लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

PursuIT

2018 : Second Half-yearly Issue
on

e-Governance

International Centre for Information Systems & Audit
of CAG of India

CONTENTS

PursuIT

Year 2018- 2nd Issue

About the Journal

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

Editorial Board

Submission of Articles

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

Feedback/Suggestions

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

Disclaimer

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

DG'S MESSAGE

e-Governance is the application of Information and Communication Technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various Stand-alone systems and services between Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G), Government to Employees (G2E) as well as back office processes and interactions within the entire government framework.

Government of India has initiated 44 Mission mode projects. They are to be implemented by the union government, state government and some integrated projects have to be implemented by both. As on date, 15 projects have been implemented completely and 15 projects are in the implementation stage. The remaining projects are in the design, development or the bidding stage.

Since its formation in 2002, iCISA has contributed to the world audit fraternity through its training programs. In the past, there has been a practice of sharing the latest developments in the Information Technology matters by way of an Online Journal PursuIT. This practice has been restarted in 2018 and the first e-Journal in this series was issued with the theme of "Emerging Threats, Risks and Vulnerabilities in the Cyber world". This is the second e-Journal in this series with the theme "e-Governance". The articles under "Audit aids" can be used to carry out the field audits and the results may be shared with us.

I hope that this e-Journal will be of immense value to the readers. A lot of effort has gone into bringing it in its present form and the efforts of the officers who have contributed to it needs to be appreciated. We will need invaluable suggestions of the readers to make it even better in days to come.

Ram Mohan Johri
Director General
iCISA

Broader Contexts of Digitization

- Sh. Vinayak Godse

Sh. Vinayak Godse has over 22 years of experience in Information Security, IT Transformation, Telecom Switching Infrastructure, Intelligent Networking and Broadband Infrastructure. Presently, he is Senior Director–Data Protection at Data Security Council of India (DSCI), he manages DSCI programs, which include 'Security and Privacy Education & Awareness', 'Policy Advocacy- engaging Governments and International Bodies', 'Content Research and Studies', 'Building Network of Security Professionals', and 'Cyber Lab Initiative for Capacity Building of Law Enforcement Agencies'. He is the principal author of the DSCI Security Framework (DSF©) and DSCI Privacy Framework (DPF©).

The advent of technology has been transforming the governance of public affairs. There is increasing realization of the role of technology in running the matters of the governance. Technology ensures transparency and optimization of cost. It helps extend the reach and makes institutions more participatory. It enhances public convenience and improves experience of stakeholders while dealing with public institutions quite significantly. Transactions delivering public services, involving transferring or exchanging financial value, have been undergoing revolutionary changes. India has recognized this quite early by setting a strategy and plan for e-Governance. Special missions were set up, dedicated infrastructures were created, and many projects were initiated to transform various aspects of governance. All efforts are now culminating into a broader agenda of Digital India, which not only lays down structure for digitization of public functions but also serves as a key motivation for charting new paradigms of digitization.

From - centralization of public grievances, online reservation of rail tickets, digital access of government laws & regulations, management of public health services delivery, collection of taxes by the local bodies, delivery of identity documents, filing personal & corporate taxes, transfer of social benefits, plans of financial inclusion, delivering services to pensioners - to centralised monitoring of power generation & distribution; digitization is now playing a central role. While it brings tremendous benefits to transforming society, the economic levers, facilitated by these transformations, are increasingly becoming digital. The goals of USD 1 trillion digital economy hinges on these transformations. Speed and urgency towards digitization is strongly witnessed not only at the central government level but also at the state and even at the level of local bodies.

Experimentations and their success are recognised and celebrated at the national level. They are emulated in other parts of the country. The immediate success of this drive is quite visible and dominant. However, for the long-term success, there is a need to examine various facets of the momentum of digitization.

Steps towards digitization go through deep cognitive efforts. There are many contexts at play when a decision of digitization of a process or an element is underway. Some contexts are parochial in nature; mostly deliberations confined to them. But, they play a dominant role in shaping the nature, character, and outcome of the digitization. They limit the gains and possibilities that a plan of digitization can deliver. If the same is seen from a larger window, taking into considerations all possible contexts, many gaps will become visible. These parochial contexts vary in the way the initiatives of digitization were devised, type of exercises carried out to determine the objectives behind them and what inputs factored in while carrying out the exercise. Evolving standards and practices provide new contexts for considerations.

Contemporary users experience new practices and design styles. This calls for giving attention to information architectures hence offering a new set of contexts. The evolving practices and techniques of organizing application services and ideas for easing transaction processing flow would add to them.

New learnings of - how resources can be effectively used, how infrastructure is planned & consumed, how IT services can be procured and set up, how IT operations can be managed and how business services can be planned and delivered - are abundantly available. Acquiring technology in a one-time exercise is getting replaced by the models promising agility and continual development. Moreover, an entire discipline of Governance Risk and Compliance, both at the enterprise level, referred as Enterprise GRC and at the level of IT, called as IT GRC, has been going through many evolutions. Science, engineering and managerial dimensions of cyber security have also been going through changes. All the above add to the broad contexts available to the plan of digitization. Digitization plans alien to these contexts may not yield long-term benefits. Such plans would fail even to achieve specific short-term and parochial objective fully.

Technology is now transitioning to a new paradigm of platformization, where infrastructure, services, and capabilities are consumed in a standardized way. A variety of platform exists in the market now. Cloud computing is replacing the on-premise, closed and confined IT implementation.

The government of India has acknowledged this in a special policy called Meghraj Policy. As per the policy, GoI has empaneled the leading cloud service providers. The government departments and bodies are advised to make cloud as the first option in their digitization plan, a significant departure from the way technology is procured now.

Consumption of the technology on a cloud platform brings together experiences from all organizations. Each of the organizations on the platform leverages from experiences of others. Data, generated from these experiences, is increasingly becoming critical to the plan of digitization. Machine learning and Artificial Intelligence algorithms experiment on this data in the scheme of digitization. The Government of India has outlined its strategy for Artificial Intelligence through a NITI Aayog paper. The digitization plans would have to factor this in their plan.

Another important change happening is increasing thrust on innovation and advice to deploy services of start-ups and Small and Medium Enterprises (SME) sector. The government departments have been finding ways to work with small firms. They have been devising challenges, organizing hackathons and piloting new technologies. Special policy interventions are opted for this. These innovations not only bring the new players but also make the applications and systems more open. They make the data generated out of transactions open and provide better ways of sharing this data.

Moreover, technologies like Digital Ledger (Blockchain) would make computing more decentralized, interdependent and consensus-driven. Internet of Things would bring a variety of new devices in the processing of transactions. Procurement, acquisition and consumption of technology will change phenomenally in the coming future.

Plans of digitization should factor these evolutions and broader contexts available from them. These contexts would shape even a small initiative taken by public institutions at any corner of the country. If their strategies don't factor these contexts while selecting their procurement model and selecting players & technologies, it would severely hamper their long-term perspectives of investment in digitization. The governance processes, IT as well as Enterprise, need significant overhauling to incorporate these contexts. The assurances and audit exercises should adapt to these transforming changes. The audit exercises without taking note of these contexts would limit their effectiveness. These broader contexts should become a reference of audit and assurance. Digitization plan in isolation are bound to create deficiencies, reduce transparency, escalate cost, fail to create desired value, introduce inefficiencies and hamper timeliness.

IT Audit Highlights: Supreme Audit Institution - Australia
ANAO audit report on myGov

The myGov digital service (myGov) is an entry portal for individuals to access the services of participating government entities. It was launched in May 2013 to provide individuals with secure online access to a range of Australian Government services in one place. The report reviewed the effectiveness of the Department of Human Services' (DHS) implementation of myGov as at November 2016. (The Digital Transformation Agency (DTA) is responsible for myGov service strategy, policy and user experience, while the DHS is responsible for administering and hosting myGov, including processes and procedures for system development and testing, security and operational performance.)

ANAO audit noted that myGov achieved nearly double the predicted number of user accounts. The report mentions that the 4-year (2012-2016) myGov project had exceeded its June 2016 target of 5.1 million accounts and six member services. As at November 2016, myGov has almost 11 million active accounts and ten member services.

myGov was expected to deliver major outcomes as outlined: improved service delivery for individuals supported by five key functionalities—single digital credential, Update Your Details, Inbox, Discoverability, data validation, improved whole-of-government online service delivery capability supported by a governance framework, standardised business processes, and common standards.

The audit confirmed that the portal has contributed to improved delivery of government services for individuals, reducing time spent in interacting with government. This benefit accrues where individuals use the myGov functionalities to receive correspondence or update their details, and in particular, where individuals link their account to at least two member services. DHS reported in its November 2016 Performance Report that 46 per cent of myGov accounts were linked to two or more services.

Three of the five planned key functionalities have been delivered, enabling individuals to access government services online using a single digital credential; notify changes of personal contact details; and receive digital correspondence securely.

The myGov platform has been hosted on high-availability infrastructure since December 2015, which has improved performance, especially during peak demand periods, with performance (monthly availability target of 99.5 per cent) consistently met. Suitable security and

privacy measures were adopted to control access and protect data stored in myGov.

The audit made two recommendations, Recommendation No.1:

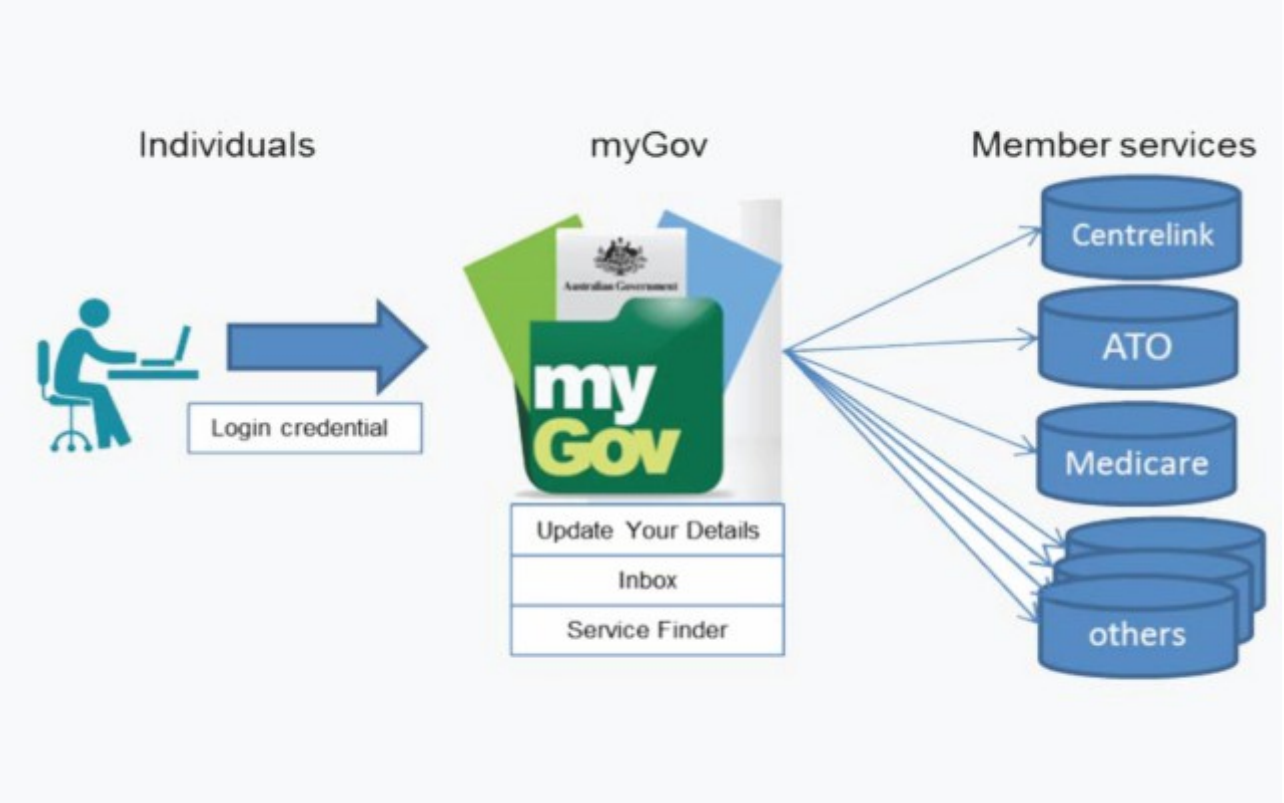
a) Digital Transformation Agency implement a strategy to target 'service delivery' Australian Government entities to provide services through myGov; and

b) Department of Human Services review existing transition support and guidance materials for entities to ensure that they effectively support targeted government entities to interface their systems with myGov functionalities.

Recommendation No.2:

The ANAO recommends that the Digital Transformation Agency in consultation with the member services, establish a performance framework, including key performance indicators focusing on outcomes, to enable an assessment of the extent to which myGov is delivering expected outcomes for users and member services, both of which have been accepted. DHS and the DTA will share responsibility for the first one, to assist more agencies to make their services available via myGov. The second recommendation to establish a framework to monitor the website's performance, will be overseen by the DTA, which will consult with member services.

Access the complete audit report by ANAO here.



IT Audit Highlights: Seventh annual progress report of the Board of Auditors on the implementation of the United Nations enterprise resource planning system (Umoja).

An enterprise resource planning system (Umoja) is being implemented across the United Nations Secretariat to replace ageing legacy systems such as the Integrated Management. The Board of Auditors was requested to conduct a comprehensive audit of the implementation of the Umoja project and to report annually to the Assembly starting at the main part of its sixty-seventh session.

In a series of reports since 2012 (A/67/164, A/68/151, A/69/158, A/70/158, A/71/180 and A/72/157), the Board of Auditors submitted information on the progress made in the implementation of the Umoja project. The original timeline and budget approved in 2008 envisaged deploying Umoja by the end of 2012 at a cost of $248.3 million. However, the implementation plans had been substantially revised on several occasions, and the deployment of full functionality is at present not expected until 2019. The current approved budget for the project up to the end of 2019 was $528.22 million, and the total expenditure up to 31 December 2017 was $439.4 million.

Umoja was implemented in different parts of the Organization (clusters), with functionality split into three phases, as follows.

(a) Umoja Foundation

This functionality, mainly finance and procurement processes, was fully deployed across peacekeeping operations from November 2013, in special political missions from March 2014 and across remaining United Nations Secretariat entities in two clusters from June and November 2015;

(b) Umoja Extension 1 (UE1)

This functionality, mainly comprising of payroll and human resources management processes (including travel) was deployed across Secretariat entities and peacekeeping operations in two clusters from June and November 2015. Most non-peacekeeping Secretariat entities therefore received Umoja Foundation and UE1 functionality at the same time (Umoja Integration);

(C) Umoja Extension 2 (UE2)

This functionality will include key business processes, such as budget formulation, fundraising and implementing partners, programme management, supply chain management and conference and event management, and is currently scheduled to be deployed by the end of 2018. Both quantitative and qualitative benefits are expected to accrue from the deployment of UE2.

The key findings in the seventh annual progress report of the Board of Auditors on the implementation of the United Nations enterprise resource planning system (Umoja) are:

Managing benefits realization: The Board noted that end-to-end process management is a

significant change triggered by Umoja. However, the Board also observed that there was no documented plan in place to aid the Secretariat in establishing a clear and transparent record of the realization of qualitative and quantitative Umoja benefits.

User access provisioning: As of 18 February 2018, there were 2,996 unlocked user accounts in Umoja for staff members who had separated in 2016 and 2017, all with valid end-dates of "31.12.9999". Of those 2,996 former staff members with active user IDs, 1,105 had accessed Umoja after separation, 236 had accessed Umoja more than 90 days after separation and 19 had accessed Umoja more than one year after separation.

Access management: According to the relevant control procedure, the access rights should be removed in case a service is not accessed for more than three consecutive months. The Board observed that although as of 18 February 2018, 469 users had not logged on to Umoja for more than 90 days, their accounts remained active in Umoja and Unite. The Board also noted an absence of annual reviews of access management.

Segregation of duties: The Board analysed the enterprise role assignments for any possible segregation of duties conflicts as defined by the enterprise role guide and found that there were 1,146 users with 3,948 conflicting roles.

Business continuity and disaster recovery planning: The Board noted that a disaster recovery exercise was simulated on 6 May and 3 June 2017. This exercise also aimed to check if the recovery time objective of 4 hours, the recovery point objective of 10 minutes and the maximum agreed downtime of eight hours could be met. The Board observed that the actual recovery time that was achieved in the exercise was 18 hours and 35 minutes for the failover exercise, while it was 7 hours and 15 minutes for the failback exercise. In addition, it was noted that the actual recovery point in both the exercises was 0 minutes. Thus, while the recovery point objective was met in both the failover and the failback exercises, the recovery time objective was not met in either exercise. Moreover, the maximum downtime was breached in respect of the failover exercise, while it was adhered to in the failback exercise.

Change management: The Board's analysis of the change request database indicated that, of the 235 change request items requested by business users that were pending for review, 41 change requests (17 per cent) had been pending for more than one year.

Mainstreaming Umoja: The Board is of the view that it is important to consider various factors in the mainstreaming plan, such as the ongoing reform agenda, the timelines of UE2 deployments and the large scope for continuous improvements in Umoja functionalities. Umoja stabilization may require some time after full functionality deployments. Moreover, the scope for improvements in functionality through a continuous improvement programme is likely to extend beyond the mandated project period.

Access Full Report

https://undocs.org/en/A/73/169

Audit Highlights: Supreme Audit Institution- India

Information Technology Audit on e-Procurement Project

Name of State Audit Office: **PAG (Audit) Himachal Pradesh**

Name of the Project: **State MMP : e-Procurement**

Introduction:

e-Procurement is a collaborative procurement of goods, services as well as selection of bidder for award of works by using internet and related technologies for bringing efficiency and transparency. e-Procurement process also results in competitiveness and saving of cost and time by shortening of procurement cycle. The State Government (Information Technology Department, Himachal Pradesh) introduced (June 2011) electronic procurement (e-Procurement) project aimed at increasing the efficiency and transparency in procurement of goods, works and services. The performance audit of the conception and implementation of the project was done during March 2017 to June 2017 to assess its effectiveness.

Highlights:

- Only one module (e-Tendering) out of seven modules of e-Procurement had been considered for implementation in 26 out of 90 organisations in the State. Even in the e-Tendering module the critical activities such as online opening of bids, negotiations and award of contract is being done manually.

- Business rules have not been mapped in the application software leading to irregular opening of the tenders before the stipulated period.

- Use of same digital signature certificate by multiple users and participation in the tendering process defeated the very purpose of secured online bidding.

- Time cycle in processing of tenders through e-Procurement system could not be reduced due to non-revision of tendering rules, and time taken in processing of tenders during 2011-17 ranged between 122 and 554 days.

- Performance of multiple jobs by single user due to non-segregation of duties rendered the system susceptible to high risk and will make it impossible to enforce accountability.

- There was a shortfall of 98 per cent in providing training to the prospective bidders for effective use of e-Procurement system and monitoring was also inadequate as the requisite meetings of the Core Committee were not held.

Access Full Report

https://cag.gov.in/sites/default/files/audit_report_files/Report_No_6_of_2017_%E2%80%93_Social_General_and_Economic_Sector_Government_of_Himachal%20_Pradesh.pdf

Page No. 75 to 96

e-Governance project in Registration and Stamps Department (iSARITA)- March 2015

Name of the State Audit Office: **AG (Audit) II, Maharashtra, Nagpur**

Nature of the Project: **State MMP**

Introduction

- The Department initiated its e-Governance project in 2002 with development of a software application named SARITA (Stamps and Registration Information Technology Application). A web based application iSARITA (integrated SARITA) was implemented (July 2012) and developed by NIC.

The operating system used for the servers is RED HAT Linux and back end database tool is "PostGres SQL 9.2" and VB is used as front end.

Highlights:

1. The application lacked validation controls which resulted into storing of multiple entries of same transaction relating to payment of stamp duty leading to inflation of the reported figures to the tune of ₹ 2.91 crore.
2. The application was prone to risk of registering the documents without proper authority and defeated very purpose of having biometric and digital data.
3. Incomplete data was found in respect of scanned images of the documents, digital photographs and biometric data of thumb impression of parties and witnesses.
4. Due to weak logical security control, system was susceptible to the risk of suspected backend changes with no audit trail to locate the event through security logs.

Access Full Report

http://icisa.cag.gov.in/view/pdf/aHR0cDovL2ljaXNhLmNhZy5nb3YuaW4vYXVkaXRfcmVwb3J0LzIxLzYwMzVhMjU3OGI3MzlkOGViNTM2OTk1MTc5NjJiNTFjLnBkZg

#Tech-Kid

SOURCE

https://www.facebook.com/IIC4u/photos/pcb.10156024892663403/10156024892233403/?type=3&theater

Integrity Issues to kept in Perspective during Audit of e-Procurement Systems (Part - II)

- Sh. Jitendra Kohli

Sh. Jitendra Kohli graduated as an Electrical Engineer from IIT Delhi. He is the Founder-Managing Director of ElectronicTender, an e-Procurement technology lab. He has been researching for over 18-years in the area of e-Procurement with focus on 'Integrity and Transparency issues of Public-Procurement'. His papers on e-Procurement have been published at many reputed international conferences in USA, EU, etc. He is the innovator and chief-architect of Electronic-Tendering-Engine®, a cutting-edge e-Procurement/e-Tendering/e-Auction software for Public-Procurement, which is licensed to independent service-providers for setting-up portals. In public-interest, he has shared important aspects of his ground-breaking research with vigilance/regulatory authorities to prevent mal-practices in e-Procurement.

Background:

It is suggested that this article be read in continuation of the article with a similar title published in the May 2018 of PursuIT (iCISA, 2018). The prequel to this article focused on two most critical areas of e-Procurement, viz. – vulnerabilities in some commonly used methodologies for 'bid-encryption' (which is the electronic equivalent of bid-sealing used in the manual/ paper-based tendering), and deficiencies in the manner in which the 'online public tender opening event' is conducted which makes it more of an eyewash, leaving immense scope for manipulation. Unchecked malpractices in these two critical aspects can severely compromise the fairness and transparency of the public-procurement process. Keeping in perspective the national guidelines on e-Procurement, viz. the DeitY-Guidelines dated 31st August 2011, and the final report issued by the e-Tendering expert group (e-TEG) appointed by the European Commission, the article also elucidated some remedial measures to overcome, or at least mitigate, some of these critical threats. This discussion is being continued here with the objective of ensuring 'Integrity' in the e-Procurement systems being used for public-procurement.

Events which Vindicate the Apprehensions:

Since the writing of the previous article, some events have unfolded in the last few months that vindicate the apprehensions expressed in that article regarding manipulation of bids in e-Procurement systems deployed within our country, and elsewhere. A case in point is the recent 'e-Tender scam in the State of Madhya Pradesh'. Some excerpts from a report published in the Economic Times dated 6th September 2018 (The Economic Times, 2018), are being highlighted below for the purpose of discussion:

"... issued show cause notices (SCNs) to service providers Tata Consultancy Services and Antares System on June 6 ...While TCS was given the responsibility for maintenance of the helpdesk, hardware and training, Antares was assigned the task of application development and

maintenance … Both did not deny, in their responses to the SCN, that cyber fraud was committed but at the same time the two did not accept responsibilities for the breach … Though both the internal reports of TCS and Antares submitted to MPSEDC have clearly established that the encrypted data was compromised to benefit three private bidders … The MP e-Procurement application stipulates that a vendor's bidding data should be encrypted using Department Tender Opening Authority's digital certificate. Simultaneously, the vendor bidding data can be decrypted using TOA's encryption certificate keys … Multiple parties are involved in the cyber fraud. The prime suspects are TOAs, persons having good knowledge about how tenders are hosted and processed, and backend person who could have accessed IT infra and able to copy encrypted bid data. Lastly, bidders who wanted to win tenders by becoming L1. … Antares … response: *We have replied to the SCN. The irregularities did not happen in the application but outside. Someone who had keys would have probably done it ...*"

Based on the above excerpts from the Economic Times report, this is a case of 'Scenario-1' of 'Bid-Encryption' methodology as described on page-16 of PursuIT (May 2018 issue). Apart from the fact this method of bid-encryption has obvious vulnerabilities, it seems from the news-report that even the remedial measures required to mitigate the risks associated with this methodology, as discussed in the article (with reference to the DeitY-Guidelines) were missing! The claim that this happened outside the application is misleading to the extent that the overall system is not just the application but also includes the database. As mentioned in the Economic Times report, "...backend person who could have accessed IT infra and able to copy encrypted bid data" indicates a copy of the encrypted data was made clandestinely from the database that is an intrinsic part of the overall e-tendering system. The decryption of this clandestine copy can be done outside the system. So even assuming that the irregularities did not happen in the application but outside, as claimed by the party to whom the SCN was issued, the fact remains that it could happen outside because of the weakness of the application design and an intrinsically vulnerable methodology of bid encryption.

To recap, in the previous article, on page-14 of PursuIT (May 2018 issue), it was mentioned:

"As anticipated in the DeitY-Guidelines, due to the vulnerabilities relating to Bid-Confidentiality existing in some e-Procurement systems, it is understood that there is already some kind of e-Tendering link in operation in some places, which can help favoured bidders to know competition-prices in a large tender (15-30 minutes before the 'deadline for bid submission'), and to help them change their bids suitably."

In public-interest, for over 15-years, the author has been sharing with vigilance and regulatory authorities in India and some other countries, information about the vulnerabilities in most e-Procurement systems, as well as, possible remedial measures. While some officers and authorities took note of the suggestions given by the author, by and large the suggestions met with scepticism, resistance and quite often downright hostility. A typical refrain of the sceptics was -- "The points being made by you look fine, but these points are theoretical.

No fraud has been reported. So we cannot take action." There is an old saying, "Prevention is better than cure". If these authorities had taken preventive measures, scams like the e-Tender scam in Madhya Pradesh (and many more such scams which could be taking place in other States and organizations, but are unreported) would not have taken place. Reference may be made to page-13 of PursuIT (May 2018).

Other Reports Confirming Mal-Practices in e-Procurement Systems

Since the reporting of the MP's e-Tender scam, some persons from the industry have come forth to share information (or rather confess) about what is happening on the ground. Some salient revelations, which corroborate the apprehensions outlined in the previous article are presented below:

- Misuse of PKI encryption and decryption certificates/ keys: As mentioned on page-15 of PursuIT (May 2018 issue), "To prevent misuse by the e-Procurement service provider, the e-Procurement service provider or the portal operator should not be selling or providing PKI encryption and decryption certificates/ keys to the users of the portal."

The reality on the ground is that this practice (or rather malpractice) is rampant. Most service providers take an agency from the licensed Certifying Authority for selling such encryption/ decryption keys. The risk in this regard is basically in e-Procurement systems where bid-encryption is done as described on page-16 of PursuIT (May 2018 issue) under 'Scenario-1: Where asymmetric encryption methodology using Public-Key/ DSC or Encryption Certificate of an officer of the Buyer organization, or any other Public-Key specified by the Buyer organization is used for bid-encryption'.

When the service provider sells such keys to the tender-opening officers (TOE officers), a copy of the encryption/ decryption keys remains with the service provider. So even without connivance of the TOE officers (or the TOA officers as mentioned in the Economic Times news report about the MP's e-Tender scam), the decryption key can be misused.

The situation is compounded by the fact that the mal-intentioned e-Procurement service-providers manage to influence the purchasing-authority which is issuing the RFP, for 'selection of an e-Procurement service provider', by getting a condition inserted in the RFP that the selected service provider has to provide digital signature keys (including encryption/ decryption keys).

Remedy: Apart from the remedies already discussed in the previous article, it must be ensured that in e-Procurement systems where bid-encryption is done as described under Scenario-1 of the previous article, the asymmetric bid encryption/ decryption keys should be procured by the purchasing-entity officers directly only from an independent Government body or a Certifying Authority (CA) that has no direct or indirect interest in the e- Procurement system/ portal.

Post-TOE Tampering of the Bids/ Comparative Statements (CS) or Charts:

These malpractices can take place where the e-Procurement system is such that the Online TOE is not done transparently in the interactive/ simultaneous online presence of bidders, and the salient points of the bids are not shared instantly and automatically with the bidders as soon as each bid is opened. In other words, these flawed e-Procurement systems do not comply properly with the recommendations made in section 6.3 of Annexure- I of Deity-Guidelines dated 31st August 2011. To that extent, the online TOE in such systems is more of an eyewash.

As reported, Excel Sheets (constituting the bids) which are downloaded by the TOE-Officers along with the service provider's personnel, are later tampered to help some conniving bidders. In some cases no comparative statement (CS) is shared with the bidders, and in some cases the tampered comparative statement (CS) is subsequently shared with the bidders after many hours, or even many days. In most cases, the competing bidders will have no clue about the tampering.

Remedy: Only those e-Procurement systems should be allowed to function, where the Online TOE is actually an 'Online Public TOE', and is conducted transparently in the interactive/ simultaneous online presence of bidders. Further, the salient points of the bids should be shared instantly and automatically with the bidders as soon as each bid (technical or financial) of each bidder is opened. The integrity of a processed comparative statement (CS) posted after some delay (i.e. time-gap after the bid opening) would always be questionable. In other words, the e-Procurement system should comply fully (in letter and spirit) with the recommendations made in section 6.3 of Annexure-I of Deity-Guidelines dated 31st August 2011. If this has not been done, such systems should not be certified by STQC for compliance with DeitY-Guidelines dated 31st August 2011.

- Furthermore, in case of all e-Procurement systems (which fall under Scenarios 1, 2, and 4 of bid-encryption methodology as described in the previous article), there should be a 'standard operating procedure (SOP)', whereby the one-way-hash (OWH) of each bid as submitted, and as opened (and salient points inducted in the comparative statement) should be matched 'each and every time'. Most importantly, this SOP should be performed automatically, or by the authorized officers of the purchasing-entity in the interactive/ simultaneous online presence of bidders, and certainly not by the technical support personnel of the e-Procurement service-provider

Further, this process of matching should be logged and available for subsequent auditing by an independent agency.

- Fake/ expired STQC certificates (for compliance with DeitY-Guidelines) with changed dates are sometimes submitted to conniving officers in the department that is to use the system. These officers do not bother to validate the certificates.

- ·An e-Procurement service provider, takes STQC certificate for one of its portals but uses that certificate for running many more portals of the same service-provider which are not STQC certified for compliance with DeitY-Guidelines dated 31st August 2011.

Sample Checklist for 'Audit of some Other Important Aspects of e-Procurement Systems':

In the prequel of this article, under the last section with the heading, 'Other Important Functionalities', it was mentioned that "Checks similar to those delineated above have to be developed and conducted for other important functionalities relating to e-Procurement, such as – Password-generation and storage, authentication of electronic records, facilitation of various types of bidding methodologies, user organization's virtual administrative hierarchy, audit-trails, et al". These functionalities are now being covered in this article. The following checklists should be perused in continuation of the checklists for two critical functionalities covered in the previous article, viz. –

1. **Bid-Encryption Methodology; and**
2. **Online Public Tender Opening Event.**
3. **Authentication of Electronic Records:**

Background-Note with reference to GFR and IT Act 2000 (and The IT (Amendment) Act, 2008)

With reference to IT Act 2000 (and The IT (Amendment) Act, 2008), on p-72 of Annexure-IV of DeitY-Guidelines dated 31st August 2011, it is mentioned that:

"1 (iii) By the use of a public key of the subscriber/ signer, it should be possible to verify the electronic record. This may be read in conjunction with Sch-2, 13 85B(2)(b) - *except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.*

(Explanation: This implies that important electronic records of an e-Procurement application, like – Tender Notice, Corrigenda, Tender Documents, Addenda, Clarifications to Tender Documents, Bids, etc. should not only be electronically signed, there should also be provision in the e-Procurement application, like – Tender Notice, Corrigenda, Tender Documents, Addenda, Clarifications to Tender Documents, Bids, etc. should not only be electronically signed, there should also be provision in the e-Procurement application to verify the electronic signatures)."

The requirement of transparent Tender Notice, Corrigenda, Tender Documents, Addenda etc., as required under Rules-149, 150, 151, 180, 181 of GFR, is also elucidated in Annexure-III of DeitY-Guidelines dated 31st August 2011 on pages 57 to 70. Note: the 'Rule Numbers' of GFR-2005 rules may have changed in the GFR-2017. However, to be consistent with the DeitY-Guidelines, GFR rule numbers (in GFR 2005) as given in the DeitY-Guidelines are being mentioned here.

In addition to the comments/ references of IT Act 2000 (and The IT (Amendment) Act, 2008) and GFR given in the 'Background-Note' above, please note the following:

Section 6.1 of Annexure-I of DeitY-Guidelines (p-31, 32, 33) dated 31st August 2011 requires:

"For authenticity and for assurance that it has not been tampered, the electronic Tender Notice (which is an electronic record), should have an audit-trail within the application of its creation/ approval/ posting. Also, the tender notice should be digitally signed by an authorized officer of the Purchase/ Buyer organization…"

"…At the time of online sale/ downloading of the tender documents, official serial number should be given along with the receipt…"

"…For authenticity and for assurance that it has not been tampered, the electronic Corrigendum (which is an electronic record), should have an audit-trail within the application of its creation/ approval / posting. Also, the Corrigendum should be digitally signed by an authorized officer of the Purchase/ Buyer organization…"

"…For authenticity and for assurance that it has not been tampered, the electronic Tender Documents (which is an electronic record), should have an audit-trail within the application of its posting. Also, the Tender Documents should be digitally signed by an authorized officer of the Purchase/ Buyer organization…"

"…For authenticity and for assurance that it has not been tampered, the electronic Addendum (which is an electronic record), should have an audit-trail within the application of its approval/ posting. Also, the Addendum should be digitally signed by an authorized officer of the Purchase/ Buyer organization…"

An **Office Order No. 43/7/04 dated 2nd July 2004 was issued by the CVC** which also addressed the above mentioned issue under the sub-heading, 'Issues Connected with Data Security, Legality and Authenticity of Bid Documents', along with a Technical Note from NIC. Some excerpts are as follows:

"…certain parties may alter the downloaded documents and submit their bids in such altered tender documents which may lead to legal complications…

…The provisions of digital signatures through Certifying Authority can be used to ensure that in case of any forgery or alteration in

downloaded documents it is technically feasible to prove what the original document was. There are sufficient legal provisions under IT Act to ensure …"

"…1. Integrity of Document: The documents should be digitally signed by the person submitting them…"

"…4. Download Procedure:

a. The user verifies the digital signature of the document on the website…"

An e-Procurement system should have functionality as prescribed in DeitY-Guidelines (excerpts reproduced above) and the CVC Office Order. If this has not been done, such systems should not be certified by STQC for compliance with DeitY-Guidelines dated 31st August 2011.

Functionality to be Checked	Inference/ Conclusion
• Is the Online Tender Notice digitally signed by one of the authorized users of the Buyer organization before it is posted online? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing the Tender Notice? • Is the Online Corrigendum to Tender Notice digitally signed by one of the authorized users of the Buyer organization before it is posted online? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing the Corrigendum to Tender Notice? • Are the Tender Documents digitally signed by one of the authorized users of the Buyer organization before it is posted online? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing the Tender Notice? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing/ downloading the Tender Documents? • Is the Addendum to Tender Documents digitally signed by one of the authorized users of the Buyer organization before it is posted online? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing/ downloading the Addendum to Tender Documents?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

Functionality to be Checked	Inference/ Conclusion
• Is the Response to Query pertaining Tender Documents (Clarification to Tender Documents) digitally signed by one of the authorized users of the Buyer organization before it is posted online? • If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing/ downloading the Response? • Are the bids digitally signed by an authorized user of a bidder organization, specifically authorized for that tender? • If the answer to the above is 'Yes' is there an online facility in the system itself for verifying the digital signature by an officer during the Online Public TOE?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

4. Facilitation of various Types of Bidding-Methodologies:

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections -- 1.2, 3.1, Annexure-I (sections 1.2, 5.1, 6.1), Annexure-II, Annexure-III and Reference Document-1. An e-Procurement system should have functionality as prescribed in DeitY-Guidelines. If this has not been done, such systems should not be certified by STQC for compliance with DeitY-Guidelines dated 31st August 2011.

Functionality to be Checked	Inference/ Conclusion
• Is facility available online for one or more of the following Bidding Methodologies? • Single-stage, single- envelope • Single-stage, two- envelope • Two stage (with facility for 'technical conformance', and if required, 'revised tender documents') • Two-stage, two- envelope • Any of the above, combined with a Pre-qualification stage • In any of the above, facility for submission of one or more Alternative bids (if allowed by the Buyer) • In any of the above, after having submitted the 'original' bid for each bid-part, facility to a bidder to submit: 'Modification' bid 'Substitution' bid or 'Withdrawal'	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

5. User Organization's Virtual Administrative Hierarchy:

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections – 2.0, 3.0, *Annexure-I (section 5.1),* and Annexure-II (Table-5). An e-Procurement system should have functionality as prescribed in DeitY-Guidelines. If this has not been done, such systems should not be certified by STQC for compliance with DeitY-Guidelines dated 31st August 2011.

Functionality to be Checked	Inference/ Conclusion
• Is there a facility within a Buyer organization to create an online Administrative Hierarchy (such as different departments and authorized users at more than one level)? • If 'Yes', can different tenders be handled by different departments of a Buyer organization created above? • Can different users of a Buyer organization be authorized for different activities of a tender, and can such users be changed from tender to tender, and during the course of a tender after the tender has been notified? • Is there a facility within a Supplier organization to create an online Administrative Hierarchy (such as different sales-departments and authorized users at more than one level)? • If 'Yes', can different tenders be handled by different sales-departments of a Supplier organization created above? • Can different users of a Supplier organization be authorized for different activities of a tender, and can such users be changed from tender to tender, and during the course of a tender after the tender has been notified?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

6. Password-Generation and Storage :

Background-Note with reference to DeitY Guidelines dated 31st August 2011

Section 3.1 of DeitY-Guidelines (p-6, 7) dated 31st August 2011 requires: "e-Procurement System should not provide read access to password to the Administrator. e-Procurement System further should not have "forgot password" feature which provides administrator-generated or system-generated temporary password. Once the password is forgotten, a new password may be allotted following a set of processes needed for allotment of password. The forget password request shall be digitally signed…"

Section 7.2 of Annexure-I of DeitY-Guidelines (p-39) dated 31st August 2011 requires: "…For security reasons, Administrators of the e-Tendering application/ portal should not have any access to the passwords of the various users. Neither should the Administrators be able to generate passwords for the users."

"**Guidance and recommended practices:** The Administrators of the e-tendering application/portal should not have any access to the passwords of the various users. Neither the software should allow the Administrator to generate password for the users. The designer/ developer should factor this at the design stage/development stage, i.e. the e-procurement system has to satisfactorily address the above requirements through suitable functionality built into the e-procurement application."

An e-Procurement system should have functionality as prescribed in DeitY-Guidelines (excerpts reproduced above). If this has not been done, such systems should not be certified by STQC for compliance with DeitY-Guidelines dated 31st August 2011.

Functionality to be Checked	Inference/ Conclusion
• Is the Password created by the user himself at the client-end, or is it generated by the system and then communicated to the user?[Note: A password generated by the system (which is accessible to the administrator) and then communicated to the user is not in accordance with the DeitY-Guidelines] • Is the Password created/ generated above encrypted? If so, is it encrypted at the client-end? • In case of 'Forgot Password', is the New Password created by the user himself at the client-end after due diligence by the system/ service-provider? • In case of 'Change-Password', is the New Password created by the user himself at the client-end?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

Functionality to be Checked	Inference/ Conclusion
• Does the user account remain unlocked even in case of a number of un-successful attempts? [Note: Instead of locking the user account in the above scenario, the system should have a system of alerting the concerned user after a specified number of unsuccessful attempts, and a mechanism to break the continuity of multiple attempts.]	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

7. Audit Trails :

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections – 3.1, Annexure-I (sections 2.2, 3.1, 5.1, 5.2, 6.1, 7.4, Summary- Analysis of Risk of eProcurement Systems), Annexure-II, and Annexure-III.

Functionality to be Checked	Inference/ Conclusion
• Are detailed Audit Trails created for various activities conducted by a Buyer organization? • Is there a facility to authorize a special person to generate/ access such Audit Trail Reports? • Are detailed Audit Trails created for various activities conducted by a Supplier organization? • Is there a facility to authorize a special person to generate/ access such Audit Trail Reports?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*

REFERENCES

I) iCISA (2018), PursuIT May 2018 Issue, Audit Aids: Integrity Issues to be kept in Perspective during Audit of e-Procurement Systems. Available at **http://icisa.cag.gov.in/view/pdf/aHR0cDovL2ljaXNhLmNhZy5nb3YuaW4vcmVzb3VyY2VfZmlsZXMvOWY0MDFlMDY1MzVhMDQyZTdiMTIwNGZiNzBmOTg0ZGIucGRm** **[Retrieved September, 2018]**

II) Apart from the 'References' given in the above mentioned article, the following news report has been quoted in this article.

The Economic Times (2018). e-tender scam looms large over Madhya Pradesh Government, published on 6th September 2018. [Online]. Available at **https://economictimes.indiatimes.com/news/politics-and-nation/e-tender-scam-looms-large-over-madhya-pradesh-government/articleshow/65694727.cms** **[Retrieved September, 2018]**

SOURCE

Periotti Cartoons

https://www.reddit.com/r/forwardsfromgrandma/comments/8o9yzi/kids_these_days_dont_learn_anything_in_school/

Audit of Digital Payment Systems

- an Assurance Framework for the Indian Context

- Ms. Narmadha R. & Sh. Deepak Vishwanathan

"Ms. Narmadha R. is presently working as Sr. DAG (Accounts; Administration) in the O/o. AG (A&E). Tamilnadu. Her IT experience includes Data Analytics related activities at Centre for Data Management and Analytics, in O/o. CAG of India and IT audit and IT research related activities in iCISA. Also, she is CISA qualified."

"Sh. Deepak Viswanathan joined the IAAD as probationary Section Officer (civil) in 2002. He is a Certified Information Systems Auditor and has been part of Information Systems Audits related to computerization of various state receipt departments of the Government of Karnataka. He is currently working as Information Systems Faculty at RTI, Chennai."

ABSTRACT

This paper seeks to trace the digital payment scenario in India, describe the enabling technology and survey the regulatory framework within which it operates. Digital payment systems are fraught with security threats, many of which operate at the technical level but quite a few also seek to exploit the naivety and indiscretions of the end users. Hence an assurance framework for digital payment security should attempt to address the problem from several fronts - technical, legal, user-awareness, third party management and grievance redressal. Since regulatory frameworks strive to achieve a balance between security on the one hand and industrial dynamism on the other, taking care of neither being too restrictive on the players nor being too permissive, it may be necessary for an assurance program, in addition to testing compliance to existing laws, to evaluate the system on a scale based on contemporary industry best practices as well. In this paper the current digital payment modes in India are described along with the associated threat landscape. Finally attempt is made to synthesize the tenets of existing regulatory frameworks and best practices into an assurance program for testing the confidentiality, integrity and availability factors related to the digital payment modes in India.

INTRODUCTION

With the advent of digital money, traditional modes of transactions have given way to a multitude of delivery channels that require the interplay of enabling technologies, protocols and several intermediary service providers. Digital payment, also known as electronic payment, is a virtual transfer of funds between the banks of the payer (Issuing Bank) and that of the payee (Acquiring Bank). The payer and the payee use digital modes to send and receive money. No hard cash is involved and all the transactions are completed online. The transaction is real-time and instant (in most cases).

The digital economy provides India a way to start off the journey toward becoming a developed nation without waiting for costly and time consuming industrial infrastructure

investments to bear fruit. India's economy is rapidly converting into a digital economy which is expected to touch the $1-trillion mark by 2022. By 2030, India will be a $10-trillion economy, with half of this accounted for by the digital economy. This makes it more critical to cover the risks of the payment process from an audit perspective.

Merits and demerits

Digital money, for this reason, epitomizes an abrupt turn around in the way transactions were conducted in this country. As with any transformation that is sudden and revolutionary in character, it comes with a host of benefits that make it appear as an elixir to all existing ills, and on the other hand, with drawbacks that hardly seem to matter. It is not until the transformation has progressed considerably that the consequences of digital adoption become visible. Here is a brief consideration of the relative merits and demerits of digital money that should, on the one hand, equip us to better harvest its potential benefits and on the other, put us on guard against the possible hazards

Merits	Demerits
• **Time savings**. Money transfer between virtual accounts usually takes just a few minutes in addition to the saving on travel time to the vendor premises and the waiting time spent in queues.	• **Restrictions**. Each payment system has its limits regarding the maximum amount in the account, the number of transactions per day and the amount of output.
• **Payment History**. Digital payments retain a trail of transactions that can be verified and traced easily.	• **The lack of anonymity**. An obvious consequence of the availability of trail is the loss of anonymity.
• .**Reduced risk of loss and theft**. Digital systems have security features that protect the users from physical theft of money.	• **The risk of being hacked**. However digital systems are susceptible to digital modes of fraud like identity theft that can result in loss of money.
• **User-friendly**. Usually every service is designed to reach the widest possible audience, so it has the intuitively understandable user interface. In addition, there is always the opportunity to submit a question to a support team, which often works 24/7.	• **Interoperability**. Usually the majority of electronic payment systems do not cooperate with each other.

Merits	Demerits
• **Convenience**. All the transfers can be performed at anytime, anywhere. It's enough to have an access to the Internet. • **Low commissions**. Low overheads of digital payments ensure that the commission is usually never more than 1 percent of the transacted value	• **The necessity of Internet access**. If Internet connection fails, you cannot get to your online account.

Stakeholders

Digital payment systems operate at a higher level of complexity and involve the interplay of technology, communications, specialized devices and specialized services. Typically a transaction is effected through the involvement of:

- ✓ Customers
- ✓ Vendors
- ✓ Banks (Account providers, card providers etc.)
- ✓ Internet Service Providers
- ✓ Gateway authenticators (Middlemen who provide gateways for making the payment)
- ✓ Device manufacturers
- ✓ Software providers
- ✓ Regulatory
- ✓ Authorities

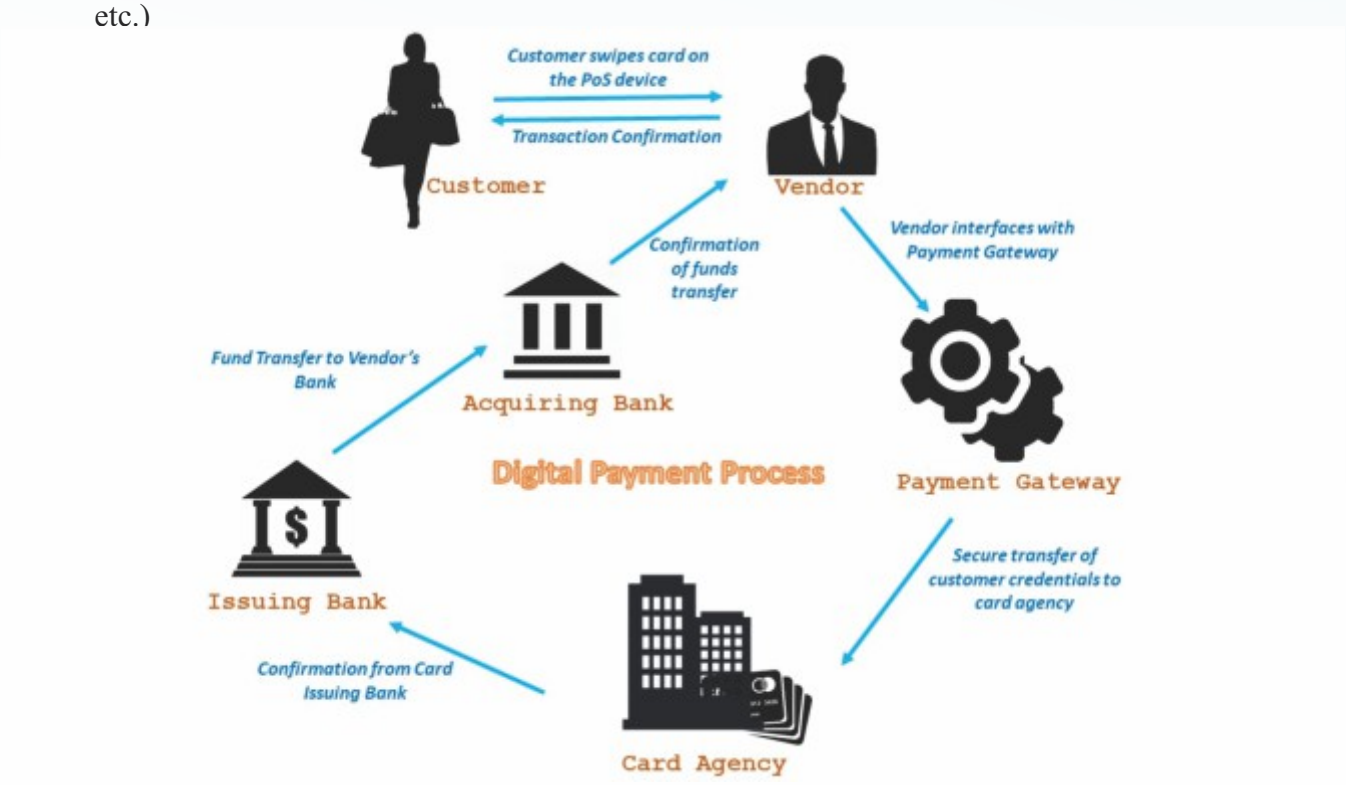


Figure 1: The Digital Payment Process

The system requires interfaces and communication channels between the customer (payer) to his bank (issuer), issuer to acquirer, and acquirer (merchant's bank) to the merchant. These channels and interfaces should enable the secure exchange of authentication and financial information between the participating banks/financial institutions. With greater sophistication the universe of threats has expanded and vulnerabilities exist at each step and interface. The following is a description of the main players involved in digital transactions, delivery channels and enabling technologies in the Indian scenario.

Payment Service Providers

Such channels are typically provided by intermediary players who go by the generic term of payment service providers. The following are the major roles under which financial services can be classified:

1. **Payment Gateway:** A payment gateway (PG) is an online application that conducts payment authorizations for merchants, securely connecting an e-Commerce application or in-house payment application to the internet banking portals of participating financial institutions. It encrypts authentication credentials of the customers' payment instrument as well as details of the purchase and routes the same to the merchants' banks for transaction authentication. PayU, PayUMoney, CCAvenue, EBS, DirecPay etc., are some of the PG options available in India.
2. **Payment Aggregator:** PG services provided to merchants involve the payment of fees (Transfer Development Rights – TDRs) for each transaction as a percent of the transaction value. The TDR can be reduced if the merchants can guarantee a substantial transaction volume. Payment aggregators are intermediaries that subscribe to a PG on behalf of a number of client companies. Since the aggregate transaction volume is high, it is possible to bring down TDR rates.

Delivery Channels

Digital payment systems have revolutionized the way funds are obtained and transferred. The huge inconvenience associated with carrying cash about, with the attendant threat of theft of money, the difficulties of safe custody, delivery to the rightful recipient and authenticity and validity of acknowledgement, particularly where intermediaries are involved where the major problems associated with hard cash. There was also the problem of limited traceability of transactions. The advent digital money has, in one go, resolved these issues and made monetary transactions convenient and transparent. The following are a few delivery channels of digital payments currently prevalent in India.

1. **Banking Cards (Debit/Credit Cards)**

Banking cards are Pre-paid Payment Instruments (PPIs) issued by banking institutions which offer the facility for purchase at stores (through Point of Sale (PoS) devices), and on the internet.

2. **Internet Banking**

It is an electronic payment system that enables customers of a bank or other financial institution to conduct financial transactions through the financial institution's website.

3. **Mobile Banking**

Mobile banking service is offered by banks or other financial institutions to enable customers to conduct financial transactions remotely using mobile devices. Each Bank/Financial institution which offers this service provides its own mobile banking application to be installed in the mobile device.

4. **Unstructured Supplementary Service Data (USSD)**

This is a service that facilitates mobile banking transactions using basic feature mobile phones which does not have internet data facility. Customers can dial a prescribed number on their mobile phone and transact through an interactive menu displayed on the mobile screen. Services include interbank account to account fund transfer, balance enquiry, mini statement etc.

5. **Aadhaar Enabled Payment System (AEPS)**

AEPS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using Aadhaar authentication.

6. **Mobile Wallets**

Mobile wallets are mobile phone applications that allow the customer to link his/her credit/debit card information to the mobile device, permitting the customer to use the mobile device for cash transactions instead of the cards.

7. **Micro ATMs/ Point-of-Sale (PoS) devices:** are devices that are connected to banks across the country, permitting even small scale merchants to instantly deposit or withdraw funds regardless of the bank associated with the merchant.

8. **Unified Payments Interface (UPI)**

UPI is a mobile payment interface developed by the National Payment Corporation of India, which provides access to multiple bank accounts from a single mobile application (of any participating bank) to enable seamless fund routing, merchant payments, peer-to-peer" collect requests etc.

9. **Bharat Interface for Money (BHIM):** BHIM is a mobile application that allows users to make payments using the UPI application. This also works in collaboration

with UPI and transactions can be carried out using a VPA. One can link his/her bank account with the BHIM interface easily. It is also possible to link multiple bank accounts. The BHIM app can be used by anyone who has a mobile number, debit card and a valid bank account. Money can be sent to different bank accounts, virtual addresses or to an Aadhaar number. There are also many banks that have collaborated with the NPCI and BHIM to allow customers to use this interface.

10. Enabling Technologies

Digital payments methods harness available technologies to provide greater convenience and simplicity of usage to users. Some of the newer forms of customer authentication and funds transfer are the following:

1. **Quick Response (QR) Codes:** This is a two dimensional matrix bar code that stores encoded information, which can be decoded using a QR Code scanner and associated application. QR decoding applications are now available as mobile apps, enabling the scanning of QR codes using the built-in mobile camera and decoding the same within the device. The encoded information may relate to product information, or even the website of the merchants payment gateway.
2. **Near Field Communication (NFC):** is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over an NFC compatible PoS device to send information without needing to touch the devices together or go through multiple steps setting up a connection.
3. **Authentication using wearables:** This is a technology related to the concept of internet of things (IoT). Customers can simplify the authentication process at a merchant store by tapping a piece of jewelry or wrist watch that carries the credentials and make payments without having to go through the steps of card swiping and pin entry.
4. **Biometric authentication:** It is also possible to harness biometric technology like face recognition to authenticate the customer and enable transfer of money to the merchant.

AUDIT PERSPECTIVE ON RISKS INVOLVED IN A DIGITAL TRANSACTION

While addressing the safety, security and transparency issues related to cash transactions, the digital payment systems, with its interplay of myriad intermediaries, protocols and technologies, come with a host of their own specific vulnerabilities. These range from the hazards associated with the technologies involved, inadequate regulation and availability of policy frameworks, often to a complete lack of awareness on the part of prospective users. Any attempt to promote digital transactions, therefore, need to be accompanied by a multipronged risk mitigation process involving policy development, regulation and customer awareness. Vulnerabilities confronting digital payment systems can be broadly classified as below:

RISKS		Mitigation Approach		
		User Awareness	Regulation	Merchant/PSP end control
1.	Perception and adaptability risks of lay users whose exposure to technology is limited (rural population, people from low income/education strata).	●		
2.	Lack of adequate grievance redressal mechanisms	●	●	●
3.	Though the transaction cost of a digital payment is typically low, for the lay user the convenience comes with the requirement of investment in smartphones, computers, internet connections etc.			
4.	Theft of identity, data etc. from the third party stakeholders may result in the loss of confidentiality and/or money for the customers and loss of credibility for the service provider.		●	●

5.	Weaknesses in specific regulations/laws covering various aspects of digital transactions that may not adequately provide for: 1. The legal structure for implementing an electronic signature law 2. The legal recognition of an electronic signature 3. The relationship among licensing, accreditation and limitation of liability 4. How technical standards interact with the law 5. Cross-border recognition		●	
6.	Susceptibility of payment systems to denial of service attacks, hacking and such cybercrimes.		●	●
7.	Delay in payment recognition on account of transaction failure after the amount is debited from the account.			●
8.	Lack of clearly defined boundaries in a digital transaction makes it difficult to fix the responsibility for failed transactions.		●	
9.	Instantaneous services pose a challenge for fraud countermeasures as the time span for analytical mechanisms dramatically decreases.			●
10.	Malicious QR Codes may lead the customer to make payments to the accounts of the perpetrator, or to phishing websites that steal their personal information or exploit their device itself.	●	●	
11.	Protocols adopted for communication of information might have weak encryption standards that are susceptible to interception and theft of data.		●	●
12.	Mobile applications that are on offer in app stores might carry malicious codes or back doors that could be exploited later to compromise the device or data.	●		
13.	Payment interface applications developed by third party vendors may contain security vulnerabilities that can be exploited by customers.		●	●
14.	The mobile device is susceptible to phishing attacks resulting in theft of identity and credentials.	●		
15.	Theft of credentials can also happen through malware attacking the mobile device.	●		
16.	SMS spoofing as part of social engineering to lure users to malicious websites.	●		
17.	Physical loss of digital devices like mobile phones may result in the information becoming available to malicious perpetrators.	●		

18.	Vulnerabilities in the code or configuration of mobile applications that are used for mobile banking can be exploited by malicious intruders.		●	●
19.	Fake mobile applications may be developed by malicious agents and made available in popular market places.	●		●
20.	IoT Devices lack the common standards in security like encryption, and are therefore more susceptible to malware, data theft and similar attacks than digital devices.	●	●	●

In fact these risks cannot be termed as static. They are dynamic risks as new challenges keep evolving with the advent of new technological innovations and communication protocols being developed.

The various laws and the regulatory frameworks act as a guidance mechanism and it is the internal control framework and constant monitoring of the payment mechanisms through audit, which will provide the assurance needed.

REGULATORY FRAMEWORKS

To keep up with the explosive pace at which the digital payment systems proliferated and spread in India, there has been a progressive development of policies, guidelines and rules that sought to regulate the main players and protect the interests of the customers. The following table summarizes the efforts on the part of the government and regulatory bodies in this direction during the past decade.

Timeline	Policy/ Regulation/ Guideline
December 2007	**The Payment and Settlement Systems Act, 2007** The Central Act was enacted to *provide for the regulation and supervision of payment systems in India and to designate the Reserve Bank of India as the authority for that purpose.* It can be looked upon as an early attempt to bring regulation to the activities of the main service providers of digital payment systems. Payment system was defined as a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. It includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations etc. The Act specified that no payment system should operate without the authorization issued by RBI. The RBI was empowered to conduct necessary enquiries before issue such authorization and to prescribe standards under which such systems should operate. It also laid down the rights and duties of system providers provided for settlement of disputes.

July 2013

National Cyber Security Policy, 2013

The GoI released the National Cyber Security Policy in July 2013 with a view to laying down the broad principles within which the cyber ecosystem of the country can be regulated and made secure for the use of the general public. The policy envisaged the creation of a National nodal agency to coordinate all matters of cyber security in the country, and to encourage organizations to designate a Chief Information Security Officer, develop IT policies and to commit adequate budgetary resources for implementing cyber security initiatives. It also provided for the creation of an assurance framework for designing security policies and ensuring adherence to global security standards and best practices.

The policy seeks to encourage use of open standards to facilitate interoperability among services. It provides for the creation of a regulatory framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space and to mandate periodic audit and evaluation of the security of the information infrastructure.

The National Level Computer Emergency Response Team (CERT-In) was envisaged as a nodal agency for coordination of cyber security efforts towards crisis management. To further the spread of e-Governance to all sections, the policy outlined the broad requirements of infrastructure, human resources, research and development, user awareness and the development of effective public private partnerships. The policy was sought to be operationalized through the promulgation of detailed guidelines and plans of action at various levels.

November 2016

Guidelines for Adoption of Electronic Payments & Receipts, MeitY, GoI

The guidelines were formulated to enable all government departments to collect and make payments in an electronic mode, against the back drop of the move to transfer the funds under central schemes directly to the beneficiaries (Direct Beneficiary Transfer – DBT).

The Digital India Program of the GoI aimed at providing electronic payment systems for all Government payments and receipts by 31 March 2016 and at least 90 percent of all payments and receipts to be made online by 31 December 2016. To achieve this, the Government Departments required a framework to engage with various payment service providers and actionable instructions to adopt modes of transaction for various services/ payment channels. The guideline sought to enable departments to expeditiously enable electronic payments and receipts leveraging all the payment channels.

The document attempted a categorization of services offered by departments on the basis of IT readiness with respect to payments integration, and brought out separate guidelines for Citizen/Business to Government, Government to Citizen/Business, between Government Departments, and Departments to employees.

Annexures to the document provide lists of licensed Payment Service Providers, white label ATM operators, authorized Prepaid Payment Instruments, payment aggregators etc.

December 2016

CERT-In Advisory (CIAD-2016-0069): Safeguarding Smart Phones against Cyber Attacks

The Indian Computer Emergency Response Team, MeitY, GoI, brings out advisory notes that outline the threat landscape associated with digital applications and suggest best practices for users. These are not regulatory in nature and are essentially steps in the direction of generating beneficiary awareness.

The present document sought to inform users about attack vectors like denial of service, cryptocurrency mining, mobile phishing and ransomware attacks associated with the use of Smart Phones and suggested best practices including use of passwords and encryption, avoiding following unknown web links, avoiding jail breaking and rooting of devices, avoiding unknown Wi-Fi networks, updating of OS and instructions on how to dispose off the device after use.

December 2016

CERT-In Advisory (CIAD-2016-0070): Securing Mobile Banking

This document identified threats to mobile banking like mobile banking malwares, Phishing/ SMiShing/ Vishing attacks, Jail broken or rooted devices, outdated operating systems and non-secure network connections. Suggested best practices included use of security software, strong passwords, not storing sensitive information on the mobile phone, reporting theft of devices immediately to the service provider, suggesting trusted sources for download of mobile banking applications

December 2016

CERT-In Advisory (CIAD-2016-0071): Mobile and Cloud Data Security

This advisory note reviewed the progressive migration of data to digital devices and to the cloud storage and processing systems and identified the steps to be taken to protect such data. The document recommended the use of multifactor authentication, authorization, access control methods in the mobile devices, along with encryption of data in storage as well as transit. It also advised use of Mobile Device Management (MDM) and Mobile Application Management (MAM) systems for monitoring, updating and configuring devices properly.

March 2017

Information Technology (Security of Prepaid Payment Instruments) Rules 2017, Draft

Under powers conferred by Sections 10 and 87 of the Information Technology Act, 2000, MeitY, GoI brought out the draft rules for security of PPIs and posted it for public comments. The rules are intended to ensure adequate integrity, security and confidentiality of electronic payments effected through prepaid payment instruments.

The Rules (draft) require every PPI issuer to develop an Information Security Policy and privacy policy, perform risk assessment, observe due diligence in the identification and authentication of customers and protecting their personal information. Personal information has been clearly defined and terms of its protection determined. The rules require the service providers to adopt end-to-end encryption for data exchange, ensure traceability of transactions at every step, retention of information, reporting of cyber incidents, customer education, grievance redressal and adoption of appropriate security standards

October 2017

Master Direction on Issuance and Operation of Prepaid Payment Instruments

These directions were issued by RBI in October 2017 and updated as on December 2017 for the purpose of providing a framework for authorization, regulation and supervision of PPI service providers in the country, to foster competition and encourage innovation in this segment while also ensuring safety and security of customers and to provide for interoperability among PPIs. The document lays down detailed procedures for application, authorization, deployment of money collected from customers, security and fraud prevention, grievance redressal, and audit of issuers of PPI instruments.

CONCLUSION

With the Government of India seeking to leverage a wide variety of payment channels for delivery of services, particularly scheme funds directly to the beneficiaries under the Direct Beneficiary Transfer program, it is necessary to develop assurance programs with a comprehensive as well as specific approach, to make an initial general review to be followed by a detailed evaluation of the particular aspects of the payment instrument/delivery channel. It has been attempted in the following programs to address the general and specific aspects of delivery through Prepaid Payment Instruments, focusing on compliance to existing regulations.

AUDIT PROGRAMS

A. Preliminary Assessment

Audit of digital payment systems adopted by a government/public sector body should involve a general review of issues related to organizational control, technology, security of communication channels and user/beneficiary awareness. The following audit checks may be exercised as a preliminary to a more detailed assessment on the basis of available standards and best practices.

1. **Organizational Issues:** Risk analysis, research, resource adequacy & monitoring
   a. Has the department made an assessment of the specific risks associated with the particular digital payment method adopted/ proposed to be adopted?
   b. Whether the risk assessment was carried out in a structured and documented manner?
   c. Whether the assessment is comprehensive and includes all known threat vectors?
   d. Whether a structured program of continuous research into emerging threats and mitigation measures established in the department?
   e. Whether available anti-malware solutions have been researched to identify the best possible solution to be distributed/recommended?
   f. Whether there is adequate administrative and financial commitment for adoption of mitigation measures?

g. Whether a system is established to log transactions, in line with available best practices/regulations?

h. Whether unusual patterns of use are defined and specific checks established to automatically monitor and report such transactions?

I. Has the department established a round the clock incidence response/ grievance redressal mechanism?

j. Whether adequate staff and resources have been assigned to the incidence response/ grievance redressal function?

k. Is the response time monitored and steps taken to ensure prompt and effective response?

2. **Technology:** Choice of solutions adopted, acquisition practices, secure SDLC

a. When a digital payment technology /platform is adopted/ recommended for adoption by users, a thorough scrutiny has been conducted to ensure that the same is free from backdoors, malicious codes etc.

b. Whether secure development practices have been adopted in development of the payment application?

c. Whether communication channels are secured by robust encryption methods?

3. **User/ beneficiary education and awareness**

a. Whether a dedicated program for beneficiary education established?

b. Whether each beneficiary is informed of the specific risks and mitigation measures at the time of enrollment?

c. Whether information is imparted in a simple and easy to understand manner, in the vernacular of the intended beneficiaries?

d. Whether continuous education through leaflets or other media effected?

e. Whether awareness of phishing and social engineering modes included in the continuous education program?

f. A mature appreciation of the threat landscape or alertness to the same cannot be expected of the entire beneficiary population. Hence it would be ideal to have adequate protection to the beneficiaries' money in the form of insurance coverage. In this context:

g. Are affordable insurance schemes covering loss of money due to digital threats conceived/made available to beneficiaries?

h. Are the terms of such insurance, if available, easy in a manner not to be an additional burden on his/her resources?

B. Audit of Pre-Paid Instruments – Detailed Compliance Testing

Prepaid Payment Instruments (PPI) is defined as payment instruments that facilitate purchase of goods and services, including funds transfer, against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card. The prepaid instruments can be issued as smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers and any such instrument which can be used to access the prepaid instrument.[1]

Prepaid instruments are broadly classified as[2]:

1. Closed System PPIs: issued by an entity for facilitating the purchase of goods and services from that entity only and do not permit cash withdrawal. As these instruments cannot be used for payments or settlement for third party services, the issuance and operation of such instruments is not classified as payment systems requiring approval/ authorization by the RBI.
2. Semi-closed System PPIs: these are used for purchase of goods and services, including financial services, remittance facilities etc., at a group of clearly identified merchant locations/ establishments which have a specific contract with the issuer (or contract through a payment aggregator/ payment gateway) to accept the PPIs as payment instruments. These instruments do not permit cash withdrawal, irrespective of whether they are issued by banks or non-banks
3. Open System PPIs: These PPIs are issued only by banks and are used at any merchant for purchase of goods and services, including financial services, remittance facilities etc. Banks issuing such PPIs shall also facilitate cash withdrawal at ATMs/ Point-of-Sale (PoS)/ Business Correspondents etc.

Two major steps in the development of a regulatory framework for effective control digital payment systems were the introduction of Master Direction on Issuance and Operation of Prepaid Payment Instruments (MDPPI) by RBI in October 2017 and the Department of Electronics and Information Technology, Government of India bringing out the Draft Rules for Security of Prepaid Payment Instruments (SPPI). These two documents, as discussed before, seek to build a regulatory framework that encourages competition and dynamism in the industry on the one hand and provides for customer protection on the other. An assurance framework for audit of a PPI instrument adopted for delivery of Government funds is proposed as below based on the tenets of the above documents. The relevant provision of the Master Direction (MDPPI) or Draft Rule (SPPI) is referenced against each audit question.

[1] Information Technology (Security of Prepaid Payment Instruments) Rules 2017 – Draft, Ministry of Electronics and Information Technology, Government of India

[2] Master Directions on Issuance and Operation of Prepaid Payment, Reserve Bank of India, October 2017

1. Eligibility, Approval & Authorization

S.No.	Audit Questions	Reference
1.	Banks: Whether the PPI issuer meets the eligibility criteria set by the regulatory department of RBI (for semi-closed and open system PPIs)?	MDPPI3.1
2.	Non-banking PPI issuer: Whether eligibility criteria for issue of semi-closed PPIs have been met?	MDPPI3.2
3.	Whether PPIs have been issued after obtaining proper approval from RBI?	MDPPI 3.1,3.2
4.	Whether the PPI Issuer has developed an information security policy for security of prepaid instruments operated by it?	SPPIRule 3
5.	Whether the issuer has adopted and published on its website and mobile applications, a privacy policy?	SPPIRule 4
6.	Whether terms and conditions for use is published in a simple language capable of being understood by a simple person?	SPPIRule 4
7.	Whether the privacy policy includes: a. Information collected directly from the customer and information collected otherwise? b. Uses of the information? c. Period of retention of the information? d. Purposes for which information can be disclosed and the recipients? e. Sharing of information with law enforcement agencies? f. Security practices and procedures? g. Name and contact details of grievance redressal officer and mechanism for such redressal?	SPPIRule 4
8.	Whether a risk assessment was carried out to identify the risks associated with the security of the payment system?	SPPIRule 5
9.	Whether adequate security measures are implemented to address the identified risks?	
10.	Whether the security measures are reviewed periodically?	
11.	Whether there has been any incident of security breach? If so, whether the security measures were reviewed in the light of the same and appropriate modifications carried out?	

2. Customer Protection & Grievance Redressal

S.No.	Audit Questions	Reference
12.	PPI issuers shall disclose all important terms and conditions in clear and simple language (preferably in English, Hindi and a local language) to the holder while issuing the Instrument including. All charges and fees associated with the use of the instrument Expiry period and related terms and conditions.	MDPPI 16.1
13.	Whether the issuer has put in place a formal, publicly disclosed customer grievance redressal framework?	MDPPI 16.2
14.	Whether a nodal officer for handling customer complaints designated?	MDPPI 16.2
15.	Whether escalation matrix and turn-around-times for complaint resolution clearly defined?	MDPPI 16.2
16.	Whether the complaint facility is clearly accessible? Through internet? Through mobile?	
17.	Whether a customer protection and grievance redressal policy is formulated, approved and disseminated to all users in clear and simple language (preferably in English, Hindi and a local language)?	MDPPI 16.2
18.	Whether customer care contact details (telephone numbers, email addresses and postal addresses) are available on website, mobile apps and cards?	MDPPI 16.2
19.	Whether the above contact details of nodal officers similarly made available?	MDPPI 16.2
20.	Whether PPI agents display proper signage of the PPI issuer and the above contact details?	MDPPI 16.2
21.	**Complaint tracking:** Whether complaint numbers are assigned and communicated to the complainants and facility to track the status of the same made available?	MDPPI 16.2
22.	Whether action is initiated preferably within 48 hours, and resolved not later than 30 days from the date of receipt of such grievance? **Audit Tests:** a Number of complaints b. Average initiation and resolution times of complaints c. Pattern of complaints – whether systemic causes of complaints are investigated and resolved through process re-engineering, adoption of proper security measures etc.	MDPPI 16.2

23.	Whether detailed list of authorized/designated agents are made available on the website/mobile app?	MDPPI 16.2
24.	Evaluate the adequacy, reach and effectiveness of the consumer awareness programs for secure use of the instruments, including a. Confidentiality of passwords b. Procedure to be followed in case of loss or theft of card or authentication data c. Procedure to be followed if any fraud/abuse is detected	MDPPI 16.3
25.	**Customer liability**: whether the amount and process of determining customer liability in case of unauthorized/ fraudulent use PPIs clearly outlined and disseminated to the customers?	MDPPI 16.4
26.	Whether the above process is in line with RBI (Department of Banking Regulation) circular DBR NO. Leg.BC.78/09.07.005/2017-18 dated 06/07/2017 on customer protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions?	
27.	**Account Statement:** Whether detailed account statement can be generated at least for the past 6 months? Whether transaction history for at least the last 10 transactions made available?	MDPPI 16.5
28.	**Report on Complaints and action taken status:** Whether quarterly returns in the required format is being submitted to the designated authority in a timely manner?	MDPPI 16.7
29.	**Transparency:** a. Whether uniformity of charges at agent level is ensured? b. Whether information on charges are disclosed and effectively disseminated? c. Whether contract with agents contain specific clauses to prohibit them from charging fees to customers directly for services rendered on behalf f the PPI issuer? d. Whether retail outlets/sub-agents are required to post a signage indicating their status as service providers for the PPI issuer? e. Whether a receipt is given for the fee collected from customers?	MDPPI 16.8
30.	Whether FAQs are displayed on the websites/mobile apps?	MDPPI 16.10

3. Information System Security

S.No.	Audit Questions	Reference
	Security Frameworks	
31.	Whether source code of key application systems have been subjected to source code audit to ensure the same is free from embedded fraudulent/ malicious code?	MDPPI 17.4
32.	If not whether an assurance has been obtained from application providers/ OEMs[3] to that effect?	MDPPI 17.4
33.	Whether Security Operations Centre (SOC) is established for centralized monitoring of security incidents?	MDPPI 17.4
34.	Whether server and mobile application level logs are integrated and a mechanism is established to monitor the same at the SOC?	MDPPI 17.4
35.	Whether a system is established to detect and log phishing attacks and rogue mobile apps?	MDPPI 17.4
36.	Whether the PPI issuer has subscribed to anti phishing and anti-rogue apps for protection against the above?	MDPPI 17.4
37.	Whether a risk based transaction monitoring/ surveillance process has been established?	
	IS Audit	
38.	Non-Banking Entity: Whether system audit, including cyber security audit is being done by a CERT-IN empaneled auditor annually?	MDPPI 17.1
39.	Whether the system audit report is submitted to the regional office of DPSS, RBI within two months of closure of every financial year?	MDPPI 17.1

[3] Original Equipment Manufacturer

40.	Whether such audit has covered: **a.** Effectiveness of security control design (Test of Design-ToD)? **b.** Operating effectiveness (Test of Operating Effectiveness-ToE)? **c.** Adequacy of deployed technology for safe, secure and efficient operation? **d.** Evaluation of hardware structure, operating systems and key application systems? **e.** Access controls on key applications? **f.** Disaster recovery planning? **g.** Training of staff managing systems and applications? **h.** Documentation? **i.** Adequacy of information security governance? **j.** Adherence to best practices in application security lifecycle, patch/vulnerability and change management? **k.** Adherence to process flow approved by RBI?	MDPPI 17.3

Sneak Peak

1. Tokenization

Tokenization is emerging as an important

technology to secure mobile payments, according to industry experts. Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information without compromising on security.

In the payments space, tokenization is the process of replacing the 16-digit payment card account number with a unique digital token in mobile and online transactions. In the payment card industry, it can be used for mobile payments. For example, payments using mobile wallets. Tokenization could also be enabled to work with different technologies, and has been extensively used in contactless payment applications such as magnetic technology in the case of Samsung Pay, NFC (near-field communication) in the case of Apple Pay and Android Pay, and sound-based technology of ToneTag. "If a cardholder decides to add their personal account number to a mobile device or digital wallet, Visa will issue a token behind the scenes. Then when the Visa account holder initiates transactions with mobile devices using their digital account number, the token, and not the primary account number, will be used to process the transaction, just like a traditional card payment."

Tokenization is a new layer of security for digital payments without adding friction to the shopping experience. It does not require merchants to make major changes to their current payment acceptance systems. The biggest benefit to all involved is that payment card numbers are no longer used or saved where unauthorized access can occur.

For customers, this means added security and convenience. It eliminates the need to enter and re-enter the account number when shopping on a smartphone, tablet or computer.

It is safer than magnetic strips because tokens don't carry the consumer's primary account number, there is less risk in storing tokens on mobile devices online by e-Commerce merchants, and in cloud-based mobile platforms and applications. Even if it is hacked, there wouldn't be anything of use as it devalues the entire data.

REFERENCE

https://www.livemint.com/Industry/9yWh8YCOEAhh6M9Af39kOJ/How-tokenization-secures-digital-payments.html

2. One travel card for public transport across India

India will shortly unveil a one-nation-one-card policy for public transport that will bring seamless connectivity between various modes of transport, NITI Aayog.

A robust transportation sector was the backbone for the development of any economy, especially for a densely populated developing country like India, and the focus of the nation's mobility strategy was on sustainable modes of public transport, transport-oriented planning and digitization.

As India looks out for possible alternatives, four technology-driven trends - electrification, shared mobility, connectivity and autonomous driving - are leading the automotive industry.

"The focus of our mobility strategy is on sustainable modes of public transport, transport oriented planning, digitisation, among others. The objective of the strategy is to plan for the citizens of India first, rather than focussing on vehicles alone, by providing sustainable mobility and accessibility by switching to a cleaner mode of transportation such as electric, ethanol, methanol, CNG , LNG and hydrogen fuel cells. For India to build a robust mobility ecosystem, it is important to develop automobile manufacturing, manufacturing of storage batteries in India, promoting the mobility change in the app–based aggregators, infrastructure and integration of mobility with renewable energy.

REFERENCE

https://www.business-standard.com/article/economy-policy/india-to-soon-have-london-like-one-nation-one-card-policy-for-transport-118090300664_1.html

3. Digi-Dhan Vyapar Yojana

Following demonetization, the government has been trying to encourage people to embrace cashless transactions. However, since it is still not a popular practice in India, the NITI Aayog or National Institution for Transforming India, has devised a way to provide the right incentives to the people in order to encourage digital transactions.

For this, the NITI Aayog has announced that it will be introducing a lottery system where digital payment makers are eligible to earn prizes on a daily and weekly basis. The rewards being offered are quite substantial and the offer is open not only to consumers but also merchants. One of the schemes which the NITI Aayog has announced these rewards under is the

Digi-Dhan Vyapar Yojana (DDVY) which is specially meant for merchants.

Features of Digi-Dhan Vyapar Yojana

- The Digi-Dhan Vyapar Yojana is meant for merchants who can take part in the daily and weekly lottery.
- Merchants will be eligible to participate in this Yojana when they carry out transactions between the range of Rs. 50 and upto Rs. 3,000.
- The focus group for the Digi-Dhan Vyapar Yojana is mainly small businesses.
- The DDV scheme has been implemented by NPCI or the National Payments Corporation of India.

- Transactions made via UPI (Unified Payments Interface), USSD, AEPS (Aadhaar Enabled Payment System) and RuPay cards will be eligible for participation under this scheme.
- Digital transactions done using personal debit cards, credit cards, e-Wallets (Paytm, Freecharge, Mobikwik, etc.) will not be eligible for participation in the draw.

REFERENCE

https://www.bankbazaar.com/saving-schemes/digi-dhan-vyapar-yojana.html?ck=Y%2BziX71XnZjIM9ZwEflsyDYlRL7gaN4W0xhuJSr9Iq7aMYwRm2IPACTQB2XBBtGG&rc=1

4. Face Recognisation in Aadhar (UIDAI)

The Unique Identification Authority of India's (UIDAI) has announced a new measure that seeks to mandate facial recognition - by taking on-the-spot live pictures - for every authentication that requires Aadhaar. Services that most commonly require Aadhaar authentication include banks, the public distribution system and issuance of a mobile SIM card, new as well as replacements.

The authority tasked with issuing the 12-digit biometric number finally announced a phased rollout of the feature, starting with telecom service providers from September 15. The plan was to implement it by the previous deadline of August 1 that had failed due to the non-readiness of some device providers.

An individual would seek authentication based on Aadhaar, the authorised machine/device being used for the purpose would also capture a picture of the face of the individual.The photo, along with the fingerprint or iris scan, would be sent to UIDAI, which will verify the details on its database, and thereafter send a confirmation of the authenticity of the individual based on the above. The authentication process is very sophisticated and will not be impacted by changes to a person's face, say, growing a beard.

The live face photo capture and its verification with the photo obtained in eKYC will be essential where Aadhaar is used for issuance of SIMs. For authentication agencies other than TSPs, the body said specific instructions will be issued on implementing this new feature but did not specify a fresh deadline.

UIDAI, the measure is being used to provide an added security layer, while also making the Aadhaar process more inclusive while curbing the possibility of fingerprint spoofing or cloning. There have been numerous instances where people have been excluded from Aadhaar authentication as their fingerprints are worn out due to old age, or since they are involved in manual labour or agriculture. The use of facial recognition will help include such people in the Aadhaar authentication process.

REFERENCE

https://timesofindia.indiatimes.com/india/face-recognition-to-be-must-for-all-aadhaar-authentications/articleshow/65522828.cms

App Watch

1. Mother and Child Tracking System (MCTS)

Mother and Child Tracking System (MCTS) is an initiative of Ministry of Health & Family Welfare to leverage information technology for ensuring delivery of full spectrum of healthcare and immunization services to pregnant women and children up to 5 years of age. It is an innovative, web-based application, developed by NIC, to facilitate and monitor service delivery as well as to establish a two way communication between the service providers and beneficiaries. Generation of work plans of ANMs (Auxiliary Nurses Midwifery), sending regular alerts to the service providers as well as beneficiaries about the services due and a user-friendly dash board for health managers at various levels to monitor delivery of services will go a long way in ensuring quality service delivery, micro birth planning, ensuring universal immunization and will have positive impact on important health indicators like Infant Mortality Rate and Maternal Mortality Ratio. It will also help in evidence based planning and continuous assessment of service delivery to pregnant women and children.

REFERENCE

http://apps.nic.in/apps/government/mother-and-child-tracking-system-mcts

2. e-Granthalaya:

A Digital Agenda for Library Automation and Networking. It consist of Library Management Software for computerization of Government Libraries. The software provides Web based Data Entry solution to the libraries. The software generates e-Catalogs of library documents and provides various kinds of online services to the Library members. The Application is available at NIC Cloud for online utilization by registered libraries. It works with Library automation, Library management Software and Digital library.

SOURCE

Times of India

http://itoons.in/2018/08/10/comic-parked/

The following are the features of the e-Granthalaya

Computerization of Government Libraries

The software provides GUI for the library staff who can enter books catalog details and details of members.

Cataloging Service

Under the Service, software provides solutions to add data for books and other resources with other facilities like Stock Verification, Barcode Generation Facility, etc.

Circulation Service

Under this service, software provides facility for issue/return of the books along with Member Registration, etc.

Serials Control Service

Under the service, serials and magazine subscription is managed.

Catalog Access Service

e-Granthalaya provides an independent browser based GUI for searching the library catalog by the library members.

REFERENCE

http://apps.nic.in/apps/government/e-granthalaya-digital-agenda-library-automation-and-networking

1. DigiLocker

Targeted at the idea of paperless governance, DigiLocker is a platform for issuance and verification of documents & certificates in a digital way, thus eliminating the use of physical documents. Indian citizens who sign up for a DigiLocker account get a dedicated cloud storage space that is linked to their Aadhaar (UIDAI) number. Organizations that are registered with Digital Locker can push electronic copies of documents and certificates (e.g. driving license, Voter ID, School certificates) directly into citizens' lockers. Citizens can also upload scanned copies of their legacy documents in their accounts. These legacy documents can be electronically signed using the eSign facility.

The platform has the following benefits:

Citizens can access their digital documents anytime, anywhere and share it online. This is convenient and time saving.

It reduces the administrative overhead of Government departments by minimizing the use of paper.

Digital Locker makes it easier to validate the authenticity of documents as they are issued directly by the registered issuers.

Self-uploaded documents can be digitally signed using the eSign facility (which is similar to the process of self-attestation).

The following are the key stakeholders in the DigiLocker system:

Issuer: Entity issuing e-Documents to individuals in a standard format and making them electronically available e.g. CBSE, Registrar Office, Income Tax department, etc.

Requester: Entity requesting secure access to a particular e-Document stored within a repository (e.g. University, Passport Office, Regional Transport Office, etc.)

Resident: An individual who uses the Digital Locker service based on Aadhaar number.

The main technology components of the DigiLocker system are:

Repository: Collection of e-Documents that is exposed via standard APIs for secure, real-time access.

Access Gateway: Secure online mechanism for requesters to access e-Documents from various repositories in real-time using URI (Uniform Resource Indicator).

DigiLocker Portal: Dedicated cloud based personal storage space, linked to each resident's Aadhaar for storing e-Documents, or URIs of e-Documents.

REFERENCE

https://digilocker.gov.in/about.php

SOURCE

http://www.martybucella.com/C50.gif

QUIZ

Try this Out

1. Which of the following technique is used for identifying individuals uniquely?
   a. Phishing
   b. RFID (Radio frequency identification)
   c. Hacking
   d. Biometric identification

2. What is the key activity in phase 1 of e-Government project life cycle?
   a. define clear vision & objectives
   b. needs assessment
   c. All of these
   d. prioritization of services

3. An organization's ability to tailor its products and services to its customers is referred as _____.
   a. Adaption
   b. Mass customization
   c. Target commerce or T-commerce
   d. Specialization

4. What is not an key activity in phase 2 of e-Government project life cycle
   a. None of these
   b. assessment of business services
   c. assessment of business functions
   d. prioritization of services

5. What is the key factor responsible for success of an e-Government project?
   a. Defining clear and measurable project goals
   b. All of these
   c. Adequate resources
   d. Adequate time

6. What model does electronic payment of customs duty by Customs department, refer to
   a. G2B
   b. B2B
   c. B2C
   d. B2G

7. Which institution was set up by Government of India to catalyse e-Governance activities
   a. FICCI
   b. NASSCOM
   c. MIT
   d. NIC

8. What does sustainability class consists, as per EAF model
   a. Commercial sustainability
   b. Legal sustainability
   c. Organisational sustainability
   d. All of these

9. What does the term CSC expand to under NeGP
   a. Certified Services Centre
   b. Common Services Centre
   c. Commercial Services Centre
   d. Central Services Centre

10. What does the term IaaS expand to
    a. Illegal land removal as an Service
    b. Ideation as an Service
    c. Infrastructure as a Service
    d. Illiteracy removal as an Service

11. Which interaction model refers to the usage of electronic means between public and government?
    a. All of these
    b. G2C
    c. G2G
    d. G2B

12. What forms the core of e-Governance implementation
    a. Network
    b. Database
    c. e-MIS
    d. Regulations

13. Which domain does MCA 21 e-Governance project focus upon
    a. Immigration
    b. Pension
    c. Passport
    d. Corporate Affairs

14. What is not a key activity in phase 2 of e-Government project life cycle
    a. prioritization of services
    b. assessment of business services
    c. None of these
    d. assessment of business functions

15. What monetary limit implies an open tender?
    a. Above or equal to 10 lakh
    b. Above or equal to 5 lakh
    c. Above or equal to 25 lakh
    d. Above or equal to 15 lakh

16. By security in e-Commerce we mean
    i. Protecting an organization's data resource from unauthorized access
    ii. Preventing disasters from happening
    iii. Authenticating messages received by an organization
    iv. Protecting messages sent on the internet from being read and understood by unauthorized persons/organizations
    a. I, ii
    b. ii, iii
    c. iii, iv
    d. i, iii, iv

17. Which portal has been created which will serve as the National Digital Infrastructure for Teachers?
    a. Margdarshan
    b. Diksha Portal
    c. Shikshak
    d. None

18. What is the name of the platform that is launched to enable women employees to file complaints related to sexual harassment at the work place?
    a. e-Harassment portal
    b. She-box portal
    c. e-shikayat portal
    d. None

19. e-Learning technology based on
    a. Video Conferencing technology
    b. Streaming audio & video
    c. Computer based training
    d. All of the above

20. _____is the process of buying, selling or exchanging products, services & information via computer net works

a. e-Business
b. e-Commerce
c. e-Governance
d. e-Education

**Answers will be published in next issue of the Journal.

Answers to the Quiz published in previous issue of Journal (May 2018 issue)

Q.No.	Answer	Q.No.	Answer
1.	D	9.	D
2.	D	10.	D
3.	C	11.	D
4.	D	12.	B
5.	A	13.	C
6.	D	14.	D
7.	C	15.	C
8.	B		

SOURCE

Cartoonist(s): Dave Coverly

Comic/Cartoon: Speed Bump

http://www.thecomicstrips.com/store/add.php?iid=134814

Update Corner

Li-Fi

Li-Fi is a technology for wireless communication between devices using light to transmit data and position. Li-Fi stands for Light Fidelity and is a Visible Light Communications (VLC) system which runs wireless communications that travel at very high speeds. With Li-Fi, your light bulb is essentially your router. It uses common household LED light bulbs to enable data transfer, boasting speeds of up to 224 gigabits per second. Li-Fi and Wi-Fi are quite similar as both transmit data electromagnetically.

However, Wi-Fi uses radio waves, while Li-Fi runs on visible light waves.

It is predicted that future home and building automation will be highly dependent on the Li-Fi technology for being secure and fast. As light cannot penetrate through walls, the signal cannot be hacked from a remote location, making it secure.

REFERENCE

https://en.wikipedia.org/wiki/Li-Fi

Wireless Charging Technology

Wireless charging uses an electromagnetic field to transfer energy between two objects through electromagetic induction. This technology is based on initial works of electricity pioneer Nikola Tesla. Tesla worked on the magnetic resonant coupling – the ability to transmit electricity through the air by creating a magnetic field between two circuits, a transmitter and a receiver.

Today, the field is witnessing a revolution, with nearly a half dozen wireless charging technologies in use, all aimed at cutting cables to everything from smartphones, laptops to kitchen appliances and cars.

Wireless charging is making inroads in the healthcare, automotive and manufacturing industries because it offers the promise of increased mobility and advances that could allow tiny internet of things (IoT) devices to get power many feet away from a charger.

REFERENCE

https://en.wikipedia.org/wiki/Inductive_charging

3D Printing

3D printing or additive manufacturing is a process that builds layers to create three dimensional solid objects from a digital file/model. 3D printing is a method of creating physical 3D models of objects using a series of additive or layered material in succession to create a complete 3D object.

3D printing helps in manufacturing complex 3D shapes using less material than traditional manufacturing methods. The 3D printing process is completed by segregating the 'graphical data input' into separate object layers. The layered graphical data is sent to the 3D printer, which prints layer by layer, using appropriate material for each layer, until the 3D object is completely printed.

SOURCE

https://www.facebook.com/IIC4u/photos/pcb.1015602
4892663403/10156024891923403/?type=3&theater

e-Panchayat: A Tool for Empowering Panchayati Raj

- Sh. Jugal Kumar Verma

Sh. Jugal Kumar Verma has over 4 years of experience in auditing public sector organizations. He did his Bachelor of Engineering in Electronics and Telecommunication. His areas of expertise are electronics switching components and Radio frequency communications.

Abstract

The Ministry of Panchayati Raj (MoPR) has undertaken e-Panchayat Mission Mode Project (e-Panchayat MMP) with a view to introduce and strengthen e-Governance in Panchayati Raj Institutions (PRIs) across the country and build associated capacities of the PRIs for effective adoption of the e-Governance initiative.

Introduction

"Panchayati Raj" is a South Asian political system mainly noticed in India, Pakistan, Bangladesh and Nepal. It is the oldest system of local government in the Indian subcontinent. The word "Panchayat" literally means "assembly of five wise and respected elders" chosen and accepted by the local community. The local governance system was given constitutional authority by way of the 73rd and 74th constitutional amendments. The importance of local governance system has been on the rise, ever since.

The vast majority of India's population lives in the villages and the Panchayats (Village level governance units also known as Panchayati Raj Institutions (PRIs) represent the face of the governance for these villagers. The PRIs include approximate 2 lakh 38 thousand Gram Panchayat under Ministry of Panchayati Raj (MoPR), Government of India (GOI).

Background of e-Panchayat:

The seventh Round Table conference of State Ministers of Panchayati Raj, organized by the Ministry of Panchayati Raj (MoPR) held at Jaipur in December 2004 recommended taking e-Governance in Panchayati Raj Institutions (e-PRI) as mission mode through NIC and other solution providers. The MMP aimed at overcoming the challenges being faced in the villages such as lack of reliable communication infrastructure, delay in providing basic services to the citizens (Licenses, Certificate etc.), low revenue mobilization for implementing schemes at the Gram Panchayat Level and lack of monitoring mechanism for schemes.

Subsequently National e-Governance Plan identified e-Panchayats as one of the Mission Mode Projects (MMP) which aims at computerization of Gram Panchayats developed after a detailed system study by NIC and prioritized the functions to be automated in shape of 12 applications. Ramchandrapuram village near Hyderabad, has become India's first e-Panchayat, enabling villagers to settle disputes through an express web-enabled system.

Objectives of e-Panchayat:

The key objectives of e-Panchayat Mission Mode Project are to use ICT (Information Communication Technology) for:

- Automation of internal workflow processes of Panchayats
- Improving the delivery of services to citizens
- Capacity building of Panchayat Representatives and Officials
- Social Audit
- Transparency, Accountability, Efficiency and RTI compliance of Panchayats
- Improving governance of local self-government.
- Use of IT for electronic tagging and tracking of funds transferred to Panchayats from higher level of governments, including rapid bank transfer of funds, tracking fund transfers to, expenditures of the Panchayats.
- Improving internal management processes and decision making in Panchayats.

Illustration:

Governments at both the Central and State levels have the vision and strategies to bridge the digital divide and provide supporting infrastructure in rural areas to enhance the capacity of Panchayats. ActionSoft is one of the applications available under e-Panchayat Mission Mode Project. The application facilitates reporting of physical and financial progress of the activities included in the Action Plan(s) of the Rural Local Bodies (RLBs) and Urban Local Bodies (ULBs). The progress of the activities undertaken by the RLBs and ULBs, utilizing various Central/ State specific schemes and/ or other sources of funds can be monitored through ActionSoft.

Key Challenges in e-Panchayat

The key challenges being faced for implementation of computerization in Panchayats include the following:

- **High Capacity Building:** No Back-end support at all levels of PRIs/PR Departments for operationalising/ computerization of services.

- **No Centralized decision support system:** (MIS) for monitoring the schemes and taking informed decisions.

- **Lack of adequate infrastructure and Manpower**: The adequate infrastructure and manpower is unavailable and is absent at all levels.

- **Geographical problems:** Corporate networks reside on reliable and controlled networks. Government networks have to go into all areas which are even unfriendly to live. It is, however, costly to wire up all the villages in the country. So, e-Panchayat systems need to use the wireless systems like satellite networks to ensure the availability of applications into rural and remote areas irrespective of the geographical issues.

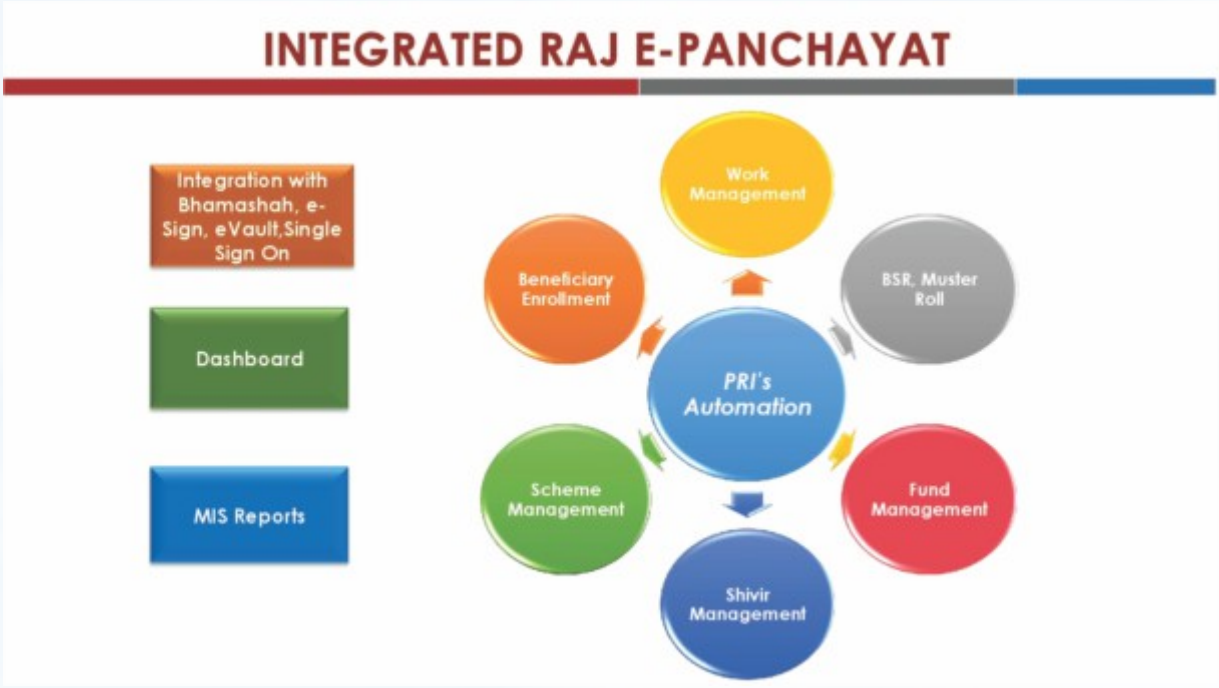
- **Privacy and Security:** A critical obstacle in implementing e-Panchayat is the privacy and security of an individual's personal data that he/she provides to obtain government services. Measures should be taken to protect the sensitive personal data of the people stored or used in these projects. Lack of effective security standards limits the growth of various e-Panchayat services that contain personal information.

- **Hesitation to change:** Humans are always reluctant to change. Now e-Panchayat also means change of the existing system of manual working to computerized systems, which are generally disapproved by the employees. People generally dislike it as they need to learn new things in it for which they need to give in more time and effort.

- **Literacy/ Level of Education:** Most Gram (village) Panchayat representatives and villagers are not computer-literate; even a simple computer application would be difficult to handle for them

- .**Local Language content creation:** Content creation in the local language is another challenge. English is still an alien language in rural areas.

Process of e-Panchayat as MMP under e-Goverance



The process of e-Governance has already been started. The Government of India has decided to open one lakh common services centers across the country under National e-Government Plan (NeGP) in order to make all Government services accessible to the common man in his locality, and ensure efficiency, transparency and reliability of such services at affordable costs to realise the basic needs of the common man. Now the Government of India has initiated the process to equip all Gram Panchayats with computers, or provide access to computers with broadband connectivity. All Panchayats at all levels need to be equipped with computing hardware and connectivity over the next few years. The approach would be to first use the kiosks being set up under the NeGP's Common Services Centres (CSCs) initiative. For the remaining Panchayats, it is proposed to engage independent service providers who would be selected on the basis of a bidding process. It has also been planned to equip all Panchayats with necessary software and skills to handle e-Governance for better delivery of services to citizens. The other major component of e-Panchayats would be that of capacity building of functionaries of Panchayati Raj Institutions.

The infrastructure that is proposed to be created through e-PRI would be utilised for training of elected representatives about their responsibilities and for giving them functional knowledge of the schemes that are implemented through the Panchayats or their statutory committees.

How e-Panchayat works?

The Government of India's ambitious Digital India Programme encompasses implementation of new ideas, innovative solutions and making technology central to the governance. For effective adoption of the e-Panchayat at PRIs, Panchayat Enterprise Suite (PES) has been developed and conceptualized by NIC which comprises 12 Core Common applications to operationalize the e-Panchayat.

Panchayat Enterprise Suite (PES)

At present, Panchayat Enterprise Suite has been deployed/operational with 11 Core Common Applications and GIS layer module is under conceptualisation, as detailed below:

a) Local Government Directory: Captures all details of local governments and assigns a unique code to the Panchayats. It also maps Panchayats with Assembly and Parliamentary Constituencies.

b) Area Profiler: Captures geographic, demographic, infrastructural, socio-economic and natural resources profile of a village/panchayat.

c) PlanPlus: Helps Panchayats, Urban Local Bodies and line departments in preparing Perspective, Annual and Action Plan.

d) PriaSoft: Captures receipt & expenditure details through voucher entries and automatically generates cash book, registers, etc.

e) ActionSoft: Facilitates monitoring of physical & financial outcomes/outputs under various Programmes.

f) National Asset Directory: Captures details of assets created/maintained; helps avoid duplication of works

g) Service Plus: A dynamic metadata-based service delivery portal to help in providing electronic delivery of all services in all States.

h) Social Audit: Captures details of statutory meetings held at ZP/BP/GP levels and prepares reports for social audit.

i) Training and National Panchayat Portal: Portal to address training needs of stakeholders including citizens, their feedback, training materials etc.

j) National Panchayat Portal: Dynamic Web site for each Panchayat to share information in public domain.

k) Geographic Information System: A spatial layer to view all data generated by all Applications on a GIS map.

l) Audit Online: Audit Online aims to facilitate audit of Government Institutions online.

Audit Online

Audit Online is one of the generic and open source applications developed as a part of Panchayat Enterprise Suite (PES) under e-Panchayat Mission Mode Project (MMP) initiated by the Ministry of Panchayati Raj (MoPR). Audit Online facilitates the financial audit of accounts at all the three levels of Panchayats viz. District, Block and Village Panchayats, Urban Local Bodies (ULB) and Line department by Auditors (State AG/Local Fund Auditor). Audit Online facilitates recording details for both Internal and External Audits as per the defined process. The software not only facilitates the online and offline audit of accounts but also serves the purpose of maintaining the past audit records of the auditee with associated list of the auditors and audit team involved in the audit and acts as a good financial audit tool and improves transparency & accountability. Also the information is available in public domain and for usage by other PES application.

Audit of PriaSoft in Tamilnadu, 2016:-

Panchayati Raj Institutions Accounting Software (PRIA Soft) was developed by National Informatics Centre (NIC) in 2009 to establish centralised accounting software for use by all the three tiers of PRIs.

Performance Audit on "IT support to Panchayat Accounts including Accounting of Major Schemes" revealed the following:

- Hardware procured for Rs. 10.98 crore was not put to use for the intended purpose resulting in blocking up of capital.
- Training in PRIA Soft was not fully imparted and data were not entered in all the formats prescribed by the Comptroller and Auditor General of India.
- Data entry work was outsourced in contravention to the instructions.
- Multiple nomenclatures were used for single Object Head resulting in incorrect generation of Annual Receipt and Payment Accounts and Ledger Accounts.
- Inadequate input control resulted in duplicate bank accounts numbers.
- Receipts and expenditure were incorrectly classified in PRIA Soft.
- Receipts and expenditure incurred by District Rural Development Agencies for PRIs were not accounted for in PRIA Soft since receipts and expenditure Heads of Accounts were incorrectly operated in PRIA Soft.
- There were multiple users for same login id and password.

- Fake vouchers were entered and cash book in PRIA Soft was not reconciled with the pass books of bank, post office or treasury. While PRIA Soft was stated to be fully implemented, the accounts produced by PRIA Soft were not the system of record.

Conclusion:

e-Panchayat is the need of the hour as people in rural areas are still deprived of basic facilities for a decent life. Common wisdom says that poverty and deprivation exist not only due to lack of resources but also persist because of inefficient and malfunctioning institutions. In the emerging knowledge society and information revolution, Panchayats should not be left in isolation. They should be provided with adequate technological resources in order to be able to play a meaningful role in the course of development.

States should enhance Gram Sabha powers to make them effective instruments of participatory decision-making and ensuring accountability of PRIs in local development planning. IT is going to play a very important role in this futuristic devolution of powers.

REFERENCES

http://www.panchayat.gov.in

http://www.panchayat.gov.in/documents/10198/59543/USQ%201863.pdf

http://www.ijritcc.org/download/browse/Volume_5_Issues/June_17_Volume_5_Issue_6/1497342687_13-06-2017.pdf

http://meity.gov.in/about-meity/functions-of-meity

http://panchayatonline.gov.in/viewPESHome.do

http://auditonline.gov.in/

https://en.wikipedia.org/wiki/Panchayati_raj

http://www.panchayat.gov.in/documents/10198/0/06.PRIASOFT%20-%20AUDIT%20APPLICATION%20-%20NIC.pdf

CAG as an Enabler for Government

- Ms. S. Vijayavanitha

Professor Vijayavanitha Sankarapandian, CISA, CIA is a professor of finance at Manipal University, (Bangalore, India). Prior to this, she served as resident audit officer in the office of the Comptroller and Auditor General (CAG) of India where she handled finance and IT audits of large government enterprises for nearly two decades. Some of her significant audit findings were tabled at the Parliament of India. She has been an active committee member of ISACA Bangalore, Chapter, India, for the last two years. She is also a member of The Institute of Internal Auditors.

Introduction:

e-Governance has been picking up more prominence and importance for any government of the world, today. In this era of digitization, not only for the purpose of the faster development and growth, but also due to its inherent quality of high transparency, low cost, reduced corruption, better security, interoperability, accessibility, trustworthiness, standardization and host of other benefits that bring to the governments that wants to serve people of their country are opting for e-Governance.

However, there is no guarantee that e-Governance projects will progress as expected within the stipulated budget and timeframe, unless these are well monitored and nurtured from time to time. This is where the need arises for an agency which can help the government in achieving its objectives that it set out, through the various government companies and corporations, by continuously evaluating, monitoring and reporting on them, at the minimum, to the government. This agency role can be played by the CAG, as it will transform it, to be an enabler role for the government, to its existing auditing role.

Why CAG -The Enabler:

CAG, being Supreme Audit Institution (SAI) of India has the mandate to audit the public sector, which can be utilized further to convert itself from an audit institution to be an Enabler for the government. CAG knows the public sector capability, weakness and strength more than any other external agency or the government, as it has been working with them closely and is well aware of public sector's financial, compliance and its performance status. Who else can be better suited other than CAG to play the role of the Enabler in giving the government required inputs on the public sector and working with public sector to have it aligned to government direction and objective?

In order to sustain the ecosystem of e-Governance, it is very important that the enabler role is played fulltime by the governance team in each and every organization to sustain and evolve with the development of technology and the needs of the future.

Technology is playing a major role currently and will be so in the future. However, for the technology and process to be successful and sustained, it is important that right people govern these ecosystems.

Enabler Model:

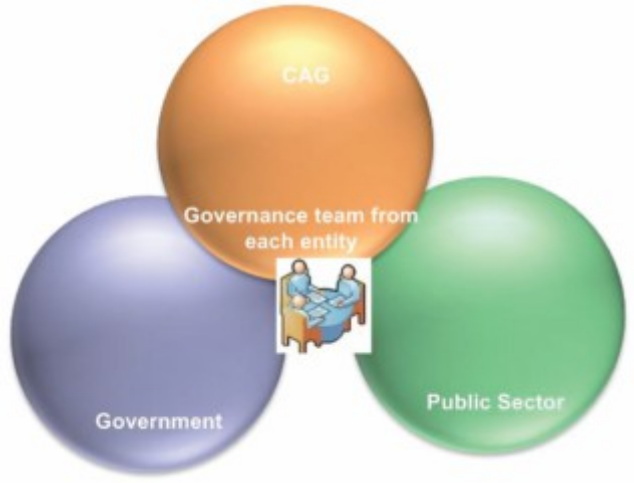
The enabler model will continue to include the existing roles and responsibilities in the three main types of audit being carried out by CAG, financial, compliance and performance audit. Enabler or Alignment audit, will be the new addition to dawn the role of enabler and will be a direct reporting engagement.

In IT (Amendment) Act 2008/2011, all organization that are handling information are recommended to get themselves ISO IS/ISO/IEC 27001 certified, by a government approved, independent auditor. Government is coming out with personal data protection bill and many supporting policies to strengthen the digital platform. In this direction, their priorities for public infrastructure (e-Kranti) is to use cloud by default, offer integrated services, and follow the industry standard standards and protocols. All this will soon lead to providing a platform for the merging of many IT and security areas and their responsibility. It would not be a surprise, if CAG would have to do only attestation engagement in the compliance and performance audit, in the future.

Advancement in the information, communication and technology has brought the otherwise disparate government departments together and much closer than ever before leading to consolidation, inter-operability and sharing of information and data with each other thereby making the e-Governance a must in all public sectors at the minimum possible, at all the levels of operations.

Government should be the role model by incorporating a governance model, which will sustain and evolve with the desired ecosystem for digital transformation in the country for the future. In order to establish alignment of the government direction and objectives, it is necessary that a dedicated governance team is established for its purpose within each of them, government, the public sectors and the CAG.

A simple representation (Figure) of the same is shown below:



Goverance model for Enabler Model

This governance team will be primarily responsible for evaluation, monitoring and reporting, as required on the alignment to the direction, objectives and requirements of the present day government.

Governance teams will have to be empowered appropriately to perform their roles and their roles are properly scoped and objectives are well-defined. The governance team will be responsible for the governance as appropriate to their respective organization, primarily alignment with government for Public sector governance team, setting of direction and objectives by the government governance team and CAG governance team will ensure that the alignment is set, metric for measurement of alignment and periodic monitoring of performance against it, by auditing/compliance review and then reporting to the government through CAG the governance team required in each of the entity.

Enabler Audit:

A brief and very high level outline on the approach to do the alignment audit is outlined and a detailed approach can be extrapolated or extracted from COBIT 5 on governance. Enabler word used in this article, is not to be confused with that, in the COBIT 5- "Enablers", as they are meant in different context, in both. COBIT 5, a business framework for the governance and management of Enterprise IT. The framework is very similar and can be leveraged upon by the government to align the public sector for its objectives. As the government is on fast track to achieve digitized India, all public sector and its services would have to be digitized in some form, or the other. Which makes e-Governance an integral part of all public sector, and therefore the governance team, becomes the most important backbone for meeting these objectives.

Alignment of goals, as explained in detail in COBIT 5 by cascading of the goals for an enterprise IT, a similar guideline can be developed and used by public sectors to align to the government objectives. Alignment with cascading of goals is shown in the figure below. Though the mapping of goals can be extended up to the level of process and practices, the enabler audit should at the minimum be done at the highest level of Vision, Mission, Values, Principles, Policies and framework.

The remaining in the list of category in COBIT 5 for which alignment is necessary, is in the process, organizational structure, culture-ethics-behaviour, information, services-infrastructure-applications, people-skills-competencies, which may not be required to be audited during the early stages of enabler audit, and maybe to some extent, as it may anyway be covered by the IT or compliance audit. Non-IT related practices and standards are also to be aligned to get the best results. Auditing becomes much simpler by following a standard framework or standards, as it is done with "RBI guidelines mapping with COBIT 5" for information security, an example of how the guidelines from RBI can be implemented by the banks in India.CAG governance team needs to work with the government and its various agencies, like NITI Aayog and National e-Governance Division (NeGD), who translate the government's direction and objectives to a plan - National e-Governance Plan (NeGP) that can be taken forward by the various public sectors. These and other various agencies will provide the necessary technical and infrastructure support and guidance to public sector as well. The role of governance team will be to ensure these plans are translated into goals and are cascaded down, in the public sector to align it. Key Roles and Activities are depicted in the figure.

Fig: Goals Cascade for Alignment

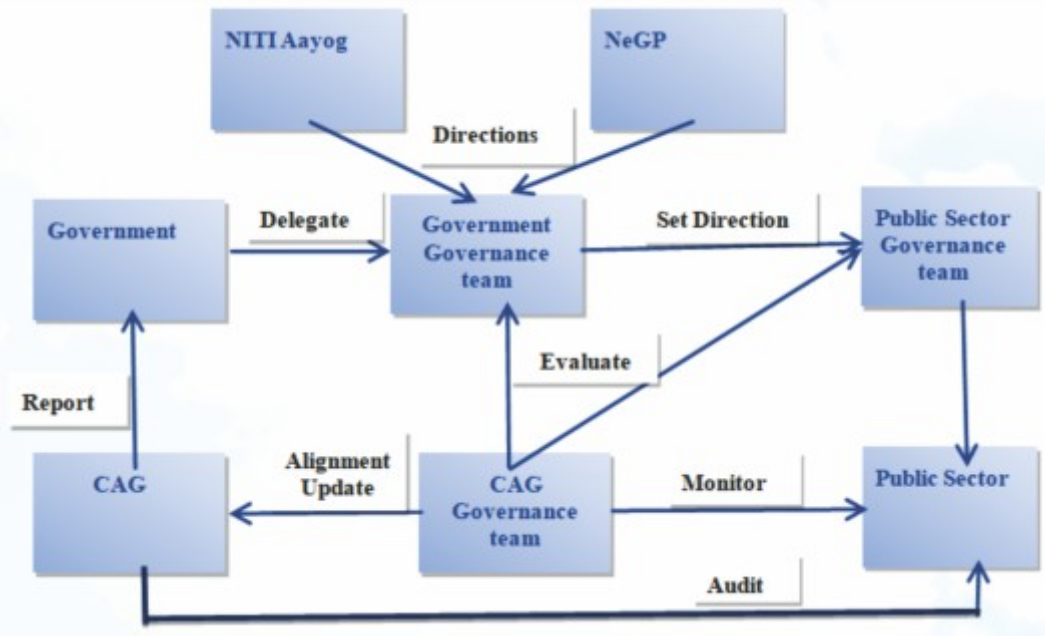


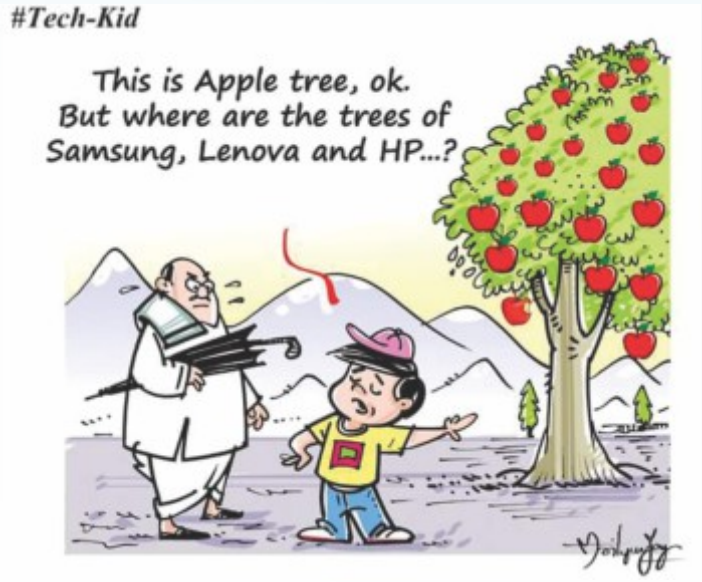
Fig: Key Roles and Activities

Conclusion:

Transformation of CAG from audit role, to that of enabler role will be a crucial step towards deriving extra benefits from the expertise, skills and competencies of CAG. In the present legal framework it may not be practically feasible to carry out a full-fledged alignment audit as it may amount to stepping into the shoes of the Government by the Auditor and for carrying out full-fledged alignment audit may require amendments at different levels on the constitutional provisions, Acts, Regulations, and legislations. However, on an experimental basis, part of the alignment audit can be carried out under the existing -performance audit umbrella of 3E's, extended to 4E's, Economy, Efficiency, Effectiveness, and the "Enabler".

Author's Note

The views and opinions expressed in this article are those of the authors and do not necessarily represent the views of government, CAG or the public sectors. Assumptions made may not be reflective of the actual status as on today. The roles, activities and relationship between different entities may not reflect the actuals. The article is forward looking into the near future, if the pace of the current digital transformation continues rapidly



SOURCE

Cartoon by Mrityunjay:
https://www.facebook.com/IIC4u/photos/pcb.1015602489
2663403/10156024892038403/?type=3&theater

e-Courses

C-DAC has developed a number of indigenous solutions for content management, evaluation and assessment, virtual classroom, collaboration for e-Learning domain. Some of the solutions are listed below:

- e-Shikshak is a learning management system with rich support for Indian languages.
- National Online Examination System (NOES) is an examination system primarily aimed at conducting recruitment.
- Online Labs (OLabs) for school lab experiments provides students with the ease and convenience of conducting experiments over the Internet.
- Veda is a general purpose online testing and question banking system, primarily supporting multiple choice questions (including its variant forms such as match the following).
- Video conferencing solutions for building virtual classrooms supporting synchronous lectures are also available from C-DAC.
- e-Saadhya (Saral Anukulaney Adhyayan) an Adaptable and Accessible e-Learning framework for the children with mild mental retardation and Autism, is being developed with the domain support from National Institute for the Mentally Handicapped (NIMH) with local language support in three Indian languages Hindi, Telugu and Kannada.
- An Academic Networking portal for the faculty members, students, and academic institutions to network and share information about courses, academic events, projects, etc. has been created through a portal called SEEKHA (www.seekha.in)

REFERENCES

- https://egovtraining.maharashtra.gov.in/1035/Home
- http://ecoursesonline.iasri.res.in/course/index.php?categoryid=100
- http://lms.negd.in/
- https://www.cdac.in/index.aspx?id=st_pr_esikshak
- https://www.cdac.in/index.aspx?id=st_pr_esavya
- https://www.cdac.in/index.aspx?id=st_pr_qaael
- https://www.cdac.in/index.aspx?id=st_el_ebasta
- https://www.cdac.in/index.aspx?id=st_el_mhrd
- https://www.cdac.in/index.aspx?id=st_el_mysikshak
- https://www.cdac.in/index.aspx?id=st_el_aiims

REFERENCES

Swayam Courses

- https://swayam.gov.in/courses/5053-e-governance
- https://swayam.gov.in/courses/4212-ict-in-teaching-and-learning
- https://swayam.gov.in/courses/5238-refresher-course-on-leadership-and-governance-in-higher-education
- https://swayam.gov.in/courses/5214-redefining-laboratory-instruction-using-virtual-laboratory
- https://swayam.gov.in/courses/public?level=null&type=upcomin

N.P.T.E.L Courses

- https://nptel.ac.in/noc/individual_course.php?id=noc18-ge01
- https://nptel.ac.in/noc/individual_course.php?id=noc15-cs11

Spoken Tutorial visit website : http://www.spoken-tutorial.org

Virtual Labs visit website : http://www.vlab.co.in

Talk to Teacher visit website : http://www.aview.in

SOURCE

https://timesofindia.indiatimes.com/humour/cartoons/itoons/photostory/62693898.cms

Disclaimer

This Journal is conceived, designed and presented by International Centre for Information Systems and Audit (iCISA) which is a field Office of SAI, India, i.e. CAG of India, for internal circulation within Indian Audit and Accounts Department only.

This Journal aims to share with readers the latest developments in the field of Information Technology and shall be used for information ONLY. Though all efforts have been made to ensure the accuracy of the facts and figures, the same shall not be construed as statement of law or used for any legal purposes. In case of any ambiguity or doubts users are advised to check it with the authors and officers of iCISA before taking any decision based on information contained therein. The contents of this journal are meant for informational purposes only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this journal.

This Journal has provided web links to various outside websites also for information ONLY and hence does not assume any responsibility for the contents included therein.

Compiled & Designed By:

Ms. Swati Pandey, Director, iCISA
Ms. Narmadha R., Director (R&I), iCISA (Former)
Sh. Abhay Singh, Dy. Director (R&I), iCISA
Sh. Mukesh Sharma, Sr. AO (R&I), iCISA,
Sh. Vijay Kumar, Sr. Auditor (R&I), iCISA