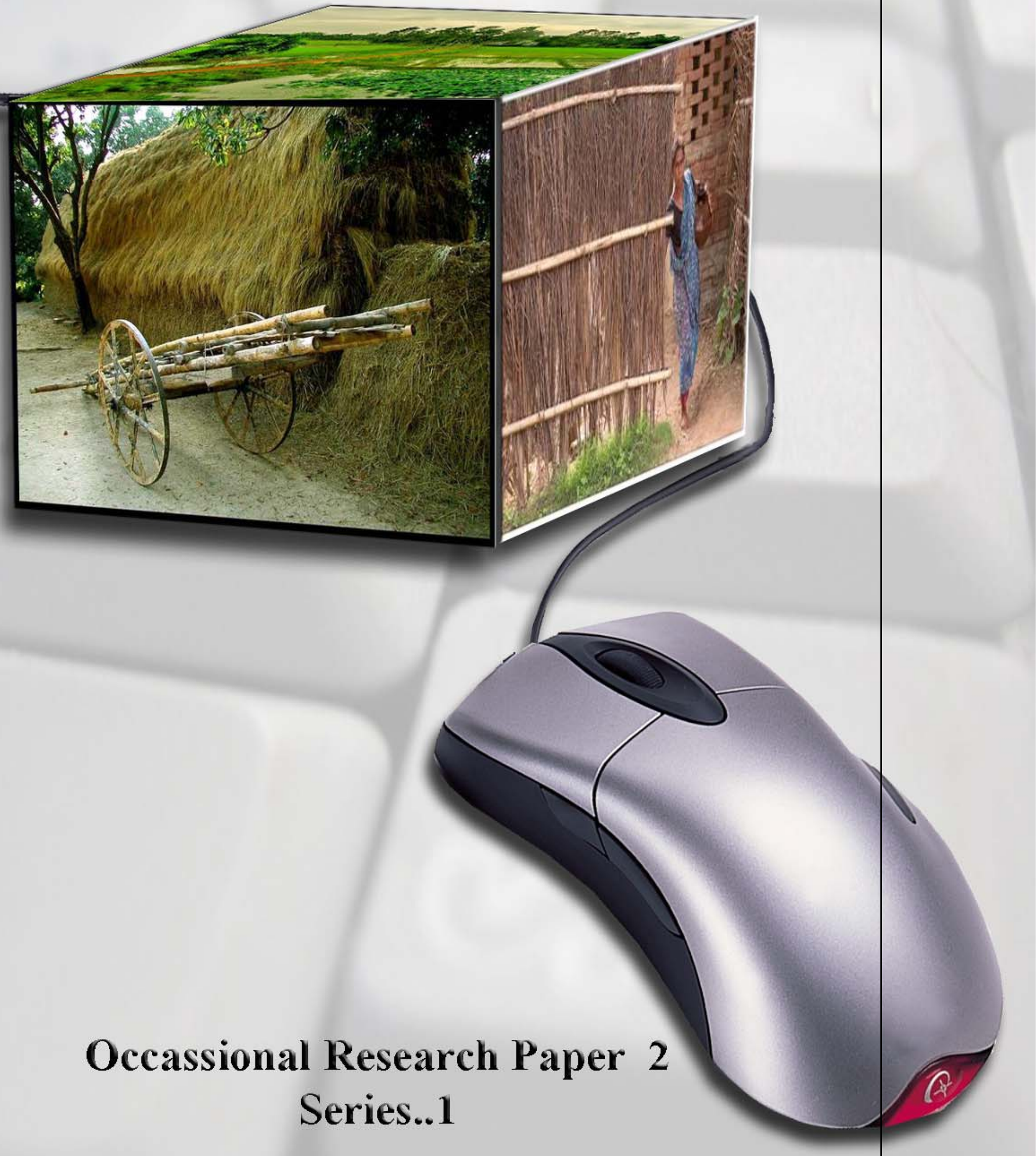
IS Audit
in
Panchayati Raj Institutions



Occassional Research Paper 2
Series..1

Regional Training Institute, Kolkata
Indian Audit and Accounts Department
June 2008

IS Audit
in
Panchayati Raj Institutions

Occasional Research Paper 2   Series..1

Regional Training Institute, Kolkata

Indian Audit and Accounts Department

June 2008

Table of contents

Introduction

The 73rd and 74th Constitutional Amendments in 1992 were a watershed development in the evolution of local self-governing institutions in India. These Amendments paved the way for a legitimate and authoritative third tier of governance along with the existing structures of the Union and State Governments. The Panchayati Raj Institutions (PRIs) and Urban Local Bodies were recognized as ‘institutions of local self-government’ with specifically mandated policy and structural frameworks, devolved fiscal powers to mobilize resources, and a network of functional and operational responsibilities along with the potential transfer of decision-making functionaries and administrative capacity to the grassroots level.

The establishment of a three –tier structure of local self-government in rural areas with Panchayats at the village, intermediate and district levels has led to a transformatory role for these agencies to function as:

- Institutions of self-government
- Institutions for planning economic development and ensuring social justice in 29 specified areas of responsibility.
- As corollaries and agents of Central and State Governments in implementation of entrusted schemes.

The establishment of decentralized and participatory rural governance in India has been embedded in a context of dramatic developments in the diffusion of Information and Communication Technology (ICT) in the processes and systems of governance. A global consensus has emerged in the 21st century that good governance should be participatory, consensus-oriented, accountable, transparent, responsive, effective, efficient, equitable, inclusive and bound by the rule of law. The utilization of ICT as a tool of good governance implies therefore that the application of ICT will ‘change how citizens relate to Governments as much as it changes how citizens relate to each other’. E-governance or the application of electronic means in the interaction between Government and citizens, Government and business and in internal government operations is thus, in its widest connotation a powerful citizen-centric, communication and participatory democratic process.

E-governance has the potential to enable ordinary citizenry to constantly interface with government mechanisms and systems.

In this Paper, the second in our Research Paper Series an attempt has been made to understand, review and analyse the application of e-governance and ICT methodologies specifically in the context of PRI's. This endeavour is in view of the association of the Comptroller and Auditor General of India with the improvement of accountability frameworks in the effective and efficient use of public funds in local governance; and fulfillment of the larger objectives of decentralization.

The use of IT enabled technology in particular in the realm of funds-flow tracking at various levels of the funds-flow chain of fiscal devolution structures is a critical asset of e-governance in PRI's.

This Paper has been prepared incorporating the conceptual and policy frameworks of e-governance in Panchayati Raj Institutions, relevant guidelines and best practices concerning an audit of IT Systems as issued by the Office of the Comptroller and Auditor General of India, as well as inputs obtained from an exposure gained by two of our core faculty members Shri Sujit Kumar Das and Shri Soumyendra Nath Chattopadhyay to the system software being utilized at present in Panchayati Raj Institutions in West Bengal.

The Paper is structured as follows:

The initial chapters review the key policy paradigms of Electronic Governance in Panchayati Raj Institutions (PRI's) including

- Specific opportunities afforded by the vision of the National E-Governance Plan 2006 with reference to the Mission Mode Project of PRI's.
- Selected operationalised areas of e-governance in different states.

The subsequent chapters attempt to provide a thematic link between the policy frameworks of E-governance and potential areas of IS Audit in PRI's. Empirical details have been provided from an examination of two key e-based MIS platforms currently in operation in West Bengal PRI's.

This is an initial effort in appraising and analyzing the area of e-governance in Panchayati Raj Institutions. Given the nature of the theme, we welcome and earnestly solicit suggestions and feedback from all our readers, so that we can improve our future efforts. These may kindly be sent to rtiKolkata@cag.gov.in.

Sayantani Jafa
Principal Director

Chapter I

Electronic Governance in Panchayati Raj Institutions: Specific Opportunities

The Constitution (73rd Amendment) Act, 1992 was introduced to decentralize governance, planning and development and to empower people at grassroots level.

Thus the Constitution empowered the PRIs to function as “institutions of self-government.” It represented a historic opportunity to transform the face of rural India. The amendment established Panchayati Raj: a system of local democracy through local councils known as Panchayats at the village, intermediate and district level. The amendment mandated that resources, responsibility and decision-making power be devolved from the Central and State governments and placed in the hands of grassroots units with elections every five years. To ensure that the Panchayats themselves stay accountable to all the people of their constituency, they are required to hold meetings of the village assemblies (Gram Sabhas) several times each year, with a quorum of citizens attending.

This amendment specified 29 areas of responsibility, covering all key aspects of village life, which States may transfer to the Panchayats — along with sufficient resources and decision-making authority.

Understanding the importance of the meetings of the Gram Sabha as proximate unit of grassroots and participative democracy, the Seventh Roundtable of the Panchayati Raj Ministers held in Jaipur in December 2004 recognized ICT enabled e-Governance as ‘a decision-making support system for Panchayats themselves, a tool for transparency, disclosure of information to citizens, social audit, a means for better and convergent delivery of services to citizens, a means for improving internal management and efficiency of Panchayats, a means for capacity building of representatives and officials of the Panchayats and as an e-Procurement medium’. Accordingly, all Panchayats in the country were to be provided with fully equipped communication centres. It was also decided that the investment in the infrastructure for these centres would be coming from the Rural Development Fund and the maintenance cost met through a levy imposed on private operators and the Department of Telecommunication (DoT).

The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 10 components, on 18 May 2006 with the centrality of citizen services delivery and use of ICT and e-Governance to improve these. One of the MMPs pertained to Panchayati Raj Institutions as one of the key projects under NeGP.

Introduction of ICT at Panchayat level was expected to allow experimentation with the technology and also give immense opportunity to people at grassroots level to handle technology, be it relating to software, hardware, networking, power supply or any other issue due to which such technology has been traditionally denied to them. Finally, it was to create an improved cyberspace covering the entire government spectrum of the country, where information would flow seamlessly.

The term e-Governance has different connotations:

- **e-Administration**—The use of ICTs to modernize the state; the creation of data repositories for MIS, computerisation of records.
- **e-Services**—The emphasis here is to bring the state closer to the citizens. Examples include provision of online services. E-administration and e-services together constitute what is generally termed e-government.
- **e-Governance**—The use of IS to improve the ability of government to address the needs of society. It includes the publishing of policy and programme related information to transact with citizens. It extends beyond provision of on-line services and covers the use of IS for strategic planning and reaching development goals of the government.
- **e-Democracy**—The use of IS to facilitate the ability of all sections of society to participate in the governance of the state. The remit is much broader here with a stated emphasis on transparency, accountability and participation. Examples could include online disclosure policies, online grievance redress forums and e-referendums, which are conceptually more potent.

Based on the above, the following imperatives made a case for introducing e-Governance in Panchayati Raj Institutions:

a. They can handle the financial accounting as well as financial reporting guidelines vis- à-vis Panchayat Funds and all schemes and functions being implemented through Panchayati Raj Institutions. These could include all governmental and non-governmental fund flows; schemes and fund usage (including contracts awarded and money paid) etc.

b. Enhance their ability to generate, manage and collect local revenue.

c. They are able to automate their own functioning, e.g., records of the minutes of meetings of the Gram Sabha etc. – the information made available could reflect governance structure and decisions taken; profiles of elected representatives and the role played by them; details of Non Government Organisations present in the village.

d. To provide external visibility for all the above mentioned areas for enhanced public participation so that there is transparency and ability to facilitate social audits strengthening the Panchayati Raj based delivery systems.

e. They are able to better participate in the District Planning process and bring in an element of felt needs to the plans. The planning efficacy would depend on a comprehensive resource profiling – amongst other things this should include the resident register of every person in the Gram Panchayat including photographs and personal details like place of stay, educational qualifications, health status; complete map of the villages/habitations, showing each house (possible geo-location), field, roads, schools, Panchayat office, markets, hospitals, places of worship; and, map and topological data showing water flow, feed of weather parameters (including rainfall) year by year, ground water levels; details of local produce - crops, vegetables, handicrafts, industrial output; electricity consumed and available infrastructure like roads, electricity, telecom and major waterworks etc. The planning tools could include modules for financial planning, water management and soil and land management tools etc.

f. They can offer the citizen services that have been devolved to them with a provision of adding more services as they get devolved.

g. Provide external linkages for speedy and transparent transfer of funds; markets; communication with state and central government departments etc.

h. As a mechanism for capacity building.

Chapter II

E-Governance in PRI's: A Brief Overview of Policy Paradigms, Action Plans and On-going Projects

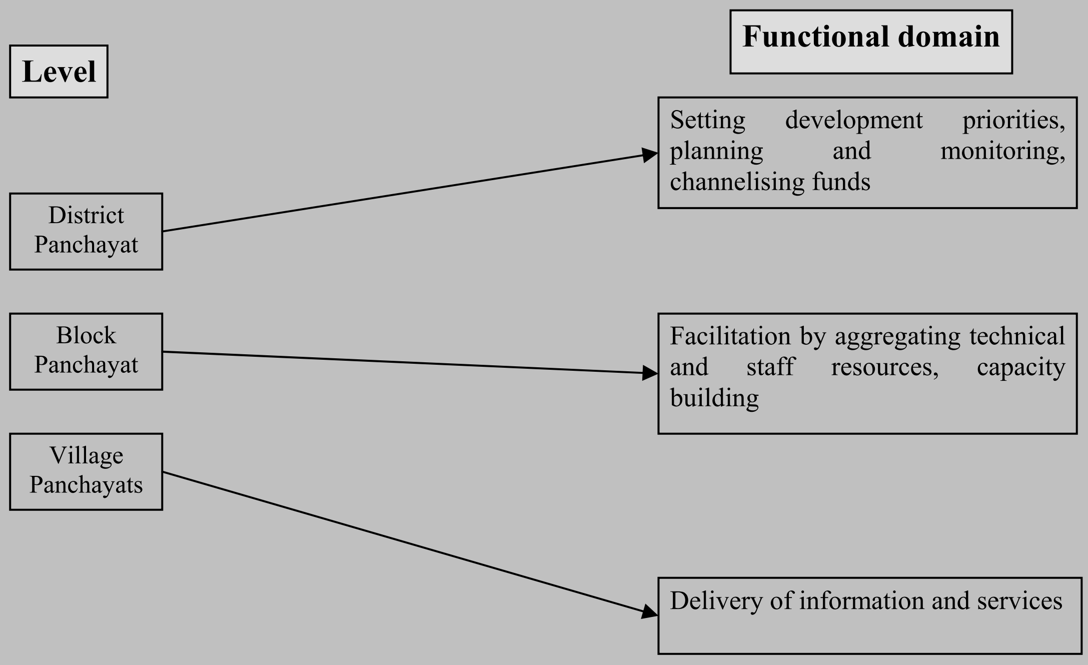
(a) Policy Framework:-

Round Table of State Panchayati Raj Ministers at Jaipur recommended introduction of Information and Communication Technology towards enhancing Panchayat capacity so that they can perform their constitutionally and legislatively mandated functions better.

Consensus to position IS as-

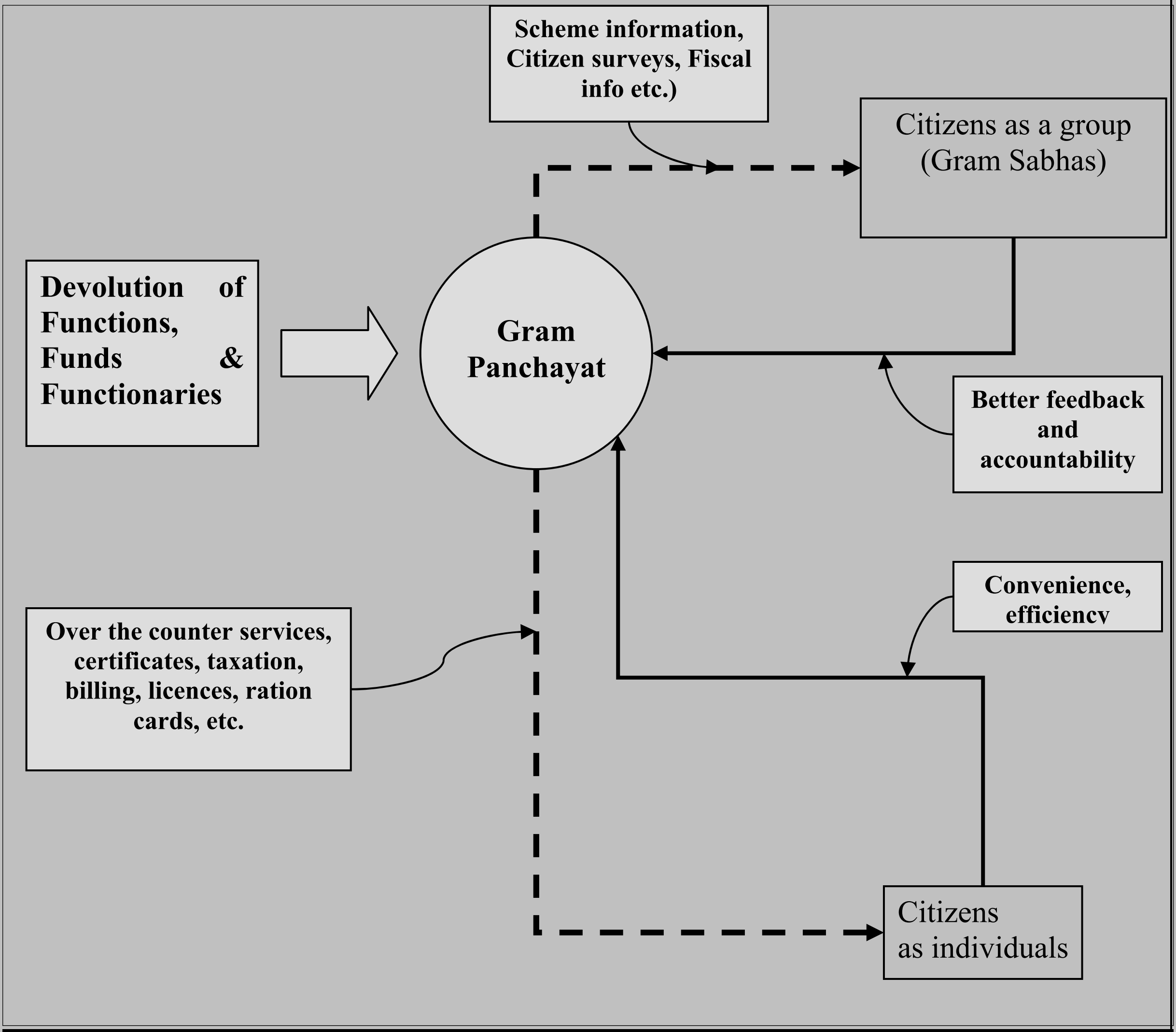
- Decision making support system for Panchayats
- Tool for transparency,
- Disclosure of information to citizens,
- Social audit,
- Better and convergent delivery of services to citizens,
- Improving internal management and efficiency of Panchayats,
- A means for capacity building,
- As an e-Procurement medium.

Overview of the Panchayati Raj Institutions


Level
Functional domain
District Panchayat
Block Panchayat
Village Panchayats
Setting development priorities, planning and monitoring, channelising funds
Facilitation by aggregating technical and staff resources, capacity building
Delivery of information and services

For e-governance Gram Panchayat is a unique institution, for the following reasons:

- Requirement of keeping the Gram Sabha well informed by the GP
- Benefits to citizens flowing from over the counter services.


Scheme information, Citizen surveys, Fiscal info etc.)
Citizens as a group (Gram Sabhas)
Devolution of Functions, Funds & Functionaries
Gram Panchayat
Better feedback and accountability
Convenience, efficiencv
Over the counter services, certificates, taxation, billing, licences, ration cards, etc.
Citizens as individuals

Potential e-governance Services for Gram Sabhas include:

- Dissemination of internal processes of Gram Panchayats: (agendas, resolutions, voting record),
- Proceedings of Gram Sabhas and action taken,
- Progress Reports,
- Dissemination of data (family surveys, property lists, BPL lists, pensions, censuses),
- Services data: (education, health, water and sanitation),
- Natural resources and biodiversity data,
- Databases on Panchayat members and staffing details,
- Availability of government and private infrastructure and village habitat planning
- Aimed at aiding Gram Sabhas to take better informed decisions

Gram Panchayat services for citizens would include:

- Licensing and No Objection Certificates, (trade, running shops, hotels, industries cinematography),
- House-related services, (construction licenses, property ownership records and certification, property tax and related cesses, house or site allotment and change of land use,
- Grievances and petitions on civic services, such as those relating to water supply repairs, streetlight repairs, road and drain cleaning and repairs and garbage disposal,
- Implementation of schemes entrusted to the Panchayats, such as ration cards, pensions, midday meals, school textbooks,
- Certificates: Birth and Death, Income, Solvency.

In tabular format, a summary of proposed e-governance functions at the GP and GS levels is as follows:-

Sl. No.	Objective	Benefits	Strategies
1.	Equip all GPs with working computers, or access to working computers	Lays basic foundation for e-governance at GP level	Responsibility of State governments
2.	Deploy basic software for core functional areas to all GPs.	Will strengthen all GP level governance	Some basic software suites ready; repository of software required
3.	Build capacity to handle software in all GPs	Will improve GP capacity to plan and implement.	States to prepare plans and present for funding
4.	Delivery of Panchayat services to citizens / Gram Sabha	Ensure efficiency and transparency in service delivery	Birth and death certificates, licenses, income and solvency certificates, pensions, ration cards, land records
5.	Deconstruct higher level databases to Gram Panchayat level	Converging information at GP level helps GPs and Gram Sabhas to take better informed decisions	Census, education, health, water and sanitation databases on priority
6.	Build national net-community of GPs through National Panchayat Portal	Help peer learning, rapid up-scaling of good examples, access to technical assistance and correctives.	Portal established, States to first start putting existing data online, followed by Panchayats doing so when enabled
7.	Build systems for electronic tagging and tracking of funds devolved to Panchayats	Ensures transparency and efficiency in fiscal transfers and expenditure tracking	Panchayat Bank accounts databases to be completed by States; States to post details of allocation, receipt & transfer of 12th Finance Commission funds on National Panchayat Portals

Targets for PRIs in India

- 2,40,000 Panchayats to be equipped with computing hardware
- At least 2 people with computing skills in each Gram Panchayat: 5 lakh computer literates working within or in close association with Panchayati Raj.
- 2,40,000 websites organically interlinked with and forming National Panchayat Portal

National Panchayat Portal http://panchayat.nic.in

- A versatile front-end in terms of dynamic website for Panchayats, with information, content and services needed by people,
- Links Citizens with Panchayats,
- Links Panchayats with each other, allows access to information & services provided by MoPR, State Panchayati Raj Departments.

Features offered:

- Gateway to portals of MoPR, State Government PR Departments (35), District Panchayats (560), Intermediate Panchayats (6096) & Village Panchayats (2,40,000).
- Content may be uploaded directly by Panchayat concerned, or through linking portal to already available back-end software solutions
- No technical skills required to use NPP. Each Panchayat required to regularly upload relevant data related to devolved functions using easily learnt data-entry skills.

Implementation of programme by States

- States can choose scope and sequence on basis of suggested models.
- Panchayats can be targeted on priority, based on criteria such as regional coverage, mix of strong and weak Panchayats, availability of infrastructure etc.
- Approximately 35 to 40 percent Panchayats to be covered in first year,
- E-literacy plan for Panchayats should coincide with procurement processes, so that trained operators start functioning immediately,
- State-wise evaluation at end of first year.

(b) A Brief Overview of some E-governance Projects:-

These details have been culled from official policy pronouncements as available for public information

Karnataka

In April 1999 Bellandur Gram Panchayat of Karnataka, about 40 km away from Bangalore, successfully introduced administration through computers. First, measures were taken up to step up the collection of local taxes. Revenue increased from a mere Rs 60,000 in ’93 to Rs. 25 lakh in ’99. With more funds available for development purpose, the Panchayat was in a better position to address people’s problems. The computerisation of Panchayat records was achieved through an investment of Rs 70,000 raised locally. By pressing a key, a resident of the village can have a look at all relevant data like land holdings of each family, taxes due from them and the list of beneficiaries under various housing and employment schemes. Fresh applications for power and water connections are also computerised for disposal at the monthly Panchayat meetings. The paper work has been minimised as computer operators issue all receipts.

Madhya Pradesh

In September 1999, the Task Force appointed by the State Government of Madhya Pradesh suggested an expansion programme of information technology in the State. The committee recommended that all ‘District Governments’, Zilla Panchayats, Block Panchayats and Gram Panchayats should be computerised by the year 2003. This was with a view to encouraging participation of rural people in the development process.

In January 2000 the State Government launched the Gyandoot project, opening the first rural cyber café of the state at village Dhehri Saryaya in Dhar district. As many as 21 such cyber cafes, named Suchanalayas (Information Centres), have become operational in five blocks of the district under the Gyandoot project. In Dhar, 311 Gram Panchayats have been connected through 21 such Suchanalayas. Information on prices of main agricultural produce in markets, copies of relevant records for obtaining loans from the government and financial institutions and other purposes, online registration of public grievances and e-mail replies are provided through this network. The Zilla Panchayat has provided Rs. 25 lakh for the project and would receive as commission 10 per cent out of the income of these centres.

In March 2000 a website on district governments was developed with vital information about district governments on the Internet. A decision was also taken to computerise the Urban Administration and Development Directorate as part of the state government’s plan to promote use of information technology in government work. Detailed information relating to reservations and elections, administrative staff, income and expenditure, budget, taxation and recovery, movable and immovable property, basic facilities like water supply, cleanliness and street lighting, slum development plans, colonisation and fire brigade services in respect of all urban civic bodies would be fed into computers at the Head of the Department level.

Haryana

In October 1999, the Fatehabad district of Haryana was the first in the country to have a district computer network linking all sub-divisions, tehsils (administrative unit), sub- tehsils (administrative unit), blocks, municipal committees and district offices to a dual server installed at the district headquarters. It was also the first district to release a CD-ROM about its revenue data and the first in the state to have its own website on the Internet.

Current e-Governance projects in different States & Union Territory

eGRAM of Government of Gujarat

This project is to set-up a telecom infrastructure to connect 13,716 village panchayats and Common Service Centres in the state. The panchayat offices/eGRAMs are expected to form a socio-economic network supporting information dissemination and facilitating e-governance initiatives in the state. The connectivity will also facilitate point to point and point to multipoint video conferencing services, Voice Over Internet Protocol services and both intra and Internet services from these village panchayats and Common Service Centres.

Akshaya

As part of Kerala’s e-literacy campaign, Akshaya e-Centers are being set up throughout Kerala. These centers will initially provide e-literacy to one member from every household and act as ICT dissemination nodes and delivery points in every village. All Akshaya e Centres would have Internet connectivity and would be networked with a centralized operating center.

Arunachal Pradesh Community Information Center

Community Information Center (CIC) was dedicated to the people of the eight North-Eastern states as a new structure of localised governance. Each is well-equipped with modern infrastructure. Each center has two CIC operators as managers and for providing services to the public. Basic services to be provided by CICs include Internet access and e-mail, printing, data entry and word processing and training for the local populace. Most CICs charge nominal amounts from users for services which helps them to meet day-to-day running expenses. To ensure future financial sustainability of this enterprise, it is proposed to use the Community Information Centers for e-entertainment.

Bhoomi

Karnataka started Bhoomi as a major initiative to computerize land records to ensure more secure title deeds and roll-back the rampant cases of corruption. The existing registry of the 20 million land records of 6.7 million land owners in 176 taluks of Karnataka have been computerised and organized into a database. The government intends to sustain Bhoomi and replicate it at many more delivery points at sub-district levels, by positioning the land records database by ensuring kiosk operators a minimum income. Bhoomi is keen on private sector involvement and options are being explored for partnerships with the private sector for 'retailing'.

CARD

The Computer-aided Administration of Registration Department in Andhra Pradesh is designed to eliminate the maladies affecting the conventional registration system by introducing electronic delivery of all registration services. CARD was initiated to meet objectives to demystify the registration process, bring speed, efficiency, consistency and reliability, substantially improve the citizen interface etc. Six months following the launch of the CARD project, about 80% of all land registration transactions in AP were carried out electronically. Since 60% of the documents, Encumbrance Certificates (ECs) and certified copies relate to agricultural properties, the success of the CARD project has great benefit for the rural farming community.

Community Learning Center Project (CLC)

The Community Learning Centre is a joint initiative between the Azim Premji Foundation (APF) and the State government of Karnataka. The government contributes towards hardware and other related expenses per CLC. The Foundation takes care of management and the training of Young India fellows (YIFs) who manage the CLCs. Each CLC is housed in a separate room in the school and is equipped with five to eight computers. The CLCs are used to enhance classroom learning during school hours. In the first phase, 35 CLCs were launched in Bangalore, Kolar and Mandya districts. In the second phase, 55 CLCs were inaugurated across 11 districts within one month and in the third phase, 135 CLCs were launched in other districts.

Dairy Information System Kiosk (DISK)

The DISK application targeted at the booming dairy sector has been tested for two milk collection societies by the Indian Institute of Management Ahmedabad's e-governance center. The project consists of two basic components—an application running at the rural milk collection society that could be provided Internet connectivity and a portal at the district level serving transactional and information needs of all members. DISK has helped in the automation of the milk buying process at 2,500 rural milk collection societies and has been pilot tested in two co-operative villages of Amul dairy in Kheda district. Software called

AkashGanga has been developed with special features to enable speedier collection of milk and faster disbursement of payments to dairy farmers.

Fast, Reliable, Instant, Efficient Network for the Disbursement of Services (FRIENDS)

FRIENDS is part of the Kerala State IT Mission. Its counters handle 1,000 types of payment bills originating out of various PSUs. The payments that citizens can make include utility payments for electricity and water, revenue taxes, license fees, motor vehicle taxes, university fees, etc. Firewalls safeguard data from manipulation. The application has provisions for adding more modules and for rolling back incorrect entries without affecting the database even at the user level. One important feature of FRIENDS is a provision for adding more modules and a queue management system.

GramSampark

'Gramsampark' is a flagship ICT product of the state of Madhya Pradesh. A complete database of available resources, basic amenities, beneficiaries of government programmes and public grievances in all the 51,000 villages of Madhya Pradesh can be obtained by accessing the concerned website. Gramsampark has three sections-Gram Paridrashya (village scenario), Samasya Nivaran (grievance redress) and Gram Prahari (village sentinel). An eleven-point monitoring system has been put in place whereby programmes are monitored village-wise every month. Four more programmes are under the monitoring system, which includes untouchability-eradication, women's empowerment, water conservation and campaigns for sanitation.

Lok Mitra

The Lok Mitra project provides people of Hamirpur in Himachal Pradesh information about vacancies, tenders, market rates, matrimonial services, village e-mail. An interesting feature is that citizens can use the IS enabled system as a grievance redress system. The project has been extended to cover all the districts of Himachal Pradesh.

Mahiti Shakti

This project operates at Gujarat like a single window through which the citizens can access information related to all aspects of the government's functioning, various benefit schemes and services ranging from obtaining ration cards to getting sanction for old age pension. Anyone who wishes to avail the benefit has to go to his/her nearest designated STD/ISD kiosk, submit the necessary documents to the Info Kiosk owner and fill in the required form online. For online submission of application, the Info Kiosk owner charges Rs. 10 for the application form and Rs 20 for submission. The taluks of Halol, Kalol, Santrampur, Jambughoda, Ghogamba, Kahmpur, Lunawada, Morwa and Shahera have such info-kiosks.

Chapter III

Need for IS Audit in Panchayati Raj Institutions

Computers themselves have moved from being just electronic data processing (EDP) systems to the realm of Information Technology Systems since they not only process data but store, utilize and communicate a wide variety of information that influences decision making at various levels of an organisation. With the advent and growth of computer network systems, **computer systems are now Information Systems (IS)**. Thus, the term "EDP audit" has been replaced by such terms as "**Information Technology Audit**" and "**Information Systems Audit**".

The auditor is being increasingly faced with the challenge of collecting audit evidence within an IS environment. An IS environment introduces various risks and these very risks give rise to the need for IS Audit. **Because of the greater inherent risks to data integrity, privacy, etc. in an IS as compared to a manual system, an independent audit is required to provide assurance that adequate measures have been designed and are operated to minimize exposure to the various risks.**

Definition of IS Audit

IS audit may be defined as

"the process of collecting and analyzing evidence in an IS environment in order to conclude against the pre-defined audit objectives".

It is a broad term that includes -

- **Financial Audits -** to assess the correctness of an organization's financial statements,
- **Operational Audits -** evaluation of internal control structure,
- **Information Systems Audit (including Performance Audit),**
- **Specialized Audits -** evaluation of services provided by a third party such as outsourcing etc.

Objectives of IS Audit

The objectives of IS audit include assessment and evaluation of processes that

- **Ensures asset safeguarding** –'assets' include the following five types of assets:
  - ✓ ***Data -*** external and internal data, structured and non-structured data, graphics, sound, system documentation etc.
  - ✓ ***Application Systems -*** manual and programmed procedures.

- ✓ ***Technology*** - hardware, operating systems, database management systems, networking, multimedia, etc.
- ✓ ***Facilities*** - Resources to house and support information systems, supplies etc.
- ✓ ***People*** - Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

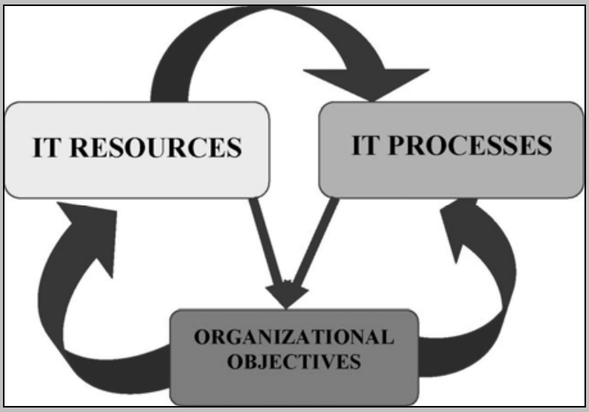
- **Ensures that the following seven attributes of data or information are maintained:**
  - ✓ ***Effectiveness*** - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner. Deals with system effectiveness - evaluating whether the IS meets the overall objectives of top management and users.
  - ✓ ***Efficiency*** - concerns the provision of information through the optimal (most productive and economical) usage of resources. Deals with system efficiency – efficient systems use optimum resources to achieve the required objectives
  - ✓ ***Confidentiality*** - concerns protection of sensitive information from unauthorized disclosure.
  - ✓ ***Integrity*** - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.
  - ✓ ***Availability*** - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.
  - ✓ ***Compliance*** - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria. This essentially means that systems need to operate within the ambit of rules, regulations and/or conditions of the organisation. For example, an FIR to be filed normally requires signature of the complainant as per rules, and needs to be reengineered by changing the rules to permit web based complaints. Similarly, banking operations will have to conform to the banking regulations and legislation. It is also the duty of the IS Auditor to see that the work practices are in tune with the laws of the land such as the IS Act promulgated by the Government of India.
  - ✓ ***Reliability of information*** - relates to systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing

information for reporting to the regulatory bodies regarding compliance with laws and regulations.

Thus, the objective of IS Audit is-

examining whether the IS processes and IS resources combine together to fulfill the intended objectives of the organisation to ensure Effectiveness, Efficiency and Economy in its operations while complying with the extant rules.

This can be depicted diagrammatically in the next page:



The pre-defined audit objectives would vary according to the nature of audit –

Financial Audit / VFM Audit in IS Environment or IS Audit?

- If the audit were **a financial audit**, then the primary audit objective would be to render **an independent opinion as to whether the financial statements of the audited entity reflect a true and fair view of the financial condition of the entity**. Such an audit could also be termed as an IS audit if the entity's accounting system had been substantially computerized and so the **auditor needs to form an opinion regarding the extent of reliance that can be placed on the IS.**

- If the audit is **a VFM audit**, then the primary audit object would be **to assess whether the audited entity obtained value for money from its business operations.** In this case too, the audit could be referred to as an IS audit if IS was being significantly used and so the **auditor needs to form an opinion regarding the extent of reliance that could be placed on the IS**.

- Where audit assesses and reports on the **IS** itself without certifying the financial statements of the entity or assessing the performance of the entity in terms of its business operations. This has become quite common in view of the complexity and huge cost of information systems and the consequent need of the entity management for an independent assessment of the quality of the information system itself. Thus it takes on the nature of a ***systems audit*** and not a system based audit as in the earlier instances. **In such a system audit of IS, the audit objective would generally be to determine whether the IS -**

- ✓ safeguards assets,
- ✓ maintains data integrity,
- ✓ consumes resources efficiently and
- ✓ helps to meet organisational objectives.

A common factor of the above three types of IS Audit are the **formation of an opinion regarding the degree of reliance that can be placed on the IS in the audited organization**.

Evidence Collection and Evaluation

Types of Audit Evidence

When planning the IS audit work in PRIs, the auditor should take into account the type of the audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Physical audit evidence is generally more reliable than the representations of an individual.

The types of audit evidence, which the auditor should consider using, include:

- ✓ **Observed process and existence of physical items;**
- ✓ **Documentary audit evidence (including electronic records);**
- ✓ **Analysis (including IS enabled analysis using CAATs).**

Physical evidence is obtained by observing. It is desirable to corroborate physical evidence, particularly if it is crucial to any audit findings. One of the most desirable corroboration of physical evidence is the acceptance of such evidence by the authorities of ZPs, PSs or GPs.

Physical verification is the inspection or count by the auditor of tangible asset. The auditor can physically inspect office of ZPs, PSs or GPs for the presence of computers, terminals, printers etc. The location of the computers in these offices should be visited for the visual verification of the presence of water and smoke detectors, fire extinguishers etc. Also, the location of the devices should be clearly marked and visible. Auditor has to ensure that physical access controls are designed to protect the organisation from unauthorised access.

In IS where there is considerable importance given to the **physical environment of the systems**, audit also has to ensure that the environment conforms to acceptable norms. The aspects verified could range from the location of the fire extinguishers to physical access controls to an inventory of media in an offsite storage location. In such cases observation and corroboration of observed evidence is important.

Potential methods for collection of IS audit evidence in PRIs:

- Auditors can use interviews to obtain both qualitative and quantitative information during evidence collection work.
- System analysts and programmers of the P&RD Deptt. can be interviewed to obtain a better understanding of the functions and controls embedded within the system.
- Clerical/data entry staff of the ZPs, PSs or GPs can be interviewed to determine how they correct input data that the application system identifies as inaccurate or incomplete.
- Staff of ZPs, PSs or GPs who deals with the application system can be interviewed to determine their perceptions of how the system has affected the quality of their working life.
- Before gathering the above mentioned information it is necessary for the auditor to:
    - ✓ Identify those personnel within the office of ZPs, PSs or GPs who can provide with the best information of an interview topic (Organisation charts often are a first source of information on the appropriate respondents).
    - ✓ Identify clearly the objectives of the interview and make a list of the information to be sought during the interview. General information should be requested at the beginning and end of interviews. Specific information should be requested toward the middle of interviews. Information requested at the beginning of interviews should be neither controversial nor sensitive.
    - ✓ As soon as possible after the termination of interviews, auditors should prepare a report. During the preparation of interview reports, auditors should have two major objectives. First, attempt should be made to separate fact from opinion. Second, auditors should attempt to assimilate the information they obtain during an interview and determine what it means for their overall audit objectives.

Chapter IV

E-Governance and Applications used in Panchayati Raj Institutions– An Illustrative Study

Department of Panchayats and Rural Development, West Bengal is the nodal Department of the state for management of change in the data processing system from Manual System to Information System in all three tiers of PRIs i.e. Gram Panchayats (GP), Panchayat Samitis (PS) and Zilla Parishads (ZP). Out of 3354 GPs, data are being processed and kept with GPMS (Gram Panchayats Management System) in 289 GPs. Likewise, in all ZPs and in 53 PSs data are being processed and kept with IFMS (Integrated Fund Management System). However, so far, all these GPs, PSs and ZPs are not interlinked online with each other. This means they keep and process the data and generate various reports independently to send the same to the concerned monitoring office.

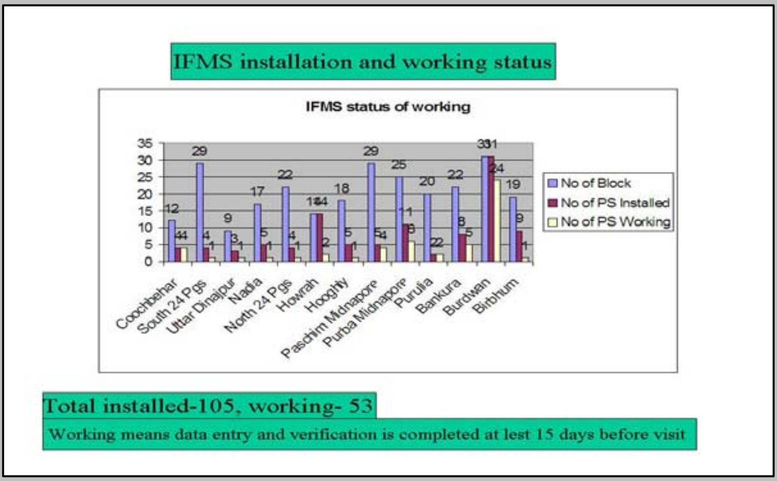
Maintenance of accounts of Zilla Parishads in West Bengal

The narrative reports of the Department of Panchayat and Rural Development further stated that for better financial management of the Zilla Parishads the SARAL (IFMS) software has been installed at all the 18 Zilla Parishads including the Siliguri Mahakuma Parishad after rationalizing and customizing their initial data. The Zilla Parishads are now maintaining their accounts through this software. The Department claimed that this had resulted in quick compilation, monitoring and correction of detected discrepancies of financial data by the Zilla Parishads.

Computerization of PS and GP accounts

105 Panchayat Samitis were brought under the anvil of computerization out of which only 53 PSs were functioning properly. The district wise position of installation and proper functioning of the software is shown in Graph-1.

Graph-1
Progress of Computerisation of Panchayat Samitis

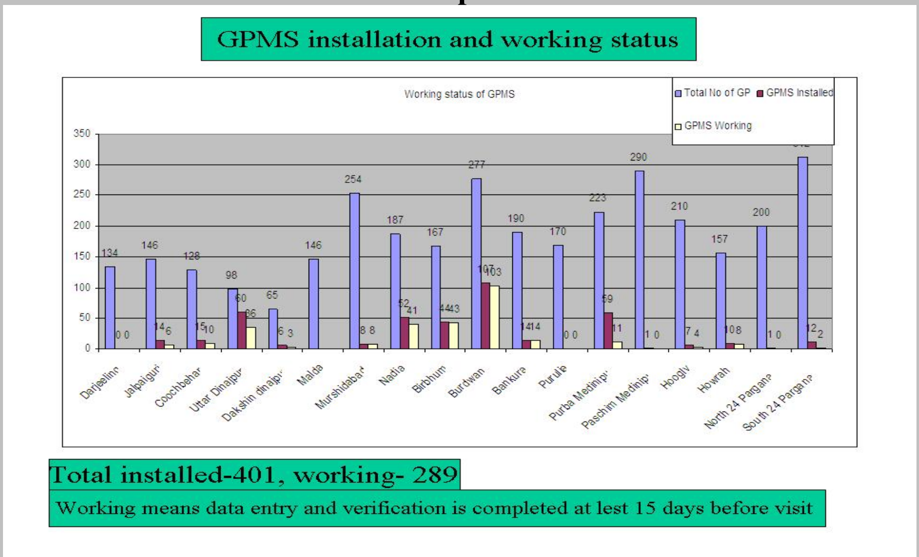

IFMS installation and working status

Total installed-105, working- 53

Working means data entry and verification is completed at lest 15 days before visit

So far as use of the GPMS is concerned, the software was installed in 401 GPs, out of those the same was functioning properly in 289 GPs. The district wise position is shown in Graph 2.

Graph 2



GPMS installation and working status

Total installed-401, working- 289

Working means data entry and verification is completed at lest 15 days before visit

(*Source : Administrative Report 2006-07 of P&RD Department*)

Potential areas of Audit Analysis:

i) At the beginning of the year 2006-07 the target of installing IFMS was 45% of total Panchayat Samities i.e., about 150 numbers. But actually only 105 numbers could be installed. The shortfall in target could be examined.

ii) Out of 105 installed locations only 53 locations are working. Is the absence of properly functioning systems elsewhere due to hardware/software failures or manpower-centric?

iii) If the reasons for non-achievement of target of installations or non-functioning of the system even after installation are due to lack of competent human resources, Audit may review the policy of recruitment and also the training programmes, if any.

iv) How are the non-functioning systems at different locations sought to be operationalised?

v) Similar queries emerge in the cases of Gram Panchayats where GPMS software was installed but was non-functional. There was also lagging behind the targets of overall computerization.

vi) In fully non-functional or partially functional systems in the case of both software platforms was there a parallel run of manual procedures?

vii) According to the recommendations of the Expert Group, there may be some governmental and non governmental efforts to augment the training of PRI officials and elected members by imparting training. Financial assistance to the States has been envisaged to augment their efforts. Audit should see whether coordinated and systematic approach was followed as per the need of the Department. They should also evaluate the efficacy of such training and capacity building interventions.

viii) There are three types of target groups for these capacity building interventions:

a) Elected members of the Panchayats

b) Field level bureaucracy/functionaries

c) Policy makers in the nodal Department

Audit may see whether all the above three types have been included in the above policy.

ix) The Expert Group recommended that the implementation of IS projects in PRIs should have two or more categories of Panchayats (high, medium, low) based on their overall preparedness and different plans should be worked out for each of the categories. The Panchayats with high preparedness should be encouraged to take up the integration of the three tiers of Panchayats. Similarly, Panchayats with low preparedness could be put on the local standalone automation model. Medium category panchayats could be allowed to take up more functions. Audit may see, how far this policy could be implemented in the PRIs under study.

x) The Expert Group recommended that all application software should be built in a platform-independent manner so that they can be reused and replicated across the country. Audit may see to what extent this recommendation could be implemented in the above.

xi) Currently, there is no dedicated network extended up to Gram Panchayat level in the state of West Bengal. Both NICNET & SWAN are contemplating last mile connectivity through broadband, dial-up and VSAT. The Expert Group recommended that for Gram Panchayats, the following connectivity options may be explored in the given order:

- Broadband connection with minimum 256 KBPS (wired or wireless)
- Dial-up and
- VSAT

Audit may see whether the policies of the Department are in line with the above.

Applications used in PRIs of West Bengal – System Architecture

Saral (Integrated Fund Monitoring System)

Area of Application

This software is being used in Zilla Parishad & Panchayat Samitis of West Bengal for monitoring of funds released against different schemes sponsored by State Government or Central Government.

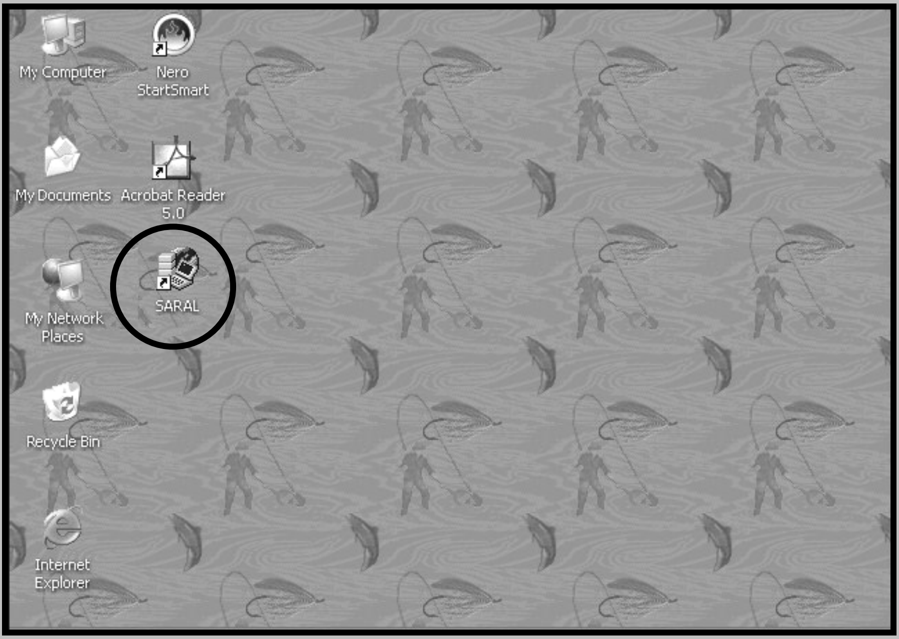
Purpose of this package

- To monitor and control the funds of different schemes and to keep up-to-date information against each scheme;
- Monitoring
    - Receipt of funds from different sources;
    - Receipt of various grants
    - Distribution of funds to different heads as per demand
    - Payment from fund heads and grant heads;
    - Up-dated Balance for various funds and grants;
    - Flow of money
    - Progress of each work under different schemes.
    - Keeping records of
        - Different sanctioned works,
        - Details of approved contractors, work orders, funds released to the contractors, physical progress of work.
- To generate various Accounts Reports e.g..
    - Debit Voucher
    - Credit Voucher
    - Challan
    - Cashier Receipt
    - Cash Book
    - Subsidiary Cash Book
    - General Ledger
    - Cash Analysis
    - Receipt Payment Accounts
    - Cheque Issue Register – Bank A/C wise
    - Register of Cheque Book – Bank A/C wise
    - Advance Register – Employee wise, LSG wise, Job Work wise, Scheme wise
    - Issue of letter to Defaulter for Adjustment,
    - Register for Cheque-in-transit,
    - Details of Un-cashed-self Cheque
    - Head wise liquid cash,
    - Head wise Advance,
    - Head wise Cheque-in-Transit.

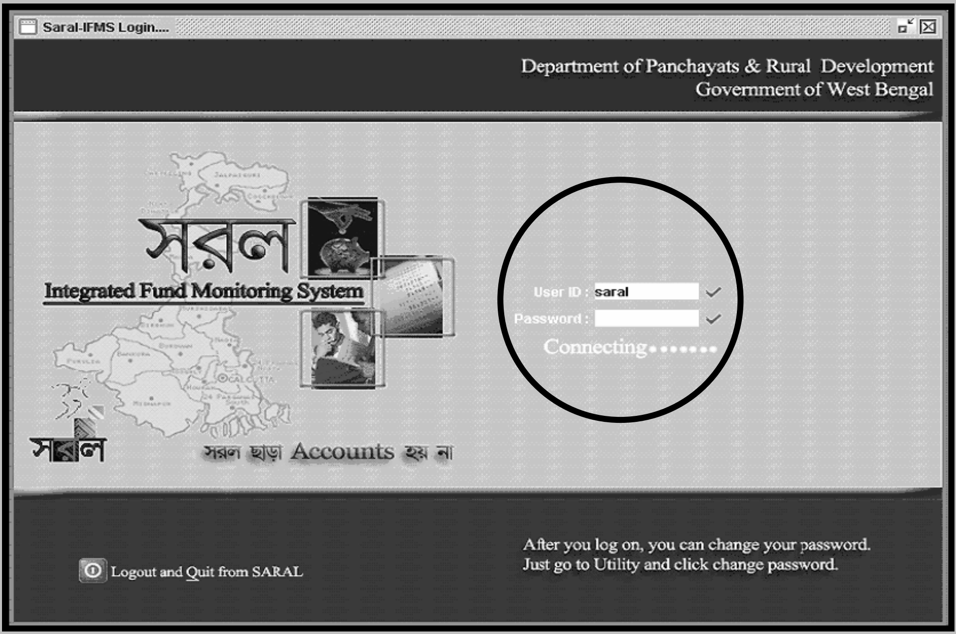
How to open Saral

To open Saral application –

- Find the Saral icon on desktop
- Double click the icon.



Login screen of Saral



Saral-IFMS Login....

Department of Panchayats & Rural Development
Government of West Bengal

সরল

Integrated Fund Monitoring System

User ID : saral

Password :

Connecting•••••••

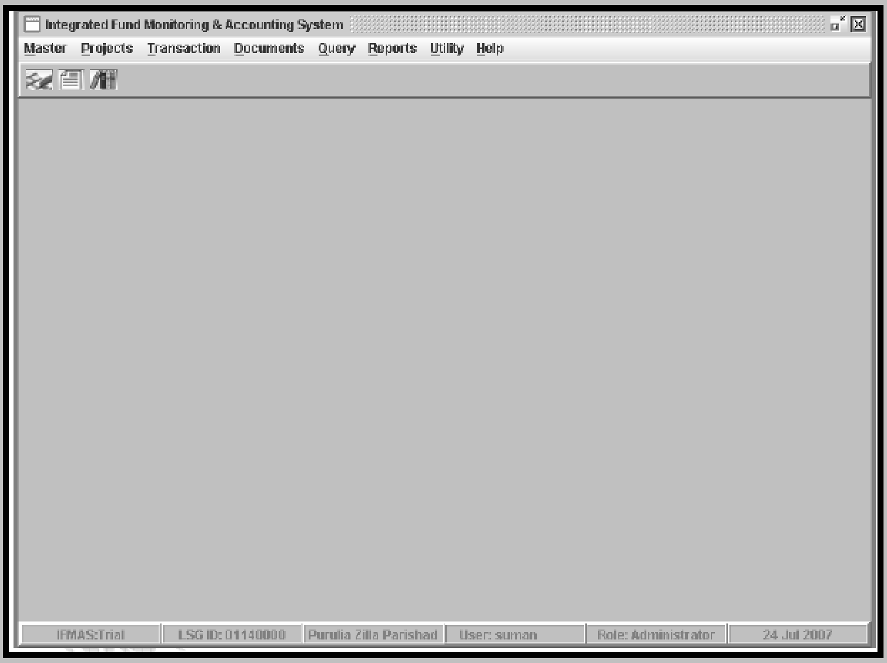
সরল ছাড়া Accounts হয় না

Logout and Quit from SARAL

After you log on, you can change your password.
Just go to Utility and click change password.

- Enter correct user ID and Password to enter the Main Menu.

Main Menu Screen of Saral



IFMAS:Trial | LSG ID: 01140000 | Purulia Zilla Parishad | User: suman | Role: Administrator | 24 Jul 2007

Familiarisation with different Buttons

Following buttons are available in various screens. When the button is active it means one can click it to execute that function. An inactive button indicates that the function of that button is non-executable at that time.

Button	Function
Save	To save entered data in the computer.
Clear	To clear any data or any unsaved voucher / journal / challan.
Search	To search any specific voucher / journal / challan or any other data.
Generate	To see any Report e.g. Cash Book / General Ledger / Cash Analysis. (Respective date / dates is to be filled up first)
Print	To take print out.
Voucher	To view a voucher.
Delete	To delete any entered data.
Query	To get any specific voucher.

Insert	To insert any data to a voucher.
Show details	To view information in more detailed form.
● Add	To add new data.
● Query	To get any specific data that is already saved.
● Verify	To authorise a saved and unverified voucher This can not be done by a user using User Password.
● Modify	To edit an unverified voucher. A verified voucher cannot be edited.
● Hide	To hide any data.
✎	To enter directly into voucher-entry mode.
📄	To see Voucher / Casher Receipt / Challan directly.
📚	To see Accounts Report (Non-schematic) directly.
↙	To minimize the Saral screen.
🔍	To query directly.
💾	To take back-up.
?	To get help for using this application.
☒	To close the Saral window.
⏻	To Logout and Quit from Saral.

Main Menus of Saral

- Master
- Projects
- Transaction
- Document
- Query
- Reports
- Utility
- Help

Master Menu contains following sub-menus:

- Employee
- Contractor
- Job Worker
- LSG (Local self Government)
- Department
- Financial Institution
  - Financial Institution
  - Financial Institution Branch
  - Cheque Book
- Scheme
- GL (General Ledger) Group
- Receipt Payment Group
- LF (Local Fund) Group
- Sthayee Samiti
- Scheme Group
- Account Code
  - Nominal Account Code
  - Real Account Code
- Opening Balance
  - OB for Nominal Account
  - OB for Real Account

Projects Menu contains following sub-menus:

- Meeting
- Project
- Approved Tender
- Work Order
- Utilization Certificate

Transaction Menu contains following sub-menus:

- Voucher Entry
- Query (Accounts Non-Schematic)

Documents Menu contains following sub-menus:

- Voucher / CR / Challan
- Cheque Receipt / Issue Registers
- Cash-in-Transit Register
- Advance Register

Query Menu contains following sub-menus:

- Headwise Balance
- Headwise Transit

- Headwise Advance
- Headwise Deduction from Contractor
- Contractorwise Deduction

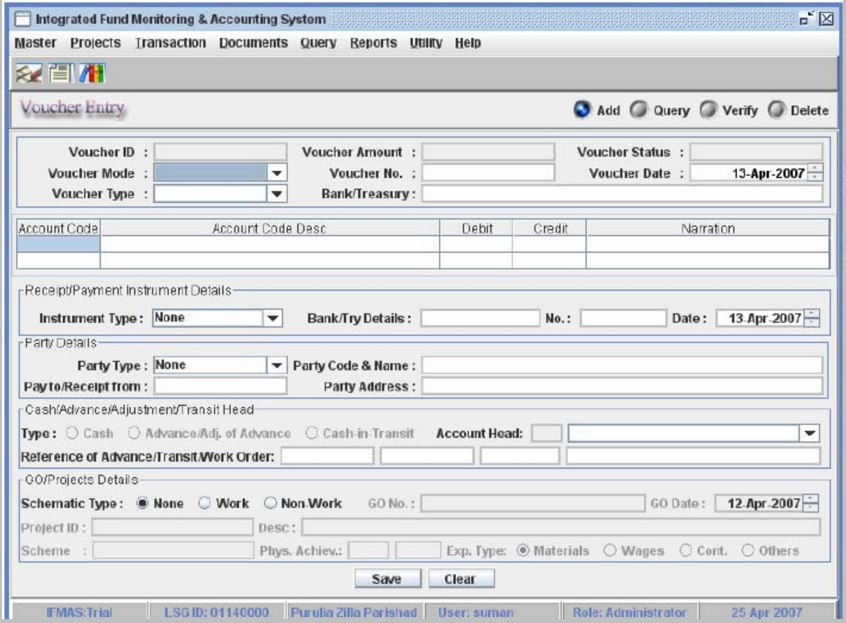
Reports Menu contains following sub-menus:

- Accounts (Non-Schematic)
- Accounts (Schematic)

Utility Menu contains following sub-menus:

- Monthly Accounts Closing
- User Login Master maintenance
- Change Password
- System Administrator
- Login / Logout information
- Bank / Try Reconciliation

Voucher Entry Screen – gateway of the application



● Add ○ Query ○ Verify ○ Delete

Voucher ID :
Voucher Amount :
Voucher Status :
Voucher Mode :
Voucher No. :
Voucher Date : 13-Apr-2007
Voucher Type :
Bank/Treasury :

Receipt/Payment Instrument Details
Instrument Type : None
Bank/Try Details :
No. :
Date : 13-Apr-2007

Party Details
Party Type : None
Party Code & Name :
Pay to/Receipt from :
Party Address :

Cash/Advance/Adjustment/Transit Head
Type : ○ Cash ○ Advance/Adj. of Advance ○ Cash-in-Transit
Account Head:
Reference of Advance/Transit/Work Order:

GO/Projects Details
Schematic Type : ● None ○ Work ○ Non-Work
GO No. :
GO Date : 12-Apr-2007
Project ID :
Desc :
Scheme :
Phys. Achiev.:
Exp. Type: ● Materials ○ Wages ○ Cont. ○ Others

IFMAS:Trial | LSG ID: 01140000 | Purulia Zilla Parishad | User: suman | Role: Administrator | 25 Apr 2007

Voucher Entry Screen

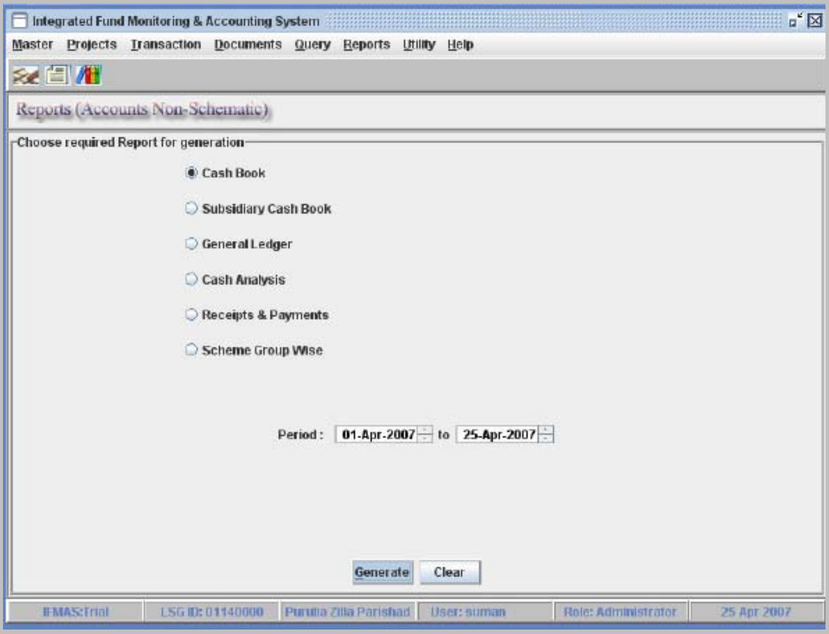
Receipt / Payment entry is done through this screen.

Following are the menus and their functions available in the Voucher Entry Screen–

1. **Add:** To enter a new voucher
2. **Delete:** To delete any non-verified voucher or non-verified challan. A verified voucher or Challan cannot be deleted.
3. **Query:** To see details of any specific voucher or vouchers of any specific period.
4. **Verify:** ‘Supervisor’ users verify the vouchers through this mode. “Operator’ users do not have any access to this mode.

To see the Cash Book:

Click Report →Accounts (Non Schematic) → specify period →Generate.



Reports (Accounts Non-Schematic)

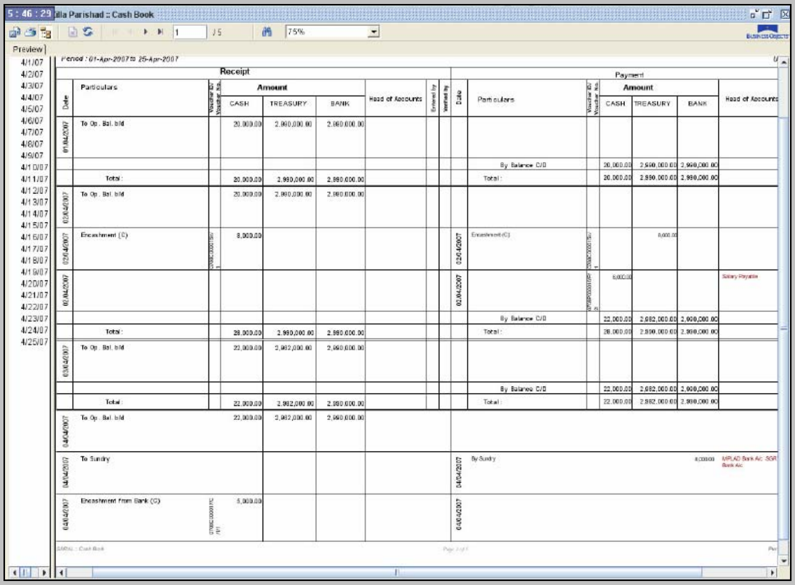
Choose required Report for generation

- ● Cash Book
- ○ Subsidiary Cash Book
- ○ General Ledger
- ○ Cash Analysis
- ○ Receipts & Payments
- ○ Scheme Group Wise

Period : 01-Apr-2007 to 25-Apr-2007

Generate Clear

IFMAS:Trial | LSG ID: 01140000 | Purulia Zilla Parishad | User: suman | Role: Administrator | 25 Apr 2007



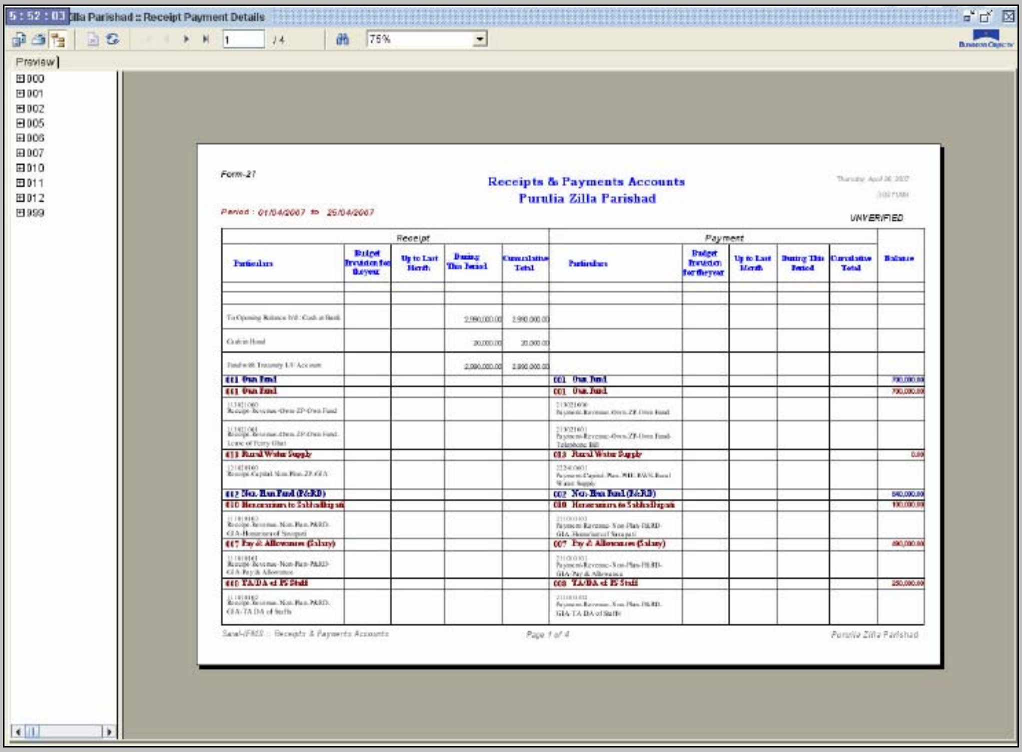
Period : 01-Apr-2007 to 25-Apr-2007

Receipt									Payment						
Date	Particulars	Voucher ID/ Voucher No.	Amount			Head of Accounts	Entered by	Verified by	Date	Particulars	Voucher ID/ Voucher No.	Amount			Head of Accounts
			CASH	TREASURY	BANK							CASH	TREASURY	BANK	
01/04/2007	To Op. Bal. b/d		20,000.00	2,990,000.00	2,990,000.00										
										By Balance C/D		20,000.00	2,990,000.00	2,990,000.00	
	Total :		20,000.00	2,990,000.00	2,990,000.00					Total :		20,000.00	2,990,000.00	2,990,000.00	
02/04/2007	To Op. Bal. b/d		20,000.00	2,990,000.00	2,990,000.00										
02/04/2007	Encashment (C)	[illegible]	8,000.00						02/04/2007	Encashment (C)	[illegible]		8,000.00		
02/04/2007									02/04/2007		[illegible]	6,000.00			Salary Payable
										By Balance C/D		22,000.00	2,982,000.00	2,990,000.00	
	Total :		28,000.00	2,990,000.00	2,990,000.00					Total :		28,000.00	2,990,000.00	2,990,000.00	
03/04/2007	To Op. Bal. b/d		22,000.00	2,982,000.00	2,990,000.00										
										By Balance C/D		22,000.00	2,982,000.00	2,990,000.00	
	Total :		22,000.00	2,982,000.00	2,990,000.00					Total :		22,000.00	2,982,000.00	2,990,000.00	
04/04/2007	To Op. Bal. b/d		22,000.00	2,982,000.00	2,990,000.00										
04/04/2007	To Sundry								04/04/2007	By Sundry				8,000.00	MPLAD Bank A/c: SGR Bank A/c
04/04/2007	Encashment from Bank (C)	[illegible]	5,000.00						04/04/2007						

Cash Book Screen

To see the Receipt & Payment Account

Click Report → Accounts Non-Schematic → Receipt/ Payment Button → specify period →Generate.



Form-27

Receipts & Payments Accounts
Purulia Zilla Parishad

Thursday, April 26, 2007
[illegible]

Period : 01/04/2007 to 25/04/2007

UNVERIFIED

Receipt					Payment					
Particulars	Budget Provision for the year	Up to Last Month	During This Period	Cumulative Total	Particulars	Budget Provision for the year	Up to Last Month	During This Period	Cumulative Total	Balance
To Opening Balance b/d : Cash at Bank			2,990,000.00	2,990,000.00						
Cash in Hand			20,000.00	20,000.00						
Fund with Treasury LF Account			2,090,000.00	2,090,000.00						
001 Own Fund					001 Own Fund					700,000.00
001 Own Fund					001 Own Fund					700,000.00
[illegible] Receipt-Revenue-Own-ZP-Own Fund					[illegible] Payment-Revenue-Own-ZP-Own Fund					
[illegible] Receipt-Revenue-Own-ZP-Own Fund-Lease of Ferry Ghat					[illegible] Payment-Revenue-Own-ZP-Own Fund-Telephone Bill					
013 Rural Water Supply					013 Rural Water Supply					0.00
[illegible] Receipt-Capital-Non-Plan-ZP-GIA					[illegible] Payment-Capital-Plan-PHE-RWS-Rural Water Supply					
002 Non-Plan Fund (P&RD)					002 Non-Plan Fund (P&RD)					840,000.00
010 Honorarium to Sabhadhipati					010 Honorarium to Sabhadhipati					100,000.00
[illegible] Receipt-Revenue-Non-Plan-P&RD-GIA-Honorarium of Savapati					[illegible] Payment-Revenue-Non-Plan-P&RD-GIA-Honorarium of Savapati					
007 Pay & Allowances (Salary)					007 Pay & Allowances (Salary)					490,000.00
[illegible] Receipt-Revenue-Non-Plan-P&RD-GIA-Pay & Allowance					[illegible] Payment-Revenue-Non-Plan-P&RD-GIA-Pay & Allowance					
008 TA/DA of PS Staff					008 TA/DA of PS Staff					250,000.00
[illegible] Receipt-Revenue-Non-Plan-P&RD-GIA-TA DA of Staffs					[illegible] Payment-Revenue-Non-Plan-P&RD-GIA-TA DA of Staffs					

Saral-IFMS :: Receipts & Payments Accounts   Page 1 of 4   Purulia Zilla Parishad

Receipt & Payment Account (Form 27) Screen

In IFMS software any financial transaction has to be entered through Voucher Entry Screen. This screen has several features which will categorise the voucher type. These features include:

1. Voucher ID – This is unique in character and automatically generated.
2. Voucher Mode – All vouchers are categorised into three modes. These are-
   a. Payment
   b. Receipt and
   c. None (e.g. in case of Journal or Contra Voucher)
3. Voucher No. – This number is unique.
   a. If the Voucher Mode is ‘Payment’, the number starts with ‘P’;
   b. If the Voucher Mode is ‘Receipt’, the number starts with ‘R’;
   c. If the Voucher Mode is ‘Contra’, the number starts with ‘C’.
   d. If the Voucher Mode is ‘Journal’, the number starts with ‘J’.

Thus a voucher No. P/1/04/05-06 indicates-

P	= Payment
1	= Voucher Serial No.

04 = Entry Month i.e April

05-06 = Financial Year

4. Voucher Type – Following are the four types of voucher types
    a. T = Treasury
    b. C = Cash
    c. B = Bank
    d. N = Contra
    e. J = Journal
5. Party Type – There are five types of Party Type
    a. None
    b. Contractor
    c. Employees
    d. LSG
    e. Others
6. Voucher Narration – Reasons for the transaction is written here e.g. 'Encashment from Treasury', 'Fund Transfer from TSC to Mid-Day Meal'.
7. Instrument Type – It indicates the mode of transaction e.g. cheque, challan, Advice, by Transfer, Token, Bank Interest, Bank Cheques.

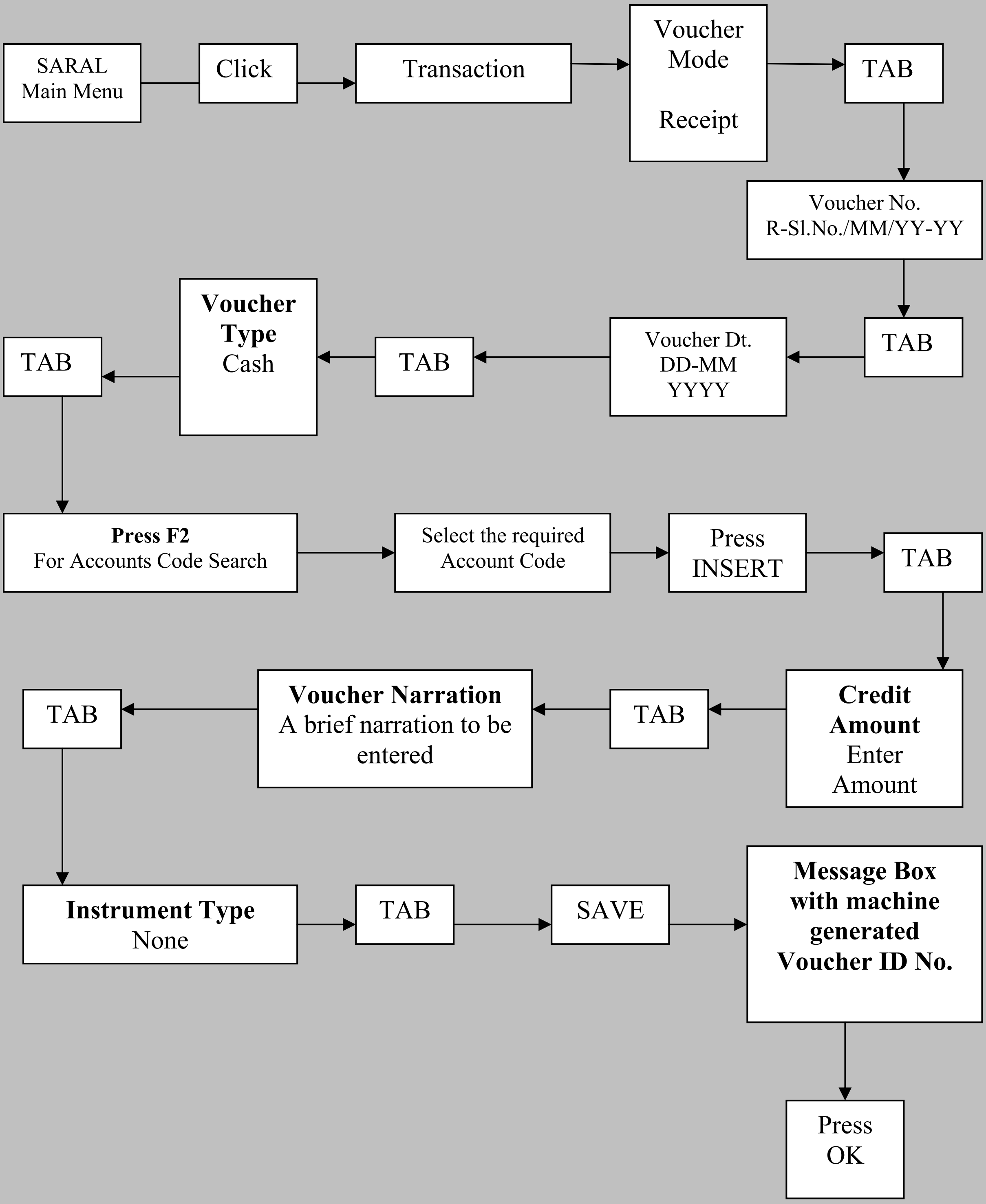
If any payment is to be done through cheque, the Instrument Type will be 'Cheque'. If the transaction type is 'Contra', 'Cash' or 'Journal' then Instrument Type will be NN. In case of 'Treasury' type of transaction, the Instrument Type will be 'Cheque' or 'Challan'.

8. Voucher Net Amount – The amount of transaction is entered here.

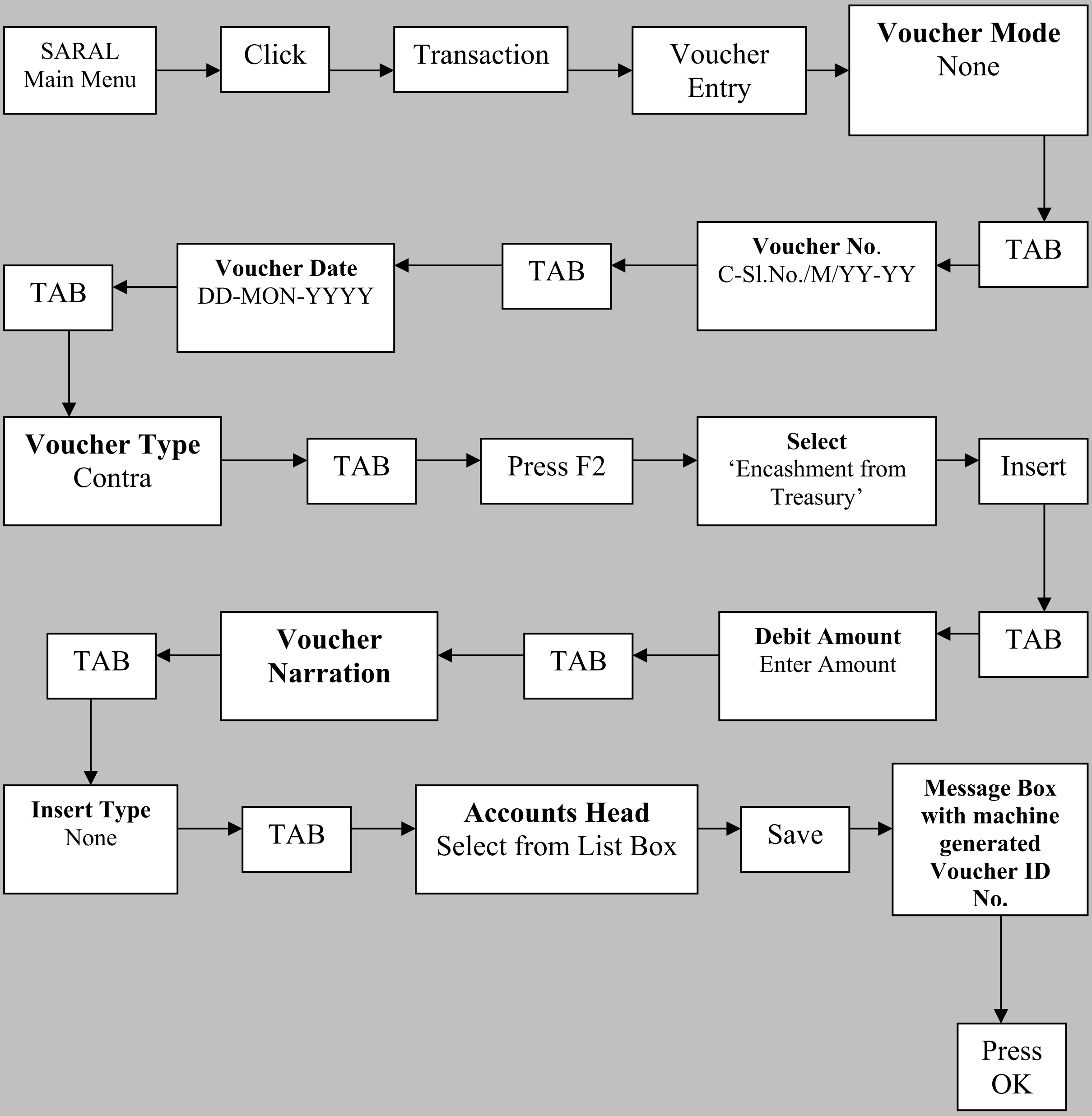
There are seven mandatory fields which, one user can not leave blank while entering a new voucher. These are-

1. Voucher No.
2. Voucher Date
3. Voucher Type
4. Instrument Type
5. Voucher Mode
6. Voucher Narration
7. Account Code

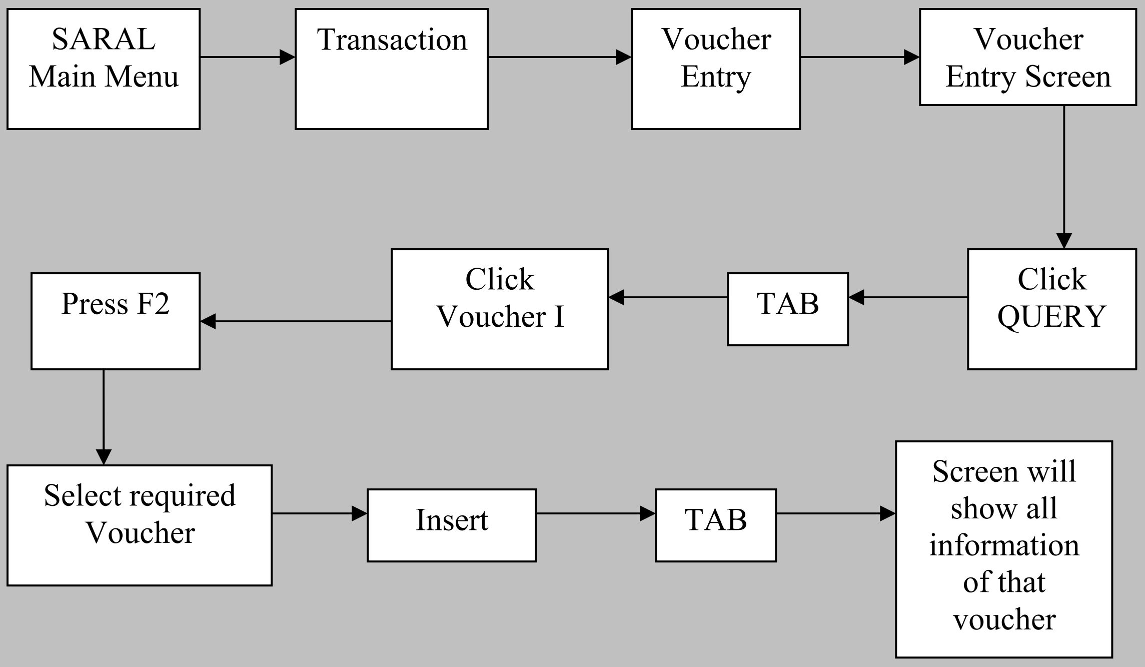
For entering a voucher of cash receipt, the following sequences are maintained:


SARAL Main Menu
Click
Transaction
Voucher Mode Receipt
TAB
Voucher No. R-Sl.No./MM/YY-YY
TAB
Voucher Dt. DD-MM YYYY
TAB
Voucher Type Cash
TAB
Press F2 For Accounts Code Search
Select the required Account Code
Press INSERT
TAB
Credit Amount Enter Amount
TAB
Voucher Narration A brief narration to be entered
TAB
Instrument Type None
TAB
SAVE
Message Box with machine generated Voucher ID No.
Press OK

For entering a voucher of Contra Entry e.g. ‘Encashment from Treasury’ following sequences are maintained:-

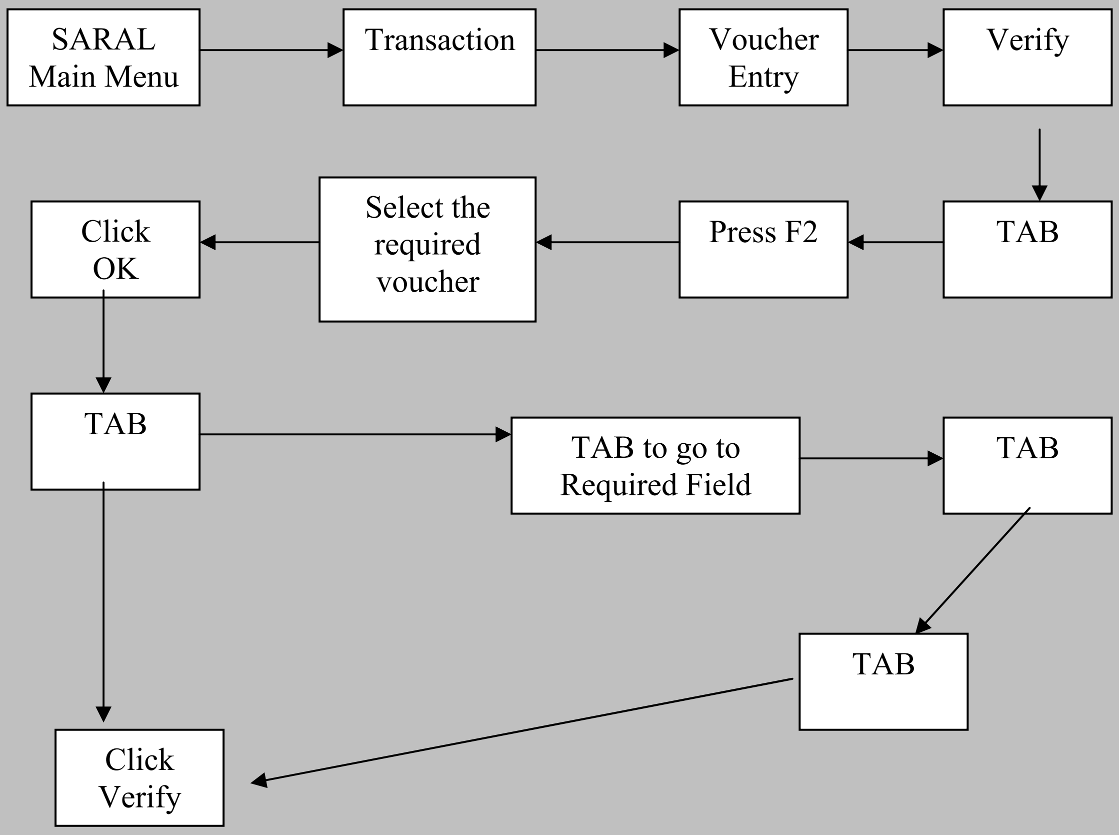


To make query of a voucher following sequences are maintained:-

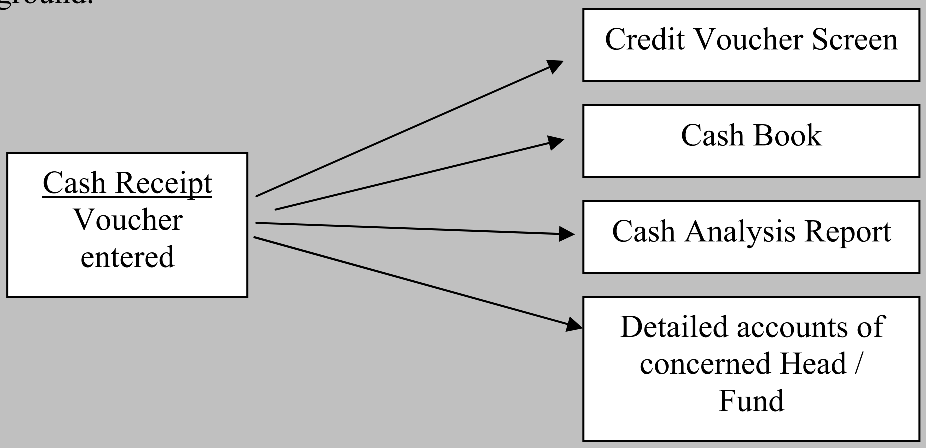


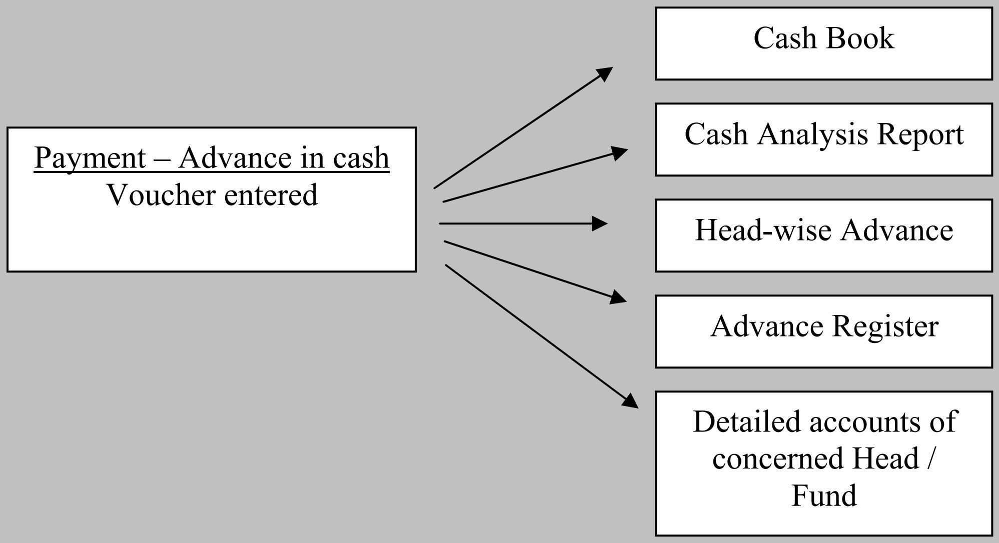
Modification and verification of voucher:

All vouchers are verified by authority higher than user level. Once a voucher is verified it cannot be deleted. To verify a voucher following sequences are maintained:



Once a voucher is entered the following resultant documents are automatically generated in background.





While entering vouchers, this software automatically generate / update different types of related accounts / statements like Receipt and Payment Accounts, Current Balance, Cash-at-Bank, Fund-with-Treasury Ledger Folio Accounts, Monthly Closing Balance.

Gram Panchayat Management System

Area of Application

This software is being used in Gram Panchayats of West Bengal to keep data in a more organised way. There are three levels of users for this software:

1. Data Operator User
2. Supervisory User
3. Administrative User

Data Operator user cannot modify, delete or verify any data. These functions can only be done by Supervisory / Administrative Users. Following data are kept in this programme and documents generated:

1. Staff Details
2. Information on Mouza
3. Information on Panchayat Sansad
4. Information on concerned village
5. Registration of Trade License and collection of cash in this regard
6. Issue of Trade License
7. Registration of Birth
8. Issue of Birth Certificate
9. Registration of death
10. Issue of Death Certificate
11. Accounts keeping
12. Accounts of different schemes
13. Register of Banking transaction
14. Register of First Check in transit
15. Ledger Master
16. Bank Adjustment Ledger
17. General Cash Book
18. General Ledger
19. General Sub Ledger
20. Cheque Register
21. Income Expenditure Statement etc.

To open GPMS from Desktop

Click Desktop GPMS Icon → Log on screen → Enter User ID and Password

Familiarisation with different Buttons

Following buttons are available in various screens. When the button is active it means one can click it to execute that function. An inactive button indicates that the function of that button is non-executable at that time.

Button	Function		
⏮ First	To see the first record	◂ Prev	To see the previous record
▸ Next	To see the next record	⏭ Last	To see the last record
Add	To add any record	Edit	To modify any data
✕ Delete	To delete any record	Save	To save any record
Verify	To verify any record	Find	To find any record
↶ Cancel	To cancel any record	Exit	To exit from the current screen

Main Menus of GPMS

Master:

- Staff Details
  - Mouza Master
  - Part Details
  - Para Master
- Trade Master
  - Trade Certificate Registration Master
  - Birth Certificate Registration Master
  - Death Registration Master
- Scheme Master
- Bank Account Book
- Ledger Master
- Bank Adjustment Ledger
- Collection Head
- Expenditure Head

Public Relation:

- Trade Certificate issues
- Birth Certificate issues
- Death Certificate Issue

Accounts

- Collection
- Expenditure
- Ledger Adjustment
- Bank Deposit
- Bank Withdrawal
- Bank Adjustment
- Cheque Encashment

Repot

- General Cash Book
- General Ledger
- General Sub Ledger
- Cheque Register
- Compiled Collection and Expenditure Report
- Bank Book
- Subsidiary Cash Book

Utility

- Gram Panchayat Information
- Current Working Date
- First Cheque in Transit
- Password
- Query BuilderBackup

How to enter data in Master

Master →staff details→Add

Here one form appears, where data like name, designation, basic pay, religion, caste, date of joining, date of birth, name of father/husband, nominee’s name and relation, home district, home police station, nearest railway station, home/town/city/village’s name, qualification and other interests are entered and saved pressing save button below.

Similarly,

Master →Mouja Master→Add

For keeping information on Mouza, including name, code, area, population

Master →Part details→Add

For keeping information like Part No., Gram Sansad Name, Mouza, Post Office and details of Members

Master →Para Master→Add

For keeping information of Paras under the Panchayat including Para no., Para name, Village name, Part No.

Master →Trade Master→Add

For keeping information like trade code, types of trade, description

Master →Trade Certificate Registration Master→Add

For keeping information on Trade Registration No.(come serially by default) & date, name of the applicant, name of trade, type of trade (selected from a given list), Part Number, Remarks-if any

Master →Material Master→Add

For keeping information on Office stationary, Building Material, Tubewell Material this option is used. Data stored include Item Code, Item Unit, Item Description

Master →Birth Registration Master→Add

For keeping information of Birth Certificate Registration No., First name, Middle name, Last name, Date of Birth, Sex, Name of Father/Mother, Name of the Para, Part Number, Address

Master →Death Registration Master→Add

For keeping information of Death Certificate Registration No., Name of the Person, Date of Death, Sex, Age, Name of Father/Husband, Address, Part No., Para name, Place of Death

Master →Scheme Master→Add

For keeping Scheme Serial No (Serially generated by default), Name of the Scheme, Type of the scheme, Share of State, Centre, Other

Master →Bank Account Book→Add

For keeping information of Account No., Date of Opening of Account, Scheme Account Head (e.g. SGRY, IAY), Name & Address of the Bank, Cash at Bank, Cash in Hand on that date as per Cash Book and as per Pass Book.

Master →Ledger Master→Add

For keeping information of Ledger Folio No, Ledger Head, Administrative Head, Upasamity, Ledger Type, Scheme Name, Bank Account No., Ledger Opening Balance

Master →Bank Adjustment Ledger→Add

For keeping information like Pass Book Account No, Scheme Account Head, Name of Bank, Ledger Head

Master →Collection Budget→Add

For keeping information regarding Ledger Head, Budget Estimate for Preceding Year, Actual Income for Preceding Year, Budget Estimate for the Next Year

Master →Expenditure Budget→Add

For keeping information regarding Ledger Head, Budget Estimate for Preceding Year, Actual Income for Preceding Year, Budget Estimate for the Next Year

Master →Collection Head→Add

For keeping information like Collection Registration No., Collection Head, Scheme Name, Bank Account No., Particulars

Master →Expenditure Head→Add

For keeping information like Collection Registration No., Collection Head, Scheme Name, Bank Account No., Particulars

Issue of Certificates through GPMS

A) Issue of Trade Certificate

Public Relation →Trade Certificate→Trade Certificate Issue→Add

Trade Certificates are issued containing information like Trade Certificate Issue No., Trade Registration No., Matfarakka No., Date of Issue, Name of the Applicant, Name of Trade. After entering the data, print button is clicked to see the print preview. Print out may be generated for issue to the trader.

B) Issue of Birth Certificate

Public Relation →Birth Certificate→Birth Certificate Issue→Add

Birth Certificates are issued containing information like Birth Certificate Issue No. & date, Birth Registration No. & date (can be picked up from the entries made during Birth Registration Master above), First, Middle and Last Name of the Child, Date of Birth, Sex, Father & Mother's name, Part No., Para Name, Place of Birth. Rest as above.

C) Issue of Death Certificate

Public Relation →Death Certificate→Death Certificate Issue→Add

Death Certificates are issued containing information like Death Certificate Issue No.& date, Death Registration No. & date (can be picked up from the entries made during Death Registration Master above), First, Middle and Last Name of the Child, Date of Death, Sex, Father /Husband's name, Part No., Para Name, Place of Birth. Rest as above.

Other jobs done through GPMS

A) Issue of Matfarakka

Accounts→Collection→Add

Matfarakka contains No. & Date, Name, Address, Collection Head, Ledger Head, Bank Name, Account No., Receipt Mode (cash, cheque, draft, memo, TFR), Particular, Receipt Amount. After saving the data, the same can be issued after printing.

B) Recording of Expenditure

Accounts→Expenditure→Add

Any expenditure entails Voucher No. & date, Name & Address of the person to whom the amount is paid, Expenditure Head, Ledger Head, Name, Account No. & Address of the Bank which is involved in the transaction, Payment Mode (cash, cheque, draft, memo, TFR), Particulars, Payment Amount. These entries further generate different reports.

C) Adjustment of Ledger

Accounts→Ledger Adjustment→ Add

The job of any adjustment between one Account Head and other Sub-Heads of the Account can be done through GPMS through the above procedure. The data to be inserted for this transaction are Ledger Adjustment No. (serially generated by default) & date, From Ledger Head, To Ledger Head, Particulars, Posting Amount

D) Adjustment of Bank Account

Accounts→Bank Adjustment→ Add

There are four types of transactions for which Bank Adjustments are required 1) Bank Charges for Cheque encashment 2) Bank Charges 3) Bank interest 4) Bank to Bank transfer. These can be effected through GPMS by the above process. The data to be entered are Adjustment No. & date, Adjustment Type, From Bank Account No., To Bank Account No., Particulars, Deposit Amount.

E) Deposit at Bank

Accounts→Bank Deposit→Add

Three types of deposits viz. a) Cash Deposit b) Bank Cheque Deposit c) Bank to Bank Cheque Deposit. Related data to be entered along with Bank Adjustment are Deposit No. & Date, Deposit Type, Matfarakka No., Bank Account No., Cheque details, Particulars, Deposit Amount

F) Withdrawal from Bank

Accounts→Bank Withdrawal→Add

The corresponding entries of data for this type of transactions are Withdrawal No. & Date, Bank Account No. (selected from list), Bank Name (automatically appear on selecting Bank Account No.), Cheque No. & Date, Particulars, Withdrawal Amount.

F) Cheque Encashment at Bank

Accounts→Bank Withdrawal→ Add

The related data on this transactions are Issued/Received Cheque Encashment No. & date, Encashment Type, Cheque No.& Date, Bank Name, Account No., Account Head, Description, Cheque Amount & Encashment Amount.

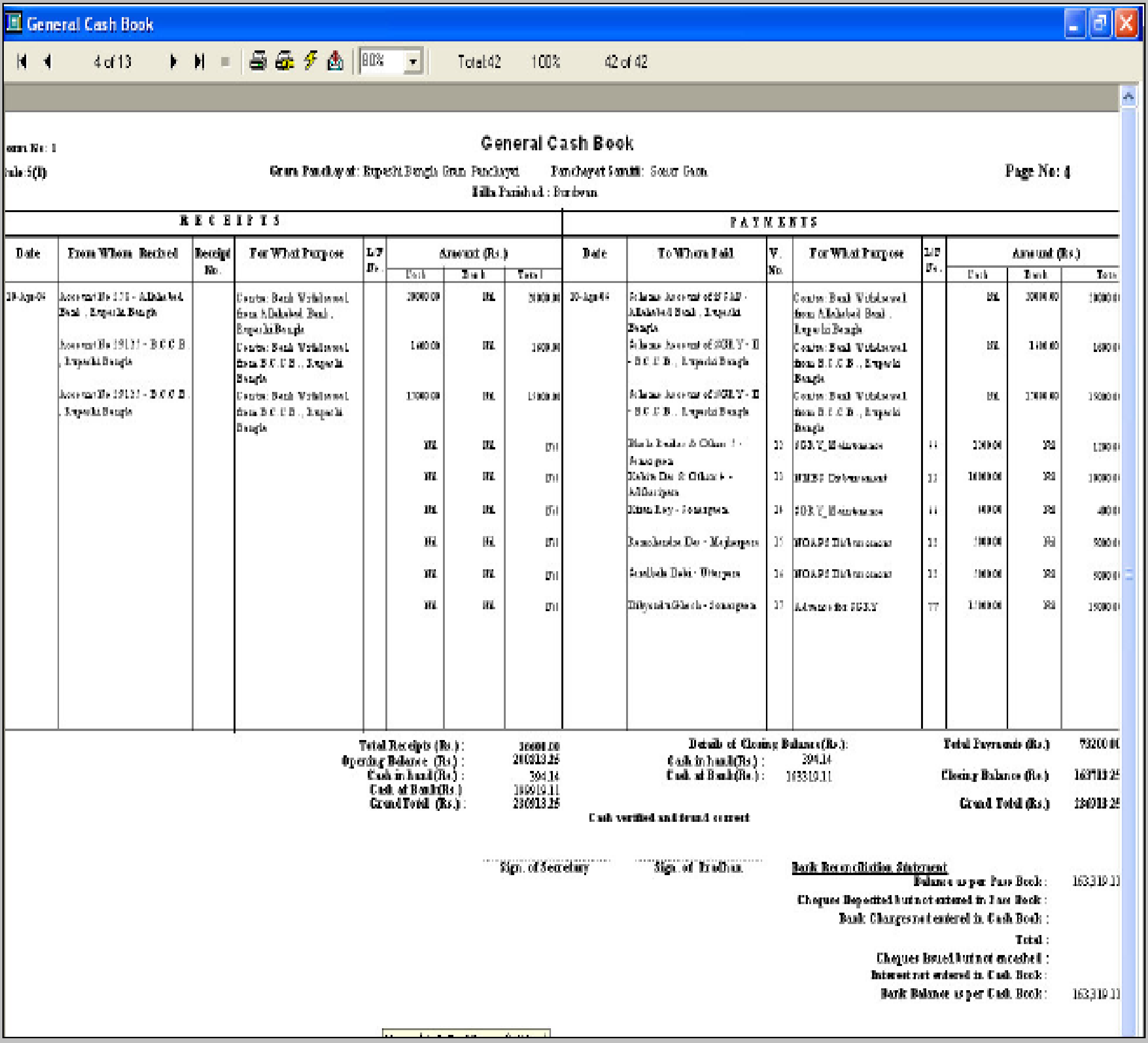
Reports generated through GPMS

A) General Cash Book

Report→General Cash Book→Set Date→Print

The General Cash Book of any period can be generated by setting the From Date and To Date and clicking Print to get the print preview. The Cash Transaction so far done through GPMS are automatically brought under this report date-wise indicating Opening Balance & Closing Balance along with Bank Reconciliation Statement.

An example of General Cash Book



General Cash Book

Form No: 1
Rule 5(II)

Gram Panchayat: Rupeshi Bangla Gram Panchayat   Panchayat Samiti: Sonar Gram
Zilla Parishad : Burdwan

Page No: 4

RECEIPTS								PAYMENTS							
Date	From Whom Recived	Receipt No.	For What Purpose	L/F No.	Amount (Rs.)			Date	To Whom Paid	V. No.	For What Purpose	L/F No.	Amount (Rs.)		
					Cash	Bank	Total						Cash	Bank	Total
20-Apr-08	Account No 135 - Allahabad Bank , Rupeshi Bangla		Contra: Bank Withdrawal from Allahabad Bank , Rupeshi Bangla		20000.00	Nil	20000.00	20-Apr-08	Scheme Account of BSFAD - Allahabad Bank , Rupeshi Bangla		Contra: Bank Withdrawal from Allahabad Bank , Rupeshi Bangla		Nil	20000.00	20000.00
	Account No 19121 - B.C.C.B. , Rupeshi Bangla		Contra: Bank Withdrawal from B.C.C.B. , Rupeshi Bangla		1600.00	Nil	1600.00		Scheme Account of SGRY - II - B.C.C.B. , Rupeshi Bangla		Contra: Bank Withdrawal from B.C.C.B. , Rupeshi Bangla		Nil	1600.00	1600.00
	Account No 19121 - B.C.C.B. , Rupeshi Bangla		Contra: Bank Withdrawal from B.C.C.B. , Rupeshi Bangla		15000.00	Nil	15000.00		Scheme Account of SGRY - II - B.C.C.B. , Rupeshi Bangla		Contra: Bank Withdrawal from B.C.C.B. , Rupeshi Bangla		Nil	15000.00	15000.00
					Nil	Nil	Nil		Bholanath Das & Others 1 - Amarpur	32	SGRY_Maintenance	44	1200.00	Nil	1200.00
					Nil	Nil	Nil		Kabir Das & Others 4 - Adilbaripur	33	NREGS Disbursement	22	10000.00	Nil	10000.00
					Nil	Nil	Nil		Kiran Roy - Sonarpur	34	SGRY_Maintenance	44	400.00	Nil	400.00
					Nil	Nil	Nil		Ramchandra Das - Majherpara	35	NOAPS Disbursement	33	5000.00	Nil	5000.00
					Nil	Nil	Nil		Anadibala Debi - Uttarpara	36	NOAPS Disbursement	33	5000.00	Nil	5000.00
					Nil	Nil	Nil		Dibyendu Ghosh - Sonarpur	37	Advance for SGRY	77	15000.00	Nil	15000.00

Total Receipts (Rs.) : 36600.00
Opening Balance (Rs.) : 200313.25
Cash in hand(Rs.) : 394.14
Cash at Bank(Rs.) : 199919.11
Grand Total (Rs.) : 236913.25

Details of Closing Balance(Rs.):
Cash in hand(Rs.) : 394.14
Cash at Bank(Rs.) : 163319.11

Total Payments (Rs.) 73200.00
Closing Balance (Rs.) 163713.25
Grand Total (Rs.) 236913.25

Cash verified and found correct

Sign. of Secretary   Sign. of Pradhan

Bank Reconciliation Statement

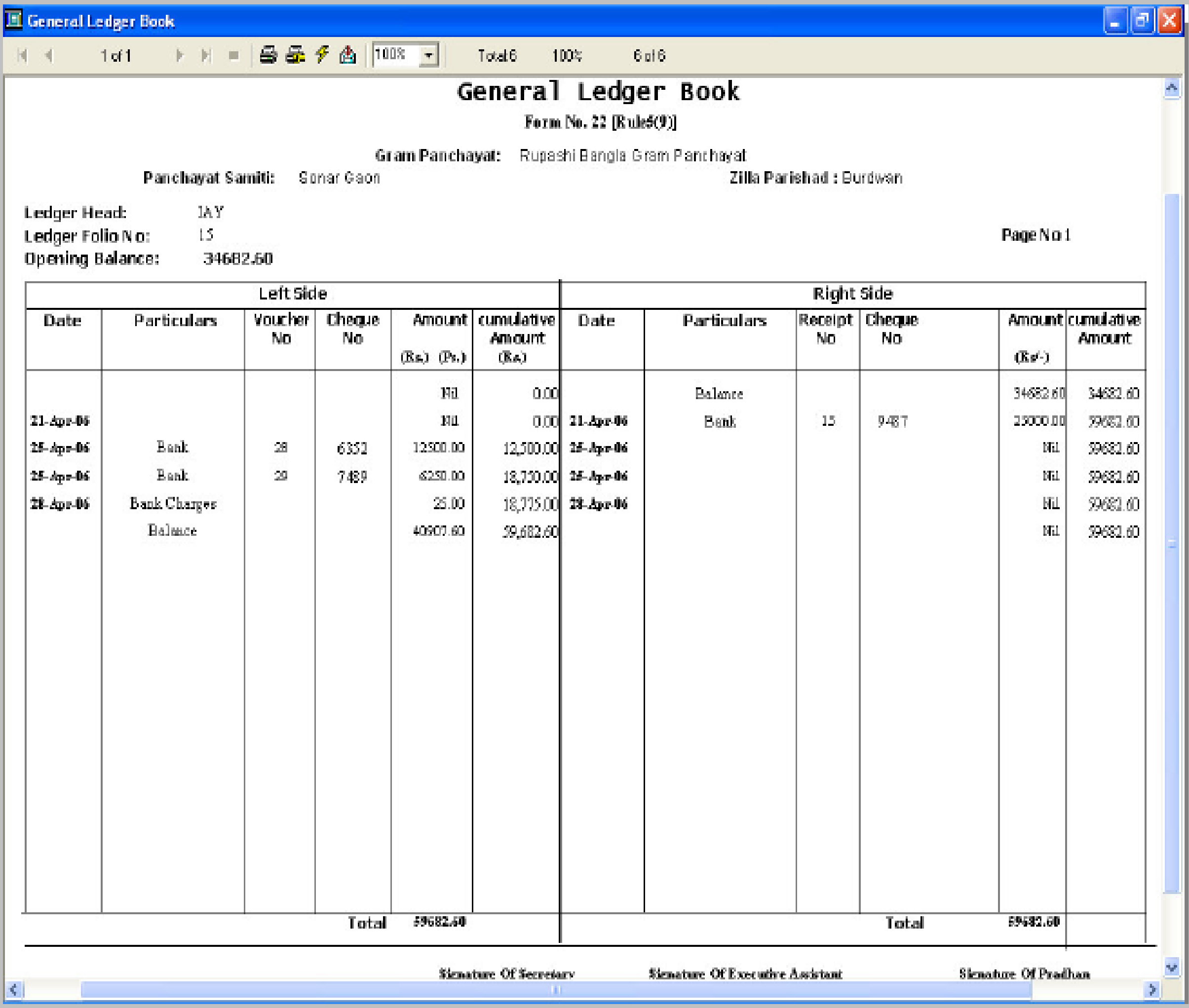
Balance as per Pass Book :	163,319.11
Cheques Deposited but not entered in Pass Book :	
Bank Charges not entered in Cash Book :	
Total :	
Cheques Issued but not encashed :	
Interest not entered in Cash Book :	
Bank Balance as per Cash Book :	163,319.11

B) General Ledger

Report→General Ledger Book→Select Ledger Head →Set Date→Print

The General Ledger Book of any period can be generated by setting the From Date and To Date and clicking Print to get the print preview. The Transaction so far done under the selected Ledger Head through GPMS are automatically brought under this report date-wise indicating Opening Balance & Closing Balance during the said period.

An example of General Ledger Book



General Ledger Book

Form No. 22 [Rule5(9)]

Gram Panchayat: Rupashi Bangla Gram Panchayat

Panchayat Samiti: Sonar Gaon
Zilla Parishad : Burdwan

Ledger Head: JAY
Ledger Folio No: 15
Opening Balance: 34682.60

Page No 1

Left Side						Right Side					
Date	Particulars	Voucher No	Cheque No	Amount (Rs.) (Ps.)	cumulative Amount (Rs.)	Date	Particulars	Receipt No	Cheque No	Amount (Rs/-)	cumulative Amount
				Nil	0.00		Balance			34682.60	34682.60
21-Apr-06				Nil	0.00	21-Apr-06	Bank	15	9487	25000.00	59682.60
25-Apr-06	Bank	28	6352	12500.00	12,500.00	25-Apr-06				Nil	59682.60
25-Apr-06	Bank	29	7489	6250.00	18,750.00	25-Apr-06				Nil	59682.60
28-Apr-06	Bank Charges			25.00	18,775.00	28-Apr-06				Nil	59682.60
	Balance			40907.60	59,682.60					Nil	59682.60
			Total	59682.60					Total	59682.60	

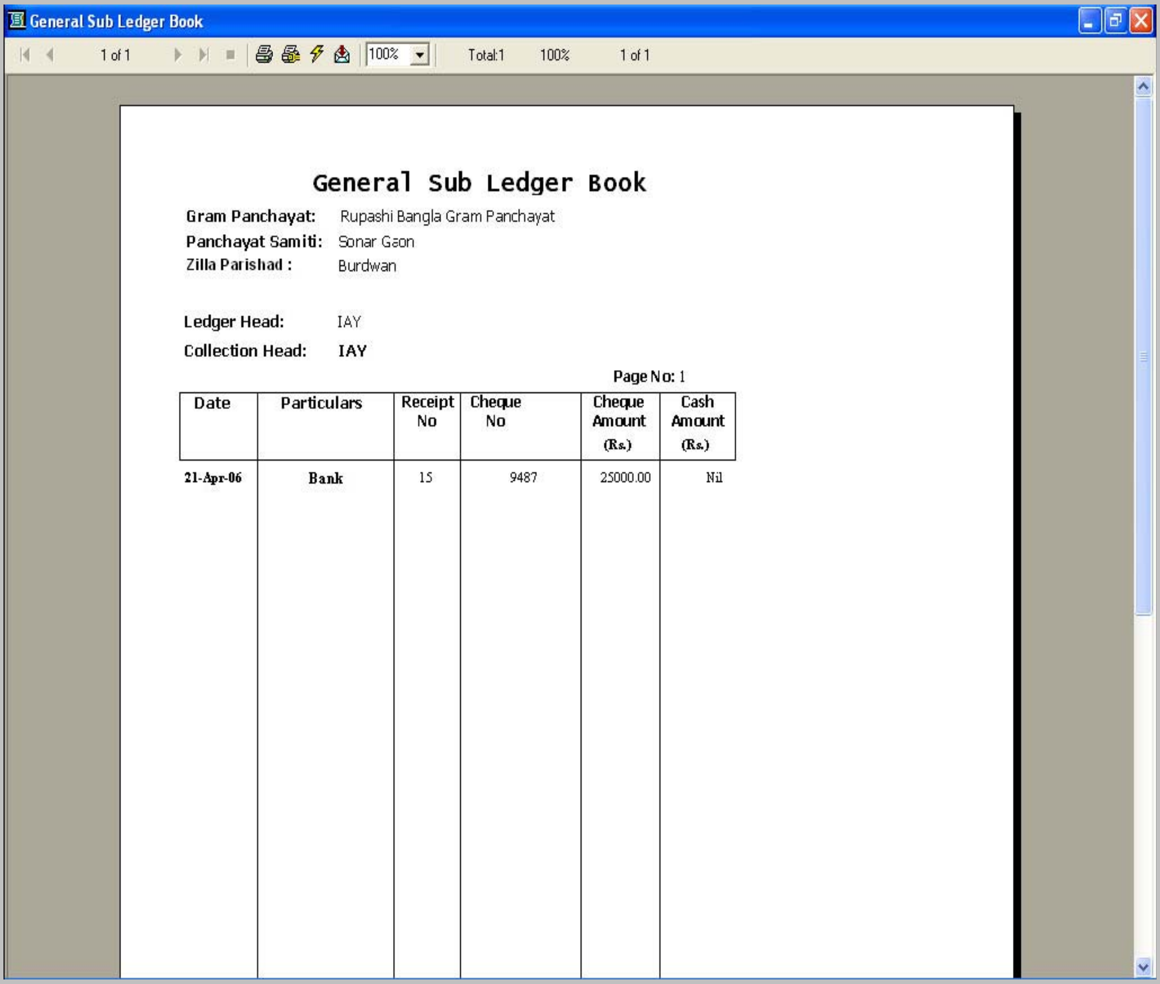
Signature Of Secretary Signature Of Executive Assistant Signature Of Pradhan

C) General Sub Ledger (Collection Head/Expenditure Head)

Report→General Sub Ledger Book→Select Ledger Head→Select Collection Head / Expenditure Head→Set Date→Print

The General Sub Ledger Book of any period can be generated by setting the From Date and To Date and clicking Print to get the print preview. Two Radio Buttons are there one for Collection Head and the other for Expenditure Head. The Transaction so far done under the selected Ledger Head through GPMS (Collection/Expenditure) are automatically brought under this report date-wise.

<u>An example of General Sub Ledger Book</u>



General Sub Ledger Book

Gram Panchayat: Rupashi Bangla Gram Panchayat
Panchayat Samiti: Sonar Gaon
Zilla Parishad : Burdwan

Ledger Head: IAY
Collection Head: IAY

Page No: 1

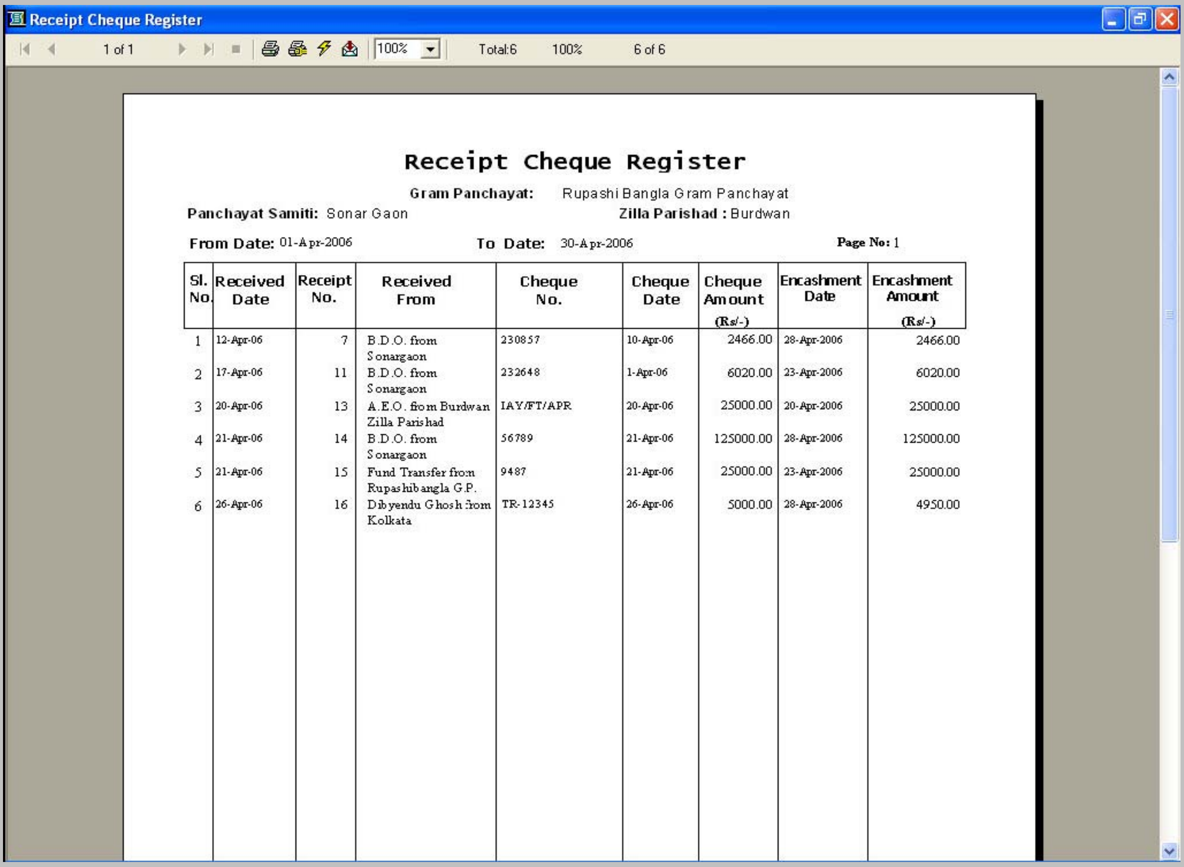
Date	Particulars	Receipt No	Cheque No	Cheque Amount (Rs.)	Cash Amount (Rs.)
21-Apr-06	Bank	15	9487	25000.00	Nil

D) Cheque Register

Report→Cheque Register→Select Received /Issued→Set Date→Print

The Cheque Register of any period can be generated by setting the From Date and To Date and clicking Print to get the print preview. Two Radio Buttons are there one for Received and the other for Issued. The Transaction so far done under any Ledger Head through GPMS (Received /Issued) are automatically brought under this report date-wise the encashment dates are also generated along with the respective amounts of the Cheques.

An example of Cheque Register (Received)



Receipt Cheque Register

Gram Panchayat: Rupashi Bangla Gram Panchayat

Panchayat Samiti: Sonar Gaon

Zilla Parishad : Burdwan

From Date: 01-Apr-2006

To Date: 30-Apr-2006

Page No: 1

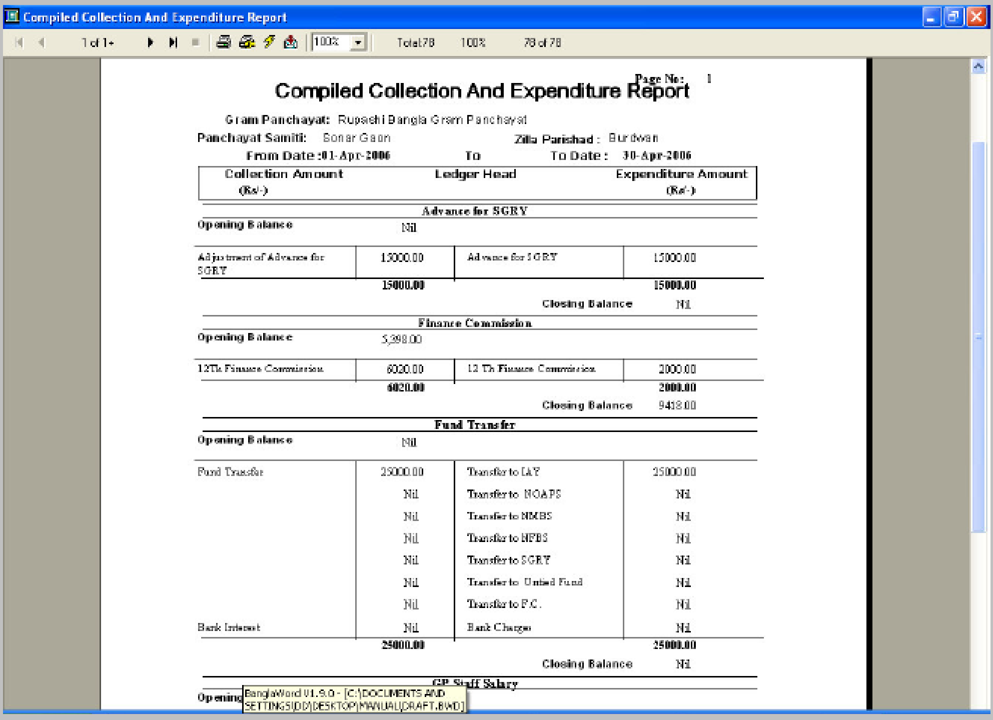
Sl. No.	Received Date	Receipt No.	Received From	Cheque No.	Cheque Date	Cheque Amount (Rs/-)	Encashment Date	Encashment Amount (Rs/-)
1	12-Apr-06	7	B.D.O. from Sonargaon	230857	10-Apr-06	2466.00	28-Apr-2006	2466.00
2	17-Apr-06	11	B.D.O. from Sonargaon	232648	1-Apr-06	6020.00	23-Apr-2006	6020.00
3	20-Apr-06	13	A.E.O. from Burdwan Zilla Parishad	IAY/FT/APR	20-Apr-06	25000.00	20-Apr-2006	25000.00
4	21-Apr-06	14	B.D.O. from Sonargaon	56789	21-Apr-06	125000.00	28-Apr-2006	125000.00
5	21-Apr-06	15	Fund Transfer from Rupashibangla G.P.	9487	21-Apr-06	25000.00	23-Apr-2006	25000.00
6	26-Apr-06	16	Dibyendu Ghosh from Kolkata	TR-12345	26-Apr-06	5000.00	28-Apr-2006	4950.00

E) Compiled Collection and Expenditure Report

Report→Compiled Collection and Expenditure Report→Set Date→Print

The Compiled Collection and Expenditure Report (Head-wise) of any period can be generated by setting the From Date and To Date and clicking Print to get the print preview. The Transaction so far done under any Ledger Head through GPMS (Received /Issued) are automatically brought under this report along with Opening Balance and Closing Balance at the end of the selected period.

An example of Compiled Collection and Expenditure Report



Page No: 1

Compiled Collection And Expenditure Report

Gram Panchayat: Rupashi Bangla Gram Panchayat

Panchayat Samiti: Sonar Gaon Zilla Parishad : Burdwan

From Date :01-Apr-2006 To To Date : 30-Apr-2006

Collection Amount (Rs/-)		Ledger Head	Expenditure Amount (Rs/-)
		Advance for SGRY	
Opening Balance	Nil		
Adjustment of Advance for SGRY	15000.00	Advance for SGRY	15000.00
	15000.00		**15000.00**
		Closing Balance	Nil
		Finance Commission	
Opening Balance	5,398.00		
12Th Finance Commission	6020.00	12 Th Finance Commission	2000.00
	6020.00		**2000.00**
		Closing Balance	9418.00
		Fund Transfer	
Opening Balance	Nil		
Fund Transfer	25000.00	Transfer to IAY	25000.00
	Nil	Transfer to NOAPS	Nil
	Nil	Transfer to NMBS	Nil
	Nil	Transfer to NFBS	Nil
	Nil	Transfer to SGRY	Nil
	Nil	Transfer to United Fund	Nil
	Nil	Transfer to F.C.	Nil
Bank Interest	Nil	Bank Charges	Nil
	25000.00		**25000.00**
		Closing Balance	Nil
		GP Staff Salary	
Opening			

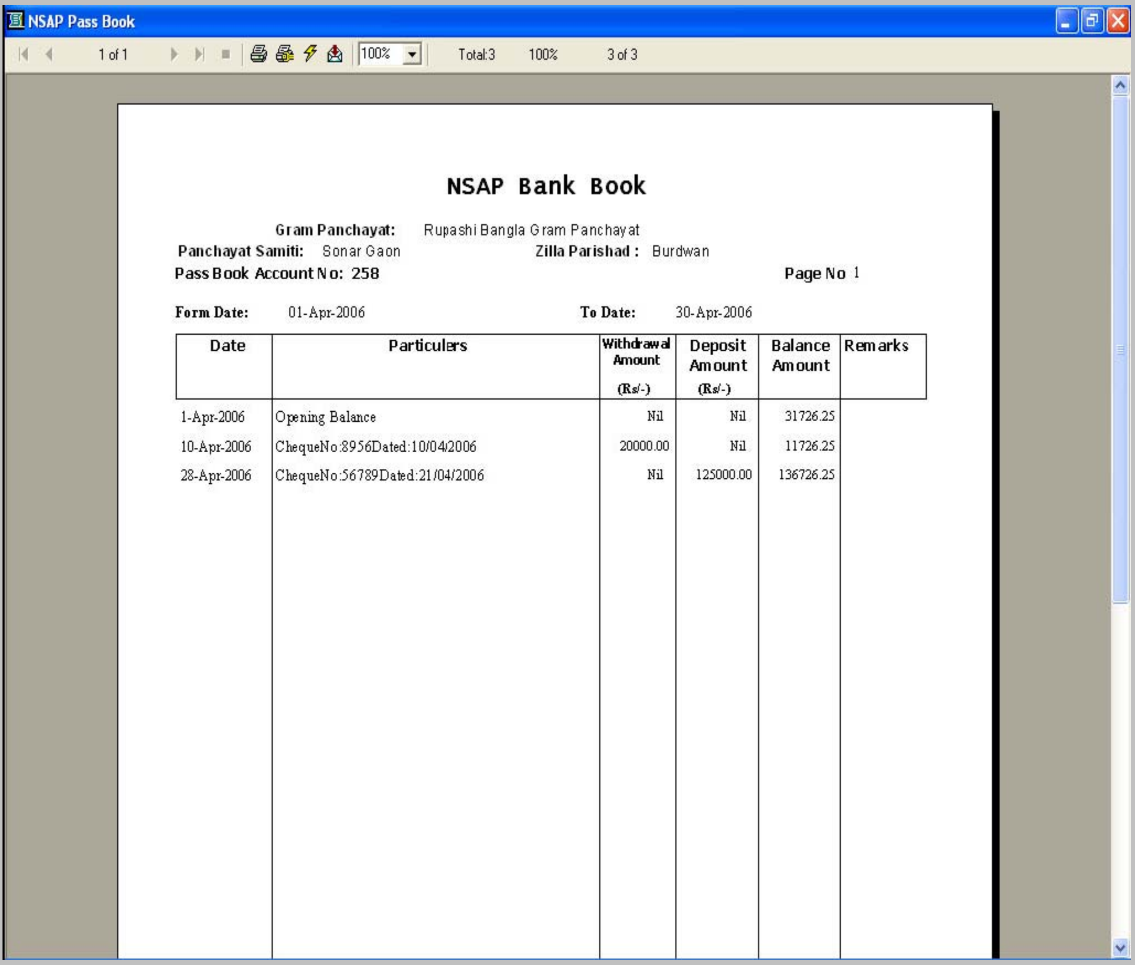
BanglaWord V1.9.0 - [C:\DOCUMENTS AND SETTINGS\DD\DESKTOP\MANUAL\DRAFT.BWD]

F) Bank Book

Report→Bank Book→Select Pass Book Account No. →Set Date→Print

The Bank Book Statement of any period can be generated by setting Pass Book Account No. and the From Date and To Date and clicking Print to get the print preview. The Transaction so far done under any that account through GPMS are automatically brought under this report along with Opening Balance and Balance Amount at the end of the selected period.

An example of Bank Book Report



NSAP Bank Book

Gram Panchayat: Rupashi Bangla Gram Panchayat
Panchayat Samiti: Sonar Gaon Zilla Parishad : Burdwan
Pass Book Account No: 258 Page No 1

Form Date: 01-Apr-2006 To Date: 30-Apr-2006

Date	Particulers	Withdrawal Amount (Rs/-)	Deposit Amount (Rs/-)	Balance Amount	Remarks
1-Apr-2006	Opening Balance	Nil	Nil	31726.25	
10-Apr-2006	ChequeNo:8956Dated:10/04/2006	20000.00	Nil	11726.25	
28-Apr-2006	ChequeNo:56789Dated:21/04/2006	Nil	125000.00	136726.25	

Chapter V

Documents required for understanding the Panchayati Raj Institutions Information System

To understand the Information System on PRI comprehensively prior to auditing the system, the audit party may require collecting some specific information. This information may work as a basic tool of audit documentation. Following information may be collected for understanding the system:-

a) **Name of the auditee organization** - The name of the GP, PS or ZP may be mentioned where the audit inspection is being undertaken

b) **Date on which information collected** - Date on which the inspection starts

c) **Name of the IS Application** - IFMS or GPMS as the case may be

d) **Broad functional areas covered by the IS Application** - Registration and issue of Birth Certificate, Trade License, keeping accounts of different schemes and funds, information on Mouja, Village, Staff of office in case of GPMS.

Receipts of funds & grants, distribution of funds to different heads, payments made out of such funds & grants, progress of different schematic works in case of IFMS.

e) **Category of IS architecture** - PC based

f) **Category of IS application (IFMS/GPMS)** – Accounting system, Financial management system, Decision support system/MIS, e-Governance

g) **IS application on the financial and accounting aspects** – Both GPMS and IFMS bear financial and accounting aspects of PRIs

h) i) **Software used for IFMS** - Windows XP as Operating System, Database maintained in Oracle at the back end

ii) **Software used for GPMS** - Windows XP as Operating System, Database maintained in Access

i) **Whether the IS is a mission critical system/essential system -** Essential System

j) **Existence of proper and effective documentation** -Availability

a) The System Design Document (SDD)
b) User Requirement Survey (URS)
c) System Requirement Survey (SRS)
d) User Manual Documents

k) **Total investment on the IS project** -Availability

a) Hardware items
b) Proprietary software
c) Application System development cost
d) Manpower training cost
e) Maintenance of the all components (recurring)

l) **Number of persons engaged for operation of the system-** Availability

m) **Does the organisation transmit/receive data to/from other organisations-** Availability

(*C&AG's guidelines on this point is given in Annexure I)*

Chapter VI

Scope for IS Audit in PRIs

During the course of audit in the IS system of PRIs, the auditor should assess the scope of Audit in the system. The results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If auditors obtain evidence that specific control procedures are ineffective, they may find it necessary to re-evaluate earlier conclusions and other planning decisions made based on those conclusions.

During an audit of MIS (Management Information System) like IFMS/GPMS operational in PRIs, the information generated by the MIS being used by the organization in decision-making should be audited comprehensively. Some specific information on the system can highlight the scope of IS Audit team in and guide them towards the items which require detailed investigation. These are mentioned below :-

- **Investment made in the System**
  Higher the investment higher the risk
- **Criticality of the system**
  Both the IFMS & GPMS are Support Functions as these deal with functions like Financial Accounting of different funds and Schemes, various services to the citizen. The risk is less than the system having Business Critical Operations.
- **General state of computerization in PRIs of West Bengal**
  More the area computerized more the risk
- **Number of PCs/Desktops used for the system**
  More the number of PCs, more the risk
- **Mode of network- LAN/Intranet/Internet**
  System is very risk prone, if it is Web based
- **No. of locations the system is functioning at**
  More the no. of locations, more the risk
- **Dependency on the system**
  if
  a) Outputs are used for business critical operations /revenue generation
  b) Outputs are used to prepare Financial Statements
  c) Outputs are manually checked before making payments/raising bills
  Risk diminishes from a) to c).
- **Access to data either through web or any other means**
  If public can view the data in a dynamic manner
  If public can transact on-line
  Risk is more in the second case
- **Number of dedicated IS Staff in the Organization**
  More the numbers, more the risk

- **No. of end-users of the system**
  More the numbers, more the risk
- **No. of years the system is in operation**
  More the numbers, less the risk
- **Method of processing of the system Batch Processing/ On Line Transaction Processing**
  On line Transaction Processing is more risk prone
- **Documentation of formal change management procedures**
  Non-maintenance of documented change management procedures enhance risk
- **Frequency of changes made to the applications**
  Higher the frequency, higher the risk
- **Availability of documented and approved Disaster Recovery Plan**
  Non-availability of Disaster Recovery Plan enhances the risk factor
- **Use of any security software**
  Non-utilization of firewalls, anti-virus software makes the system vulnerable
- **Volume of data in the system**
  More the volume, more the risk

(*C&AG's guidelines on this point is given in Annexure II*)

Chapter VII

These issues have been conceptualized based upon a preliminary study of the selected MIS software being used in PRIs in West Bengal. As a broad generic, its applicability to similar e-governance platforms in other states can be assessed.

In setting out the potential areas of Audit focus, an evaluation of :

-Policy mapping contours

-General controls built in at various stages of the Information System

-Effectiveness of security administration and access controls

-Identification of potential areas of risk and

-Overall assessment of the efficacy of the Information System both in terms of resources utilized and deliverables achieved is taken into purview at the level of the controlling line department and at the level of field units of grassroots governance

General items which can be looked into by Information System Audit Parties in PRIs with reference to selected software

1) Strategic Plan for IS

The introduction of GPMS and IFMS software in West Bengal was envisaged as an implementation of e-governance processes for wider dissemination of information to citizens at the grassroots level to achieve transparency, facilitate social audit and strengthen decision making support systems for Panchayati Raj Institutions. Department of Panchayats and Rural Development (P&RD), Govt. of West Bengal, is the controlling nodal department of the PRIs of West Bengal which has set up the IS wing for PRIs. Therefore, this Department should have a well documented Strategic Plan which should cover inter-alia the appropriateness with the business goal, financial information system, requisite human resources, procedures of monitoring the e-governance activities and formation of a Steering Committee for monitoring and evaluation purposes. Auditor should see that the strategic IS plan for the Department

P&RD has fulfilled the business goals. To draw a conclusion in this regard, the following points would need examination:-

a) How appropriate is the P&RD's Strategic Plan?
b) Has it been documented and approved at appropriate authority level?
c) Is it kept up to date?
d) Does it cover the financial information system?
e) Are IS staff of GPs, PSs & ZPs informed of the issues?
f) Does the Strategic Plan identify target dates, resources, and personnel needed to accomplish the plan?
g) Are there procedures for monitoring its implementation?
h) Are current IS activities consistent with the Plan?
i) Is there a Steering Committee with well defined roles and responsibilities for monitoring and evaluation purposes?

2) Policies for recruitment & training

Keeping the business needs of PRIs in view, the recruitment & training policies are to be arranged. In PRIs entry of data by Data Entry Operator and validation of data by supervisory staff are to be digitized through Information System. Therefore, necessary capacity building for using Information Technology is essential both at the time of recruitment and during service. Audit should see that a suitable policy has been framed for screening and recruitment as per requirement of the IS environment of the PRIs. There should be frequent updating of skills of end users and regular arrangement of trainings. The training should meet the business need. Training should provide general awareness on security issues. For smooth and uninterrupted functioning of the IS, training need analysis is important. Audit should also review this.

3) Physical protection of the IS facility.

Physical protection of the IS in case of GPMS/IFMS is essential as the data fed by PRI staff into the System is unique for each Panchayat and any addition/alteration of fund against such Project is made on that amount to show the current actual balance. Therefore, the data must be kept secured, so that nobody can alter the same for any mala fide intention. To prevent this there should be appropriate security plan in place for providing centralised direction and control over information system security. There should be a centralised security organisation responsible for ensuring only appropriate access to system resources. Auditor should also see that IS management authority of P&RD, the controlling line Department of the State Government has taken care of potential problems in the system before the occurrence of any problem and necessary arrangements have been made to prevent an error, omission or malicious act from occurring. Another point that needs to be looked into by audit is that there are provisions for detection and reporting of the occurrence of an error, omission or malicious act to the higher authority. Application of such detection may be reviewed, if any.

4) Backup staff

To run the IS system of P&RD smoothly, back up staff in case of absenteeism is necessary. Auditor should look into the matter with a view to observe that there is a system of reporting to top management and appropriate direction received from management side. There should be an appropriate policies and procedures in relation to retention of electronic records. Audit should also see whether this is in vogue.

5) Password Policy

In Information System based applications, passwords play a vital role in restricting unauthorized access. In both GPMS and IFMS software, there are passwords to restrict unauthorized access to the data maintained there. There are separate levels of accessing the data. One user (e.g. data entry operator) can only enter data for creation of records with user-level password, but he can not verify, validate or delete after verification with it. The supervisory level is empowered to do such kind of jobs by using supervisory level password. Thus, in this manner, the data are kept validated and secured. The auditor should see whether there is a documented policy on this and this policy is maintained everywhere. The secrecy of passwords should be maintained scrupulously and passwords changed frequently for security.

6) Hardware Requirement

After looking at the computerization efforts in GPs in Karnataka, the Expert Group formed by the Ministry of Panchayati Raj felt that a minimum of one PC would be sufficient to cater to the computerization requirements of GPs with population less than 10,000. Accordingly, the Expert Group recommended that one PC, one printer and one UPS is to be the minimum requirement at the GP level.

Auditor should see that the above minimum infrastructure is available in all the GPS in West Bengal where GPMS is installed. For example, hard copies of the reports can not be obtained for verification, if there is no printer.

7) Data Centres

Large volumes of data are generated for assets and citizen related data on PRI functioning. Such data needs to be maintained and secured in a central repository where sufficient infrastructure and manpower is available. If field units operate in a stand-alone mode, as in the case of West Bengal, it would be absolutely necessary that such data is regularly uploaded by P&RD staff to the central repository. This clearly suggests a need to establish data centers to cater to the security and maintenance needs of data. In order to meet this requirement, the Expert Group recommended that the existing servers kept in the data centers established by Government of India may be utilized by ZP, PS & GP exclusively. Auditor should see whether this system is in vogue in West Bengal.

8) Document Retention Policies

For any sound IS system every organization should have adequate documentation policies which include documentation to be up to date, comprehensive and available to the appropriate staff. The best method of keeping documentation is a media library. This should be systematically inventoried and there should be a housekeeping procedures to protect the contents of media library. The responsibilities for media library management should be assigned to some specific members of IS staff. There should be a media backup and restoration strategy which include the media backups storage at different location, say in a different building of GP office or in another GP office. The storage site should be periodically reviewed regarding physical access. The retention period and storage terms should be defined in the strategy. Audit should review the Documentation Policy of the P&RD keeping these points in view.

9) Controls over IS budgetary process and Acquisition

The P&RD department should keep IS budgetary process consistent with the organisation’s long and short term business processes. The objectives, scope and requirements of the acquisition should be clearly defined and documented including any integration issues that need to be addressed like upgradation of the hardware based on technology changes. There should be policies and procedures to monitor the comparison of actual cost and projected cost based on department’s cost accounting system. The department should ensure that the delivery of services by the IS function is cost justified and in line with industry costs. A structured approach comprising all the key acquisition activities and deliverables, timelines may help acquisition process and minimize acquisition and project risks. During the audit of IS in PRIs, audit should keep the above points in view. It should also see that an effective preventive maintenance program is in place for all significant equipment, equipment’s downtime is kept within reasonable limits, procedures to update documentation whenever changes are made in the hardware exist. Coverage of software by adequate license, recording of changes in the applications, emergency change procedures are to be addressed in operation manuals and exception reporting system should be in place.

10) Controls over Program Change

P&RD department should have a methodology for initiation and approval of program changes, if any required for business need. These changes should cover the entire application and any difficulties arising during implementation may be resolved. These changes are to be incorporated in the operational manual immediately. During the testing process, users of all level of GPMS/IFMS should be involved in the process. Back up of all the relevant records and files should be taken before any change is implemented. The risk prone areas like unauthorised changes, erroneous processing & reporting, use of unauthorised hardware and software, problems with emergency changes may be explored by audit along with the above mentioned areas.

11) Disaster recovery controls

The P&RD department should possess a documented disaster recovery plan which should support the business goals. This plan should cover inter-alia identification of management individuals having authority to declare a disaster, responsibilities and functions of designated team, provision for remote storage of emergency procedures/manuals, established processing priorities to be followed, provisions for reserve supplies, back up of all master files and transaction files to accomplish its mission after re-starting its operations, retrieve and protect the information maintained, keeping intact all the organisational activities after the disaster. Failure in these areas may entail the department a loss in terms of money, goodwill, human resources and capital assets. Audit should review the plan keeping notes of the above.

12) Input Controls

Input controls are the application controls which seek to minimize the risk of incorrect data entry by making validation checks, duplicate checks and other related controls. These provide the earliest opportunity to detect and correct possible mistakes. For data preparation in IFMS/GPMS measures should be taken by the concerned officials to ensure completeness, accuracy and validity of data. This may be achieved by separation of duties between origination, approval and conversion of source documents into data, keeping source document for long to allow reconstruction in the event of loss, litigation inquiries or regulatory requirements, maintaining trail to identify source of input, appropriate handling of erroneously input data. There should also be a procedure for balancing of record counts and control totals for all data processed, for processing of resubmitted transactions exactly as originally processed. The system should contain essential input validations with reference to codes, fields, characters, transactions, calculations, logic, units, reasonableness, sequence. It should restrict possibility of data entry by other personnel bypassing or overriding the data validation and edit controls. Auditor should observe whether the above controls are in position and active.

13) Processing Controls

Audit should examine whether documented procedures exist explaining the methods for proper processing of each application program. There should be segregation of duties in respect of processing commensurate with the business needs of PRIs. The system design documentation should provide clear instructions on system start-up, backup assignments, emergency procedures, system shutdown procedures, debugging facility, error message instructions. The history log should indicate hardware and software failure errors, processing halts, abnormal termination of jobs, operator interventions, and unusual occurrences. The system design should have a well documented procedure to identify, correct and reprocess the rejected data. In case of GPMS all the entries take place with the input of data to generate various outputs like Berth Certificate, Trade License effecting General Cash Book, Income Expenditure Statement etc. while in IFMS the outputs are Cash Book, Subsidiary Cash Book, Receipt & Payment Accounts, Cash Analysis Statement etc. effecting the balance of concerned funds and grants i.e., the flow of money. The duty of audit is to verify that the audit trail exist during the processing of data from its destination to its point of origin.

14) Output Controls

Output controls are the processing controls that ensure that the output is complete, accurate, in time and is correctly distributed. Audit should compare list of outputs which are actually being produced with the list of the outputs the system is capable of producing. It may be reviewed how many of these outputs are actually being used, whether there are reports that have never been printed, whether there are any reports/outputs which are needed but the system is unable to produce them. Audit should enquire whether there are reports not being produced, although the system is capable of producing these. If the parallel system functions, audit may compare the manually prepared reports with the computer generated reports.

15) Re-engineering Process

The functional domain of Panchayats extends to 29 subjects listed in the Eleventh Schedule. All e-Governance initiatives at the local level are to converge with the appropriate PRI as nodal point. The State Government should undertake a time-bound exercise to implement all these activities in consonance with the activity mapping with a view to disclosure to the public, delivery of services and dissemination of information to Panchayat representatives. The data collected by the Panchayats should be owned by them. Further, the data may be outsourced at a multi service kiosk centres known as Common Services Centres (CSC) or may be in the Panchayat offices. Audit should check whether activity mapping has been done by the P&RD department. If so, implementation of the same according to the time frame should also be investigated. While adding these activities in the installed system, there might be cases where any hardware or software may be procured fresh although these were procured earlier but could not be utilized in the event of implementing new activities due to lack of foresight. Audit may investigate the same.

(*C&AG's guidelines on this point is given in Annexure III*)

Specific items which can be looked into by IS Audit parties in field units of the PRIs i.e., GP, PS & ZP and with reference to selected software

a) A proper system of communication to access data from remote Gram Panchayats is to be developed for ICT initiatives to achieve the business goal i.e., devising an interface for transmitting data from the Gram Panchayats to the upper tiers of the PRIs and also to the line department. As per policy, connectivity is to be provided through WBSWAN and the system will be subsequently updated using dial up or Wi-Fi as backbone. Audit should check the progress of the work along with the implementation policy of the Department.

b) It is observed that IFMS has been installed in 105 Panchayat Samitis out of 331 PSs. These include: 4 in Coochbehar, 4 in South 24 Parganas, 3 in Uttar Dinajpur, 31 in Burdwan, 5in Nadia and 9 in Birbhum. Similarly, out of 3354 GPs, GPMS has been installed in 401 GPs which include 14 in Jalpaiguri, 15 in Coachbehar, 06 in Dakshin Dinajpur, 52 in Birbhum, 107 in Burdwan, 10 in Howrah along with other districts. Not a single GP in Malda and Purulia is provided with GPMS. Audit may see whether there is any documented installation policy in this regard and whether the same is being adhered to.

c) The most critical input in Management Information System is appropriate capacity building of the available human resources and that process also results in improved human capital of the organization. Large scale capacity building exercises have to be undertaken for getting best of the e-government initiatives. Failure of targets in respect of IFMS/GPMS installations might be due to less number of competent officials. Thus, audit may investigate whether there is any documented plan of recruiting competent officials and providing training to the existing staff and officers to cater to the need of the Department in achieving the business goal. If the same exists, audit should see whether the same is being followed.

d) In West Bengal, the data in PRI Information System is working in a stand-alone environment. Thus, the information generated in such environment is generally transmitted to the upper tier physically. Thus, there is ample scope for manipulation of data, both at the originating point, destination or during transition. There should be preventive control for security of data. Audit should see whether documented policy for such control exists and is being followed scrupulously.

e) In any organisation, where IS is in nascent stage, both manual and mechanized procedures are run for obtaining a report. This may continue for a certain period of time, which may be decided by the management. If it runs for an indefinite period of time, it results in duplication of works, misuse of man-power, improper utilization of assets, injudicious expenditure. Audit may see whether running of such parallel system were inevitable by examining their policy, criticality of the system and business strategy.

Annexure I

Documents required for understanding the Information System-Excerpts from IT Audit Manual issued by C&AG of India

The Audit party may require collecting some specific information on the IS. The questionnaire may work as a basic tool of audit documentation. This becomes the reference point for overall comprehension of the system at all stages of the field audit procedures.

1. Name of the auditee organisation:	
2. Date on which information collected :	
3. Name of the IS Application and broad functional areas covered by the IS Application:	
4. Department Head of the Auditee Organisation:	
6. Information Systems in-charge: Name: Phone No: Email:	
7. What is (are) the location(s) of the IS installation(s)?	
8. State the category of IS architecture:	A. e.g. Mainframe based or Minicomputer based or PC based or Others (pl specify)
	B. File server system or Client server system or Distributed processing system.
9. State the category of IS application. (Indicate the choice(s) applicable):	e.g. Accounting system □ Financial management system □ Inventory/Stock Management □ Decision support system/MIS □ Manufacturing/Engineering □ Payroll □ Personnel and Administration Marketing □ Sales □ e-Governance □ Research & Development □ Enterprise Resource Planning □
10. Whether the above IS application has got a bearing on the financial and accounting aspects of the organisation?	Yes □ No □
11. Software used (the Version may also be specified):	
Operating system(s)	

Network software		
Communication Software		
DBMS / RDBMS		
Front end tool		
Programming Language(s)		
Bespoke (Vendor developed)		
Utility Software		
Any other		
12. Is the IS a mission critical system or an essential system?	Mission critical system(&) □ Essential system(&&) □	
13. Does a proper and effective documentation exist eg. a) The System Design Document (SDD) b) User Requirement Survey (URS) c) System Requirement Survey (SRS) d) User Manual Documents		
14. Were these effective documentation prepared or got prepared and available?		
15. Are there items (Functions/Processes) which had been provided for in these documents which have not yet been implemented?		
16. Does the system documentation include a data flow diagram and flow chart? If yes, does the flow chart/data flow diagram represent the system correctly?		
17. Are there unfulfilled user requirements?		
18. What is the extent of customers' satisfaction?		
19. Has the application system been developed in house or by outsourcing?	In house □ Outsource □	
20. In case of outsourcing, specify the name of agency and the contracted amount:		
21. When was the system made operational?	**Month** □ □	**Year** □ □ □ □

22. What is the total investment on the IS project? Indicate the amount in lakhs of rupees against each item (&&&):

Rupees in lakhs

Hardware items	
Proprietary software	
Application System development cost	
Manpower training cost	
Maintenance of the all components	

23. Number of persons engaged for operation of the system?	**01 - 10** □ **11 - 25** □ **26 - 50** □ **51 - 100** □ **> 100** □
24.What is the average volume of transactional data generated on a monthly basis in terms of storage space?	
25. Does the system documentation provide for an audit trail of all transaction processed and maintained?	Yes □ No □
26. Is there any system in place to make modifications to the application being used on a regular basis to support the function?	Yes □ No □
27. Does the organisation transmit/receive data to/from other organisations:	Receive □ Transmit □ No □
28.Details of all Hardware items including the number of terminals etc. employed:	
29. Are more than one IS Application(s) running on the same Hardware? If Yes, specify the name(s) of such IS Application(s) apart from the application as indicated at Sl. No. 3.	

(&) *A mission critical system is an IS which directly impacts the primary function of the organisation e.g. Passenger Reservation System in Indian Railways or eSeva in AP.*

(&&) *An essential system is an IS the loss of which causes disruption of some service without disrupting primary services eg: payroll package in police department.*

(&&&) *If exact figures are not readily available, approximate figures may be provided.*

Annexure II

Scope of IS Audit in PRIs-Excerpts from IT Audit Manual issued by C&AG of India

The results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If auditors obtain evidence that specific control procedures are ineffective, they may find it necessary to re-evaluate earlier conclusions and other planning decisions made based on those conclusions.

Some applications may be mission critical applications with lapses having far reaching consequences. In such case auditor may prefer to adopt a vigorous framework in conducting the audit. But during audit of a simple MIS (Management Information System) in a non-critical department where the information generated by MIS is itself not being used by the organization in decision-making auditors may not be interested in a comprehensive audit. The nature, extent, scope and rigour of the IS audit and the resources committed for the job are dependent upon the subjective assessment of the risk parameters or in other words, criticality of the application. In order to bring some objectivity into the process, though subjectivity cannot in total be avoided, the following criticality assessment tool may be used to categorise the applications based on criticality.

	Name of the Office:		
	Preliminary Information:		
A.	Name of the Entity:		
B.	Nature of the Entity	Headquarters	
		Regional Office	
		Branch Office	
		Unit Office	
		All of the above	
C.	Name of the System		
D.	Short Description of the System:		

Questions: (*Auditor may give the marks against relevant points)*

1.	**Does the system relate to any of the following**		
	Business Critical Operations For example, Airline/Railway reservations, trading operations, telecom, banking operations, bill generation, on-line bill payment, manufacturing and processing etc.	(30)	
	Support Functions For example, Payroll, Inventory, Financial Accounting, Procurement, Marketing etc.	(25)	
2.	**Investment made in the System**		
	Less than Rs.5 lakh	(5)	
	More than Rs.5 lakh less than Rs.25 lakh	(10)	
	More than Rs.25 lakh less than Rs. 50 lakh	(15)	
	More than Rs. 50 lakh less than Rs. 1 crore	(25)	
	More than Rs. 1 crore	(30)	
3.	**General state of computerization in the entity**		
	The entity has computerized most of the Business processes	(30)	
	The entity has computerized most of the Accounting and Financial Processes	(25)	
	No business process	(0)	
4.	**Number of PCs/Desktops used for the system**		
	More than 100	(30)	
	More than 50, less than 100	(25)	
	More than 20, less than 50	(15)	
	More than 10 less than 20	(10)	
	Less than 10	(5)	
5.	**If the system is on the network, is it connected to**		
	Internal LAN and/or on intranet?	(20)	
	WAN and MAN and/or on extranet?	(25)	
	Web based /public domain?	(30)	
6.	**The system is functioning at**		
	Only one location	(10)	
	More than one, less than 5 locations	(20)	
	More than 5 locations	(30)	
	Is proposed to be expanded in more than one location	(25)	

7.	**The entity is dependant on the system in as much as**		
	Outputs are used for business critical operations /revenue generation	(30)	
	Outputs are manually checked before making payments/raising bills	(10)	
	Outputs are used to prepare Financial Statements	(15)	
	Outputs are not used at all for payment/revenue purposes	(0)	
8.	**Even though the system does not deal with financial functions, it processes data of public interest. The nature of data is such that wrong data may lead to :**		
	Failure of business	(30)	
	Erosion of credibility of the Organization	(15)	
	Financial loss to the entity	(25)	
	None of the above	(0)	
9.	**Do the public have access to such data either through web or any other means?**		
	Yes, Public can view the data in a dynamic manner	(15)	
	No, Public cannot view the data	(0)	
	Public can transact on-line	(30)	
10.	**Does the System make use of direct links to third parties e.g. EDI**		
	Yes	(20)	
	No	(0)	
11.	**Number of dedicated IS Staff in the Organization**		
	Nil	(0)	
	Less than 10	(10)	
	More than 10, less than 30	(20)	
	More than 30, less than 70	(25)	
	More than 70	(30)	
12.	**Approximately how many persons can be termed as the end-users of the system?**		
	Less than 5	(0)	
	More than 5, less than 25	(10)	
	More than 25, less than 70	(20)	
	More than 70, less than 150	(25)	
	More than 150	(30)	

13.	**The system is in operation for**		
	More than 10 years	(5)	
	Less than 10 years but more than 5 years	(10)	
	Less than 5 years but more than 2 years	(20)	
	Less than 2 years	(20)	
14.	**The system is based on**		
	Batch Processing	(10)	
	On Line Transaction Processing	(25)	
15.	**Are there formal change management procedures?**		
	Yes	(0)	
	No	(20)	
15 A.	**How often changes are made to the applications**		
	More than 5 times in a year	(30)	
	Less than 5 times in a year more than twice in a year	(20)	
	Less than twice in a year	(10)	
	Not even once in a year	(5)	
16.	**Does the entity have a documented and approved security policy?**		
	Yes	(5)	
	No	(20)	
17.	**Does the entity use any security software?**		
	Yes	(5)	
	No	(20)	
18.	**Does the entity have a Systems Security Officer?**		
	Yes	(5)	
	No	(10)	
19.	**Does the entity have a documented and approved Disaster Recovery Plan?**		
	Yes	(0)	
	No	(20)	
20.	**Volume of data in the system(including off line data) is approximately**		
	More than 10 GB	(25)	
	More than 2 GB less than 10 GB	(15)	
	Less than 2 GB	(10)	
	Less than 1 GB	(5)	
	Total Score		

As per the IS risk assessment tool given above, the points scored may be graded below:

Points scored as per risk assessment tool	**Classification of risk**
Less than 150	Low
Between 150 and 300	Medium
More than 300	High

Annexure III

General items to be looked into by Information System Audit Parties-Excerpts from IT Audit Manual issued by C&AG of India

The aim of Information System Audit is to identify and evaluate the effectiveness of controls. This system based audit yields an assurance on the system. Mere data analysis throws up many data inconsistencies/abnormalities, which are put as audit findings without any investigation. Detailed investigation may reveal a case of input mistake, data overwriting without authority or wrong programme logic. In case of wrong logic, there must be an identifiable pattern of these observations. The IS security should be observed with more seriousness. Apart from access controls, one must look for logs, authorizations, trails, back-end security. A good and secure system can identify the individual of each data entry/modification. An IS Auditor must look for reliability of the system. If the controls are weak or non-existent and it is observed that the data is unreliable or is not safe and secure, this must be brought out clearly in the report. In such unreliable system, audit should not comment on loss of money value based on analysis of unreliable data. This audit exercise can be reported either as VFM aspect or as the adverse impact which such unreliable system will have on the organization.

General Controls

General Controls are the controls applicable for entire IS. They can be computer based controls or non-computer based controls. One of the popular premises of IS Audit is that examining the application controls is of no consequence unless the general controls are strong.

- While examining controls, it is important for the audit party not to jump to audit conclusions based on the isolated instances of weak controls. Audit should check that the controls have been viewed in relation to the impact on the efficiency, security or effectiveness of the system. Further the costs of controls have to be justified based on the benefits derived. Technology is a tool that can provide any extent of granularity of control and security. However, higher costs usually associated with stronger controls and audit has to examine the risk of absence or weakness of a control compared with its cost.
- Another important caution for the audit party is that even if a critical control is absent, the party has to look for compensating controls. It is possible that the weakness in one control may be compensated with a stronger control elsewhere.

The following questionnaire may help an auditor in assessing effectiveness of the general control while auditing an IS

Organisational and Management Controls		Yes	No	KD ref.
1.	Is there a strategic IS plan for the organization based on business needs?			
2.	How appropriate is the audited body's IS strategic plan? • Has it been documented? • Has it been approved? • Is it kept up to date? • Does it cover the financial information systems? • Is staff informed of the issues?			
3.	Does the strategic plan identify target dates, resources, and personnel needed to accomplish the plan?			
4	Are there procedures for monitoring its implementation?			
5.	Are current IS activities consistent with the plan?			
6.	Is there a steering committee with well defined roles and responsibilities?			
7.	How does senior management maintain an appropriate level of interest in the audited body's IS functions? (e.g. through an IS steering committee.)			
8.	Does the organisation's internal audit function carry out IS reviews of the computerised financial systems?			
9.	Are policies for recruitment, screening and disciplinary procedures appropriate for the IS environment?			
10.	Are there procedures in place for updating the skills of end users and trainings arranged regularly?			
11.	Assess whether Training programmes are consistent with the organisation's documented minimum requirements concerning education and general awareness covering security issues.			
12.	Whether a training needs analysis is done at periodical intervals where uninterrupted functioning is essential?			
13.	Are critical jobs rotated periodically?			
14.	Does the audited body receive IS services from external sources? Have appropriate procedures been developed to meet identified risks (e.g. access rights)?			
15.	Is there a separation of duties and well defined job characteristics in the IS projects?			
16	Whether backup staff is available in case of absenteeism?			
17	Is there a system of reporting to top management and review in vogue?			
18	Does management provide appropriate direction?			
19	Are there appropriate policies and procedures in relation to retention of electronic records?			
20	Are there procedures to update strategic IS plan?			
21.	Is there a strategic security plan in place providing centralised			

	direction and control over information system security?			
22.	Is there a centralised security organisation responsible for ensuring only appropriate access to system resources?			
23.	Is there an employee instruction / training system in place that includes security awareness, ownership responsibility and virus protection requirements?			
24.	Whether preventive and detective control measures have been established by management with respect to computer viruses?			
25.	Whether password policy exists.			
26.	Whether access to security data such as security management, sensitive transaction data, passwords and cryptographic keys is limited to a need to know basis?			

An IS auditor should be aware of the following critical elements:

- **Inadequate management involvement may lead to a direction-less IS function** which, in turn does not serve the business needs. This may give rise to problems with the IS being unable to meet the business needs;
- **Poor reporting structures leading to inadequate decision making.** This may affect the organisation's ability to deliver its services and may affect its future;
- **Inappropriate or no IS planning leading to business growth being constrained** by a lack of IS resources; e.g. the manager reports to the chief executive that the system is unable to cope with an increase in sales. Overloading a computer system may lead to degradation or unavailability through communication bottle-necks or system crashes;
- **Ineffective staff who do not understand their jobs** (either through inadequate recruitment policies or a lack of staff training or supervision). This increases the risk of staff making mistakes and errors;
- **Disgruntled staff being able to sabotage the system,** for example when staff find out they are going to be disciplined or made redundant;
- **Ineffective internal audit function** which cannot satisfactorily review the computer systems and associated controls;
- **Loss of the audit trail** due to inadequate document retention policies (includes both paper and electronic media); and
- **Security policies not in place** or not enforced, leading to security breaches, data loss, fraud, and errors.

In the absence of strong personnel and training control mechanism, there may be repeated instances of data losses, unauthorised data and program amendment, and system crashes attributable to:

- Errors and omissions caused by people;
- Fraud; and
- Hardware/software failure

The following questionnaire may help an auditor in assessing effectiveness of the Internal Audit System related to IS of the auditee.

	Internal Audit	Yes	No	KD Ref.
1.	Does the organization have Internal audit section in the area of IS?			
2.	Does the organization utilize IS auditors in the internal audit functions?			
3.	Are the IS auditors trained to effectively use IS audit tools and techniques?			
4.	Is the IS audit function subject to periodic peer reviews?			
5.	Does the IS audit include an assessment of compliance with organizations policies, procedures and standards?			
6.	Does the internal audit include an analysis of internal controls?			
7.	Does the internal audit include an assessment of the application documentation?			
8.	Does the internal audit include an assessment as to whether transactions are completely and correctly processed on a timely basis?			
9.	Are the internal audit reports seen by top management?			
10	Has action being taken on the basis of recommendations in the internal audit reports?			
11	Is the periodicity of internal audit reports adequate?			
12	Whether internal audit has been involved in system development?			

Risk Areas

Basic risk areas which the external auditor may come across when reviewing internal audit’s work include:

- Internal audit not reporting to senior management.
- Management not responding to internal audit’s recommendations.
- Internal Auditor may not be empowered to carry out a full range of assessments or there may be significant restrictions on the scope of its work
- Non-availability of sufficient resources, in terms of finances and staff

The following questionnaire may help an auditor in determining if there are adequate standards and procedures for **IS Operational Controls**

	Yes	No	KD Ref.
Program change control			
Data Centre operations			
Data Base administration			
Performance monitoring			
Capacity planning			
Information security			
Contingency planning/disaster recovery			

Risk Areas

The risks associated with poorly controlled computer operations are:

- ***applications not run correctly*** (wrong applications run, or incorrect versions or wrong configuration parameters entered by operations staff, e.g. the system clock and date being incorrect which could lead to erroneous interest charges, payroll calculations etc)**;**
- ***loss or corruption of financial applications* or the underlying data files:** may result from improper or unauthorised use of system utilities. The IS operations staff may not know how to deal with processing problems or error reports. They may cause more damage then they fix;
- ***delays and disruptions in processing*.** Wrong priorities may be given to jobs**;**
- ***lack of system capacity*.** The system may be unable to process transactions in a timely manner because of overload, or lack of storage space preventing the posting of any new transactions;
- ***lack of backups and contingency planning*** increases the risk of being unable to continue processing following a disaster; and
- ***high amount of system downtime* to fix faults:** when the systems are unavailable a backlog of un-posted transactions may build up.

The following questionnaire may help an auditor in assessing **Document Retention Policies** of the auditee.

		Yes	No	KD Ref.
1.	Determine if: • Overall systems and program documentation are adhere to standards. • Documentation is complete and current.			
2.	Does the organisation have adequate IS documentation policies? Policies should ensure that documentation is up to date, comprehensive and available to appropriate staff.			
3.	Whether for media library the following exist: • Contents of media library are systematically inventoried • Housekeeping procedures exist to protect media library contents • Responsibilities for media library management have been assigned to specific members of IS staff			

	•Media back-ups and restoration strategy exists • Media back-ups are taken in accordance with the defined back-up strategy and usability of back-ups is regularly verified • Media back-ups are securely stored and storage sites periodically reviewed regarding physical access • Security and security of data files and other items • Retention periods and storage terms are defined for documents, data, programmes, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication. • Adequate procedures are in place regarding the archival of information (data and programmes) in line with legal and business requirements and enforcing accountability and reproducibility.			

Risk areas

The risks associated with inadequate documentation policies include:

- **unauthorised working practices being adopted by IS staff;**
- **increase in the number of errors being made by IS staff;**
- **the risk of system unavailability** in case the system is complex and there is no technical documentation. For example, if an organisation's network is not adequately documented and a problem occurs with the physical layer, those responsible for carrying out repairs would have difficulty in locating where the fault had occurred.

The following questionnaire may help an auditor in determining the adequacy of **Physical Controls (Access and Environment)**

		Yes	No	KD Ref.
1.	Determine if the security procedures cover: • Physical protection of the facility. • Designation and duties of the security officer(s). • Authorised data and program access levels. • Requirements for password creation and change procedures. • Requirements for access via terminals, modems or computer system (LAN) connection. • Monitoring and follow-up of security violations.			
2.	Has management established security requirements, and penal/ corrective action in case of failure, as part of contracts with third-party service providers?			
3.	Determine whether procedures are in place to update the security policy. Ensure updates to the policy and procedures are distributed to and reviewed by management.			
4.	Determine if an education program has been implemented to promote user awareness about security policies and procedures.			
5.	Determine whether there are procedures in place to prevent any unauthorised entry into the IS facilities of the organisation.			
6.	Are there adequate and effective countermeasures relating to physical security against different environmental threats e.g. fire, flood, electrical surges, lightning, etc.?			

Risk Areas

Physical Access Controls

- Accidental or intentional damage by staff.

Theft of computers or their individual components;

Bypass of logical access controls: e.g. having physical access to a fileserver can be exploited to bypass logical controls such as passwords.

Environmental Controls

- Fire/water damage (or damage from other natural disasters);
- Power: Cuts, leading to loss of data in volatile storage (RAM);
- Spikes: leading to system failures, processing errors, damage to components of equipment.
- Failure of equipment due to temperature or humidity extremes (or just outside tolerances of a few degrees);
- Static electricity: can damage delicate electrical components. Computer chips (ROM, RAM and processor) are delicate and easily damaged by static electricity shocks;
- Others: e.g. lightning strikes, etc

The following questionnaire may help an auditor in determining the adequacy of **Logical Access Controls**

		Yes	No	KD Ref.
1	Whether passwords are keyed in using nonprinting, non-displaying facilities.			
2	Whether security breaches are immediately reported for appropriate action.			
3	Does this report identifies the terminal and displays the date and time of incident.			
4	Does the system have a predetermined number of failure attempts before shutting down which can then only be started by specially authorized personnel.			
5	Is a data-access matrix used to define access levels?			
6	Does the senior management regularly review the adequacy of the data access matrix?			
7.	Whether procedures are in place for issuing, approving and monitoring application access and whether such procedures comply with the policy of “minimum access”.			
8.	How security violations are detected and reported Which can be determined by reviewing the terminal logs.			
9.	Determine that password security is in effect on all applications and assess the adequacy of controls over: • Password Change on a regular basis • Suppressing passwords’ display on a terminal.			

10.	Examine if system access levels are consistent with job functions.			
11.	Does the security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed and the nature of the access.			
12.	Are there well-defined procedures for user account management, including clear and effective linkages between user rights and current positions, as well as termination of user rights on cessation of employment etc.?			
13.	Determine that passwords are removed as soon as an individual's employment is terminated to ensure that a terminated employee cannot gain access to the computer files through an outside terminal.			
14.	Have adequate preventive, as well as detective control measures been taken by management with regard to computer viruses at all levels, ranging from high end servers to user desktops and laptops?			

Risk Areas

- Users have the access to the areas other than related to the performance of their duties, causing threats to unauthorised access, amendment or deletion in the maintained data.
- Access to very sensitive resources such as security software program which may be of mission critical nature, and
- Employees are not barred / restrained from performing incompatible functions or functions beyond their responsibility.

The following questionnaire may help an auditor in determining the **Controls over IS Acquisition**

		Yes	No	KD Ref.
1.	Consider whether • The IS budgetary process is consistent with the organisation’s process • Policies and procedures are in place to ensure the preparation and appropriate approval of an annual IS operating budget which is consistent with the organisation’s budget and long- and short-range plans, and the IS long- and short- range plans • The budgetary process is participatory with the management of the IS function’s major units contributing in its preparation.			
2.	• Policies and procedures are in place to regularly monitor actual costs and compare them with the projected costs, and the actual costs are based on the organisation’s cost accounting system • Policies and procedures are in place to guarantee that the delivery of services by the IS function is cost justified and in line with industry costs			

3.	Ensure organisational adherence to a structured approach, comprising all the key acquisition activities and deliverables, timelines and milestones etc.			
4.	Assess whether there is a defined evaluation and selection criteria, to minimize acquisition and project risks.			
5.	The objectives, scope and requirements of the acquisition should be clearly defined and documented, including any integration issues that need to be addressed.			
6.	Is there an organization policy for upgrading the hardware based on technology changes?			
7.	Is there an effective preventive maintenance program in place for all significant equipment?			
8.	Is equipment downtime kept within reasonable limits?			
9.	Is a formal inventory of all IS hardware available?			
10.	Are there procedures to update documentation whenever changes made in the hardware?			
11.	Is the software used covered by adequate license?			
12.	Is the source code (#) available and if so, accessible at what level?			
13.	Is there a system of recording changes to the applications?			
14.	Are these changes properly authorized?			
15.	Whether emergency change procedures are addressed in operation manuals?			
16.	Whether proper testing was carried out and results recorded before final implementation of application?			
17.	Is there an exception reporting system in place?			
18.	In the case of bought out software are there agreements in place for maintenance and service?			
19.	Is there a system of obtaining user feed back and reporting action taken thereon to management?			
20.	Is the application design documented?			
21.	Whether the programs are documented?			
22.	Is the testing methodology documented?			
23.	Whether operations procedures are documented?			
24.	Whether user manuals are available?			
25.	Do manuals include procedures for handling exceptions?			
26.	Are there procedures to update documentation when an application changes?			

(#) Unauthorised access to the source code of an application could be used to make amendments in the programming logic, e.g. rounding off payments to the nearest unit (paisa) and posting the rounded fraction to the programmer’s expense repayment account.

Risk Areas

Critical elements involved in the process of acquisition of IS assets are as follows:

- In IS, the scale, cost and impact of an acquisition may have a strategic significance well beyond the acquisition itself. Any serious misjudgement in the acquisition decision will impair not only the success of the underlying IS project but, in addition, the potential business benefits that are anticipated.
- Acquisitions frequently involve a significant capital investment for an organisation. In addition to the investment, the opportunity cost of the capital employed and the time/resources expended in the acquisition process add to the importance of the acquisition.

The following questionnaire may help an auditor in determining the adequacy of **Controls over Program Change**

		Yes	No	KD Ref.
1.	Verify that a methodology is used for initiation and approval of changes.			
2.	If all changes to the system security software are approved by the system security administrator.			
3.	Ensure all changes are applied to a copy of the latest production version of code.			
4.	Whether the change control log ensures all changes shown were resolved?			
5.	Whether the changes to requirements resulted in appropriate changes to development documents, such as technical and operational manual?			
6.	Whether established procedures were there for ensuring executable and source code integrity?			
7.	Verify that the changed code is tested in a segregated / controlled environment.			
8.	Determine to what extent the user is involved in the testing process.			
9.	Ensure that a back-out process is developed before any change request is implemented.			

Risk Areas

Change controls are put in place to ensure that all changes to systems configurations are authorised, tested, documented, controlled, the systems operate as intended and that there is an adequate audit trail of changes.

Conversely, the risks associated with inadequate change controls are as follows:

- ***Unauthorised changes*: accidental or deliberate but unauthorised changes to the systems. For example, if there are inadequate controls application programmers could make unauthorised amendments to programs in the live environment;
- ***Implementation problems*: for example where the change is not in time for business requirements, e.g. annual tax rates;
- ***Erroneous processing, reporting*: systems which do not process as intended. This could lead to erroneous payments, misleading reports, wrong postings of transactions and ultimately qualified accounts;
- ***Maintenance difficulties*: poor quality systems, which are difficult or expensive to maintain (e.g. due to a lack of system documentation). Where there are inadequate controls over changes there could be multiple changes to the system so that nobody is sure which versions of software, or modules are being used in the live environment. Nobody would know which bugs had been fixed, or what parameters have been altered in different versions;
- ***Use of unauthorised hardware and software*: systems (hardware and software) in use which are not authorised. This could lead to incompatibility between different parts of the system, or breach of copyright legislation; and
- ***Problems with emergency changes*: uncontrolled emergency changes to programs in the live environment leading to data loss and corruption of files.

The following questionnaire may help an auditor to check the **Business continuity and disaster recovery controls**

		Yes	No	KD Ref.
1.	Determine if IS facility has a documented disaster recovery plan.			
2.	Verify that the IS disaster recovery plan supports the goals and priorities found in the corporate business continuity plan.			
3.	Review the IS disaster recovery plan to determine if it: • Clearly identifies the management individuals who have authority to declare a disaster. • Clearly defines responsibilities for designated teams or staff members. • Explains actions to be taken in specific emergency situations. • Allows for remote storage of emergency procedures manuals. • Defines the conditions under which the backup site would be used. • Has a procedure in place for notifying the backup site. • Has a procedure for notifying employees. • Establishes processing priorities to be followed. • Provides for reserve supplies.			
4.	Determine if all critical resources are covered by the plan.			
5.	Determine if all master files and transaction files are backed up adequately to facilitate recovery.			
6.	Determine if the IS disaster recovery plan is tested periodically, including critical applications and services			

Risk Areas

The absence of a well defined and tested Business Continuity and Disaster Recovery Plan may pose the following major threats to the very existence of the organisation in the event of a disaster:

- The organisation's ability to accomplish its mission after re-starting its operations.
- To retrieve and protect the information maintained.
- To keep intact all the organisational activities after the disaster.
- To start its operations on full scale at the earliest to minimise the business loss in terms of money, goodwill, human resources and capital assets.

Input Controls

Input controls are the application controls which seek to minimize the risk of incorrect data entry by making validation checks, duplicate checks and other related controls. These provide the earliest opportunity to detect and correct possible mistakes. The following checklist can be used by an auditor to examine the input controls:

Sl No	Item	Yes	No	KD Ref.
1.	Whether for data preparation the following exist: • data preparation procedures ensure completeness, accuracy and validity • separation of duties between origination, approval and conversion of source documents into data • periodic review of source documents for proper completion and approvals occurs • Source document retention is sufficiently long to allow reconstruction in the event of loss, availability for review and audit, litigation inquiries or regulatory requirements.			
2.	For data input whether the following exist: • appropriate source document routing for approval prior to entry • proper separation of duties among submission, approval, authorisation and data entry functions • audit trail to identify source of input • appropriate handling of erroneously input data • clearly assign responsibility for enforcing proper authorisation over data.			
3.	Whether error handling procedures include: • approval of correction and resubmission of errors • individual responsibility for suspense files is defined • suspense files generate reports for non-resolved errors • suspense file prioritization scheme is available based on age and type.			
4.	Whether logs of programmes executed and transactions processed / rejected for audit trail exist?			
5.	Whether there is a control group for monitoring entry activity and investigating non-standard events, along with balancing of record counts and control totals for all data processed?			

6.	Whether written procedures exist for correcting and resubmitting data in error?			
7.	Whether resubmitted transactions are processed exactly as originally processed?			
8.	Is there adequate segregation of duties commensurate with the size of the organization and nature of functions?			
9.	Does one individual perform more than one function with reference to Data origination, data input, data processing or data distribution? If so, does compensating controls exist to protect against the risks of clubbing functions?			
10.	Is there a system of control group with responsibility for data conversion and entry of all source documents received from user departments?			
11.	Are the turnaround documents returned to user department by control group ensuring that no documents are added or lost?			
12..	Are any discrepancies in control group totals noticed? If so are they reconciled?			
13.	Does the Data Processing group (DP) group maintain a log of all the user departments' source documents received and their final disposal?			
14.	Are all the documents accounted for? If so what is the method used?			
15.	How is it ensured that all the documents are entered into the system once and only once, thereby preventing duplication?			
16.	Is there a system of documents being signed or marked to prevent reuse of data?			
17.	Is there segregation of duties to ensure that the person keying the data is not also responsible for verification of document			
18.	Does the system incorporate necessary data validation and editing errors at the earliest instant to ensure that application rejects any transaction before its entry into the system?			
19.	Are there essential input validations with reference to codes, fields, characters, transactions, calculations, logic, units, reasonableness, sequence etc?			
20.	Is there a system of special routines used that automatically validates and edit input transaction dates against predetermined cut-off dates?			
21.	Is there a possibility of data entry by other personnel bypassing or overriding the data validation and edit controls?			
22.	If so, is the authority to override restricted to only supervisory staff and to limited number of approved situations?			
23.	If the system of override exits, whether each instance of system override is logged and reviewed for appropriateness?			
24.	If data is rejected by application, are there documented procedures in place to identify, correct and reprocess such data?			
25.	Is there a system of clear and compact error messages communicating the problems so that immediate corrective action can be taken for each type of error?			

26.	How are rejected items recorded? Are they automatically written in a suspense file?			
27.	Does the automated suspense file include codes indicating error types, date and time of entry and identify the person entering data?			
28.	How are the automated suspense files used in correction and re-entry of transactions rejected by the application?			
29.	Does the automated suspense file contain information and analysis on the level of transaction errors and status of uncorrected transactions for management review?			
30.	Does management, based on the analysis, when error levels become too high, take necessary correction?			
31.	How frequently the master data (the master data is of permanent nature against a transaction data. It should not require frequent updating. In case, the master data is on more than one server, it must be consistent) is examined for its accuracy?			
32.	Is the master data accurate and authentic?			
33.	How often the master data is modified?			
34.	While modifying the master data, is a log kept of the reasons for change, who authorised the changes, who made the changes etc.? Are these changes documented with dates?			
35.	On modification, is the original data still available in any archive or is it deleted?			
36.	Are there blank fields in the Master data base as it exists today?			
37.	In case there are more than one server, does the same master data exist on all servers?			
38.	In cases, where a system has been updated and the legacy data creates problem, it may be investigated how the input controls for the new system have been on the data?			

Risk Areas

Weak input control may increase the risk of:

- entry of unauthorised data;
- data entered in to the application may be irrelevant;
- incomplete data entry;
- entry of duplicate/redundant data.

Processing Controls

Processing Controls are the application controls that ensure complete and correct processing of input data. They also ensure that incorrect transactions are not processed. The following check list may be used by an auditor in examining and evaluating processing controls:

Sl No	Item	Yes	No	KD refere
1.	Do documented procedures exist explaining the methods for proper processing of each application program?			
2.	Is there adequate segregation of duties in respect of processing commensurate with the size of the organization and nature of functions?			
3.	Does one individual perform more than one function with reference to Data origination, data input, data processing or data distribution? If so does compensating controls exist to protect against the risks of clubbing functions?			
4.	Does an effective system of operator instructions exits including system start-up procedures, backup assignments, emergency procedures, system shutdown procedures, debugging facility, error message instructions etc?			
6.	Does the console depict the history log?			
7.	Does the history log include hardware and software failure errors, processing halts, abnormal termination of jobs, operator interventions, unusual occurrences etc?			
8.	Is the history log reviewed for identification of problems and corrective action?			
9.	Are input counts reconciled with output counts to ensure completeness of data processing?			
10.	In case of data rejection, does the organization have a well documented procedure to identify, correct and reprocess data rejected?			
11.	Whether Audit trail exists depicting the flow of transaction at every point of processing upto the output stage?			
12.	Is it possible to irrefutably trace the transaction from its destination to its point of origin?			
13.	In case of direct update to files, whether transaction history file records transaction's time and date?			
16.	Is there a system of supervisory review of all corrections in place before their re-entry?			
17.	Does the organization provide for same level of security in processing corrected transactions as in the case of original transactions including supervisory review?			

In addition to the above auditors are required to undertake the following exercises:

- Examine the system of control group independently controlling data processing using batch counts, record counts, control totals, logs of input/output etc
- Examine the system of Application file process to ensure that master and transaction files are properly and completely processed.
- Examine the reconciliation between sending program output and receiving program input thereby establishing an effective control over processing.
- Examine the stage at which data validation and edit checks are performed so as to ensure the early detection and rejection of incorrect transactions.
- Examine the system of date and time stamping of transactions for log and audit trail purposes.
- Check the mechanism of accuracy in master file contents by taking periodic samples

Risk Areas

Weak process controls would lead to:

- inaccurate processing of transactions leading to wrong outputs/results.
- some of the transactions being processed by the application may remain incomplete.
- allowing for duplicate entries or processing which may lead to duplicate payment in case of payment to vendors for goods.
- unauthorised changes or amendments to the existing data.
- absence of audit trail rendering the application un-auditable.

Output Controls

Output controls are the processing controls that ensure that the output is complete, accurate, timely and is correctly distributed. The following checklist can be used for examining and evaluating the output controls in the implementation of an application:

Sl No	Item	Yes	No	KD Ref
1.	List all outputs (Reports etc.) which the system is capable of producing. This can be compared with the list of outputs which are actually being produced.			
2.	Does the system produce all its output without any manual intervention?			
3.	How many of these outputs are actually being used? Are these reliable or the auditee depends manually prepared reports?			
4.	If there are reports that have never been printed, may be examined.			
5.	Are there any reports/outputs which are needed but the system is unable to produce them? If there are reports, which are not being produced, audit must distinguish between whether the system is not capable of producing these or the system is capable but the report is not being generated? In determining the capability in producing such reports, it should be seen that the data required for producing such report is being captured and available in the system.			
6.	How many reports are still being prepared manually? It may be investigated whether the system is capable of generating the same. If yes, the reasons for preparing it manually may be explored.			
7.	Is the parallel system still functioning? If so, compare the manually prepared reports and computer generated reports.			
8.	Does a control group exist ensuring processing flow as per the schedule?			
9.	Whether output is reviewed by a control group for acceptability, accuracy and completeness?			
10.	Whether appropriate control exists in respect of production, off-site storage and issue of tapes and other magnetic and digital media?			

In addition to the above, auditor should also check the following items:

Examine the balancing and reconciliation of output as established by documented methods, if any.

- Examine the system of reconciliation of output batch control totals with input batch control totals before release of reports establishing data integrity.
- Examine the reconciliation between input record counts with output record counts by a control group before release of reports.
- Examine the system of forward linkage to trace transaction from its origin to its final output stage and hence existence of audit trail.
- Examine the system of reconciliation of computer generated batch totals with manually developed batch totals by the control group.
- Examine the system of reconciliation of computer generated record counts with manually developed record counts by the control group.
- Examine whether document methods are in place for proper handling and distribution of output.

Risk Areas

If output controls prevailing in the application are weak or are not appropriately designed, these may lead to:

- repeated errors in the output generated leading to loss of revenue, loss of creditability of the system as well as that of the organisation.
- non-availability of the data at the time when it is desired.
- availability of the data to an unauthorised person/user.
- even sometimes, the information which may be of very confidential nature may go to the wrong hands.

Annexure IV

Glossary of Terms

Audit trail A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions. Most accounting systems and database management systems include an audit trail component. In addition, there are separate audit trail software products that enable network administrators to monitor use of network resources.

Data Distinct pieces of information - usually formatted in a special way. All software is divided into two general categories: data and programs. Programs are collections of instructions for manipulating data. Data can exist in a variety of forms -- as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Strictly speaking, data is the plural of datum, a single piece of information. In practice, however, people use data as both the singular and plural form of the word. The term data is often used to distinguish binary machine-readable information from textual human-readable information. For example, some applications make a distinction between data files (files that contain binary data) and text files (files that contain ASCII data). In database management systems, data files are the files that store the database information, whereas other files, such as index files and data dictionaries, store administrative information, known as metadata.

Hardware Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips. In contrast, software is untouchable. Software exists as ideas, concepts, and symbols, but it has no substance. Books provide a useful analogy. The pages and the ink are the hardware, while the words, sentences, paragraphs, and the overall meaning are the software. A computer without software is like a book full of blank pages -- you need software to make the computer useful just as you need words to make a book meaningful.

Software Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware. The terms software and hardware are used as both nouns and adjectives. For example, you can say: "The problem lies in the software," meaning that there is a problem with the program or data, not with the computer itself. You can also say: "It's a software problem." The distinction between software and hardware is sometimes confusing because they are so integrally linked. Clearly, when you purchase a program, you are buying software. But to buy the software, you need to buy the disk (hardware) on which the software is recorded. Software is often divided into two categories:

- **systems software :** Includes the operating system and all the utilities that enable the computer to function.
- **applications software :** Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

Password A secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password. Ideally, the password should be something that nobody could guess. In practice, most people choose a password that is easy to remember, such as their name or their initials. This is one reason it is relatively easy to break into most computer systems.

Documentation Instructions for using a computer device or program. Documentation can appear in a variety of forms, the most common being manuals. When you buy a computer product (hardware or software), it almost always comes with one or more manuals that describe how to install and operate the product. In addition, many software products include an online version of the documentation that you can display on your screen or print out on a printer. A special type of online documentation is a help system, which has the documentation embedded into the program. Help systems are often called context-sensitive because they display different information depending on the user's position (context) in the application. Documentation is often divided into the following categories:

- **installation:** Describes how to install a program or device but not how to use it.
- **reference:** Detailed descriptions of particular items presented in alphabetical order. Reference documentation is designed for people who are already somewhat familiar with the product but need reminders or very specific information about a particular topic.
- **tutorial:** Teaches a user how to use the product. Tutorials move at a slower pace than reference manuals and generally contain less detail. A frequent lament from computer users is that their documentation is inscrutable. Fortunately, this situation is improving, thanks largely to advances in help systems and online tutorials. These forms of documentation make it much easier to deliver the specific information a user needs when he or she needs it.

LAN A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. There are many different types of LANs Ethernets being the most common for PCs. Most Apple Macintosh networks are based on Apple's AppleTalk network system, which is built into Macintosh computers. LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

WAN Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Physical Refers to anything pertaining to hardware. The opposite of physical is logical or virtual, which describe software objects. For example, physical memory refers to the actual RAM chips installed in a computer. Virtual memory, on the other hand, is an imaginary storage area used by programs. A physical data structure refers to the actual organization of data on a storage device. The logical data structure refers to how the information appears to a program or user. For example, a data file is a collection of information stored together. This is its logical structure. Physically, however, a file could be stored on a disk in several scattered pieces.

Logical Refers to a user's view of the way data or systems are organized. The opposite of logical is physical, which refers to the real organization of a system. For example, a logical description of a file is that it is a collection of data stored together. This is the way files appear to users.

Input Whatever goes into the computer. Input can take a variety of forms, from commands you enter from the keyboard to data from another computer or device. A device that feeds data into a computer, such as a keyboard or mouse, is called an input device. The act of entering data into a computer.

Output Anything that comes out of a computer. Output can be meaningful information or gibberish, and it can appear in a variety of forms -- as binary numbers, as characters, as pictures, and as printed pages. Output devices include display screens, loudspeakers, and printers. To give out. For example, display screens output images, printers output print, and loudspeakers output sounds.

Log To record an action. For example, to enter a record into a log file. System A group of interdependent items that interact regularly to perform a task.

- An established or organized procedure; a method.
- A computer system refers to the hardware and software components that run a computer or computers.
- An information system is a system that collects and stores data.
- System often simply refers to the operating system.

Server A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server.

- A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic.
- A database server is a computer system that processes database queries.
- Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Client The client part of client-server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

DBMS A collection of programs that enables you to store, modify, and extract information from a database. There are many different types of DBMSs, ranging from small systems that run on personal computers to huge systems that run on mainframes. The following are examples of database applications:

- computerized library systems
- automated teller machines
- flight reservation systems
- computerized parts inventory systems

From a technical standpoint, DBMSs can differ widely. The terms relational, network, flat, and hierarchical all refer to the way a DBMS organizes information internally. The internal organization can affect how quickly and flexibly you can extract information. The information from a database can be presented in a variety of formats. Most DBMSs include a report writer program that enables you to output data in the form of a report. Many DBMSs also include a graphics component that enables you to output information in the form of graphs and charts.

Data integrity Refers to the validity of data. Data integrity can be compromised in a number of ways:

- Human errors when data is entered
- Errors that occur when data is transmitted from one computer to another
- Software bugs or viruses
- Hardware malfunctions, such as disk crashes
- Natural disasters, such as fires and floods

There are many ways to minimize these threats to data integrity. These include:

- Backing up data regularly
- Controlling access to data via security mechanisms
- Designing user interfaces that prevent the input of invalid data
- Using error detection and correction software when transmitting data

Access Permission to use.

- A user can access files, directories, computers, or peripheral devices.
- More specifically, access often means to read data from or write data to a mass storage device. The time it takes to locate a single byte of information on a mass-storage device is called the access time.
- To visit a Web site.
- The act of reading data from or writing data to a storage device.
- A privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users.
- When capitalized as Access, it means short for Microsoft Access.

Mainframe Based Computer A very large and expensive computer capable of supporting hundreds, or even thousands, of users simultaneously. In the hierarchy that starts with a simple microprocessor (in watches, for example) at the bottom and moves to supercomputers at the top, mainframes are just below supercomputers. In some ways, mainframes are more powerful than supercomputers because they support more simultaneous programs. But supercomputers can execute a single program faster than a mainframe. The distinction between small mainframes and minicomputers is vague, depending really on how the manufacturer wants to market its machines.

Minicomputer A midsized computer. In size and power, minicomputers lie between workstations and mainframes. In the past decade, the distinction between large minicomputers and small mainframes has blurred, however, as has the distinction between small minicomputers and workstations. But in general, a minicomputer is a multiprocessing system capable of supporting from 4 to about 200 users simultaneously.

Preventive Control Detect problems before they occur

- Monitor both operation and inputs
- Attempt to predict potential problems before they occur and make adjustments
- Prevent an error, omission or malicious act from occurring

Detective Control Use controls that detect and report the occurrence of an error, omission or malicious act

Corrective Control Minimise the impact of a threat

- •Resolve problems discovered by detective controls
- •Identify the cause of a problem
- •Correct errors arising from a problem
- •Modify the processing systems to minimize future occurrence of the problem

ICT (information and communications technology or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are often spoken of in a particular context, such as ICTs in education, health care, or libraries.

List of Abbreviations Used

Abbreviations	Full Form
A/C	Account
CAAT	Computer Aided Audit Technique
CARD	Computer Aided Administration of Registration Department
CIC	Community Information Centre
CLC	Community Learning Centre
DBMS	Data Base Management System
DISK	Dairy Information System Kiosks
DoT	Department of Telecom
ECs	Encumbrance Certificates
EDP	Electronic Data Processing
FIR	First Information Report
FRIENDS	Fast, Reliable, Instant, Efficient Network for the Disbursement of Services
GL	General Ledger
GP	Gram Panchayat
GPMS	Gram Panchayat Management System
GS	Gram Sabha
ICT	Information and Communications technology or technologies
IFMS	Integrated Fund Monitoring System
IS	Information System
ISD	International Subscriber Dialling
IT	Information Technology
KBPS	Kilo Bytes Per Second
LF	Local Fund
LSG	Local Self Government
MIS	Management Information System
MMPs	Mission Mode Projects
MoPR	Ministry of Panchayati Raj
NeGP	National e-Governance Plan
NPP	National Panchayat Portal
OB	Opening Balance
P&RD	Panchayat and Rural Development
PC	Personal Computer
PR	Panchayati Raj
PRI	Panchayati Raj Institutions
PS	Panchayat Samiti
SDD	System Design Document
SRS	System Requirement Survey
STD	Subscriber Trunk Dialling
SWAN	State Wide Area Network
URS	User Requirement Survey
VFM	Value For Money
VSAT	Very Small Aperture Terminal
YIFs	Young India Fellows
ZP	Zilla Parishad
A/C	Account
CAAT	Computer Aided Audit Technique
CARD	Computer Aided Administration of Registration Department
CIC	Community Information Centre
CLC	Community Learning Centre
DBMS	Data Base Management System

List of References:

1. CAG's IT Audit Manual
2. IT Workshop on Introduction to IT Audit (ASOSAI), 2002
3. COBIT (Control Objective For Information Audit) Manual
4. User Manual of GPMS
5. User Manual of IFMS
6. Concerned Notifications issued by Department of Panchayat and Rural Development, Government of West Bengal
7. Administrative Report of Department of Panchayat and Rural Development, Government of West Bengal
8. www.wbprd.inc.in
9. www.panchayat.nic.in
10. www.panchayat.gov.in

Regional Training Institute, Kolkata

Cover design by: Shri Sujit Kumar Das, Assistant Audit Officer, Faculty, RTI, Kolkata