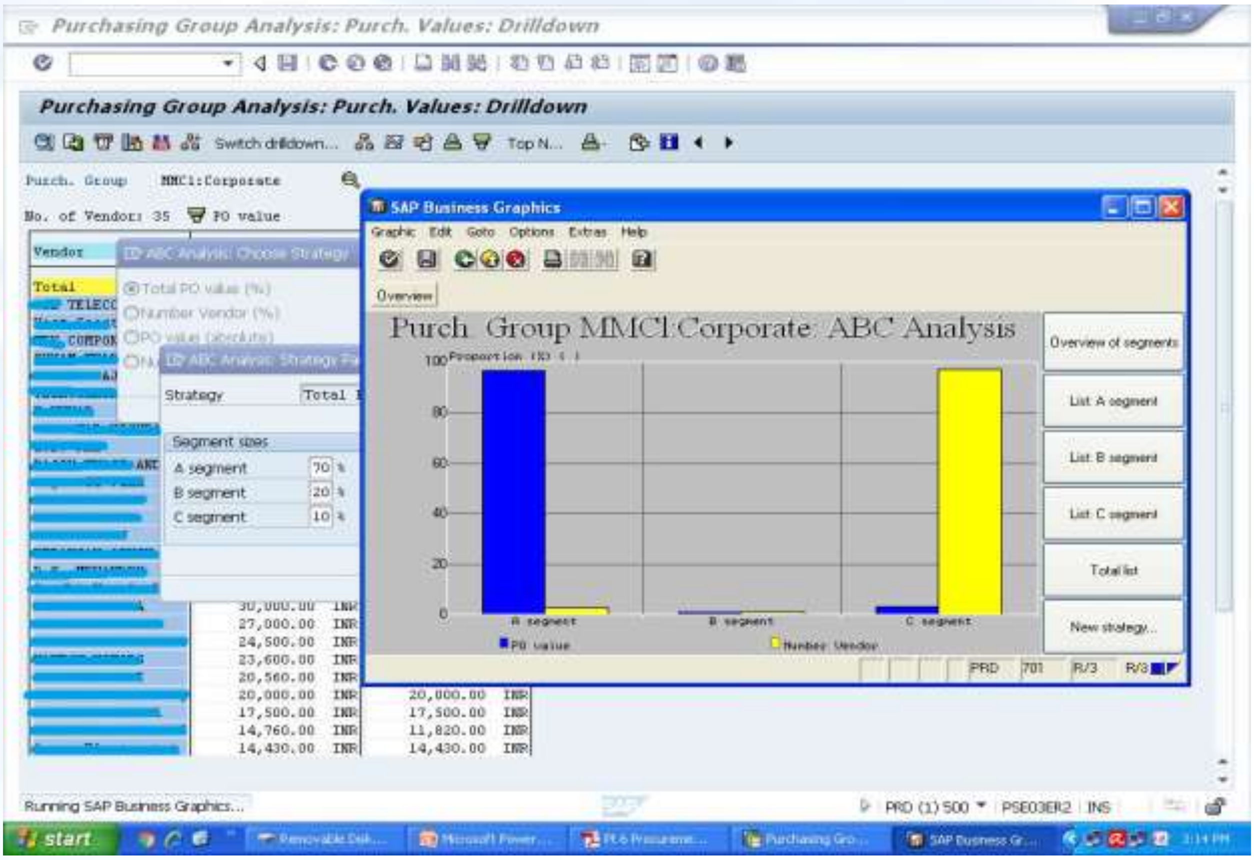
TCode/Report	Purpose
MC$0	Analysis of POs by Value
MC$2	Purchase Group Analysis By Frequency
ZFI106_V	Age-wise Analysis of Purchase from a Vendor
MC.5	Material Stock Analysis- Storage Location-wise
MC$N	Display PO Values
ZFI_MM_Posting **ZFI_MM_Recon**	Stock Value Report Duly Reconciled with GL balance
MB5L	Display GL Code-wise Stock Value
ZFI_PB_STAT	Display Payment Block Workflow
MM03	Display Material Document List
MM04	Display Changes in Materials
ME@J	Display Project-wise POs
MR51	Display Accounting Documents for Materials
FBL1N	Display Open Items (Invoices not paid)
MC40	ABC Analysis by Stock Value

The SAP Menu bars contain sub menus like ‘Switch Drill Down’ (month-wise, material-wise and vendor-wise), ABC Analysis (segment-wise, purchase group-wise), Item Changes (changes in materials), Material Stocks, Availability, Vendor, Quota Arrangement, Source List, Contract, RFQ, Purchase Requisition etc., which help the auditors in audit of procurement.

Auditors can track the complete changes in a PO right from the date of its release to the current date, by clicking ‘Item Changes’ under ‘Environment’ in the SAP Menu bar in the PO screen. Payment status on POs can be checked from the ‘Accounting Document’ and ‘Clearing Document’.

Auditors can verify from the Vendor Master details of inactive vendors, incomplete vendor fields, vendors sharing same address and other details, multiple ‘remit to’ address, vendors with no PAN/TAN, changes in Vendor Master, splitting of POs to circumvent financial powers, POs created after Invoice date, two vendors with same invoice number etc. These are some red flags, which needs further audit probe. Each transaction in SAP will create a Document with a unique number. The document header contains details on the document date, entry date, posting date, terminal Number, time, employee numbers etc., which leaves a permanent trail in SAP.

Auditors can also conduct various types of analysis for obtaining more insight on procurement made by the entity over a period for different materials from different vendors. Analysis can be material-wise, material group-wise, vendor-wise, month-wise, purchase group-wise. The menu bar has a sub menu for ABC Analysis, which will help the auditors to determine the relative importance of the different materials and on different vendors. A screenshot of the result of ABC Analysis is given in figure 4.


Purchasing Group Analysis: Purch. Values: Drilldown
Purchasing Group Analysis: Purch. Values: Drilldown
Switch drilldown...
Top N...
SAP Business Graphics
Graphic Edit Goto Options Extras Help
Overview
Purch. Group MMC1:Corporate: ABC Analysis
Proportion (%)
100
80
60
40
20
0
A segment
B segment
C segment
PO value
Number Vendor
Overview of segments
List A segment
List B segment
List C segment
Total list
New strategy...
ABC Analysis: Choose Strategy
ABC Analysis: Strategy Pa...
Running SAP Business Graphics...
start

Purch. Group MMC1:Corporate

No. of Vendor: 35 PO value

Vendor

Total

[redacted]

◉ Total PO value (%)
○ Number Vendor (%)
○ PO value (absolute)

Strategy	Total
Segment sizes	
A segment	70 %
B segment	20 %
C segment	10 %

30,000.00 INR	
27,000.00 INR	
24,500.00 INR	
23,600.00 INR	
20,560.00 INR	
20,000.00 INR	20,000.00 INR
17,500.00 INR	17,500.00 INR
14,760.00 INR	11,820.00 INR
14,430.00 INR	14,430.00 INR

Figure 4 : Result of ABC Analysis

Areas of interest in audit of procurements

Let us discuss certain procurement related specific areas of interest for auditors

GR / IR Clearing Account in SAP

Goods Received/Invoice Received (GR/IR) Clearing Account is very important in audit of procurement. It is an intermediary clearing account for goods and invoices in transit. It represents (i) goods received but invoice not received and (ii) invoice received but goods not received. The GR/IR account may also contain discrepancies between the invoice and the goods received that have not been resolved.

Invoice receipt entry is made through the Transaction Code Movement in Receipt Out (MIRO) and goods receipt entry is made through T/Code Movement in Goods Out (MIGO).

A debit balance in GR/IR account indicates that goods have been invoiced but not received and credit balance, indicates that goods have been received but not invoiced. The balance in GR/IR clearing account can also be due to quantity differences between goods received and invoice raised by the vendor.

Audit of GR/IR Clearing Account is necessary to ensure:

- the correctness of balance under GR/IR account and individual debits and credits
- clearance of balance at the end of the reporting period in respect of POs for which no supply pending
- Debits/credits are not kept pending for long, being periodically reviewed and settled.

GR/IR Account balance can be viewed using T/Code **MB5S**. We can also drill down the GR/IR Account from the Trial Balance to the transaction level. The details can be imported to Excel and an age-wise analysis can be made. By subtotalling the GR/IR account by PO line items in the Assignment field, grouping of related transactions can be made. From the document type, auditors can verify whether the missing item is on the IR side or the GR side.

Zero balance in GR/IR accounts at the end of the reporting period indicates that all items have been cleared and no goods are pending for invoices received and no invoices pending for goods received.

Hold and Park

SAP captures three dates on all transactions- (i) the Document Date which is the date available on the vendor document (eg invoice date) (ii) the Entry Date which is the date on which the transaction is entered in SAP (iii) the Posting Date which is the date on which the transaction is posted in the General Ledger. By default, a transaction is immediately captured in the General Ledger, unless it is held or parked by the user.

SAP offers the user an option to either 'hold' or 'park' a transaction without updating the General Ledger:

- 'Hold' the document: Hold is for short term when some details on the transaction is wanting. The same can be updated later and then posted in the General Ledger. If required, the transaction can be cancelled also.
- 'Park' the document: Park is for keeping the transaction pending for want of details/funds or for approval by higher authority.

A held transaction can be parked later, if necessary. Holding a transaction will not generate any document whereas parking will generate a document. Auditors can collect the details of all parked documents using the Transaction Codes FBL1N (Vendor related), FBL3N (GL related) and FBL5N (Customer related).

In the list generated, parked items are indicated by a yellow triangle. An age-wise or category-wise analysis of parked items will reveal documents held for long periods on which the auditor on the justification for parking can do further examination. Normal reasons are requirement of further verification, want of approval by higher authority, non-availability of fund etc. Unjustified parking for longer periods is indicative of lack of internal controls and chances of corruption or fraud. Unjustified parking can also result in loss/disadvantage to the Company.

One Time Vendor

The Vendor Master in SAP contains all the relevant details of the vendors with whom transactions are made by the organization. Before making payment, three-way check based on the PO, Goods Receipt and Invoice are made by the system and payments are made online to the bank account available in the Vendor Master.

The One Time Vendor (OTV) is a vendor to whom payments are not made on regular basis, but very rarely. Since the details of such vendors are not available in the Vendor master, the system-based controls are not available in the case of OTV, which makes it potential area for fraud. Organizations using SAP should enforce separate controls like, (i) posting the details and parking the documents for a second level authorization for making payments (ii) periodical review of all OTV payments by the higher management.

Auditors should pay special attention on OTV payments to ensure that there is no misuse.

Conclusion

A skilled auditor provided with the right kind of access privileges can very effectively conduct audit in SAP or any other such ERP environment. Trails of all transactions are captured in the form of Documents, which are immutable and auditors can easily track down the changes made in the database by the user.

Reference

i) *Audit Manual- Introduction to the SAP R/3 system focusing on audit aspects- Roger Odenthal*

ii) *SAP R/3 Handbook- Jose Antonio Hernandez*

iii) *Fraud Auditing in SAP R/3 Environment- Phil Moulton CA CIA MBT*

"The computer repair people take their job very seriously."

Waste Management in Indian Cites using GIS and Smart Technologies

- Dr. Nanda Dulal Das, IA&AS

ABOUT THE AUTHOR

Mr. Nanda Dulal Das did his M. Phil on "Dynamism of Agricultural Land-Use around Metropolitan Cities with a special focus on Delhi" and Ph. D. on "Convergence between Natural Resource Based Livelihood Programmes: A Case Study of Watershed Development Projects & MGNREGS" in India, from Jawaharlal Nehru University, New Delhi in the year 2009 and 2014 respectively. Mr. Das had extensively used techniques of Remote Sensing and GIS in his research. Mr. Das has worked at different times in Vidyasagar University, West Bengal Civil Service and Indian Defence Accounts Service before joining the Indian Audit & Accounts Services (2015 batch).

The Magnitude

Indian cities are faced with a massive challenge of managing wastes owing to their limited resources, lack of access to improved technologies and due to widespread absence of local-level awareness. In 2011, there were 7935 cities[1] in India and their numbers had increased by over 50 percent during the last decade (2001-11). In 2014-15, Indian cities had produced around 51 million metric tonnes of Municipal Solid Waste, with a per capita waste generation rates of 0.2-0.6 kg per day, as per Central Pollution Control Board[2]. India, as in 2018, was having the world's second highest numbers of urban dwellers with 461 million population (World Urbanisation Prospects, 2018, UN DESA)[3]. The population of Indian cities is expected to increase by another 416 million by 2050 and with an estimated per capita daily generation of 400 grams of municipal solid waste, the total annual waste generation would be above 126 million metric tonnes by 2050[4].

While generation of waste is growing exponentially with the growth of packaging industry and e-commerce in modern India, the collection and processing facilities for the municipal solid waste have not improved substantially.

[1] Data as per Census of India, 2011, available at the website of Ministry of Housing and Urban Affairs, Government of India, at http://mohua.gov.in/cms/number-of-cities--towns-by-city-size-class.php

[2] "Swachh Bharat Mission: Municipal Solid Waste Management Manual" (Part-II), (2016). Central Public Health and Environmental Engineering Organisation (CPHEEO), Ministry of Urban Development, Govt. of India.

[3] United Nations, Department of Economic and Social Affairs, Population Division, "World Urbanisation Prospects, 2018: Highlights", pp. 12.

[4] Ahluwalia, I. J. et.al. (2018), "Solid Waste Management in India: An Assessment of Resource Recovery and Environmental Impact", Working Paper No. 356, Indian Council for Research on International Economic Relations (ICRIER), pp. 30.

After the initiatives of ‘Smart Cities’ Mission in 2015, Government of India came up with comprehensive waste management rules covering almost all the aspects of waste management, in the year 2016. These are Solid Waste Management Rules, 2016[5], Plastic Waste Management Rules, 2016, Hazardous and Other Of these, the Solid Waste Management (SWM) Rules, 2016 seek to address the problem right at the point of waste generators by emphasising on segregation of wastes into bio-degradable, non-biodegradable and hazardous wastes for necessary collection and treatment. Besides, it also emphasises on waste recovery and scientific disposal.

The Focus Area

A large portion of budget of Indian cities was being spent on waste collection and transport. Even then, the overall collection efficiency of the urban solid waste is only around 70 percent, while it is around 100 percent in developed countries[6]. Moreover, while waste gets generated in the neighbourhood of the cities, they are carried to far off places as the cities start growing and environmental concerns and campaigns like dumping ‘not in my neighbourhood’ grow. This article seeks to highlight probable audit areas while studying waste management scenario in a city and areas where improvements could be made using the techniques of Remote Sensing and Geographic Information System (GIS), coupled with smart technologies. For the purpose of analysis, the waste management system of the city of Bhubaneswar in the State of Odisha, has been looked into. Selection of a suitable site for waste treatment and disposal, along-with increasing the collection efficiency by utilising smart technologies like smart dustbins, etc. are some of the plausible solutions. The later involves optimisation of size of dustbins at different locations based on historical data, optimisation of traffic route for quick and cost-effective collection and apportionment of vehicle types and numbers in terms of requirements.

Bhubaneswar Urban Agglomeration had a population of 0.88 million in the year 2011 (Census of India, 2011). Based on budget data available for the Bhubaneswar Municipal Corporation-(BMC) and analysis done, it is seen that proportion of expenditure on solid waste management has increased from 10 to 18 *percent* in the past five years. Further, the city’s population was over 1.2 million in 2015, which is growing at a rate of 24 *percent* per annum (Nanda et.al, 2019)[7]. Hence, the pressure is expected to increase on the city’s solid waste management system, which already has to take care of over 500 tons of waste per day. Remote Sensing and GIS technology has the potential to make management of waste easier starting from collection of waste, selection of waste treatment sites and selection of site for waste disposal to regular adjustment of waste management plan according to their impact on the environment. Since, many Indian cities are yet to perform waste

[5] “Solid Waste Management Rules, 2016” Ministry of Environment, Forest and Climate Change, Government of India, Available at http://moef.gov.in/wp-content/uploads/2019/10/Solid-Waste-Management-Rules-2016.pdf

[6] Shorley et. al. (2007), as cited in Nandan, A. et.al. (2017), “Recent Scenario of Solid Waste Management in India”, World Scientific News 66(2017), pp.56-74, EISSN 2392-2192.

[7] Nanda, S. and Panda, D. (2019). “Solid Waste Management in Bhubaneswar: Practices and Challenges”, International Journal of Management, Technology And Engineering, Volume IX, Issue I, Pp. 821-838, ISSN NO : 2249-7455

recovery to a large extent and a majority of waste is disposed of without treatment, the waste would contain variety of materials ranging from packaging materials, plastics, glasses and include even household bio-medical wastes.

Therefore, it is very crucial to place the waste disposal site at a location where adverse impacts of smoke, foul smell, ground-water contamination through leachate etc. can be minimised. The waste disposal site of the city of Bhubaneswar was studied as a case study.

Image 1[8] below shows the location of the BMC administrative boundary and the location of the waste disposal site at Bhuasuni:

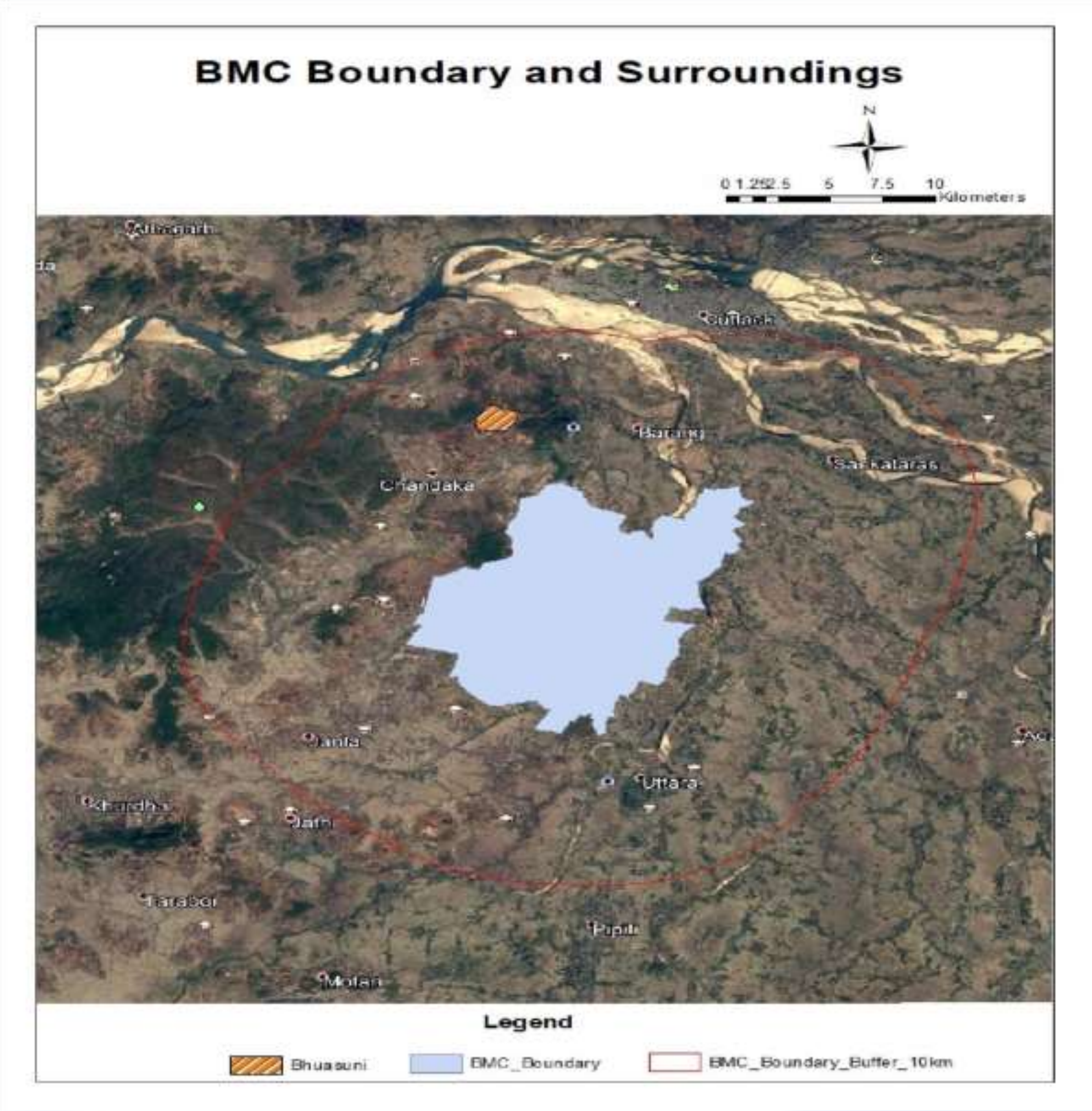


Image 1: Administrative Boundary of BMC, a Buffer Zone of 10KM and Waste Disposal Site at Bhuasuni

[8] Source: Imagery dated 31-12-2016, from Google Earth and BMC boundary from www.bmc.gov.in

In the above image, the red-shaded area in the North-west of BMC indicates the location of the final waste disposal site at the place named ‘Bhuasuni’, for the city of Bhubaneswar. It can be seen from the image-1 that the site is located within 10 KM buffer area from the main city limit. Incidentally, this site has also been envisaged as the waste disposal site for the city of Cuttack, the next largest and populous city in Odisha, which is around 15KM away, to the north-east from this site. The site comprises of around 61 acre of area and located on the fallow land[9]. Therefore, at this stage, it is understood that the availability of existing fallow land and locational advantage of the site, being in the transition zone of the twin city of Bhubaneswar and Cuttack, has been the reason for selection of this site for waste disposal. However, there are several other factors like distance from nearest lake/pond/river/stream, groundwater table, public parks, critical habitat areas, flood plain, notified habitat areas and public parks and the site seems to comply with these pre-conditions for getting environmental clearance on many counts (ibid.). Therefore, one might like to take a closer look at the site. The following images (Images 2 to 4) portray a digital elevation model, from SRTM[10] satellite data and google map for the waste disposal area:

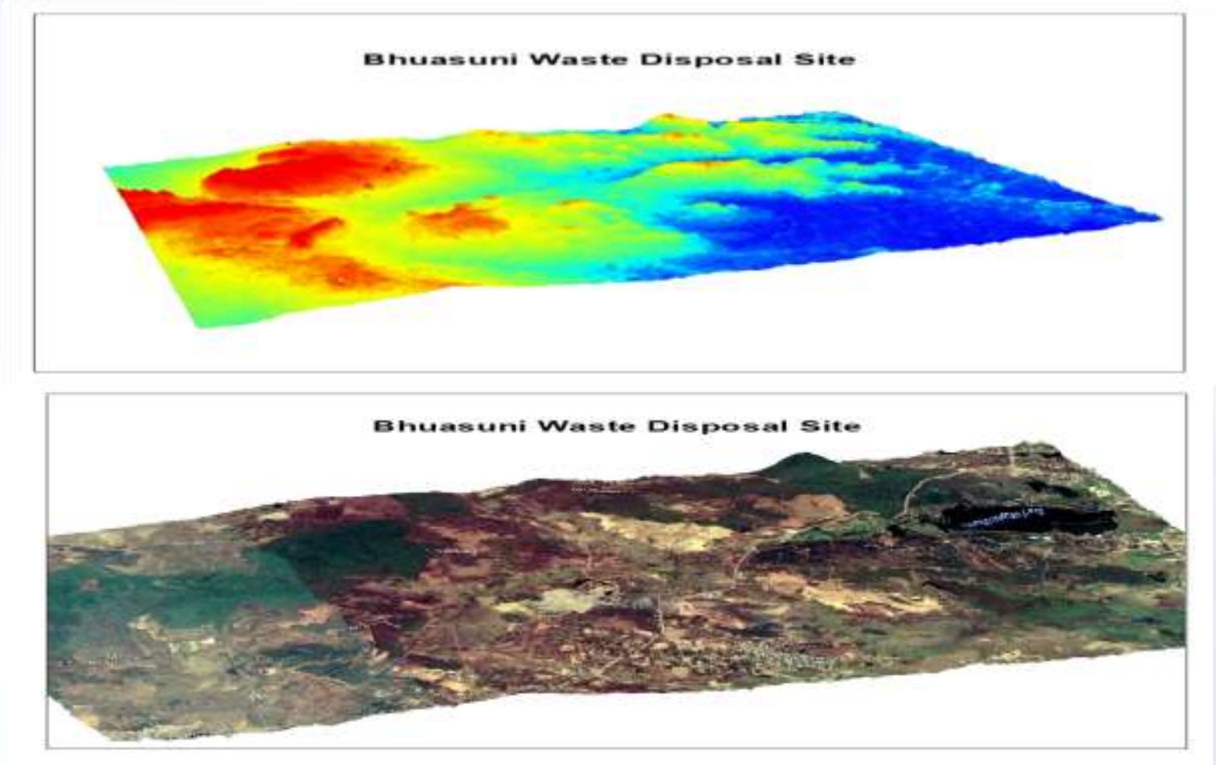


Image 2&3: Digital Elevation Model of the Bhusani Waste Disposal Site (2) and Satellite imagery superimposed for the site (3) [Height exaggerated for better visual representation]

[9] “Techno Economic Feasibility Report for Sanitary Landfill of MSW Bhubaneswar Ltd. At Bhuasuni, Daruthenga,Bhubaneswar, Odisha” (2015) as submitted by the MSW Bhubaneswar Ltd. for environmental clearance and available at http://environmentclearance.nic.in/writereaddata/Online/TOR/0_0_24_Feb_2015_1304342331TEFR.pdf

[10] Digital Elevation Model (DEM) from Shuttle Radar Topography Mission (SRTM), 90-m resolution, downloaded from https://www.usgs.gov/

Images (2 & 3) would give an idea that the waste disposal site is located in a valley region surrounded by hilly terrain on the three sides.

At this point, one needs to look into finer details from the features, associated with the disposal site, within the satellite imagery. Some of these have been brought out in the Image 4.

To add to this context, it is mentioned that the habitation, which is seen in the proximity of the waste disposal site, is the village called 'Daruthenga', the residents of which is in the forefront of leading a protest against locating the waste disposal site there. National Green Tribunal has also taken cognizance of the disposal site and a 'Technical and Economic Feasibility Report' regarding creation of an 11.5 MW waste-to-energy plant around the same site is pending for environmental clearance. Besides, the high growth rate of city population might see shifting of this waste disposal site to places far-off from the city limits, a trend which is quite visible in many developed countries.

Apart from above analysis on site suitability, GIS can also help in optimising collection of waste in a city like Bhubaneswar. At present, Bhubaneswar has a public-private partnership arrangement for solid waste management, with three private agencies catering to over 80 percent of the area under the BMC and a modest target of 100 percent waste transportation is followed with no waste treatment plan existing at present[11]. The waste generated throughout the city is collected through dustbins and transported through carts, trucks, trippers and dumpers. From around 5000 dustbins in the city, the waste is transported to around 1500 temporary storage sites (Nanda et.al, 2019). From these temporary storage sites, waste is transferred to a temporary storage depot (near Sainik School) before being finally dumped at the final disposal site, Bhuasuni (ibid).

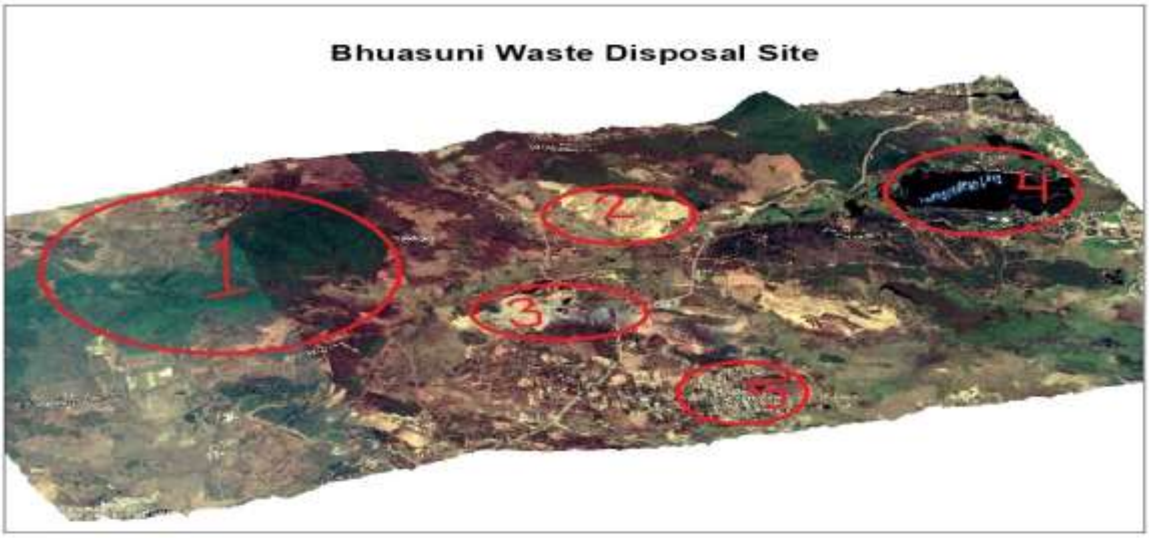


Image 4: Bhuasuni Waste Disposal Site: Issue Areas

[11] "Swachh Bhubaneswar Abhiyan", (2020). Available at https://www.bmc.gov.in/programs/swachh-bhubaneswarabhiyaan xi "Solid Waste Management (Vol. I)" (2005). United Nations Environment Programme (UNEP).

Municipalities in developing countries spend a large portion of their solid waste management budget on collection and sweeping (SWM, UNEP, 2005)[12]. Hence, cities are left with very scarce resources for treatment and disposal of waste. However, minor modifications in the existing systems like efficient design of collection routes, modifications in the collection vehicles, reduction in collection vehicle downtime and widespread public education may make available additional resources to the urban civil bodies (ibid.). One of the foremost innovations has been in the area of 'smart-bins', i.e. electronic sensor-based bins providing alerts when the bins are filled to a pre-set level. These can be set at any levels between zero and 100 *percent* of the bin volume. For example, if the bins are pre-set at 90 *percent* fill level, on reaching that level, the bins would send signals to the central control centre, which would then send signal to the nearest collection vehicle in that area. The waste would be collected accordingly and an efficient vehicle, route and mobility planning would further help in saving resources in terms of fuel consumption, traffic and time.Image 5 provides an indicative list of bins (at two levels) and route for visualisation.

In the image[13]5, indicative dustbins are shown through different colours and sizes. Wastes are collected from the primary bins and taken to the primary storage sites akin to the second layer bins marked in red which are then shifted to the depots and finally to the disposal site at Bhuasuni. Through GIS technology, it is possible to include a hierarchy of the roads, the direction of flow, timing for plying of waste collection vehicles and vehicular traffic load in different roads to derive an efficient waste collection plan.

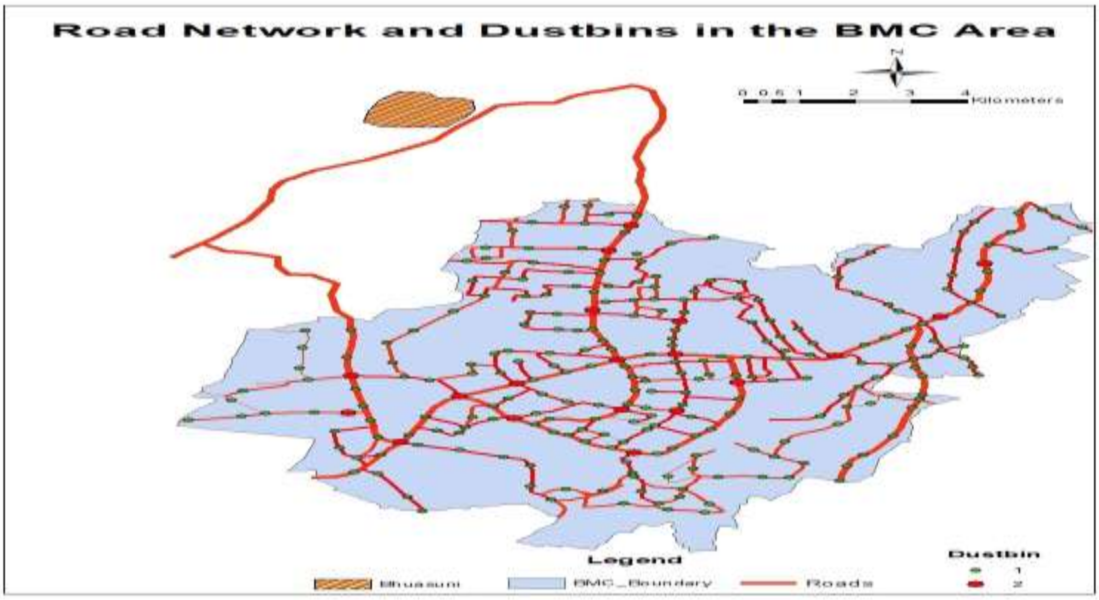


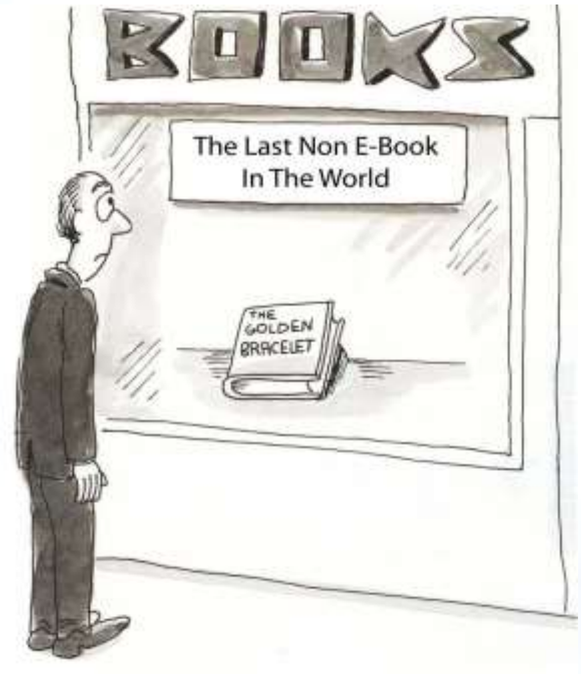
Image 5: Road Network, Dustbins and Disposal site in Bhubaneswar

[12] "Swachh Bhubaneswar Abhiyan", (2020). Available at https://www.bmc.gov.in/programs/swachh-bhubaneswar-abhiyaan

[13] (Disclaimer: The location and division of dust-bins are indicative, created only for visualisation and better understanding)

Conclusion

Concisely, Remote Sensing and GIS technology hold immense potential for auditing different aspects of waste management and in suggesting scope for improvements in the existing practice. From Remote Sensing data, identification of areas which have experienced illegal dumping of solid wastes and construction wastes can also be done in scientific manner. Although above analyses were done mostly on location-based data, the attribute data like composition of waste, stakeholders involved in collection of waste, cost involved in different activities from waste separation to waste recovery would further add several dimensions to such analysis.



Data Security in Cloud Environment

- Study Paper[14]

Introduction

Cloud computing is computing on the internet. It provides hardware platform applications as a service and enables ubiquitous access, convenience, on demand network access, and shared pool of configurable computing resources, available through internet, instead of having local servers or personal devices to handle applications. Cloud services are offered through public, private or hybrid cloud storage offerings, depending on the security needs and other considerations.

Organizations can determine their level of control with as-a-service options. These include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing takes services ("cloud services") and moves them outside an organization's firewall. Applications, storage and other services are accessed via web. The services are delivered and used over the Internet and are paid for by the cloud customer on an as-needed or pay-per-use business model.

Many organizations are moving to the cloud, due to the obvious benefits that it offers, which are ease and convenience of use, lower infrastructure requirements, ubiquitous access, increased efficiency, growing bandwidth demands, scalability etc.

To leverage these obvious benefits of cloud technology and to comply with the Jan Dhan Aadhaar-Mobile (JAM) trinity initiative of its e-Kranti scheme, the Government of India (GoI) has initiated the cloud based e-governance services delivery, to reach to the masses seamlessly. This cloud named as "MeghRaj" is set as the default cloud to be use by all the departments-at central and state level.

The Government of India (GI) cloud was launched for monitoring and management for sustainable governance. Operating in the cloud comes with greater risks than operating an on premise IT infrastructure. Moving on to cloud based services has its own associated risks and comes with a package of cloud specific threats, like poor security practices, insufficient identity, credential and access management, poor or no governance and management practices, application vulnerabilities etc. While, many departments have either already rolled their e-governance services through the cloud or are on the, verge of migrating into the cloud, they have sometimes done so, without doing the precursory groundwork and necessary checking of the various aspects, related to before, after and during the use of cloud based operations and services.

As organizations are moving their data from on-premises into cloud, it is making their data to share between the Cloud Service Providers (CSPs), Managed Service Providers (MSPs) and the cloud users.

"Every opportunity has associated risks" and in case of Government Cloud, ensuring the

[14] *Responding to the fast changing ICT landscape, iCISA has entrusted Centre for Development of Advanced Computing (C-DAC) to conduct a study on 'Data Security in Cloud Environment'. The salient points of the Study Paper are being published here.*

data security is one of the major risk. As the Government moves to the cloud, it must be vigilant to ensure the security and proper management of government information to protect the privacy of citizens and national security. The Government has specific cloud computing challenges that require careful adoption considerations, especially in areas of cyber security, continuity of operations, Information Assurance (IA), and resilience. The risks are significant as the data is sensitive and in large numbers of both public as well as the Government which is continuously on the rise. Therefore, it has become the need of the hour to understand the risks associated with the cloud, create awareness, share the knowledge with all the stakeholders, and take action to prevent, detect, and defend data from these risks.

Effective governance in the cloud is of the utmost importance, to have clear set of guidelines regarding the ownership and responsibility of the data and its security. The term governance in the cloud relates to the rules, policies, and processes used by businesses to operate in the cloud. These are the “what, when, who, and how” when it comes to cloud security and govern factors such as what assets can be used, when assets can be used, who has access to assets, and how assets should be protected against malicious entity (both inside and outside the business).

Thus, there is pressing need to not only have a sound cloud governance and management policy, but also a cloud enforcement policy to check, monitor and ensure adherence to the guidelines of the policy, by the stakeholders to manage the cloud data in a professional manner with cloud specific laws, regulations, clauses, and compliance. The regulations and guidelines are required to indicate what measures to take, if the data is lost, whom to approach, and who would be ultimately responsible for maintaining the integrity, confidentiality and availability of the data.

In the subsequent sections of the paper the present scenario in the deployment and adaptation of GI cloud, the challenges with data security in the cloud are presented and conclude with the cloud security objective, that are needed to be followed and the way forward for ensuring the same.

Overview and present scenario of GI cloud

The GoI has initiated e-Kranti with the vision of “Transforming e-Governance for Transforming Governance”, based on the learnings of National e-Government Program (NeGP) and with the aim for continuous upgradation and proliferation of the Digital India initiatives.

Amongst the key principles of e-Kranti, one of the important principles is Cloud by default, which indicates that all sensitive information of Government Departments shall be stored in a Government Cloud only, coined as MeghRaj. This was to ensure proliferation of Cloud in the government. Any Government Department may use a private cloud only after obtaining permission from Ministry of Electronics and Information Technology (MeitY), GoI, which shall do so after assessing the security and privacy aspects of the proposed cloud. The aim of the cloud policy is to realize a comprehensive vision of a government private cloud environment available for use by central and state government departments, districts and municipalities to accelerate their Information & Communication Technology (ICT)-enabled service improvements. GoI has proposed three different cloud deployment models. They are the public cloud, Government Virtual Private Cloud and Government Community Cloud.

The GI Cloud established, initially on national and state data center assets (adapted for the cloud through virtualization) is connected through existing network infrastructure such as the State Wireless-Aware Networks (SWANs), National Knowledge Network (NKN), as well as Natonal Information Centre Network (NICNET). Based on demand assessment and taking into account security related considerations, government may also engage the services of private cloud providers.

The GI Cloud will provide services to government departments, citizens and businesses through internet as well as mobile connectivity. In addition to accelerating the delivery of e-services to citizens and businesses, the government’s cloud-based service delivery platform will also support a number of other objectives including increased standardization, interoperability and integration, a move towards an operating expenses (Opex) model, the pooling of scarce, under-utilized resources and the spread of best practices. It will also support on-going cost effectiveness and manageability.

GoI has setup National Cloud under National Informatics Centre (NIC) and also has initiated setup of State Clouds, cloud computing environments at the State Level – building on or augmentation of the infrastructure investments already made, as shown in figure 5.

Based on the demand considerations, GoI has empanelled cloud service offerings of private service providers that the end-user departments can leverage in addition to the National Cloud services offered by NIC for their e-governance solutions.

The cloud providers would require common standards & guidelines on the security, interoperability, data portability, Service-Level Agreements (SLAs), contractual terms & conditions, service definitions that they would need to adhere to in order to be part of the GI Cloud environment. In order to realize the policy and facilitate cloud services adoption by the Center and States, there is a need to define the GI Cloud Reference Architecture, identify the common standards, service definitions, develop guidelines with respect to security, service delivery, interoperability and portability that the cloud service providers (CSPs) will have to adhere to and for the departments to leverage cloud services.

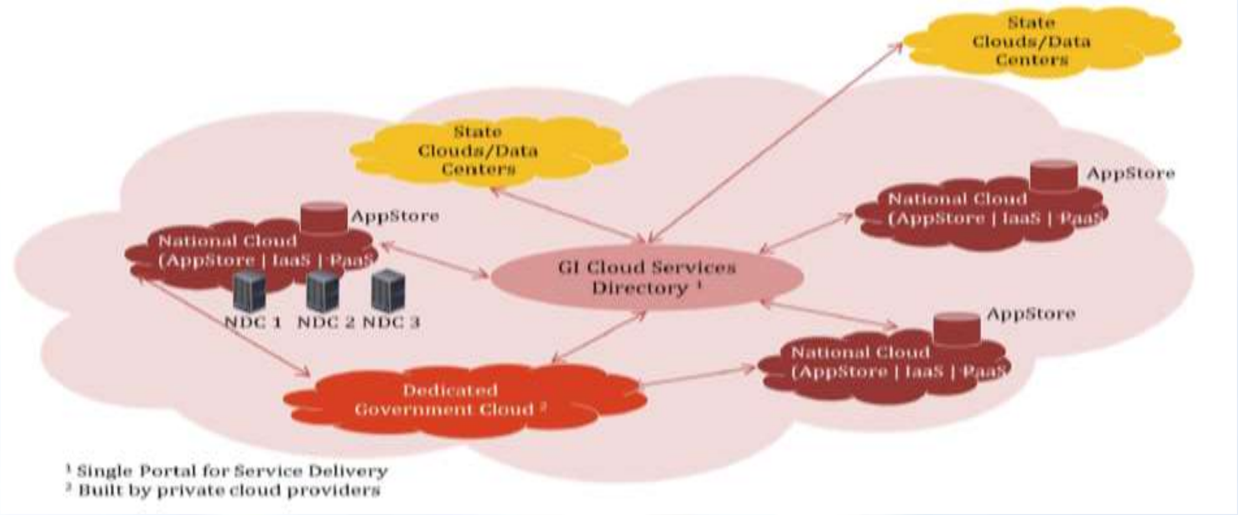

State Clouds/Data Centers
State Clouds/Data Centers
AppStore
National Cloud (AppStore | IaaS | PaaS)
AppStore
National Cloud (AppStore | IaaS | PaaS)
GI Cloud Services Directory ¹
NDC 1
NDC 2
NDC 3
AppStore
National Cloud (AppStore | IaaS | PaaS)
Dedicated Government Cloud ²
¹ Single Portal for Service Delivery
² Built by private cloud providers

Figure 5: GI Cloud Structure

Challenges in cloud security

Cloud computing is not a new technology. Rather it is a new model of IT service delivery. The cloud computing is yet to mature both in terms of technology and business readiness as well as adoption by the market. Issues like standards for security, interoperability, licensing, governance and contracting in cloud are still deliberated upon and work is in progress worldwide. Therefore, a clear understanding of the associated risks is required for the adoption of cloud computing by the users.

Securing the information systems and ensuring the confidentiality, integrity, and availability of information, information processed, stored, and transmitted are particularly relevant as these are the high-priority concerns there is higher risk being compromised in a cloud computing system. Cloud computing implementations are subject to local physical threats as well as remote, external threats. The risk matrix for onsite & cloud is indicated in figure 6.

Possible types of security challenges for cloud computing services are:

- compromises to the confidentiality and integrity of data in transit to and from a cloud provider and at rest;
- attacks which take advantage of the homogeneity and power of cloud computing systems to rapidly scale and increase the magnitude of the attack;

	On-Premise	***Colocation***	***Dedicated Hosting***	***IaaS***	***PaaS***	***SaaS***
Data	🟥	🟥	🟥	🟥	🟥	🟥
Application	🟦	🟦	🟦	🟦	🟦	🟩
Database & Other Platform Tools	🟦	🟦	🟦	🟦	🟩	🟩
Operating Systems	🟦	🟦	🟦	🟦	🟩	🟩
Virtualization & Abstraction	🟦	🟦	🟦	🟩	🟩	🟩
Server & Storage Infra	🟦	🟦	🟩	🟩	🟩	🟩
Network & Connectivity	🟦	🟩	🟩	🟩	🟩	🟩
Data Centre Facility (Non-IT Infra Power & Cooling)	🟦	🟩	🟩	🟩	🟩	🟩
🟥	***Managed by Cloud Consumer***					
🟦	***Managed by Managed Service Provider***					
🟩	***Managed by Cloud Provider***					

Figure 6: Risk Matrix for cloud services

- a consumer’s unauthorized access (through improper authentication or authorization, or exploit of vulnerabilities introduced maliciously or unintentionally) to software, data, and resources provisioned to, and owned by another authorized cloud consumer;
- increased levels of network-based attacks that exploit software not designed for an internet-based model and vulnerabilities existing in resources formerly accessed through private networks;
- limited ability to encrypt data at rest in a multi-tenancy environment;
- portability constraints resulting from the lack of standardization of cloud services Application Programming Interfaces (APIs) that preclude cloud consumer from easily migrating to a new cloud service provider when availability requirements are not met;
- attacks that exploit the physical abstraction of cloud resources and exploit a lack of transparency in audit procedures or records;
- attacks that take advantage of known, older vulnerabilities in virtual machines that have not been properly updated and patched;
- attacks that exploit inconsistencies in global privacy policies and regulations;
- attacks that exploit cloud computing supply chain vulnerabilities to include those that occur while cloud computing components are in transit from the supplier to the cloud service provider;
- insider abuse of their privileges, especially cloud provider’s personnel in high risk roles (e.g. system administrators; and
- interception of data in transit (man-in-the-middle attacks).

Thus, to accelerate the adoption of cloud computing, and to advance the deployment of cloud services, solutions coping with cloud security threats need to be addressed. Many of the threats that cloud providers and consumers face can be dealt with through traditional security processes and mechanisms such as security policies, cryptography, identity management, intrusion detection/prevention systems, and supply chain vulnerability analysis. However, risk management activities must be undertaken to determine how to mitigate the threats specific to different cloud models and to analyze existing standards for gaps that need to be addressed.

Data security standards and their applicability in cloud environment

Standards are already available in support of many of the functions and requirements for cloud computing. While many of these standards were developed in support of pre-cloud computing technologies, such as those designed for web-services and the internet, they also support the functions and requirements of cloud computing. Other standards are now being developed in specific support of cloud computing functions and requirements, such as virtualisation.

In order to ensure the security in the Cloud, environment, many standards have already evolved and each standards have their own strengths. These standards are mostly in general applicable to the cloud services, while some of them are enacted by specific countries, but still these are generic and adoptable globally.

Cloud security Objectives:

Some of the main security objectives for a cloud computing implementer should include:

- Protect consumers' data from unauthorized access, disclosure, modification or monitoring.
- Prevent unauthorized access to cloud computing infrastructure resources.
- Deploy in the cloud web applications designed and implemented for an Internet threat model.
- Challenges to prevent Internet browsers using cloud computing from attacks to mitigate end-user security vulnerabilities.
- Access control, intrusion detection, prevention solutions in cloud computing implementations and conduct an independent assessment to verify that the solutions are installed and functional.
- Define trust boundaries between cloud provider(s) and consumers to ensure that the responsibilities to implement security controls are clearly identified.
- Implement standardized APIs for interoperability and portability to support easy migration of consumers' data to other cloud providers when necessary.

Outcome

To sum up, the way forward for ensuring the confidentiality, integrity and availability of data in the cloud environment, the following measures are indicated:

- Develop detailed guidelines for different services of Cloud like IaaS, PaaS, SaaS.
- Granular level Guidelines for the End user Departments with process & Procedure for Cloud Deployment.
- Enforce the implementation of Cloud Security Policy guidelines
- Establish dedicated risk assessment process for User Dept., MSP and CSP in the implementation of Cloud security.
- Create a common platform for monitoring and guiding end user, MSP and CSP to migrate the legacy applications to Cloud.
- Interoperability & Portability of Data among the CSP / MSP guidelines to be published.
- Detailed qualification criteria for MSP's & guidelines for User Departments for selection of MSPs.
- A mechanism to be envisaged for auditing / vetting of RFP's before public domain release, to provide secondary assurance on cloud security requirements.
- Accountability on User Dept., MSP and CSP to adhere to Cloud security guidelines issued by competent authority.
- Personal & Data Privacy Laws to be formed and link the security level in cloud environment

Highlights of IT Audit report

Eighth and Ninth Annual Progress Reports of the United Nations Board of Auditors on Implementation of the United Nations Enterprise Resources Planning System - Umoja

By Mr. Naveen Singhvi

ABOUT THE AUTHOR

Mr. Naveen Singhvi is a 2008 batch officer of Indian Audit and Accounts Service. His audit assignments included Financial Audit of United Nations at New York, Remote Access Audit at ICED, Jaipur.

Umoja is an enterprise resource planning system that is aimed at modernizing a wide range of business processes spanning the United Nations administrative and support functions and systems that are essential to the efficient and effective functioning of the Organization. It is being used throughout the United Nations Secretariat including its Headquarters, offices away from Headquarters, international tribunals, field missions, some funds and programmes and institutionally linked entities of the United Nations, which have many different business models and funding and accountability structures.

The project proposal was approved by the General Assembly in December 2008. The approved project budget for Umoja up to the end of 2019 was $565.3 million and as at 31 December 2019, an expenditure of $520.1 million had been incurred. As per the original plan, Umoja was to be deployed throughout the Secretariat, in two phases, by the end of 2012. However, the deployment plans were significantly revised subsequently, and the General Assembly mandated date of completion of the project was 31 December 2020.

The United Nations Board of Auditors was requested to carry out annual audit of implementation of the project and the Board has submitted nine annual progress reports in this regard since 2012. In the two recent reports, focus of audit was on reviewing the project governance and management along with carrying out detailed review of development and deployment of individual modules of Umoja Extension 2 (the last phase of the project) and to carry out IT Audit of at least one functionality of the modules of Umoja already deployed and in use. Some of the key findings in the Eighth and Ninth progress report of the Board are summarized below:

Project Governance and Management

A multi-tier governance structure was created at different management levels with representatives from across the project and owner and user departments to review status of implementation of the project, consider change management processes requiring strategic direction, and to oversee the strategic and operational management of the project. It was noticed that the governance committees were not adequately on the progress of the Umoja project: overcoming the hurdles to its completion and with change management.

Umoja project management office followed waterfall and agile methodologies, depending on the nature of the project under implementation, for different Umoja sub-projects. It was noticed that there were various shortcomings in utilization of the project management tool, which included, among others, (a) lack of appropriate definition of inter-task dependencies in projects, (b) not reflecting dependencies among the design, build and test phases of software development in the planning tool, and (c) not identifying the critical path for the project This led to difficulties in estimating the overall time requirement for the projects. It also posed difficulties in identifying the specific constraints and causes of problems in individual projects owing to a lack of clear documentation of baseline scheduled dates, the identification of critical path of tasks and comparison of the scheduled and actual dates of completion of tasks.

Umoja Extension 2 (UE2) Deployment

Umoja extension 2 solutions (total 6 in numbers) targeted towards key activities of the Secretariat and associated entities, comprised multiple processes. Some of the key issues noticed during review of progress made towards these functionalities, which were being considered as completed, were:

(a) The blueprint technical document for one of these solutions defined different planning models It was intended that various Forms, Reports, Interfaces, Conversions, Enhancements and Workflow, known as "FRICEW" objects, would be developed under each planning model, so as to fulfil the business requirements of all related business processes. It was noticed that there were gaps in implementation of multiple FRICEW objects. Further, requirements originally included in the blueprint document in 2017, which were also listed in the work plan for the year 2019, were termed as "Wish-List" during the year 2020 indicating uncertainty regarding actual business requirements and the subsequent design, development and deployment of solutions to address them.

(b) For a second solution, it was noticed that various functionalities as identified under the blueprint technical document were yet to be deployed and there was no formal documentation of de-scoping of an important identified requirement. Resultantly the most important user department of the solution was continuing to use the legacy application.

(c) Another solution was partially developed and deployed in September 2018, but there was no further deployment during 2019 due to low user adoption. It was noticed that the process owners for processes intended to be covered under this subproject had not been identified, blueprint design document for the overall functionality to be deployed under this subproject had not been prepared and only one user department signed off on the business and user readiness on deployment of Release 1. It was also noticed that Release 1 was simplified to reduce the complexity of change management, in the absence of a required Secretariat-wide strategy for the related business process.

(d) All the six solutions had planned intra and inter solutions linkages and all the related documentation has provided that full benefits of implementing Umoja would be realized only with the achievement of integration across UE2 subprojects. However, implementation of majority of these inter-linkages was pending and it was stated that such integration would now be pursued wherever feasible and cost-effective as this was never part of the original scope and can therefore only be considered on the basis of the availability of resources for design and delivery.

Application Controls and Data Quality Issues

The functionality for processing vendor payments has been deployed as a part of the Foundation and UE1 phases of the Umoja project. Some of the key issues noticed during review of existing controls and working of this functionality were:

(a) Gaps in application controls allowed users to disable the three-way matching process while creating a purchase order, defeating the purpose of ensuring that there was a clear trail from the procurement of goods/service to their delivery and the raising of the invoice. Further, Application Controls for detecting duplicate invoices, being an optional check, was not exercised for all vendors. Moreover, there was no audit trail for modifications in the baseline date and payment terms.

(b) Weaknesses in application controls over vendor payments included non-automation of the execution of daily payment proposals, the lack of a bank balance sufficiency check within the system and non-review of role provisioning for users having access to execute payment runs.

(c) Issues in the maintenance of master data included the existence of multiple vendors against the same bank account, including staff and commercial vendors sharing the same bank account number and weaknesses in the system of updating the email details of vendors.

In addition to these areas, issues related to Risk Assessment and Mitigation, Support Functionalities of Umoja, Umoja Business Case and Mainstreaming Planning of the Umoja Project Post Completion have been deliberated in detail in these two reports. The full reports can be accessed on the following links:

- Eight Progress Report: https://undocs.org/en/A/74/153
- Ninth Progress Report: https://undocs.org/en/A/75/159

He had finally found the source of the internet.

Risk Management of e-Governance-ICT Based projects

- Dr. Charru Malhotra

ABOUT THE AUTHOR

Dr. Charru Malhotra is presently working as an Associate Professor (e-Governance and Information & Communication Technology) at The Indian Institute of Public Administration (IIPA), New Delhi, INDIA. She is also Project Coordinator for a significant capacity building 'training of trainers' module under the prestigious Digital India Program of Government of India. She has undertaken impact assessment of several e-Government initiatives of GoI and has also been National ICT Consultant (India) for Asian Development Bank (ADB) in a rural e-Governance project. she has served United Nations Development Program (UNDP), Winrock International as well as The World Bank as Short Term MIS/ GIS/ Smart Cities Consultant. She has published more than 30 research studies in reputed international and national journals and has more than 29 years of experience in the field.

Introduction

Risks are situations that pose threat of damage, liability, loss, injury or other negative vulnerabilities (external or internal in nature) and are to be avoided by preventive action. Since they have the ability to deviate organisations from their intended objectives, it is necessary that a proper identification, evaluation and prioritization of risks is undertaken to manage the risks. These steps, though sound and simple, requires detailed understanding, cooperation, coordination and collaboration of all stakeholders. This is even more required when the size and scope of the project expands to include the entire community or citizenry, in e-Governance projects. This coordination is easier to attain with projects having small Work Breakdown Structure (WBS) and Organisation Breakdown Structure (OBS). However, in a country like India, vast scope, critical nature of public services and the intricate nature of citizens' data associated with e-governance projects could further aggravate the risk-scenarios. Hence, proper risk management becomes necessary to ensure that objectives are met to in a timely, effective, and efficient manner. The objective of this study is to formulate risk management strategies, which is done by explaining the risk management of e-Governance projects and detailing the steps involved in risk management and concludes with the triangulations of the learning outcomes of the risk management processes.

Review of literature

The literature pertaining to broad areas of immediate relevance *viz.* risks and risk management were examined in order to understand the overall landscape of risks.

Risks

Project risk has been touted to be an uncertain event and if it occurs it will have an effect on one or more of the objectives of the project, such as scope, schedule, cost and quality (Bucuresti, 2015)[15]. From various studies, it has been concluded that there are broadly two categories of risks encountered by ICT based projects in government *viz.* 'Generic risks' and 'Project specific' risks (Choudhary, Banwet & Gupta, 2007)[16]. A study by Wallace, Keil and Rai (2004)[17] have classified risks in six dimensions *viz.* 'complexity', 'organizational environment', 'system requirement', 'Planning and control', 'users' and 'development team'. Risk conditions could also include aspects of the project or organization, years of ongoing risk environment that contributes to the project such as practice of immature project management, lack of integrated management systems, competing projects, or dependency on external participants who have direct control over project. Literature also points out that the influencers for risk identification in an organization includes the risk appetite or the willingness to take the risk in anticipation of a reward, risk tolerance which is the amount or volume risk for an organization and risk threshold which is the level of measures relating to the impact of risk on the project. Post identification of risks, the most important task of risk management has to be done which has been described as follows.

Risk Management

Review of literature reassures that irrespective of type, nature or scope of risks, a systematic study of risks empowers the practitioners to tackle these risks in a more structured and efficient manner. Risk management for software projects is defined in the literature as '*a set of practices that are aimed at identification, analysis and handling of risk factors to improve the chances of achieving successful project outcomes and/or avoid project failure*' (Kerzner, 2003)[18]. Risk management is necessary and can improve project outcomes, help to identify a favourable course of action, increase confidence in achieving project objectives, improve chances of success, reduce surprises and duplication of efforts too (Simister, 2004)[19] . Bannerman (2008)[20] has suggested many techniques for risk assessment and management such as building up checklists, categorising risks according to their source (client, self, task and environment) or life cycle. He further identifies certain risk mitigating strategies including 'avoidance',

[15] Bucuresti U. (2015). Risk Identification in Project Management. Procedia of Economics and Business Administration

[16] Choudhari, R. D., Banwet, D. K., & Gupta, M. P. (2007). Identifying Risk Factors in for E-governance Projects. *A. Agarwal, & VV Ramana, Foundations of E-government*, 270-277.

[17] Wallace, L., Keil, M., & Rai, A. (2004). Understanding software project risk: a cluster analysis. *Information & management*, *42*(1), 115-125

[18] Kerzner, H. (2003). Strategic planning for a project office. Project Management Journal, 34(2), 13-25.

[19] Simister, S. J. (2004). Qualitative and quantitative risk management. The Wiley guide to managing projects, 30-47.

[20] Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. Journal of Systems and Software, 81(12), 2118-2133.

‘transference’, ‘mitigation’, and ‘acceptance’ that can be used for either deferring the risk or eliminating it altogether.

Risk Management Process

Risk management is a practice with processes, methods and tools for managing risks in a project but several instances referred above, especially the case study of Health Information System (HIS), clearly delineates that despite risk management being an important step, it is usually not undertaken even by the most well-established organizations. Some of the usual justifications provided by management to avoid risk management are (a) it is difficult to predict risks, (b) the company does not want to highlight risks so as not to displease the stakeholders, (c) risk mitigation costs money. However, considering various uncertainties is helpful in the end as they reduce the project failure costs.

The task of risk management entails two steps namely ‘risk assessment’ and ‘risk control’. The first step, ‘risk assessment’, consists of risk identification, risk analysis and risk prioritization.

The second step of risk management is ‘risk control’, which consists of risk management planning, risk resolution and monitoring that is indicated in fig-7.

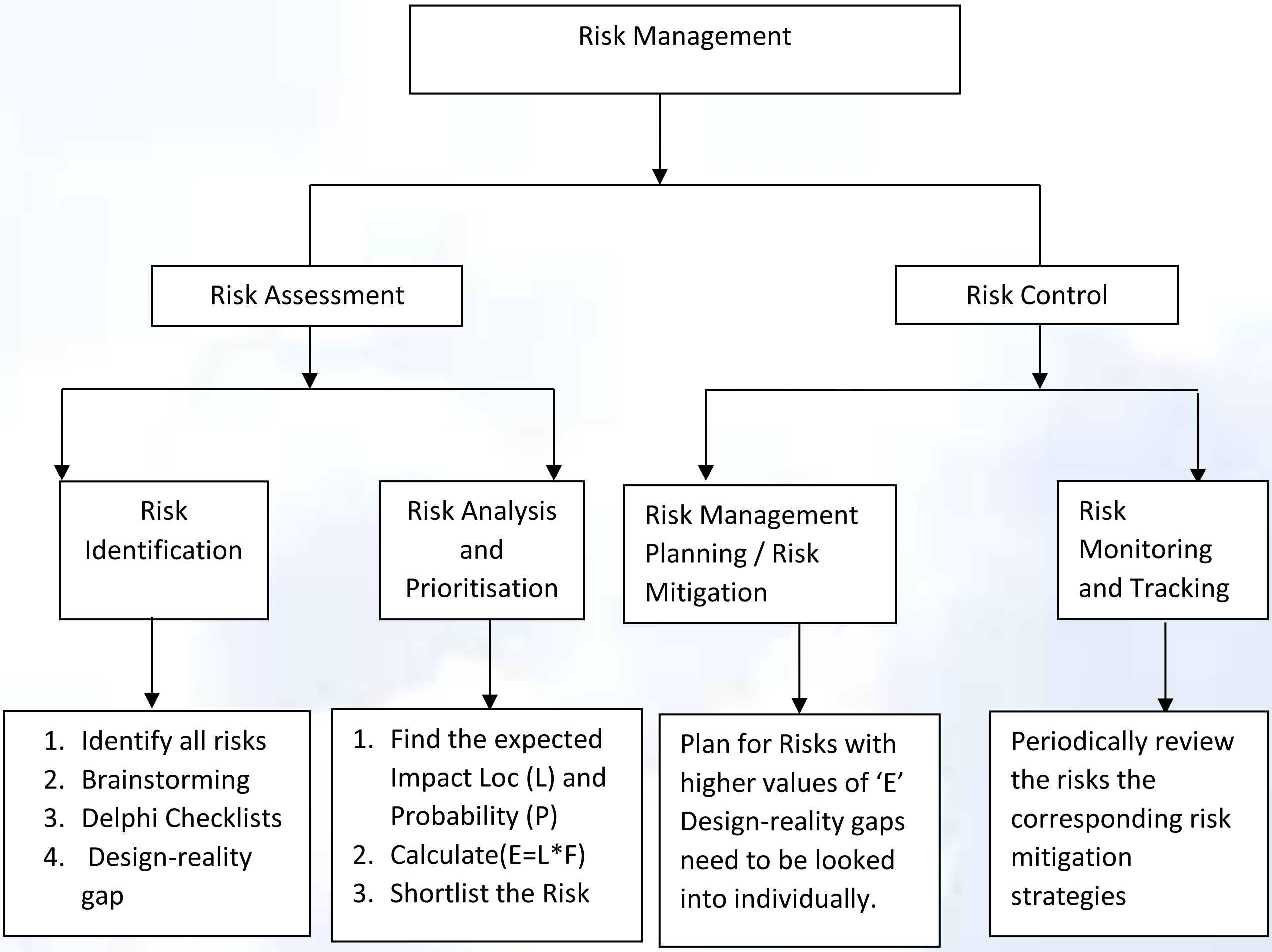

Risk Management
Risk Assessment
Risk Control
Risk Identification
Risk Analysis and Prioritisation
Risk Management Planning / Risk Mitigation
Risk Monitoring and Tracking
1. Identify all risks
2. Brainstorming
3. Delphi Checklists
4. Design-reality gap
1. Find the expected Impact Loc (L) and Probability (P)
2. Calculate(E=L*F)
3. Shortlist the Risk
Plan for Risks with higher values of ‘E’ Design-reality gaps need to be looked into individually.
Periodically review the risks the corresponding risk mitigation strategies

Figure 7: Overview of Risk Management Process

Risk assessment

The first step of risk management is risk assessment which further entails two steps viz. ‘risk identification’ and ‘risk analysis and prioritisation’.

Risk identification

The process of determining risks is a multi-stakeholder activity. The plausible risks are identified through various collaborative techniques such as brainstorming meetings of experts, Delphi rounds, workshops to elicit views of all. To avail project managers judgment and experience, other tools too could be coupled up e.g. creating checklists of frequently occurring risks compiled from study of previous projects, review of project plans, processes, cause and effect analysis, assumption analysis and work products. Review of literature presents several models/ approaches, presented herewith, to capture the data emanating from these brainstorming or project-manager based activities.

The COSO Model developed by Committee of Sponsoring Organisation of the Treadway Commission (COSO) in the year 1992 for evaluating internal control can be used to assess efficiency and effectiveness of operations, reliability of financial reporting and compliance with applicable laws and regulations. This can be used as a definitive standard against which the risks can be assessed. Heeks (2003)[21] has explained that central to e-government project success is the amount of change between ‘where are we now’ (current realities of situation) and ‘where the e-Government project wants to get us’ (models and assumptions built into the project design). This is referred to as *design-reality-gap approach*. The larger the gap between design and reality, greater are the chances of e-government failure. Heeks (2003)[22] has also suggested analysis of seven dimensions, which form an acronym *ITPOSMO* (Information, Technology, Processes, Objectives and values, Staffing and Skills, Management Systems and Structures and Other resources- time and money) for study of design-reality gap. These seven gap dimensions are expected to be exhaustive and are touted to be sufficient to provide complete information required for understanding the ground reality. Some interesting explanation for each of the components of ITPOSMO was found in the public domain (http://www.egov4dev.org/success/techniques/_idfailure_drg.shtml) and is summarized herewith:

- *Information* - the information usage that was envisaged in the design of e-Government project is to be compared with the information that had been actually used in the organisation just prior to its implementation.
- Technology –the technology requirements contained within the design of the e-Government project to be compared to the technologies (digital or otherwise) that were being used in the organisation prior to the project implementation.
- Process- the work processes expected to be undertaken in the organisation for successful implementation of the e-government project to be compared to the processes being undertaken just prior to implementation.

[21] Aguilar, F. J (1967), “Scanning the Business Environment” The Macmillian Company : New York.

[22] Aguilar, F. J (1967), “Scanning the Business Environment” The Macmillian Company : New York.

- *Objectives and Values* - the objectives and values that key stakeholders would have needed for successful implementation of the e-government project to be compared with their real objectives and values just prior to its implementation.
- *Staffing and Skills* - the staffing numbers and skill levels/types required in/by the organisation for successful implementation of the e-government project to be compared with the real situation just prior to its implementation.
- *Management* - the management systems and structures required in the organisation for successful implementation of the e-government project to be compared with the real situation just prior to implementation.
- *Other resources* – the time and money required to successfully implement and operate the e-government project compared with the time and money available just prior to implementation.

Once the risk lists have been prepared / and the gaps have been identified using any or combination of the techniques mentioned above, then these lists/gaps have to be analysed and prioritized with respect to their impact on the project, for which a detailed risk analysis activity has to be undertaken.

Risk Analysis and Prioritization

In the risk analysis activity, based on the past data as well as the manager's experience, the risks that have been identified in the previous step are labelled as 'low effect risk', 'intermediate effect risk' and 'high effect risk', depending on the loss that it may lead to if the risk occurs. This could be a direct loss, loss due to lost business opportunity or may be as intangible as reduced employee morale or as explicit as loss of customer base. For a more scientific approach, the risks can be quantified and weights may be assigned on a scale 1-10 based on their loss impact as 'low', 'medium', 'high' and 'very high' as depicted in table-2 Once the loss impact is understood, the probability is allotted for each of the identified risks on the basis of how much likelihood is there for each of the risks to occur. The risk probability could vary from 'high likelihood for it to occur', to 'may occur about half of the time' to 'unlikely to occur' (table-2). Care must be taken that a 'high' effect risk might not be a 'highly probable risk'. A veteran project leader, whose experience would stand by their side, could also subjectively quantify this likelihood/probability.

Table – 2: Quantifying the Risk Impact (Loss)

S No	Level of Consequences	Range Values for Quantifying the Impact/ Loss (L)
1	Low	0.0 – 3.0
2	Medium	4.0 – 7.0
3	High	8.0 – 9.0
4	Very High	>9.0 – 10.0

Table 3: Quantifying the Risk Probabilities

S N	Risk Probability	Range Values for Quantifying Probabilities Risk(P)
1	Low (Unlikely to occur)	0.0 – 0.3
2	Medium (Likely to occur may be half of the times)	0.4 – 0.7
3	High (Likely to Occur)	0.8 – 1.0

In the final step of this phase, for each of the risk identified and analysed, the exact consequence (also called as 'risk exposure') is calculated for each of the risks. This can be done by multiplying the 'risk impact' (table-2) with 'risk probability' (table- 3) which gives the risk exposure value (Risk Exposure, E = L * P). A high magnitude of risk exposure makes a risk high priority one. It is pertinent to mention here that either the value of risk exposure could adjudge the list of most important risks or the project manager's judgments/ experience could be availed to do so. The top few are 'chosen' for risk management planning, based on the management's priorities.

In addition, referring to the ITOPSMO paradigm suggested by Heeks (2003)[23], one can quantify the gaps on a scale of 0-10. This score shall represent the size of the design-reality gap for that dimension. A score of '0' indicates no gap, '5' indicate some degree of change between proposed design and reality and a score of '10' shall indicate complete change between the design proposal and reality. Adding up the scores of each of the seven dimension will give a score, which can be the indicative of how different the planning is from the reality. Essentially, either the value of exposure 'E' or the scores obtained by adding the individual design- reality gap in the ITOPSMO paradigm are used to take corrective actions for risks having score higher than a benchmark value, say '6' and risk control/ risk mitigation action steps should be chalked out for each of these risks. This analysis can be performed using a participative approach where the auditors, project consultant and various key stakeholders. After the risk analysis, the discussions/ workshop can move on to work out how best to close these gaps too, referred to as 'Risk Control', as elaborated herewith.

Risk Control

The final step of risk management is Risk control which further entails two steps viz. 'risk management planning' (also called as 'risk mitigation')and 'risk monitoring and tracking'.

Risk Management Planning

Proper planning is required to handle the risks shortlisted in the previous step, which is also called as 'risk mitigation' phase. In this phase, various actions required to manage/ minimise the risk consequences are identified and incorporated in their project schedules and project budgets. Management and auditors can create this action-plan as a guiding list for all the project managers.

For instance, risks arising due to shortage of technically trained work force can be mitigated by providing on-the-job training and learning-time to the project team and training should be delivered through skill specific leaders and

[23] Aguilar, F. J (1967), "Scanning the Business Environment" The Macmillian Company : New York.

mentors. The problem of high work force attrition may be resolved by preparing second-in-command, who too must be trained and well-equipped to take over , in case the need be. This can be ensured by conducting team-building exercises, by undertaking routine job rotations amongst team members and by maintaining workflow documentation for the job/ work being discharged by each of the team members. It might also be advisable to induce employee friendly policies such as work-from-home, nonmonetary incentives, supporting facilities and by gathering regular formal and informal feedbacks and review sessions with the employees. Too many requirement changes on part of the customer may also cause the project to deviate. Sign-offs on initial requirements specifications should be obtained. The clients in the beginning must sign a no-requirements change document; this should happen right at the beginning of the project, and a procedure should be in place to handle top priority exceptional requirement changes. Similarly, the performance criteria and the standards to be followed should be defined, reviewed, and confirmed by the final user right in the beginning. The project design and project execution steps must be prepared according to the fixed criteria and standards and must be regularly reviewed. Simulation of performance of critical steps should be done and the team onboard must be apprised of the same. Regular formal and informal feedback should be gathered during the project execution with risk registers maintained and updated regularly.

Risk Monitoring and Tracking

The risk management planning is followed by ‘risk monitoring and tracking’ wherein all the risk factors and their risk mitigation steps are reviewed and reported periodically. Multi-stakeholder consortiums and working groups should be established to ensure continuity of changes. A life cycle approach (Mian & Dai, 1999)[24] to assess and manage risks could be followed. The life cycle approach includes various steps *viz.* ‘Identify’ (understanding how the risks might enter the project), ‘mitigate’ (designing of systems and procedures to mitigate and manage the risks identified), ‘implement’ (training of staff and implementation of systems and procedures,) and ‘monitor’ (reviewing of performance and taking note of the lessons learnt) (figure 8).

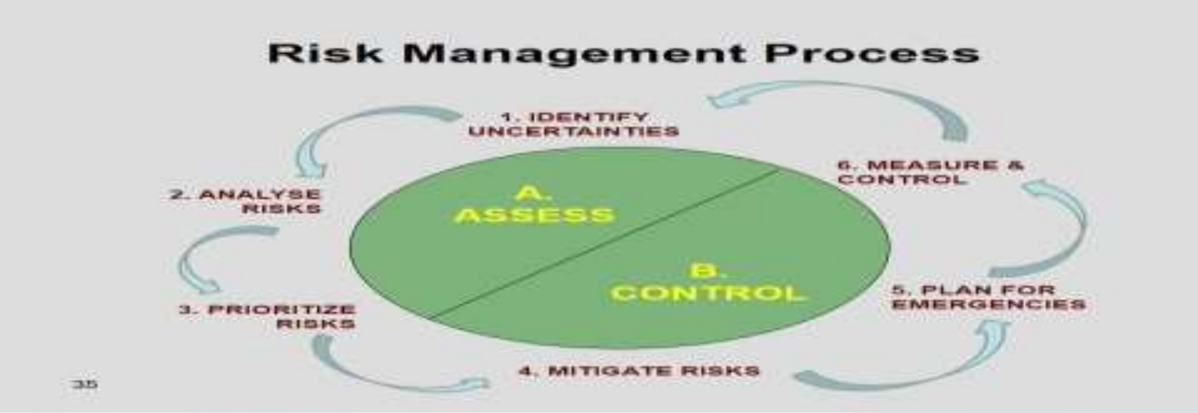


Figure 8: A Life Cycle Approach to Risk Management

[24] Mian, S. A., & Dai, C. X. (1999). Decision-making over the project life cycle: An analytical hierarchy approach. *Project Management Journal*, *30*(1), 40-52.

These methods can essentially help the project team of any ICT based government project to mitigate risks in an effective manner.

Conclusion

Risk management occurs after risk identification has been done and plays an important role in project management as this step if performed well enables the project to achieve its intended outcomes. Since this step plays such an important role in the success of the project, it requires coordinated monitoring, controlling, and applying managerial resources with a coordinated and economical effort. Also effective risk management led by the project manager results in several benefits such as increased confidence in achieving project objective, improved chances of success, reduced surprises, more precise estimates (through reduced uncertainty), reduced duplication of effort (through team awareness of risk control actions), etc. However, effective risk management is typically achieved when an organisation undertakes an active commitment to integrating risk management into their project protocols and controls. As seen from the case study as well, each and every step was properly monitored and checked which resulted in the project achieving its results in no time. The e-governance projects of India can also take cue from this case study and establish an effective plan that shall include allotting appropriate resources to perform risk management activities, creating an environment that embraces and promotes risk management at all levels of the organization and promoting training and development for risk management. Summing up, the contemporary organisations have to work in tandem with the developments of the project, be quick and receptive so that risks are identified and managed earlier in the project to help in achievement of intended outcomes

Development and utilisation of OPTIMA and AIMS software applications

-Developed in IAAD[25]

- Mr. M. Abdul Barri

Optimise Performance using Technology, Information & Management in Audit (OPTIMA)

Background

The IR Main (for watching receipt and issue of Inspection Reports) application software, which was developed in-house as a stand-alone DOS based application in FoxPro database catering to a few groups in the office of the Pr.AG (Audit-I), Chennai, was in use till 2002, after which, the application was migrated into client-server architecture with a centralized RDBMS, with VB front-end and Crystal Report as a reporting tool, utilizing the in-house skills. This application had certain difficulties like compiling the VB application whenever there was a change, deploying the compiled version in around 50 client system, installation of Oracle client in the user system etc.

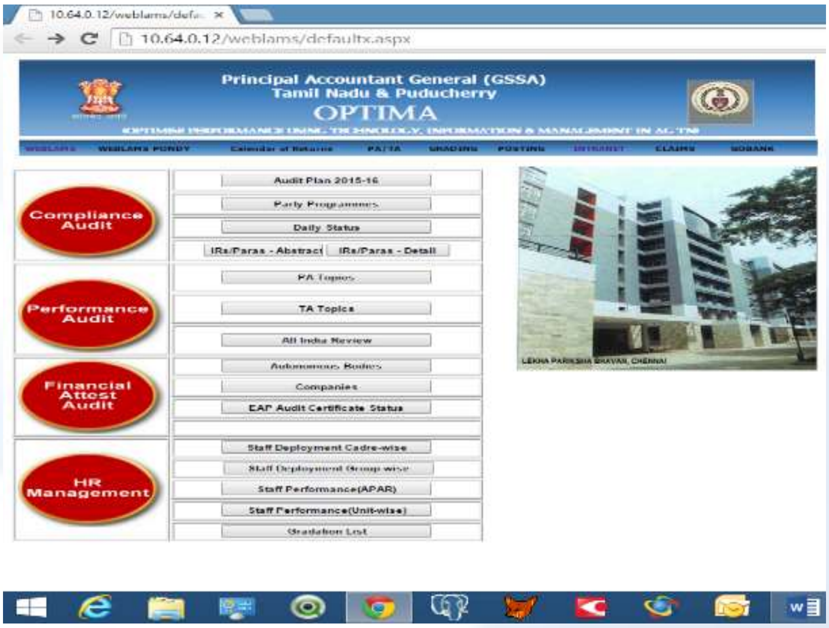


Image 6: Screenshot of Webpage

ABOUT THE AUTHER

M. Abdul Barri is currently working as a Data Manager in the office of the Principal Accountant General (Audit-I), Tamil Nadu, Chennai. He has been part of the IT Audit Team of this office since 1995 when IT Audit of Chennai Port Trust was taken up. He is conducting audit of many IT applications used by the Government Departments/Bodies/Corporations in their functional areas. So far, he has conducted more than thirty IT Audits, which included e-Governance systems and ERP. The results of audit published in the Audit Reports of the CAG of India. He was trained in Information Technology Audit in the National Audit Office, London, in 1997. He was one of the members of UN Audit Team, which conducted audit of World Food Programme in Afghanistan, Nepal and Bangkok in 2011. He was also part of the UN Audit Team, which conducted the audit of MINURSO (UN Mission) in Western Sahara in 2019

[25] *This section aims at highlighting the efforts of members of IAAD in developing in-house applications in the field of ICT for achieving some goal in official functioning thereby easing out the current manual process. i CISA does not personally endorse these applications, yet it appreciates the scientific temper shown by the members of IAAD in developing these.*

OPTIMA

To overcome these difficulties, a web-based application viz. WEBLAMS (Web-based Local Audit Management System) was developed in-house with the same RDBMS at the back-end, with front-end screens developed in asp.net using Dot Net framework, in the year 2008. The website was hosted using IIS (Internet Information Service), a web hosting software available in Windows OS in a mid-Range Server (P5 processor, 8 GB RAM and 600 GB HDD). Visual Web Developer, a Microsoft tool available in the Internet was used for writing the code of the application.

As part of WEBLAMS, individual applications catering to Posting of personnel, Intranet, Claims (Party Members' stay and tariff details), Performance Audit (PA), Financial Attest Audit, database of Government Orders (GOBANK), Calendar of Returns, Gradation List etc. were also developed in-house and hosted in the same system. In the year 2012, all the individual applications were grouped under a single window and have been integrated to give an overview of all the applications. OPTIMA provided visibility into all the important processes across various wings of the office including the branch offices at Madurai and Puducherry. The field staff can access the OPTIMA application for retrieving audit related information using the static IP.

Now, most of the requirement of IR sections/commercial wing/PA/AB have been brought into the Web-based applications. Based on the requirements of users, applications for DAK monitoring, office expenses bill processing, capture of press clippings (which are used as a lead in the field audit), database of paras sent to PAC, mapping of paras with reference to Sustainable Development Goals (SDG) in the audit report etc. were also developed and included in OPTIMA. Using the credentials, the concerned users capture the data concurrently in the password protected modules.

Data Organization and flow

All the entities, which comes under the audit purview of this office under various sections of CAG's DPC Act, have been brought into the master table called Institution Master with attributes like date of last audit, section under which audit is undertaken, audit period covered, year in which the institutions have been included in the audit plan, Unit type (A/B/C), Apex Unit/Audited Entity/Implementing Unit, HQ Group, Section and Unit. The auditee institution is uniquely identified by a 11-digit alpha code across the entire office. The package has four main transaction tables viz. Report (outstanding reports), Para (outstanding paras), Old Report (closed reports) and Old Para (closed paras).

Institutions, which have been ear-marked (planned units) for taking up of audit during the given year, are flagged and the quarterly programmes for those units are entered by the controlling sections. Any deviation in the approved quarterly programme is also to be carried out in the system. On completion of the local audit, the audit party will send the draft inspection report to Head Office (HO)within 5 days from the date of completion of audit. In HO, the draft IR will be vetted, and the IR will be issued to the audited entity within 25 days from the date of receipt of the draft IR from the audit party.

Audit Planning	Audit Programming	Inspection Report	Audit Follow -up
Inputs for compliance audit • Details of all units and sub-units • Budget and Expenditure of units • Past audit period and results	• Annual audit Plan • Planned units can only be programmed • Party tour programme generated and deviations captured	• Receipt of draft IRs within 7 days • Issue of IRs within 30 days • IRs with major/nil observations, with contributors • Periodical reports on outstanding IRs/Paras • Key word search to group similar paras for conversion to Factual Note/Draft Para	• Track Department's response • Issue of rejoinders and reminders • Clearance of Paras • Selection of IRs for review by Internal Audit

Table 4: Audit Flow

All the above processes are monitored and controlled through various reports and dashboard menus provided in the application software.

How OPTIMA help Audit Management

Audit Planning - For audit planning exercise, the various inputs required like budget, expenditure and number of paras issued against each auditee available in OPTIMA are utilised.

Audit Programming - Based on the risk-based planning exercise, the institutions are selected under each department taking into account the man-power availability. Selection of units are done purely on ranking weightage. Based on the ranking of the department, the number of institutions is derived, selected accordingly and marked in OPTIMA for inclusion in the Audit Plan. A control has been built in the software to programme only the units, which find a place in the planned list. Accordingly, the tour programmes are prepared and captured in OPTIMA. Before preparation of the tour programme, party members in the Wings are grouped cadre-wise and using the features of random sampling in IDEA package, party configuration is prepared every quarter to avoid sending the same group of people in a particular party.

Inspection Report – For making efficient control to watch the receipt and issue of IRs. Now, using the features of OPTIMA, monitoring is done on day-to-day basis (time lines and quality). Data relating to each Inspection Report issued along with gist of each para and the originator of the audit observations are captured in the system. The quality of audit is also gauged by taking into account the number of Part II A / II B paras and Nil IRs issued in an office. List of pending IRs/Paras can be generated applying many parameters viz. for a given period, department, office etc. at point of time with ease. This is required for departmental audit committee meeting for settlement of paras.

Audit follow-up – Details of settlement of paras (based on the reply from the dept.) are captured in the system along with department reference. Reminders calling for replies and rejoinders communicating to the audited entities the acceptance or otherwise of the replies received from them are also generated from the system. Internal Test Audit Section is also using OPTIMA for selection of IRs for periodical review.

Salient features of OPTIMA

- Audit Plan information like list of number of planned / programmed / audited units in a single screen along with details on request.
- The entire process of the audit cycle can be tracked sequentially.
- Party Tour Programmes including deviations and changes.
- MIS reports available for submission and monitoring.
- A rolling status of local audits and IRs as on date has been included to view details like IRs issued in last 30 days, Issue of IRs overdue and Receipt of DIRs overdue (including BO Madurai).
- Key-word search and viewing of uploaded IRs facilities are available.
- List of Next Audit Verification (NAV) paras are generated and furnished to the field Audit Parties for verification and the status updated.
- Monitoring of PA Topics, TA Topics and All India Performance.
- Monitoring of Audit of Companies and Audit of Autonomous Bodies.
- Annual Performance Appraisal Report (APAR) grading and the service history is available in a single view.
- GOBANK and Intranet for ready referencing.
- The paras included in the Audit Report, which are eventually discussed in PAC/COPU, have been brought into the system to track and monitor the stages leading to the finality of the Audit Report.

PA/TA	Audit of Companies	Audit of Autonomous Bodies	Human Resources
• Timelines • Approved Guidelines with ADM for reference • Tour Programme Current status	• List of Companies • Accounts due • Relevant time-line parameters • Status on issue of provisional comments/Issue of certificates	• Grant and expenditure details • Whether qualifies for audit • IRs with major/nill observations, with contributors • Status on issue of SARs	• Service Particulars • APAR of Staff • performance of party officials – what audit & contribution • Information on availability of all parties in a selected location

Table 5 : Audit follow-up

Auditee Information Management System (AIMS)

Introduction

Auditee Information Management System (AIMS) has been developed and maintained for improving the quality of audit output. AIMS has a collection of unstructured and structured data from various sources. The gathered information is converted into retrievable meaningful information/reports. The unstructured data are Policy Notes, Citizen Charters, Performance Budgets, Government Orders, etc. and structured data are the data dump of the databases maintained by the audit entities. This information are collected from all the departments under the audit purview of this office and grouped under the respective Wings.

Use of VLC and Treasury Data

Office-wise, Department-wise, and Scheme-wise expenditure details, budget vs expenditure etc.

are being updated by obtaining the data from VLC and Treasuries periodically. Some of the reports available in AIMS are listed below:

Drawing and Disbursing office (DDO)-wise voucher details can be obtained by applying criteria on the Auditee Institution, department-wise and District-wise for the financial years 2017-18 and 2018-19. The generated report lists out all the expenses, from which the field parties can extract exclusively the non-salaried expenses, for detailed analysis.

Users can view Head of Account-wise total budget Provision, Re-appropriation, Final Modified Grant, Total Expenditure and Excess/Savings for the selected year for that particular department/Directorate-wise. Year-wise expenditure details for the selected head of account or by using the key- word viz. Scholarship, solid waste management, pension etc. the details of expenditure can be viewed.

The sub-head nomenclature of the Head of Accounts denotes the scheme name and under this scheme, the expenditure pertaining to state scheme/central scheme/shared between central and state scheme/aided scheme also can be viewed, wing-wise, year-wise and department-wise.

Databases obtained from Auditee Institutions

With a view to make use of large volume of databases (relating to their functional activity) available with the auditee institutions, this office obtained many databases from the auditee organizations in addition to the databases obtained during the course of IT Audit of some of those institutions. At present, we have around 24 databases relating to various functionalities/activities viz. Road Accident Management, Drug Distribution and Management System, Urban Tree Information System, Chief Minister's Comprehensive Health Insurance Scheme, Old Age Pension (OAP), Educational Management Information System, Public Distribution System, Scholarship schemes BC, MBC and Minorities welfare for Colleges for the years 2016-19, Scholarship schemes for Adi Dravidar and Tribal Students for both schools and Colleges for the years 2015-18 etc.

Case Study 1: IT assisted Audit of UTIS

The data dump of Urban Tree Information System (UTIS) relating to ULBs (Municipalities and Corporations) obtained from the office of the Commissioner of Municipal Administration in April 2019 has been restored in our AIMS Server.

The queries deployed in the examination of UTIS database during IT Audit of UTIS in the year 2018 have been incorporated in the coding of the AIMS and user-friendly screens were developed for generation of various reports. Every year, the data dump will be obtained and replaced in the AIMS Server, so that up-to-date reports on audit observations found during IT from examination of database can be generated and used by the audit parties as leads for further analysis during field inspection. The sample leads are listed below:

- List of Property Tax assessments with details regarding Building Plan Approval, Building Usage, Annual Value, Half-year Tax, Plot / Built Area, Floor Detail etc. – to sample and further analysis.
- List of Legal / Litigation cases – to verify whether the demands were raised as per the court orders.
- List linking Property Tax (PT) assessments and Water Supply (WS) connections – to verify cases in which the assessments were residential as per PT and non-residential as per WS and vice-versa.
- List of Water Supply connections – to verify cases in which the inspection was done but installation was not done, since demands are raised from the date of installation and cases in which the demands were not raised.
- List of Property Tax, Water Supply and Solid Waste User Management Charges (SUC) demands – to verify cases in which the PT was paid but WS pending and vice versa and PT was paid but SUC pending and vice versa.
- List of cases in which SUC demands were not generated though PT demands were generated – Residential, Commercial and Industrial.
- List of pending services – to verify the reason for non-provision of the services to the citizens.
- List of PT assessments not included in the General Revision table – to verify the reason for their omission during General Revision.
- List of Unit Value (used to calculate the Monthly Rent Value) and Base Rate (used to calculate the Base Property Tax) captured in the system for the Municipalities / Corporations – to verify whether the rates are as per the prescribed norms.
- Listing the budgets details (Appropriation and related Expenditure) relating to the municipalities.

Case Study 2: IT assisted Audit of TNMSC

Tamil Nadu Medical Services Corporation (TNMSC) has computerized its major functional activities through two application software viz. Drug Distribution Management System (DDMS) and Warehouse Information System (WIS). DDMS is a centralized database maintained in TNMSC head office. District ware houses use WIS for carrying out their day-to-day functions. Using the database obtained from TNMSC, the following leads are available for the field parties:

- List of medicines indented by the hospitals and supplied by TNMSC.

Based on the 'Not Available' Certificate, the hospitals resort to local purchase of drugs and medicines.

- List of drugs for which stop order has been issued due to poor quality of the drugs. This report will be useful to find issue of drugs, which are not meeting the quality standards.
- List of data entry errors in the dates of manufacturing and expiry.
- List of cases detailing (i) delay in receipt of samples in TNMSC headquarters from warehouses, (ii) delay in receipt of empaneled laboratory reports/Government laboratory reports and (iii) delay in capturing laboratory test reports

"Seems like the Computer Analyst is taking his job just a little too literally."

App Watch

MADAD App

The MADAD app is offered by the Ministry of External Affairs of India (MEA). It pertains to consular services that are provided by Indian embassies in foreign locations. The app can be used to launch and track the grievances.

The grievances may be regarding a situation that involves imprisonment in a foreign land, worker abuse, repatriation, etc. Except the issues related to passport and visa.

The app can be downloaded from Google Play Store or Mac App Store

Image7: Logo of MADAD App

COVID BEEP

COVID BEEP is India's first indigenous wireless physiological parameter monitoring system for coronavirus patients. It is jointly developed by ESIC medical college, IIT Hyderabad and Electronics Corporation of India Ltd (ECIL). Its acronym is Continuous Oxygenation and Vital Information Detection Biomed ECIL ESIC Pod.

It can measure vital parameters like body temperature, blood oxygen saturation, heart rate, respiratory rate, ECG and blood pressure of patients. These parameters after measuring are remotely displayed on mobile phone via app or laptops in order to perform monitoring by the doctors upon seeing the measurement results. COVID BEEP is incorporated with Non-Invasive Blood Pressure (NIBP) monitoring, ECG monitoring and Respiratory rate.

Image8: COVID BEEP Device in working

Updates

PRAGYATA: Guidelines on Digital Education

PRAGYATA guidelines have been developed from the perspective of learners, with a focus on online or digital education for students who are presently at home due to pandemic. The guidelines on Digital/ Online Education provide a roadmap or pointers for carrying forward online education to enhance the quality of education. An exemplar helps illustrate the specific steps to be taken for

- completing the lesson plan in details;
- reviewing the availability of digital devices amongst students;
- making arrangements e.g., selecting appropriate medium, groups & time to connect with different category of students, choosing a subject theme to engage students;
- guiding parents of each family to engage with respective children;
- yak/talking with students to clear doubts;
- assigning tasks to reinforce the learning;
- tracking progress of each student and
- appreciating students & parents;

The guidelines are relevant and useful for a diverse set of stakeholders including school heads, teachers, parents, teacher educators and students. The guidelines stress upon the use of alternative academic calendar of NCERT, for both, learners having access to digital devices and learners having limited or no access.

SPOTLIGHT
Plan- Review- Arrange- Guide- Yak (talk)- Assign- Track- Appreciate
PRAGYATA
Guidelines on Digital Education
to assist school heads, teachers, parents & students in e-learning

Image 9: Logo of PRAGYATA Portal

e-Learning

Here are some links of online lectures/Courses/Videos. It will help your skill development in ERP environment.

- https://onlinecourses.swayam2.ac.in/cec19_cm03/preview
- https://onlinecourses.nptel.ac.in/noc19_mg54/preview
- https://www.udemy.com/courses/office-productivity/sap/
- https://www.youtube.com/watch?v=5JMkdGQCm4k
- https://www.udemy.com/course/sap-abap-programming-for-beginners/
- https://www.udemy.com/course/learn-sap/

Quiz Corner

Question 1: Which one of the following is not a myth about ERP

1. ERP means more work and procedures
2. ERP makes many employees redundant
3. ERP integrates and automate organization processes
4. ERP is the sole responsibility of management

Question 2: Which one of the following is not a part of an ERP implementation

1. Vendor representatives
2. Employee team
3. Consultants
4. Customer

Question 3: Which one of the following options doesn't belong to ERP Technologies

1. Data Warehousing
2. Business Reengineering
3. Data Mining
4. Manufacturing Resource Planning

Question 4: BPR is also known as

1. Business Process Reengineering
2. Business transformation
3. Business process change management
4. All of the above

Question 5: In ERP environment ROI stands for ____________

1. Repeatable Operational Information
2. Return on investment
3. Regular official information
4. None of the Above

Question 6: Which one of the following is not an ERP implementation strategy

1. Big bang strategy
2. Phased implementation
3. Half implementation
4. Parallel implementation

Question 7: Which one of the following is an ERP life cycle phase

1. Adaptation and decision
2. Acquisition and implementation
3. Use and maintenance
4. All of the Above

Question 8: Which one of the following is ERP ownership cost?

1. Hardware
2. Consultancy
3. Training
4. All of the Above

Question 9: Which one of the following is a success factor for ERP system

1. Project Planning
2. Architectural design
3. Phased approach
4. All of the Above

Question 10: Who are the primary users of SCM systems?

1. Customers, resellers, partners, suppliers and distributors
2. Accounting, finance, logistics, and production
3. Sales, marketing, customer service
4. All of the Above

Question 11: What must a system do to qualify as a true ERP solution?

1. Be flexible
2. Extend within the company
3. Be modular and closed
4. All of the Above

Question 12: ERP is combination of ______________ and ______________

1. Technology, assessment
2. Assessment, management
3. Management, technology
4. Technology, business process

Question 13: ERP information technology integrates with company's ____________ to achieve its ultimate goal.

1. Business ethics
2. Business processes
3. Management
4. Resources

Question 14: ERP is evolution of

1. manufacturing requirement planning
2. material resource planning
3. production planning
4. capacity resource planning

Question 15: MRP is evolution of

1. capacity resource planning
2. manufacturing requirement planning
3. production capacity and control
4. inventory management and control

Question 16: Which of the following services is responsible for the initial stages of ERP implementation?

1. Generation
2. Customization
3. Consulting
4. Support

Question 17: Which of the following is true?

1. ERP systems are used only for large organizations
2. ERP systems are used only in small organizations
3. ERP systems are used in both large as well as small organizations
4. ERP systems are used in long term planning

Question 18: In ERP systems, common database can allow every department of a business to

1. Store information
2. Retrieve information
3. Store and retrieve information
4. Store and process information

Question 19: ______________ word is often used in general business solutions to describe a corporate entity

1. Venture
2. Enterprise
3. System
4. Project

Question 20: ERP systems help in

1. Resolving inter departmental conflicts
2. Satisfying varying needs of customers
3. Automating business process and functions information processing etc.
4. Integrating information system

Answers to the Quiz published in previous issue of Journal (2020 first issue)

1	**C**	**10**	**C**
2	**C**	**11**	**C**
3	**C**	**12**	**C**
4	**B**	**13**	**A**
5	**D**	**14**	**C**
6	**A**	**15**	**B**
7	**D**	**16**	**D**
8	**A**	**17**	**A**
9	**A**	**18**	**B**

"I'm waiting for them to work out the bugs."