



उत्कृष्टतां अस्मिताम्
Dedicated to Truth in Plural Harmony



PURSUIT

July 2021

One IA&AD One System



PursuIT-One IAAD One System

Index

<i>Director General's Message</i>	
<i>Moving Forward with OIOS</i>	1
<i>Mr. Abhishek Singh</i>	
<i>Toolkit : Need and Purpose and designing in OIOS</i>	2
<i>Mr. Shyam Das O V</i>	
<i>An OIOS for the Future</i>	7
<i>Mr. Nanda Dulal Das</i>	
<i>Business process management in the brave new world</i>	11
<i>Ms. Abhilisha Das</i>	
<i>System Automation Initiative (SAI) Training</i>	13
<i>Ms. Sowmini Subramanyan</i>	
<i>Knowledge Management System in IAAD</i>	19
<i>Ms. Hemalatha Ravishankar</i>	
<i>Study Paper: Data Privacy</i>	23
<i>App watch</i>	36
<i>Quiz corner</i>	37



About the Journal

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

Editorial Board

Ms. ILA SINGH, Additional CTO & Director General, iCISA

Mr. K S Gopinath Narapyan, Principal Accountant General (Audit) Assam

Mr. J R Inamdar, Principal Director, iCISA

Feedback/Suggestions

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

Submission of Articles

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

Disclaimer

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

Director General's Message

PursuIT -the e-Journal of iCISA in its journey of exploring new dimensions in the Information System auditing is presenting its sixth issue with the aim to disseminate knowledge and share experiences among the officers and staff of IA&AD.

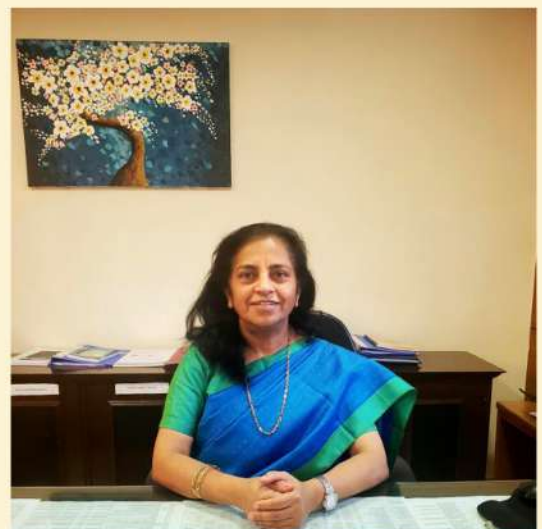
The theme of this issue is 'One IA&AD and One System (OIOS)' and therefore articles relating to need of OIOS, future of OIOS, Knowledge Management System etc. are included. Besides, an article on in-house development of SAI Training Portal, which has brought training need analysis, study material and trainee database of the IA&AD on a single platform is also included. An abridged version of study paper on Data Privacy in e-Governance prepared in collaboration with Data Security Council of India (DSCI) is also included to disseminate issues related to data security.

I am glad to appreciate efforts made by the authors of various articles and team iCISA who bring this issue in its present form and also acknowledge the efforts of members of the Editorial Board. I am hopeful that this issue will add value to the reader and looking forward for your valuable suggestions to make e-Journal better in future.



Ms. ILA SINGH

Additional CTO & Director General, iCISA



Moving Forward with OIOS

Mr. Abhishek Singh

The term "audit" in itself is comprehensive. It includes documentation of data, record, process, scheduling of audit, pursuance of audit objections, certification of accounts / process and a lot of other things besides the literal meaning. Indian Audit and Accounts Department has been carrying out this complex process of audit for more than 150 years.

As we move forward, we face more challenges and the recent pandemic has only added to them. Thus, as an intelligent being, we have an urge to make things simpler. We can add several dimensions to the word 'simpler', one of them being "sharing of resources". An audit team in Gujarat need not create something from scratch if a team of Assam has already created something similar, one more being "convenient", a government servant can authenticate a document without physically putting a signature on it and so on.

However, all such functionalities weren't feasible a decade earlier, the constraints being limited technology, internet and resource devices. Thanks to the advancement of technology, today almost every working personnel has a mobile phone and most probably with an internet connection.

The increased interconnectivity among employees has led the department to take a step ahead in form of an IT -led journey called One IAAD One system (OIOS).

The OIOS aims to facilitate sharing of data, authentication, quicker execution of routine tasks, better maintenance of records etc. on a single platform. The office of the Comptroller & Auditor General of India has a pivot role in developing the system with regular feedbacks from the field offices and deploying various mechanisms to hand hold field offices and addressing their constrains / issues. Thus, the user-friendly interface is all set to reduce paper usage and change the way audit offices work.

The system may appear anomalous to people who perceive it as something only for the tech savvy, some may not be sure about its practicality and some may mistakenly attribute human errors to its functionality hence showing less confidence in the system. These teething issues of the system will stabilize soon in a journey of partnership of whole department towards digitization of audit processes.



Toolkit : Need, purpose and designing in OIOS



Mr Shyam Das O V

Audit and other feedback mechanisms are an effective way to improve and sustain compliance with evidence-based practices of governance. Audit is carried out to verify if the system established is working well. This is done by checking records and procedures. It analyses past activities and detects the deviations / anomalies and proposes corrective actions. It mainly focuses on system's operation, procedure and documentation. Audit report is prepared based on the records produced for audit. Audit of the entire system is not possible and is done on sampling basis like Random Sampling, Stratified Sampling etc.

Further, success of any project is reflected by the achievement of expected outcome. Apart from checking the records pertaining to planning and execution of a work, beneficiary survey is an effective tool for assessment of the actual outcome of a project and is also used as a tool to further substantiate audit findings. Survey results provide a snapshot of the attitudes and behaviors – including thoughts, opinions, and comments – about our target population. This valuable feedback serves as baseline to measure and establish a benchmark to compare results over time.

The main benefits of carrying out such surveys using IT can be summarized as follows:

(a) Efficient data collection: Using IT enabled tool is an efficient way of gathering data from relatively large number of respondents. In addition, it is also possible to collect a great range of data from one respondent. We can use survey to study beliefs, values, past behaviors and attitudes among many other aspects of data collection.

(b) Simple to administer: It is very easy to undertake a survey provided one prepares the questionnaire in a meticulous manner. Responses can be quickly collated for interpreting in a simple and quick manner

(c) Inexpensive: Since surveys only entail standardized questions, lots of resource and time that are spent on vague questions can be avoided. Only the questions that are relevant to that particular project / Audit are listed and analyzed. In fact, surveys are generally much cheaper to undertake in contrast with carrying out a census.

We can create an audit toolkit through OIOS (One IAAD One System) which is used to collect data or information. The toolkit can be used for

- **Beneficiary surveys:** Mainly carried out during performance audit/compliance audit of auditees executing centrally assisted projects social security schemes viz, Mid-day meals schemes, family pension schemes, students/farmers survey, etc.
- **Collecting data during field audit in specific format:** During all india review of a particular scheme/project the data can be collected in a specified format for collating and substantiating our findings.
- **Creating Checklists:** A certain checklists can be made for our functioning or circulated among the audit team or other staff.
- **Collecting data within IAAD:** To immediately know the outcome or obtain feedback of any proposals, or getting responses for a new idea a toolkit can be designed in OIOS.

The advantages of creating a tool kit are:

- It helps in collecting data in a systematic manner
- It helps in asking consistent questions across audit units.
- It helps in collecting consistent data across samples taken for audit.

- Data thus collected can be consolidated across audit teams, beneficiaries, samples quickly.
- Data can be exported as excel file to any BI (Business Intelligence) tools for analysis.

Another added feature in OIOS is the facility of translating the created toolkit into other Indian Languages.

Data Collection Toolkit in OIOS :

Data collection toolkit module in OIOS enables users to create toolkits, search toolkits and reuse them using clone functionality. In addition to this, following features functionalities are added to this toolkit feature. If the survey collection type is a beneficiary survey, date of closure of collection of the survey can be assigned.

- Visibility rule can be set for the toolkit designed, wherein it can be clearly defined whether the toolkit is to be made visible to all or certain offices/persons etc.

- Various other functionalities such as setting up of a hint, appearance, assigning read only (for some questions) or mandatory check box and also adding expression are available in advanced options against each elements.

- These toolkits can be added to an assignment and made available to audit team during field audit execution.

A data collection toolkit typically contains questions and/or data fields which are referred to as 'Elements'. Based on the selected Element, one needs to provide question ID and question title. The elements in the data collection kit is mostly filled manually by the data collectors or by the individual concerned.

A snapshot of the Element details is shown below :

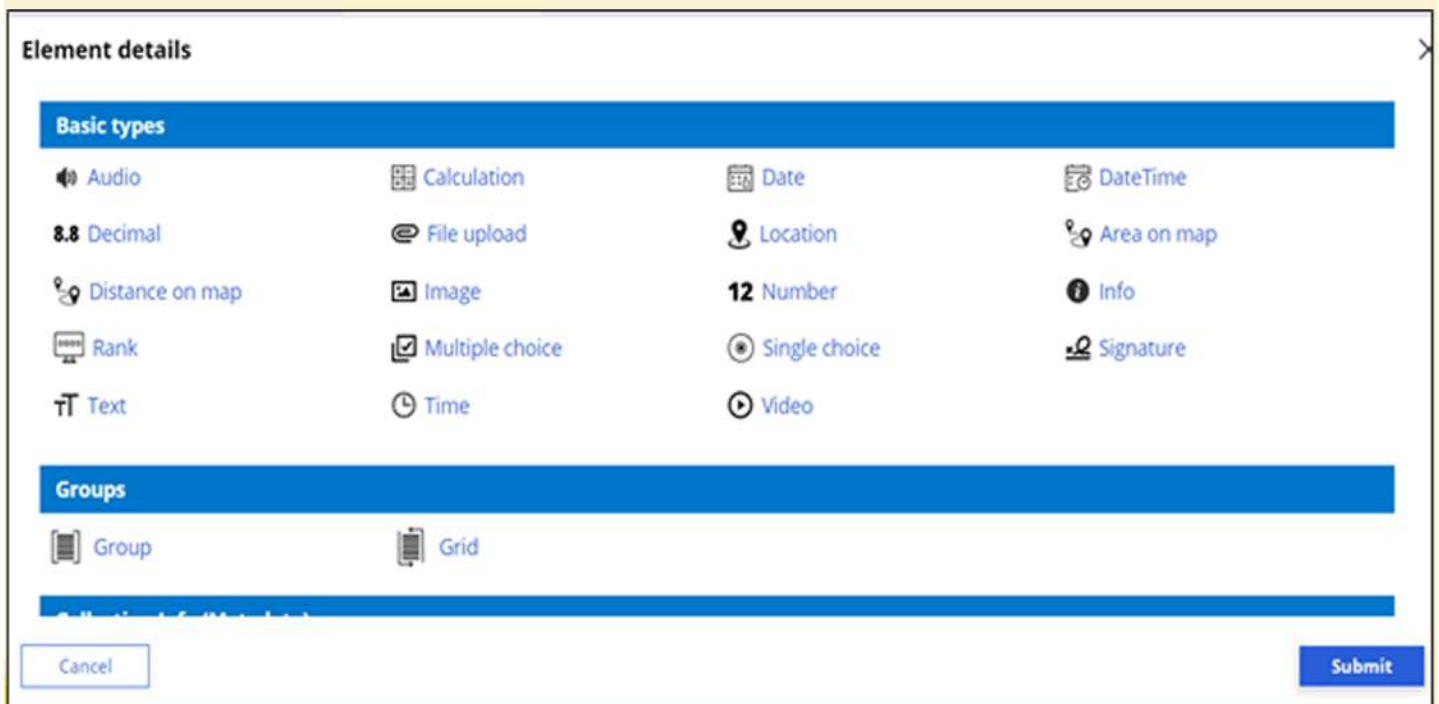


Image 1 : Snapshot of Element details

Let us have a brief look on the types of Elements which can be used in our OIOS toolkit.

Table 1: Elements of Toolkit

Element type	Description
Audio	Can be selected to create a question for adding audio files to the questionnaire.
Single Choice	Select to add single choice questions in questionnaire.
Rank	Select to add rating feature in questionnaire.
Multiple choice	Select to add multiple choice questions in questionnaire
Text	Select to add text entry option in questionnaire.
Time	Select to add time in questionnaire.
Video	Select to create question for adding video to the questionnaire.
Calculation	Select to add calculation using pull data from CSV file upload feature.
Date	Select to create a question for adding date.
Date Time	Select to create a question for adding date and time to the questionnaire.
Decimal	Select to create question for adding decimal numbers and define decimal limit.
File Upload	Select to add file upload functionality in questionnaire.
Location	Select to create question for adding location in questionnaire. (longitude and latitude)
Area on map	Select to create question for recording and adding area in questionnaire. (longitude and latitude)
Distance on map	Select to create question for recording and adding distance in questionnaire. (longitude and latitude)
Image	Select to create question for adding the option to upload image in questionnaire.
Number	Select to create question for adding numbers in questionnaire.
Info	Select to add specific information in questionnaire.
Group	Select to create question group.
Grid	Select to add table to the questionnaire.
Signature	Select to add signature to the questionnaire.

Users with the privilege to “design data collection toolkit” can create toolkit. The user, who creates the toolkit is also referred as designer. Once the toolkit is prepared and questionnaire is added, it is sent to the reviewer for review/approval.

After approval of the Questionnaire, a link is generated and the same link can be copied and sent to mail addresses of the intended survey respondents. Anyone having access to the link can fill in the questionnaire.

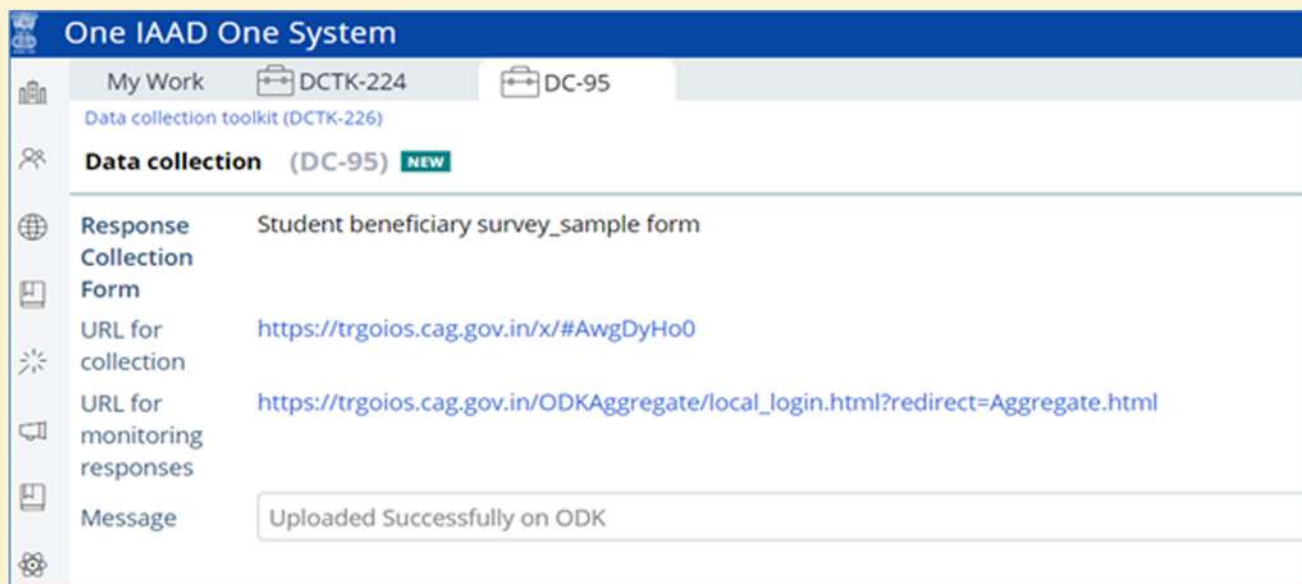


Image 2: Screenshot- Data Collection

OIOS also has features where we can see the status and number of responses received per day graphically. A screen shot of the same is shown below:

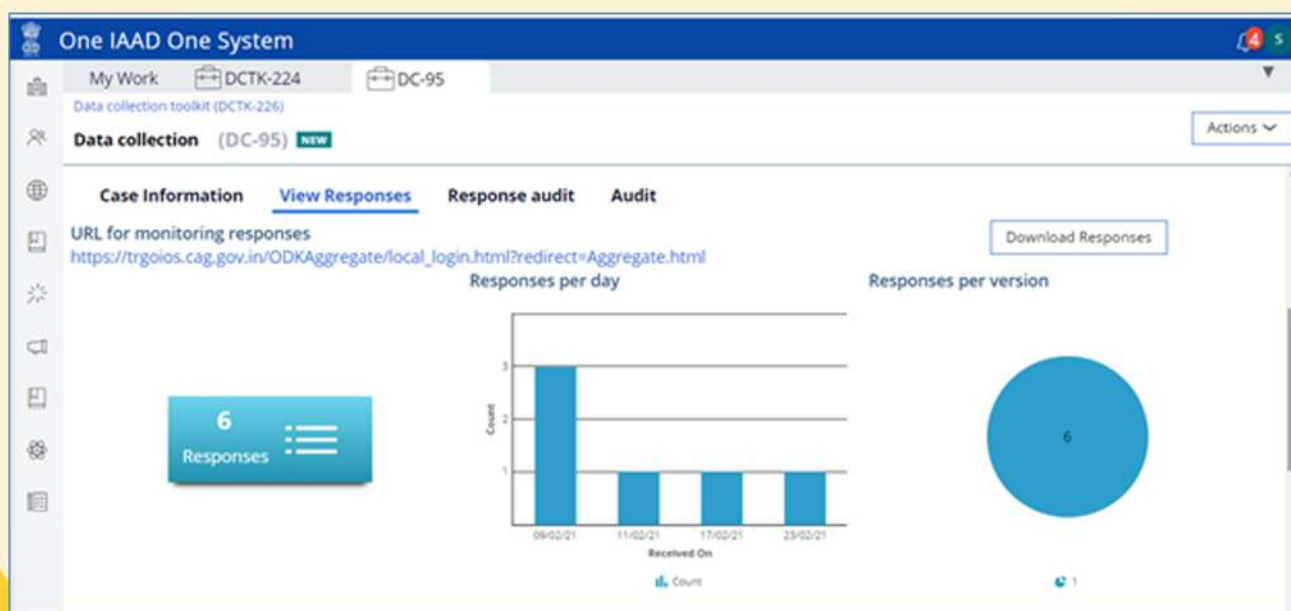
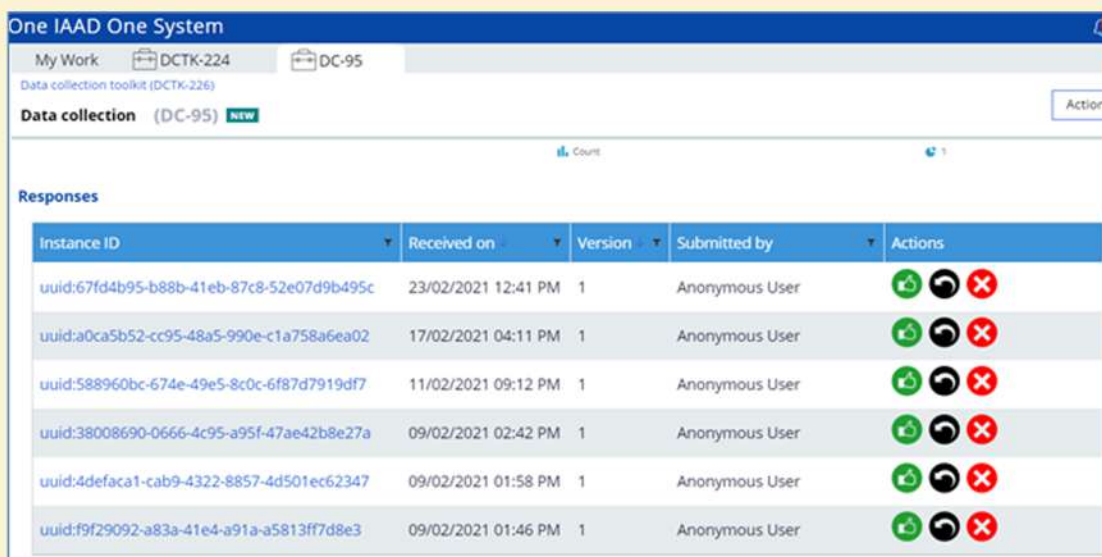


Image 3: Screenshot- Response Status

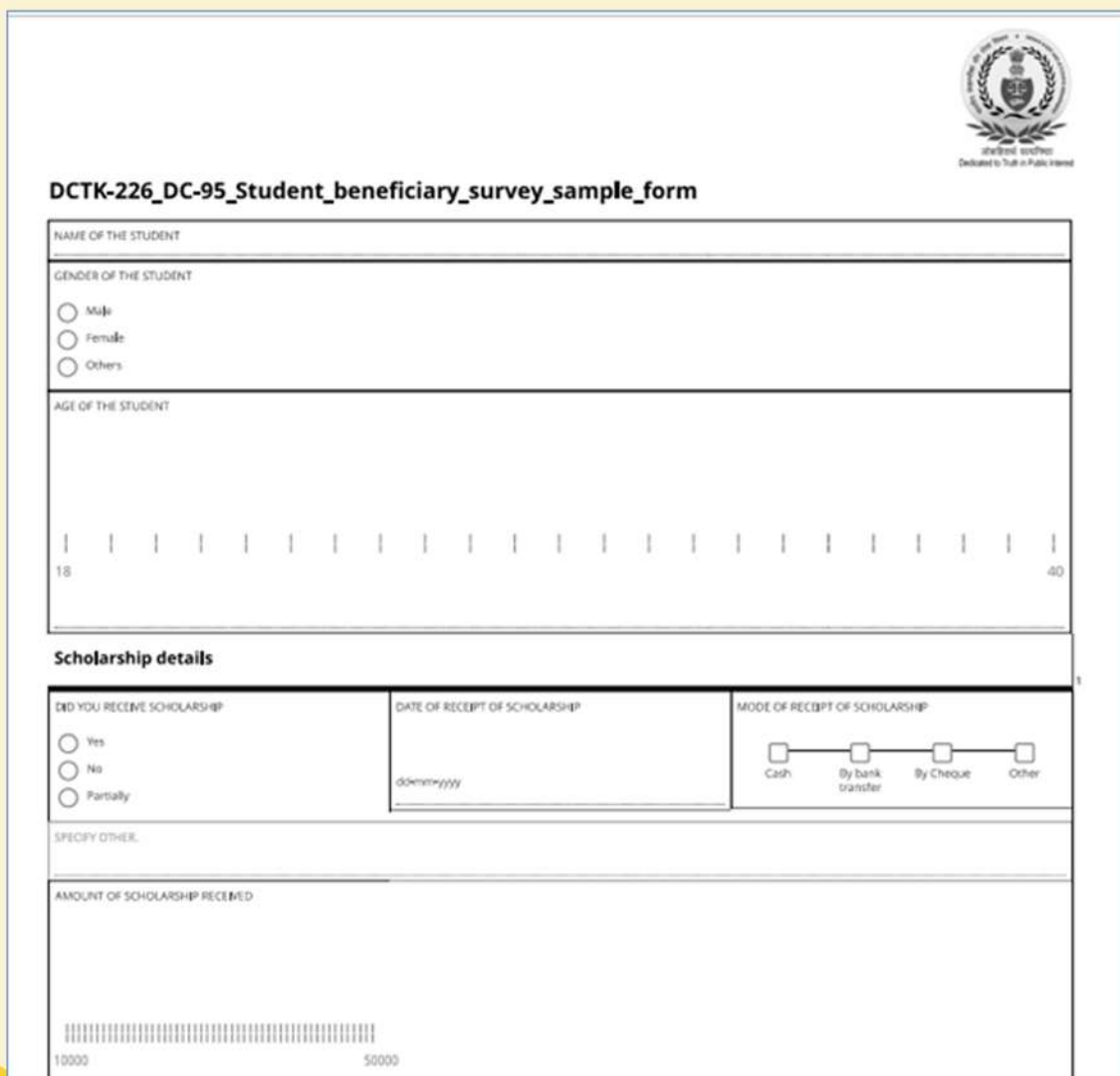
Responses received daily can be viewed and the same can be accepted/rejected/can be again resent to the beneficiary for resubmission seeking clarification. A screen shot is depicted :




Instance ID	Received on	Version	Submitted by	Actions
uuid:67fd4b95-b88b-41eb-87c8-52e07d9b495c	23/02/2021 12:41 PM	1	Anonymous User	Recycle Refresh Delete
uuid:a0ca5b52-cc95-48a5-990e-c1a758a6ea02	17/02/2021 04:11 PM	1	Anonymous User	Recycle Refresh Delete
uuid:588960bc-674e-49e5-8c0c-6f87d7919df7	11/02/2021 09:12 PM	1	Anonymous User	Recycle Refresh Delete
uuid:38008690-0666-4c95-a95f-47ae42b8e27a	09/02/2021 02:42 PM	1	Anonymous User	Recycle Refresh Delete
uuid:4defaca1-cab9-4322-8857-4d501ec62347	09/02/2021 01:58 PM	1	Anonymous User	Recycle Refresh Delete
uuid:f9f29092-a83a-41e4-a91a-a5813ff7d8e3	09/02/2021 01:46 PM	1	Anonymous User	Recycle Refresh Delete

Image 4: Screenshot-Responses

Audit toolkit is a powerful tool to empower audit teams to work together, collaborate for. A screenshot of a Basic sample survey form is depicted below:





DCTK-226_DC-95_Student_beneficiary_survey_sample_form

NAME OF THE STUDENT

GENDER OF THE STUDENT

Male
 Female
 Others

AGE OF THE STUDENT

18
40

Scholarship details

DID YOU RECEIVE SCHOLARSHIP

Yes
 No
 Partially

DATE OF RECEIPT OF SCHOLARSHIP

dd/mm/yyyy

MODE OF RECEIPT OF SCHOLARSHIP

Cash
 By bank transfer
 By Cheque
 Other

SPECIFY OTHER

AMOUNT OF SCHOLARSHIP RECEIVED

10000
50000

Image 5: Screenshot- Survey Form

OIOS for the Future

Mr. Nanda Dulal Das

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

One IA&AD One System (OIOS) Project envisions to become the ‘single source of truth’ obviating need for depending on multiple channels of communication among the different field-organs of the Indian Audit & Accounts Department. OIOS, in its first phase of implementation, seeks to integrate the process of auditing from the stages of planning to follow-up, in entirety. While data flow and storage would happen in the central server, there are features within the OIOS, which would provide much needed flexibility to the field audit teams in certain cases and yet would ensure uniformity in audit approach, needing special mention.

Audit toolkit in OIOS

Audit toolkit is akin to a platform for collecting data

from the field. Collection of data relating to different audit objectives and sub-objectives would help in uniformity as well as speed in data processing. As is known, before initiating All India or State Performance Audit or Detailed Compliance Audit (DCA), guidelines containing objectives and methodology for conducting the audit are formulated. Such guidelines may also contain several pre-developed formats through which data is required to be collected, so that analysing data collected from multiple audit parties are plausible. ‘Audit toolkit’ would contain such formats and data and information in them can be filled in by field audit parties from respective locations.

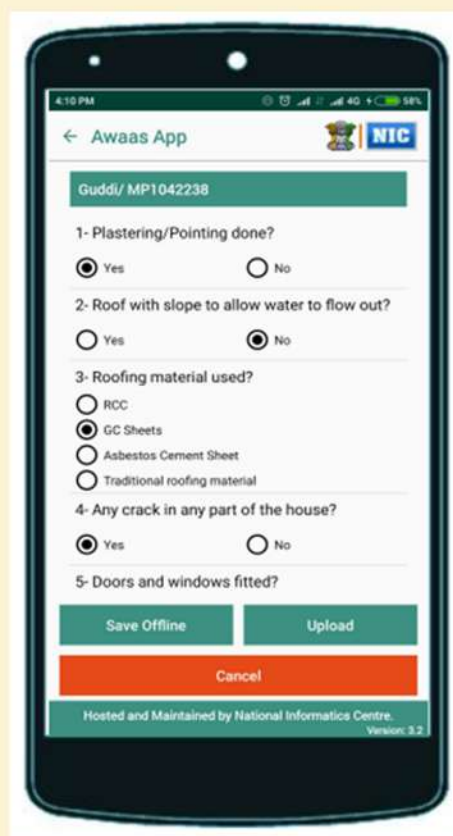
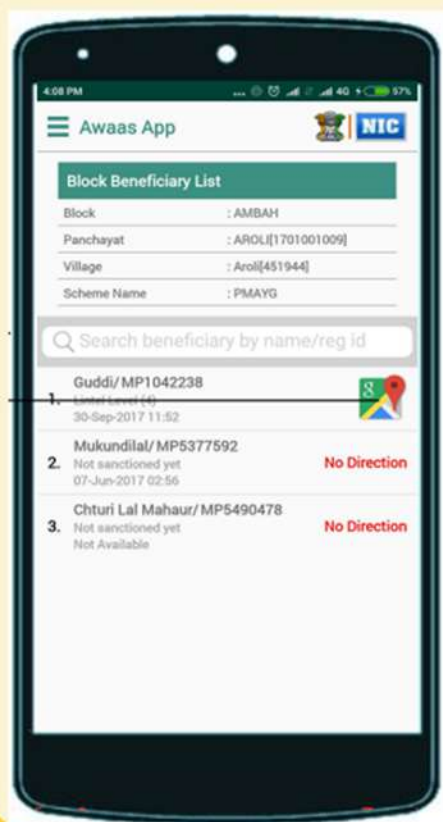


Image 6: Beneficiary listing in the PMAY-G Mobile App and format for field inspectors (can be used similarly by the auditors for beneficiary survey and audit of assets)

Development and filling up of questionnaires for beneficiary survey and other interviews can also be easily done using the toolkit.

This 'toolkit' has enormous potential if some other data bases can be linked with that of the OIOS. For example, during audit of assets developed under Pradhan Mantri Awas Yojana-Gramin (PMAY-G), if the District/Block and village-wise mapping of beneficiaries are accessed by their location from the PMAY-G database (Image 6) , selection/sampling of beneficiaries from the list and subsequent survey would be very scientific and easily monitorable. Revalidation of responses or assets can also be easily done.

As seen from above (PMAY-G), selection of beneficiaries and recording of responses are seamless. Since, the volume of data of such beneficiaries can be huge, it would pose difficulty for integration of other databases with the OIOS. However, if selection of beneficiaries is done once by central selection, the data of those sampled beneficiaries can be easily imported into the OIOS and if further integrated with locational information (GPS), the same can be a game-changer in field audit.

Any change in audit design matrix or guidelines, requiring additional data requirement during field audit, can be intimated through this toolkit to the touring audit teams easily as such changes are pushed through the central application of OIOS into the desired toolkit, provided OIOS apps are seamlessly connected through internet.

Offline utility in OIOS

This is one such utility which is best used, when remains unused. It acts like a contingency module. It is expected that OIOS offline utility would cater to the requirements of the audit teams who are

auditing in places not having good internet network availability (Image 7). This offline utility seeks to have the following functionalities :

- Enabling documents access in Knowledge Management System (KMS), provided the user selected the option of 'Make available offline' in advance [Quite like viewing YouTube videos when offline, provided they are saved in advance].
- Data collection using the toolkit (already discussed above).
- Preparation of audit requisitions, audit enquiries and audit observations (to be issued to the auditable entity after printing and signing).
- Documents including Key Documents (KDs) can be scanned and queued up for uploading, as and when network becomes available.

Similar offline utilities are used widely for implementation and monitoring of many Government programmes like Pradhan Mantri Awas Yojana-Gramin (PMAY-G) and Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), to mention a few. Like the Inspector, who is inspecting whether construction of houses in rural areas took place as per PMAY-G guidelines and have option to gather both online and offline information to be synced later (Image 8); the auditors in the IA&AD can rely on both online and offline utility for gathering information from the field,

depending on network availability and data constraints. Likewise, NREGS-Soft, application developed for capturing data on beneficiary and assets built in rural areas, has available offline utility for gathering information .



Image 7: Representational Images showing absence of internet and possibility of exploring data synchronisation when network becomes available (Source: collected images from Google)

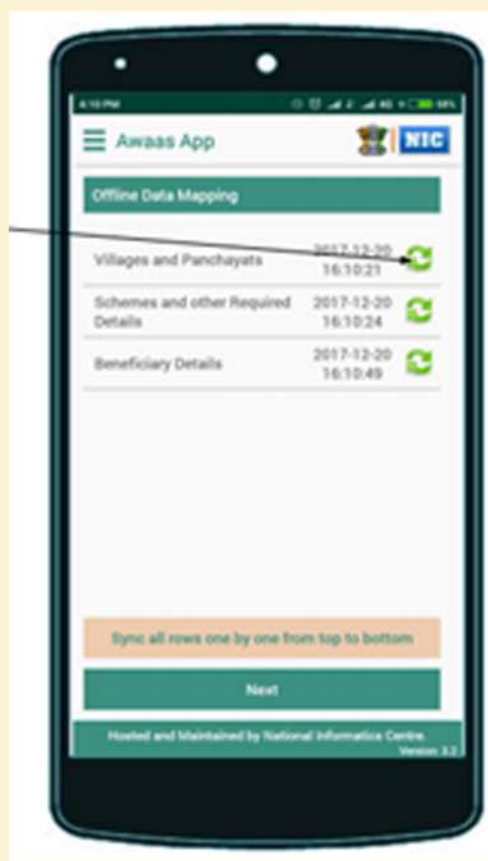
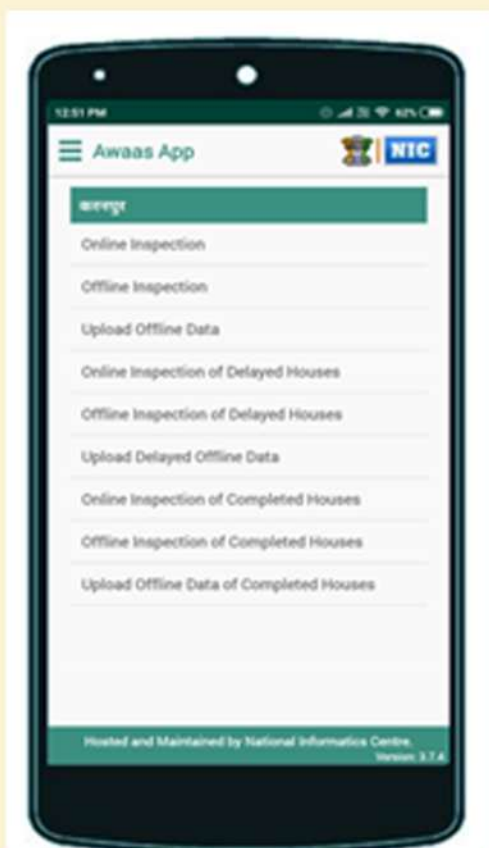


Image 8: Offline utility in PMAY-G Mobile App and option for synchronisation

Points for Pondering upon

As seen from above, data or information obtained through the offline utility can be synchronised by the auditors, when network becomes available.

Followings are the assumptions for beneficial utilisation of the above two units:

- 1) Audit teams are having compatible mobile phones and laptop, while conducting field audit.
- 2) Members of the audit team are trained to use these tools effectively.
- 3) Data can be compressed for effectively reducing the data uploading and downloading time and requirements for consumption of mobile data, given the uncertain network speed in the far-flung areas.
- 4) Adequate space is available in the device used for collecting information through 'offline utility'.

5) There shall be minimum possible disruption between the time of any update in the toolkit/central questionnaire/guidelines and the network becoming available for the members of the audit team.

While first four conditions can be met with multi-prong strategy like equipping audit teams with tablets/mobile phones/laptops; providing dongles/data cards for fulfilling mobile data requirement; technological solutions towards compressing the data which passes through the 'toolkit', internet network and the OIOS; providing additional space to the members of the audit team for offline utility; solving the last point of time-gap can be an issue towards synchronised audit program. Disruption in network connectivity can result in duplication of efforts at both the end of auditors and auditee units if the auditors have to turn back to gather data/information on the revised guidelines/questionnaires.

Following mechanisms can be thought of as solutions to overcome this problem, to a large extent:

a) Mapping at the State level for tracing out best available service-providers in different districts, which can be useful to equip the audit teams with data access from such service-providers.

b) While internet networks may not be available in many field locations, mobile network may still be available at most of the places. Therefore, sending push SMS to all the members of the audit teams informing any changes, that might have been carried out in the 'toolkit', would make the audit team aware of the change and take corrective actions, as and when required.

c) Audit teams staying in hotels/guest houses at a nodal city from where they perform the daily travel can utilise option for availing the wi-fi network of the respective hotels/guest house at the end of the day for synchronisation of offline and online database. Returning to Headquarters station in the State for uploading such information would be both cost and time prohibitive.

Internet of Things (IoT) can go a long way to help mitigate some of these problems. For example, Microsoft Edge's IoT Edge provides additional offline settings and 'time to live' utilities which save messages/information transmission until the device is connected to the internet. Similar features can also be integrated into the conceived OIOS. Therefore, for an OIOS for the future, sky is the limit.

References:

(i) Awaas Mobile Application- User Manual, Pradhan Mantri Awas Yojana-Gramin, Ministry of Rural Development, GoI< available at <https://pmayg.nic.in/netiay/Document/User-Manual-Mobileapp.pdf>

(ii) NIT for Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of 'One IA&AD One System' (OIOS) Project, Reference Number: 51-ISW/2019-One IAAD One System Project, C&AG of India, 2019. Available at https://cag.gov.in/uploads/tenders/RFP_OIOS_Project_22_8_19.pdf

(iii) Awaas Mobile Application- User Manual, Pradhan Mantri Awas Yojana-Gramin, Ministry of Rural Development, GoI< available at <https://pmayg.nic.in/netiay/Document/User-Manual-Mobileapp.pdf>

(iv) MIS for MGNREG Act, 2005, Ministry of Rural Development, GoI, available at https://nrega.nic.in/netnrega/Data/Draft_User_Manual_MIS.pdf

(v) 'Understand Extended Offline Capabilities for IoT Edge Devices, modules and child devices', Microsoft Azure's IoT Edge.

Business process management in the brave new world

Ms. Abhilisha Das has more than 14 years of experience in the IT industry. She has worked on multiple large projects in different domains in various geography. She specializes in BPM implementation and is a Pega Certified Lead System Architect. She has managed multiple large projects and is a certified scrum master. She has extensive experience in implementing the complete lifecycle of enterprise applications. She has implemented complex projects in Insurance, BFS and Government domains, working closely with end users and SMEs in Australia, USA, Canada, UK and India.

Information technology has been evolving at a breakneck speed. Along with it, various IT categories and concepts like Business Process Management (BPM), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) etc. are evolving with equal alacrity.

As Bill Gates famously said, automation applied to an efficient operation will magnify the efficiency while automation applied to an inefficient operation will magnify the inefficiency. That's where business process management fits the Bill perfectly. A well-designed BPM application can bring in the right amount of automation to operations. It can help magnify the efficiencies and limit the inefficiencies.

Let's discuss some of the latest trends in BPM application which have taken the industry by storm

Introduction of Bots: BOTs* simulate and automate a user's repetitive actions and make a time and manpower intensive process almost straight through.

Workforce collaboration: This is not at all a new concept but leveraging collaboration within the processes have become a necessity. All BPM tools are getting better and better at collaboration. With the workforce spread around, business have invested heavily on their collaboration platform. Official communication is no more restricted to emails. Users create, transfer and complete business processes over chat, WhatsApp and even social media platforms.

Low code platform: Low code or no code platforms are gaining more and more popularity over the last few years. Platforms emphasize the need of citizen developer, an subject matter expert who can define the building blocks of an application with business need in context.

Analyst reports suggest low code platform are here to stay. Its very important to analyse the trade-off of using a low-code platform which might straitjacket the application development to some extent vs an open code platform.

Increased usage of AI: Machine learning, predictive and adaptive models, Natural Learning Process and many more techniques have been increasing their influence on BPM. But as always, intelligence should be at the right steps of the business process to increase efficiency and Return On Investment. Too much can be disastrous and too less will be ineffective.

Digitalisation has been the new mantra for a few years now! However, changes adapted by businesses a few months ago in Before Covid-19 era soon became the Choluteca bridge of Honduras. Businesses with extremely restrictive IT policies had to relax a lot of these overnight. This pandemic underscored the need for rapid change and adoption for even the most stringent and conservative businesses. If business did not digitize their day-to-day work as much as they did, can you imagine how millions across the world would have been working from home during the pandemic.

IA&AD's bold step towards digitalization will prove a very timely adaptation to the need of today and readiness for tomorrow. IA&AD's processes are complex and widely varied, a one size fit all solution could never have worked for an enterprise application of IA&AD. OIOS is a great example of optimal application of Business Process Management without making the platform too restrictive for the end users. OIOS boasts the ability to adapt to the business processes of various audit streams and offices. Consider the business process management of various audit processes of planning, design and execution.

* Short for robot also known as web robots is a program that operates automated tasks over the Internet as an agent for a user or another program or simulates a human activity.

The open workflow of OIOS allows for various permutation and combinations of actors involved or revisions required. Similarly, the unique record based permission model of OIOS allows for managing permissions in a large office where the responsibilities are distributed or in smaller offices where one officer discharges multiple roles.

The next phase of OIOS can include a lot more of the latest BPM features. While we explore the trends of BPM and plan to bring in a shiny new application, we should keep in mind that any new application/feature will always face various teething problems. However, in this ever-changing new world, how much can we cater for users worried about who moved their cheese?



System Automation Initiative (SAI) Training

Ms. Sowmini Subramanyan is a Sr Audit Officer and Core Faculty (IS & KC) at RTC Bengaluru. She has worked in the areas of Direct Taxes Audit, Information Systems Audit, Civil Audit, IT Project management and Capacity building. She is a Certified Information System Auditor, has co-authored the CISA Manual 2010 and is a guest faculty at ISACA Bangalore. She was a member of the Audit teams that performed the Eighth annual review of progress of implementation of United Nations enterprise resource planning system (Umoja) at New York in 2019 and Performance review of Internal Oversight Services, WHO at Geneva in 2010. She is the Team Lead of SAI Training Application development team.

System Automation Initiative Training (SAI Training) application is a technology driven initiative implemented to automate the complete workflow of administrative activities in capacity building in Indian Audit and Accounts Department (IAAD). The distinguishing feature of the project is that it was entirely driven and developed in-house, harnessing open-source technology. In fact, SAI Training is the first in-house developed web-based application, deployed pan-India in all offices of IAAD, that aims to have every single employee of the department as its user.

Genesis of SAI Training

The project was conceived in the Conclave of Heads of Regional Training Institutes (RTIs)/Regional Training Centres (RTCs) in August 2019 wherein it was decided to develop an application to facilitate faster and smoother training operations of IA & AD and to establish a well-informed centralised training database. The idea was initiated by the then Principal Director of RTC Bengaluru, based on the initial pilot run by RTC Bengaluru. A Project Board was constituted to oversee the development of the Project and it was decided that the project would be developed by the same team which was involved in the pilot project.

SAI Training portal was built primarily on C#, Javascript, JQuery and MySQL. Access to various modules and data of the application are provided to users based on the roles assigned to them.

The application has been developed in two phases. The first phase was rolled out pan-India on 1st January 2020 after testing were done by RTI Mumbai, RTI Jammu and RTC Delhi before the pilot roll-out in December 2019 across all RTIs. The development team worked tirelessly from three different locations in addition to their regular duties.

The help desk for the project was also run by the development team in the same way. While automating the training workflow, the processes from Training Need Analysis to Training Impact Assessment were reviewed; the business process was reengineered by rationalizing and standardizing some of the processes. The Unique Perceived Benefits (UPB) of the portal are making need-based training programmes a possibility in IA&AD and lending information within three clicks.

From Supply driven to demand driven trainings

Earlier, there was no automated centralised training database to link skills to resource deployment and to identify gaps in skill acquirement. Training need analysis was performed based on limited information making training a supply driven activity

Ideally, the training needs of a department would be based on various factors, such as, the Headquarters reckoning of thrust on emerging areas in audit; the need of adapting new technology; the need of individual offices arising out of their long-term audit plans and last but not the least, the need of an employee as perceived by himself with his area of interest and background. To make training far more effective in the department, a solution for a methodical Training Need Analysis (TNA) by user offices was required to be identified.

SAI Training application provides an interface to capture these needs and assists in providing the information inputs for decision making. The application collates the training needs of all user offices of a training institute automatically for discussion and finalisation of the Annual Calendar of the Institute at the Regional Advisory Committee meetings (Image 9).

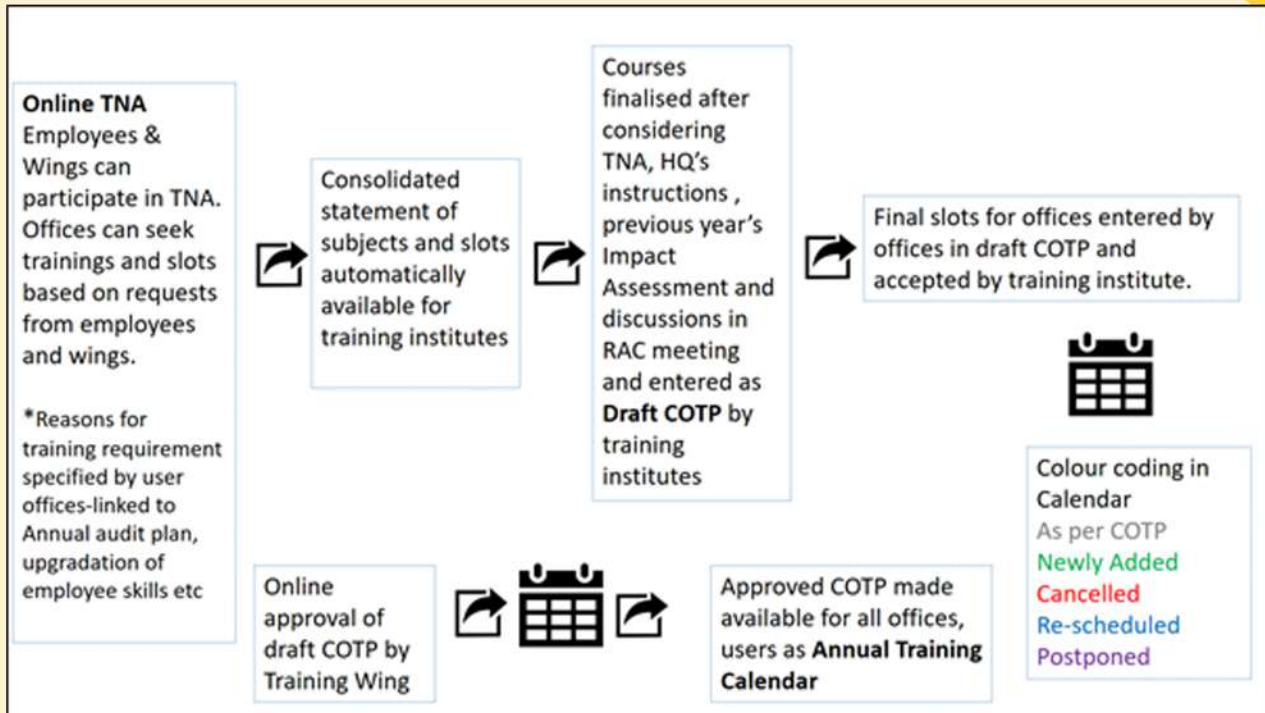


Image 9: TNA to COTP

The Online TNA module has been used by RTI Mumbai, RTI Jammu, RTI Hyderabad and RTC Bengaluru to draw the Calendar of Training Programmes (COTP) 2021-22.

Knowledge Repository and enhanced experience for employees

Auditors/Accountants competence are essential for ensuring that IA&AD fulfils its legislated mandate and addresses the challenges of the ever-changing environment they work in. The professional development of auditors/accountants is also

desirable for updated work of Supreme Audit Institutions.

To make employee participation robust and encourage continuous development a possibility, SAI Training application makes available an open knowledge repository to preserve and maintain Structured Training Modules (STMs), Case studies and other reading material for all officials in IA&AD. The participants of the training programme can assess all the materials related to the training programme anywhere, anytime.

View STMs/ Newsletters/ Research Papers/ Case Studies

View: All SEARCH

SNo	Material	Material Type	Creator	Creation date	Upload date	Download
1	STM on Special Features, Accounts and Audit of typical Companies- Electricity, Finance (NBFC), Banks and Insurance Companies for SAS (Commercial) Examination	STM	Regional Training Institute, Mumbai	04-02-2021	25-06-2021	Download
2	STM on Consolidated Financial Statements of Companies	STM	Regional Training Institute, Mumbai	03-02-2021	25-06-2021	Download
3	Audit of procurement in e-procurement environment	STM	Regional Training Institute, Hyderabad	28-01-2021	10-02-2021	Download

Image 10: Repository of STMs and other reference materials

e-Notice board to upload all circulars and notifications related to training by the Training Wing has also been provided to keep the officials well informed of the policy decisions of the department. The repository has restricted access to officials of IA&AD only.

The application provides a module - Employee participation as a one-stop-shop to view all the capacity development activities undertaken by an employee like trainings attended, future trainings nominated for and trainings facilitated as faculty. Apart from this option, participants can download bi-lingual (English & Hindi) certificates and training materials of the trainings attended. Further, the application allows employees to choose subjects they wish to get trained every year to meet their professional requirements or for academic interest. A platform has also been provided to them to convey their desire to handle classes.

Online Registration (open two days prior to the training programme) have been provided to gauge the expectations and entry behaviour of the participants to enable focussed coverage of the topics. The session-wise feedback and overall course feedback given by participants are available real-time for Training institutes and HOD of the Training institute for mid-course corrections.

Ease in nominations

Considerable time was spent both by user offices and training institutes on administrative activities related to training like consolidating nominations, issuing office orders for nominations, informing participants of change in dates of training programmes, administering attendance of participants, preparation of participation certificates and MIS reports for in-house consumption and for Headquarters.

The system has now simplified the entire process wherein administrative wings of the user offices are able to nominate from the list of employees desirous of attending a training, nominations proposed by functional wings and on the basis of gap detection. The system assists in the gap analysis by identifying the staff already trained in the subject.

The nominations are communicated through system-generated SMS/e-mail to the employees nominated for the training. Any updates/cancelation /modifications in the nominations are also captured on real-time basis and the necessary communications to all the affected parties are done instantaneously by the system.

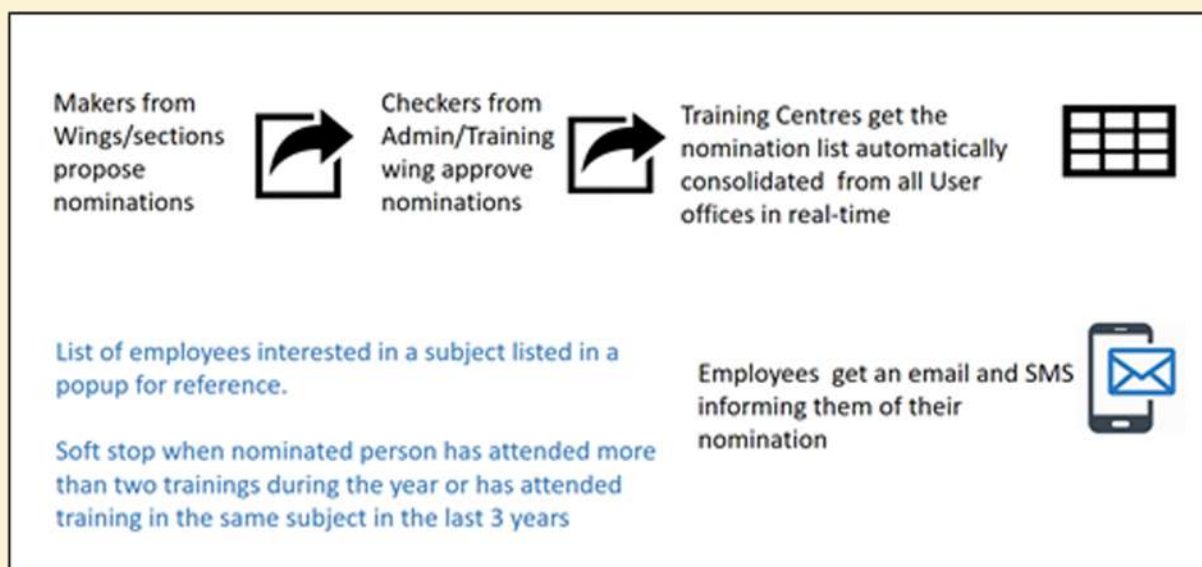


Image 11: Nomination Process

Further, the system also goes one step ahead by providing the Calendar of Training programmes of all training institutes for all employees and user offices thereby opening the possibility of nominating any officer to any training institute based on the availability of slots thereby breaking the geographical and jurisdictional barriers. Of course, the training wing has to approve implementation of this arrangement. The conduct of all-India Seminars/Workshops has been made easier as the system facilitates online requisition of slots for such events. Earlier, the requirements had to be consolidated from e-mails by the training institutes.

Training Impact assessment

Appropriate human resource management and training practices are critical enablers in formalising and structuring professionalization practices in a Supreme Audit Institution. Continuous follow-up with participants to assess the usefulness of a training programme is an important dimension in the capacity building life cycle. After completion of the learning plan, the system allows for evaluating the effectiveness of the learning programmes, by providing administration the feedback from the participants and their group officers, on how the training programme added value to their job. The automation that the system brings in on impact assessment has considerably scaled down the

required resources put in earlier when these inputs were collated and analysed manually. The system-generated MIS report allows for easy assimilation of these outcomes for updating the learning strategy and future training plans.

MIS reports and Dashboards

Learning and development form an important part of an organisation's overall strategy. Audit planning also includes systematic reviewing of work force to ensure that the required number of personnel with the essential competencies are available when needed. The BI reports in the portal contribute in assessing the current competencies of staff, the skill inventory and to perform gap analysis by comparing the organisation's capacity building goals with current levels of competence of staff. This gap analysis is also used to inform the training plan (Image 12).

MIS reports also help the training institutes in their day to day administrative activities such as faculty honorarium report, attendance report, watch on pending registrations/feedback/impact assessment forms etc.

All the MIS reports have download facility in MS-Excel/PDF. The facility is available in other modules too, wherever necessary, to facilitate approval processes outside the portal (Image 13).

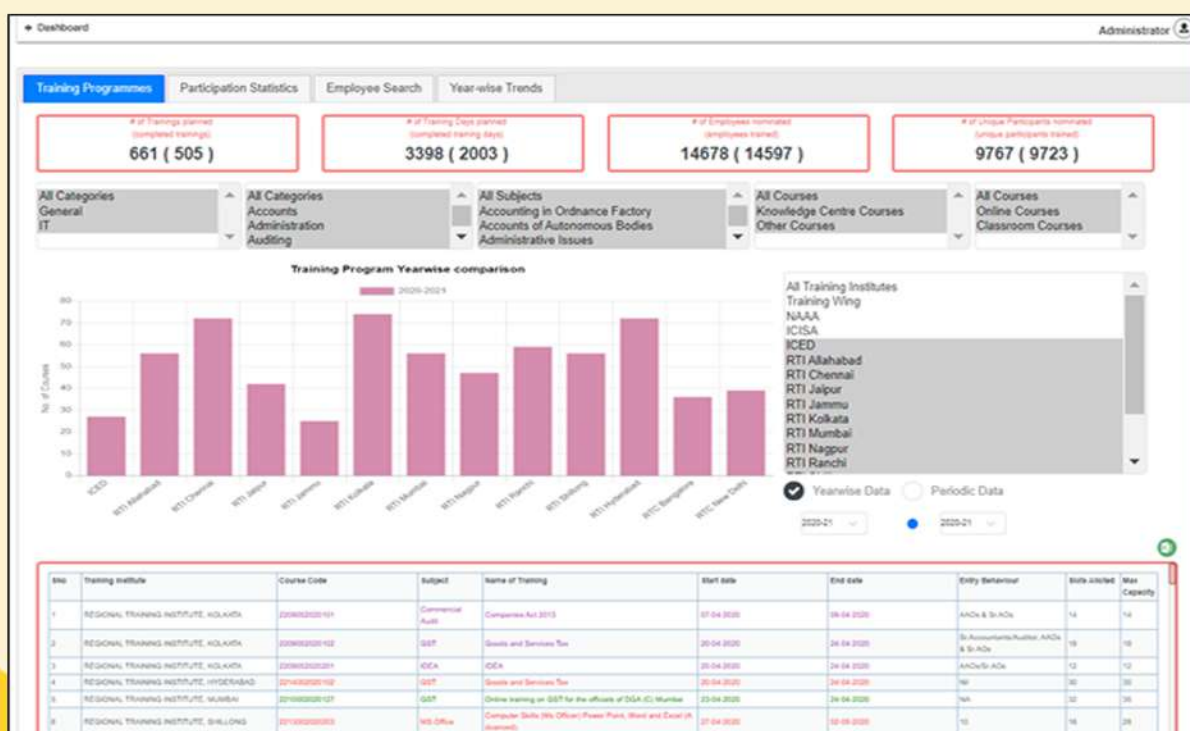


Image 12: Dashboard-Training Programmes

◆ COTP Status Report Sowmini S : TRG Institute Admin

2021-04-01 2022-03-31 All Courses **SEARCH**

No. of Courses	
Courses Scheduled in COTP	29
Addition after COTP-Approved by Trg Wing	3
Addition after COTP-Rejected by Trg Wing	0
Addition-Awaiting Approval by Trg Wing	0
Cancelled	0
Cancellation Rejected by Trg Wing	0
Cancellation Awaiting Approval by Trg Wing	0
Total Courses = Courses Scheduled in COTP + Addition after COTP-Approved by Trg Wing - Cancelled	32

Online	10
As Scheduled	10
Re-Scheduled	0
Postponed	0
Cancelled	0
ClassRoom	22
As Scheduled	21
Re-Scheduled	0
Postponed	1
Cancelled	0

Image 13: COTP status report to facilitate monitoring by Training wing

Support during COVID-19 pandemic

The COVID-19 pandemic changed the rules of the business and forced organisations to embrace new technologies to carry forward their businesses. It necessitated an agile and a multi-pronged approach to generate and share knowledge and tools on remote auditing, work-flow automations, tele-working and also capacity building. New ways of capacity building models replaced the face-to-face trainings and Instructor-Led Trainings (ILT) gave way to online or mobile learning.

SAI training came of immense avail during the pandemic and lockdown as RTI/RTCs were able to administer online courses through the portal.

The application allowed for seamless nominations from remote locations and administration of training from planning to impact assessment. The online resource pool of documents allowed easy access of training materials including video recordings of the training programmes for later reference. The mobile-compatibility of the application also proved helpful for the participants in Work-from-Home mode during the pandemic.

The approval of Calendar of all RTIs/RTCs and iCED for 2020-21 and 2021-22 was done by Training wing through the portal.

Road ahead

The application, earlier run from RTC Bengaluru, has been set up at NIC Cloud servers with automated backup services and load balancing facility. The application has been handed over to Training wing and is available through the URL to stake holder. The application will be eventually integrated with OIOS at the appropriate phase of OIOS.

Since the inception of SAI Training, 202 offices have nominated close to 47,000 participants for about 1750 training programmes including in-house trainings. The faculty database has about 3300 entries, of which 2,900 faculties have conducted trainings.

It is necessary to maintain an appropriate balance between programmes that assist staff to gain a set of required competencies (regular training programmes) and to comply with the related continuing professional development programmes (in-house trainings). The system has been extended to include in-house training programmes and trainings outside IA&AD organised by Training wing for better administration. Legacy training related data from 2018-19 onwards is being collated and ported into the database.

It is proposed to make all the forms in the portal and communications sent through the portal bi-lingual. It is intended to include Library management, Performance Monitoring Framework of Training institutes and a discussion forum for trainees and a few other MS reports in the next phase of development.

Given the immense possibility of the application in training programmes from skills assessments to skill development to impact assessment, it is imperative that the application remains agile keeping in tune with the future needs.

Credits

The credit to the success of this project goes to the SAI Training Board members for their valuable guidance and continuous monitoring of the project, the Heads of the offices of the development team members for lending their services for the project, Training wing for their steady encouragement, IS wing for infrastructure support, Training Institutes/Centres and offices in IA&AD for readily adopting the portal and providing continuous feedback to the development team.



Knowledge Management System in Indian Audit and Accounts Department

Ms. Hemalatha Ravishankar, Senior Audit Officer having experience in “Audit using IT Skills” for the past fifteen years. Conducted the audit using GIS Technology and UAV applications, as well as Conducted audit of various IT applications such as Vahan and Sarathi. She is trained in SAP System, certified in R application, Data analytics, Python and Machine Learning Algorithm. She was also part of UN Audit Team and currently deputed as Faculty Member for the implementation of OIOS.

Knowledge management provides means to share practices, expertise and learning across geographical boundaries. It reduces the risk of loss of critical knowledge which is retained by individuals. A system developed

Necessity for KMS in IAAD

1. Audit function of the IA&AD is a knowledge-based work.
2. Knowledge is an asset that helps in decision making and supports efficiency in planning, execution and adaptability in different audit assignments.
3. Knowledge must be deliberately created, consolidated and applied by the employees of IA&AD through a knowledge management system.
4. The unstructured/structured data of auditable entities forms an inherent part of knowledge.

Hence, IA&AD needs a KMS which would involve management of structured, semi-structured and unstructured information. It should handle creating new knowledge, facilitating utilization, application of current knowledge and handling outdated or invalid knowledge.

Thus, we need to provide a platform to share experience and insights and also to codify the knowledge as documented information.

Background of KMS

Individual offices/ officers in the past have taken the initiative to develop systems to maintain knowledge management system, through various models like Government Orders Bank, Knowledge Bank, Knowledge tree, Centralized audit resources wherein offices try to collect macro/micro, structured/unstructured information, such as acts, rules, government orders/ circulars/, policy notes, technical information, scheme based information, etc., about the auditee.

These systems served the intended but limited purposes. However, being localized in-house efforts and having other inherent drawbacks these could not scale up to the entire organization.

Component of OIOS

OIOS is not just an audit process management system. As it has the Knowledge Management System, which facilitates to collaboration between employees of the field audit offices and helps in institutionalization of knowledge.



Document Management System (DMS)

Audit and process guidance

All our internal documents like manuals, guidelines, practice guides are stored. Viewable to all and Professional Practice Group (PPG) is the manager of this folder.

Auditee information system

Viewable to all, each office maintains the folder relating to their part.

As of now, separate folders have been created for each state. Within which various ministries/departments folder are set. Within the ministry various Legislation (Acts, Rules, Circulars, policy notes, budget documents, etc.) are posted.

The users having privileges can post/contribute documents in the DMS.

KMS managers are given the privileges of approving/moderating the document.



Business workspace

It is a 'mini' KMS for an office and/or a wing.

Users can set the group of people who can access the workspace.

Helps in storing of information which are currently stored in a dispersed manner across many PCs / Laptops. No constraint on nature of document or capacity.

A workspace for OIOS, Chief Technical Officer (CTO) team has been created wherein, the capacity building documents, covering online Training videos, validated master data which are to be uploaded/uploaded, a Forum on How to onboard field offices were documented, and shared among specified users.




Wiki

A wiki would act primarily as a collaborative tool, where everyone can view and contribute to the information within it.

Wiki, consists of complete layout of the document in the right side panel and indexed base navigation panel on the left side. This utility can be made use for,

- Frequently Asked Questions
- Knowledge base for specific topics
- Technical help for IS activities
- Case studies.

OIOS user manual explaining step by step by process and short videos of each process are made available in KMS, which can be accessed by everyone.




Technical Forum

KMS is accessible only by authorized officials of IAAD.

Solution would also provide for a ‘Technical Forum’ which would serve as a platform for officials of IA&AD to discuss technical aspects relating to the same.

Forums can be made use for discussion open to the users by allowing the trainees/users to communicate with each other, discuss any questions they may have relating to the content, provide solutions and interact with each other.

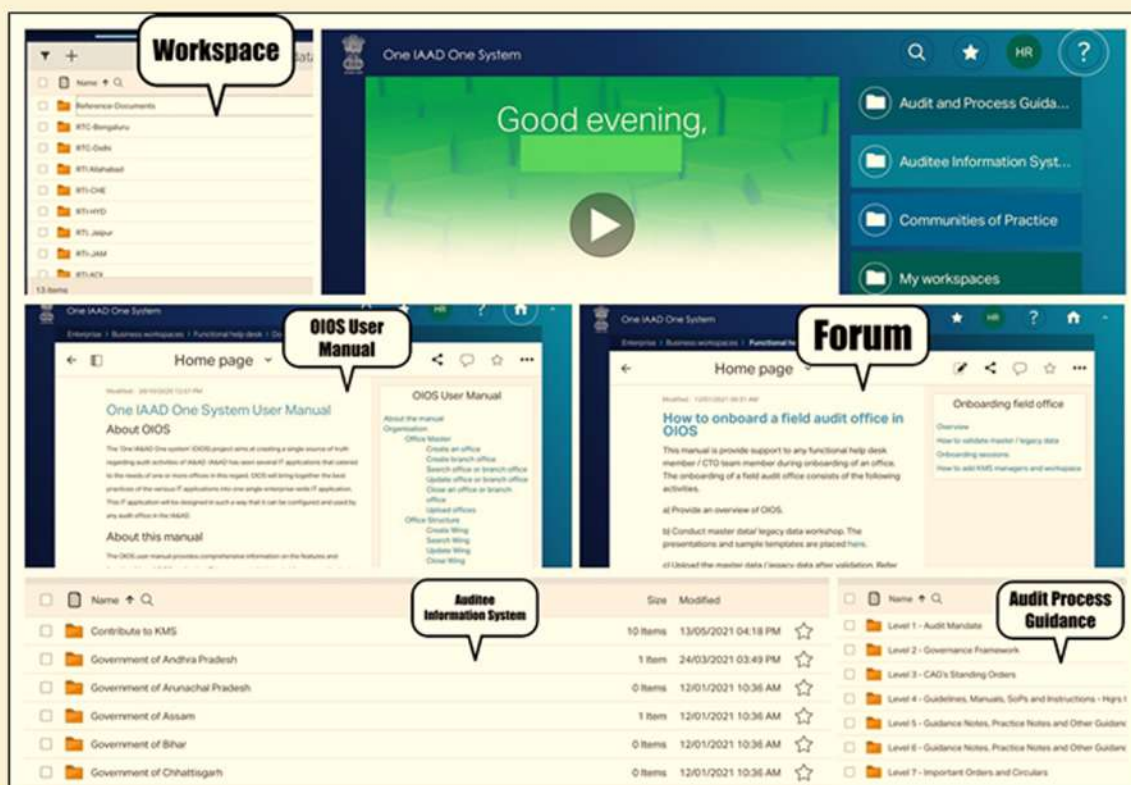


Search Tool

Provide for both basic and advanced search with logical operators, suggestive search/predictive text with facility to auto complete and search history.

Search results would be displayed in categories across knowledge base, documents, wiki articles, and media reports. The user will be allowed to filter his search results based on criteria such as document category, time frame of publication of document, author, etc.

Look and feel of KMS



The screenshot displays the 'One IAAD One System' home interface. At the top, a 'Good evening,' message is shown. The main area is divided into several sections:

- Workspace:** A list of folders for different regions like WTC Bangalore, WTC Delhi, etc.
- OIOS User Manual:** A document titled 'One IAAD One System User Manual About OIOS' with a table of contents including 'About the manual', 'Office Master', 'Office Structure', and 'Clear Wing'.
- Forum:** A section titled 'How to onboard a field audit office in OIOS' with an 'Orboarding field office' sub-section.
- Audit Information System:** A table listing various documents with columns for Name, Size, and Modified date.
- Audit Process Guidance:** A list of levels from Level 1 to Level 7, including 'Audit Mandate', 'Governance Framework', and 'CAD's Standing Orders'.

Image 14: Home Screen of KMS

Roles involved in the Business Process

Administrator
<ul style="list-style-type: none"> maintaining the master data relating to the audit guidance document such as document type, classification schema, etc
Preparer
<ul style="list-style-type: none"> initiating the draft of the guidance document/ contributes to KMS making amendments to the guidance document and assures the quality maintaining consistency of the guidance document. appropriately classifying the document and attaching the keywords to the document to facilitate keyword search.
Stakeholder
<ul style="list-style-type: none"> users who use the document. provides feedback during draft stage and can request for additional details, clarifications and able to search for the guidance document drilling down through the classification schema or perform a keyword / full-text search of the content.

Way forward

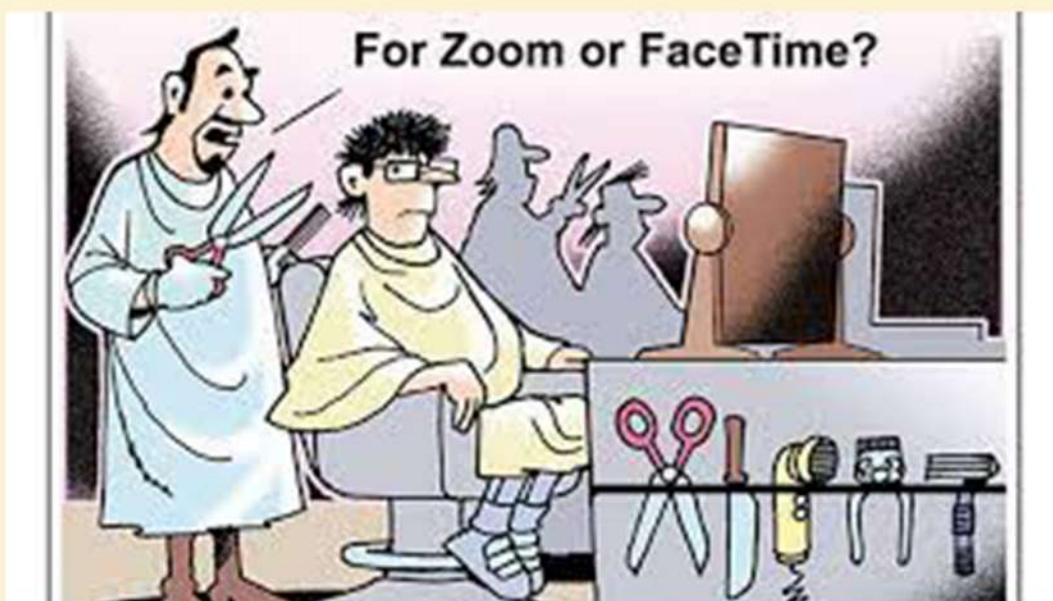
Finally, it is important to understand the KMS module is only a means to knowledge management.

Expanding the KMS repository rests with the ultimate contributors.

While growing, there may be provision to capture- Functions of each department, Statistics of the department, Master information of the department specific (like list of roads, bridges... in the case of Highways department, Board minutes, Balance

sheet in the case of PSUs) List of scheme/projects auditee unit wise, the scheme wise physical and financial targets for each auditee units, facility to capture and display the progressive information of each scheme at the time of field visit. Really, there could be endless possibilities to add on in KMS.

It is vital to address the organizational culture and develop knowledge management enablers in order to achieve the outcomes of a KMS.



STUDY PAPER*: DATA PRIVACY

Introduction

India is fast emerging as a global front runner in digital adoption. Digitization and technology are bringing incredible opportunities for the Indian economy and is set to play a major role in the economic and social transformation for the nation. The Government of India has also sought to tap into this transformative potential of digitization through the Digital India Initiative. Envisaging delivery of a host of welfare services and to foster an environment of digital literacy and awareness.

The Honourable Supreme Court of India recognized 'Right to Privacy' as a Fundamental Right guaranteed under Part-III of the Indian Constitution and also Information Privacy comes under the scope of Right to Privacy.

It would become imperative for government departments to create visibility and transparency around the purposes and usage of personal data of Indian residents and incorporate practices such as privacy by design and Privacy best practices before launching in schemes /undertaking new projects.

The guiding thought behind the formulation of this standard is creating a Privacy Assurance Program for assessing E-Governance Projects, that make use of the online medium for dissemination of government services, through service delivery websites, portals and mobile applications. The program (a) sets the standard in each case and (b) provides an assurance of complying with the specific standard.

e-Governance Statutory Framework in India

The Information Technology Act, 2000 and the Information Technology (Electronic Service Delivery) Rules 2011

The Rules prescribe strict standards to maintain the security, confidentiality and sanctity of all personal information used during electronic service delivery transactions. Confidentiality of data is given attention under the Rules with the incorporation of a provision whereby all service providers are required to submit a declaration stating that the data of every individual transaction and citizen will be protected.

In the event of an unauthorised disclosure without consent, the service provider will be debarred from providing that service further. The Rules remain silent on numerous other safeguards which ought to form part of a comprehensive legal framework protecting electronic service delivery. For instance, anonymization/obfuscation and deletion policies are excluded from the ambit of the Rules, despite their core importance to serve the end of confidentiality. Privacy principles such as collection limitation and purpose limitation delineate the precise use of databases. The Rules do not provide for provisions enunciating the appropriate uses of databases.

Right to Information Act, 2005

The advent of the information age has redefined the fundamentals of service delivery by the Government. In this vein, the Right to Information Act, 2005 (RTI Act), that came into force on 12 October 2005, served as the seminal legislation in modern India with a revolutionary essence of giving citizens the right to know about in governance. It is undisputed that e-governance and RTI are complementary to each other.

The RTI Act arms citizens with the right to access information held by the government and leads towards transparency in working of public authorities.

However, it is pertinent to note that the RTI Act while serving as an empowering tool in the hands of the citizens of India, but susceptible to breach privacy of individuals.

Road to Open Data

The NDSAP is designed to promote data sharing and enable access to Government owned data for national planning and development. The policy states three types of access: open, registered and restricted. Further, the NDSAP requires every Department to identify datasets based on the categories of Negative List or Open List.

**Responding to the fast changing ICT landscape, iCISA has entrusted Data Security Council of India (DSCI) to conduct a study on 'Data Privacy'. The salient points of the Study Paper are being published here.*

State Level Electronic Service Delivery

On the State level, many States have laid out their vision to create knowledge societies by using Information Technology for development, governance and ensure the last citizen gains access to benefits with the use of such technology. In this vein, the Electronic Service Delivery model has been adopted by states in India as a pioneering effort for efficient and effective governance. In 2006, the Government approved the National e-governance Plan to provide services electronically, such as processing of passports, registration of companies etc. In 2008, the Second Administrative Reforms Commission highlighted the need for a legal framework to implement e-governance. This was followed by the amendments made to the Information Technology Act, 2000 in 2008 to enable government departments to deliver services electronically. It is pursuant to Section 90 of the Information Technology Act, 2000, that many States notified Rules for electronic service delivery under the IT Act.

Cyber Security Policy at State and Central Level

With the inspiration from the National Cyber Security Policy 2013, the states of Andhra Pradesh, Telangana and Haryana introduced their cyber security policies. Telangana's Cyber Security Policy released in September 2016, aimed at critical information infrastructure protection, government network, e-governance, education and skill training among others. Andhra Pradesh has been a fore-runner in the use of ICTs extensively for delivery of public services quality. The e-Pragati Program being implemented by the Government on a whole-of-government approach, whereby all e-Governance systems are interconnected and integrated to provide a wide range of services online. The Vision of the Andhra Pradesh Cyber Security Policy 2017 is 'to create a robust cyber ecosystem, wherein the citizens transact online securely and take steps to protect their identity, privacy and finances online, the businesses conduct their operations without any disruption or damage and the Government ensures that its data and ICT systems are secure'. As a part of the e-Pragati Program, the Government shall design, develop and deploy a holistic and prioritised e-Pragati Security Architecture. The Government shall also establish an institutional mechanism for e-Pragati Security Governance under an e-Pragati Chief Information Security Officer. The country's maiden State Cyber

Security Policy was launched in September 2017 ensuring confidentiality and integrity of the critical IT and ICT data from unauthorised use, disclosure, modification and disposal. To address the cyber security challenges and following the tenets of the Digital India initiative of the Government, the Haryana state realised the need to establish a State Cyber Security Policy Framework as per the National Cyber Security Policy, to serve as an umbrella framework for defining and guiding the actions related to security in the cyberspace. For improved implementation of e-governance, it is essential for the Government to frame laws that fully incorporate the established as well as emerging technology; in conjunct with inherent privacy safeguards for maintaining the sanctity of personal information.

Data Privacy Assessment of e-Governance Projects

The exercise to gauge the privacy posture of e-Governance projects is twofold. Firstly, to examine the selected sample of e-governance projects against the existing privacy framework in India, i.e. the provisions that create privacy obligations under the Information Technology Act, 2000. Although these provisions have been created keeping in mind 'body corporates' and ensuring their accountability to protect data privacy of data subject (provider of information). It was felt that in the absence of an overarching framework that regulates the operation of government projects with respect to privacy, the same yardstick may be used to examine e-Governance projects. Secondly, the assessment of the aforementioned projects would be done against a model audit assurance standard that has been created by examining various global privacy legislations and best practices. The assessment in both instances has been carried out based on established assessment parameters-- Privacy Principles and Best Practices. These principles and best practices have been supplemented with audit checklists to help audits carry out these assessments.

(A) SPDI Rules Assessment Parameters

The Principles and best practices that have been inscribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have been depicted in the image 15.

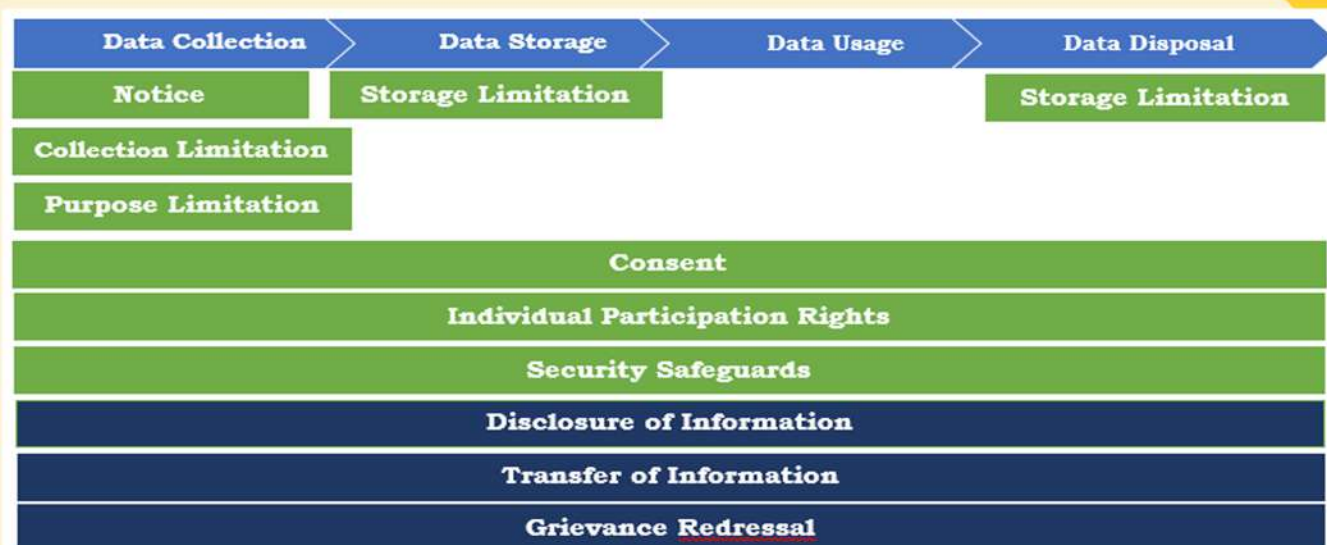


Image 15: Principal & Best Practice Parameter

There are 7 key privacy principles and 3 best practices that will form the foundation for assessment in this segment. But, it is important to note since these requirements have been designed for private sector entities, so some restrictions have been placed on their application to keep them relevant for the assessment of E-Governance Projects. These restrictions have been highlighted to the following sections.

Privacy Principles

Notice

Privacy notice is a public statement of how the entity applies data protection principles to processing Personal Information. It is a statement that describes how the entity collects, uses, retains and discloses personal information of a data subject.

As per Rule 4, a privacy policy for handling of or dealing in personal information including sensitive personal data or information should be displayed on the website of the entity and should be communicated to the provider of information (Data Subject).

This policy should be clear and easily accessible and mention type of personal or sensitive personal

data or information collected, purpose of collection and usage of such information; disclosure of information including sensitive personal data or information as provided and reasonable security practices and procedures implemented.

Storage Limitation

Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. This principle creates an obligation on the entity to establish and document standard retention periods for different categories of personal data.

As per Rule 5(4), sensitive personal data or information should not be retained for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

Collection Limitation

Entities should collect personal information from users that is adequate, relevant and limited to what is necessary in relation to the purpose of processing.

As per Rule 5(2) and Rule 5(3), information should be collected for a lawful purpose connected with a function or activity alone; such collection of sensitive personal data or information should be considered necessary for that purpose. The subject should also be informed about the nature of collection and identity of the agency collecting and the intended receipts of the information.

Purpose Limitation

This principle aims to ensure that the entity is clear and open about the reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

The framework laid down under section 43A of Information Technology Act, 2000, clubs the purpose and usage limitation principles under Rule 5 (5). As per this rule the information collected should be used for the purpose for which it has been collected.

Consent

Consent signifies any freely given, informed and unambiguous indication of the data subject's wishes by which they can signify agreement to the processing of their personal information referring. Consent can be obtained by a clear affirmative action.

However, consent maybe not be necessary in all instances of processing. There are certain kind of processing activities which necessitate that the data subject provides their personal data through non-consensual grounds such as function of state. This principle would not be applicable in its entirety in our assessment as the selected e-Governance projects carry out collection of data for provision of schemes and services that may be deemed as falling under function of state. Keeping this in mind the assessment of this principle would be restricted to provision of 'optional data' or 'additional data', i.e. data collection which is outside the scope of the purpose of provision of government services.

Individual Participation Rights

Through these rights, users can make a specific request and be assured that their personal information is not being misused for purposes other than legitimate purpose.

As per Rule 5(6), only to right access and correction has been extended to the data subject.

Security Safeguards

This principle places a responsibility on the entity to ensure the reasonable security practises have been put in place around processing of personal data.

As per Rule 8, the entity must implement such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets.

Best Practices

Disclosure of Information

As per Rule 6, disclosure of sensitive personal data or information by the entity any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

Transfer of Information

As per rule 7, the transfer of information may be allowed only if it is necessary for the performance of the lawful contract between the entity or any person on its behalf and provider of information or where such person has consented to data transfer.

Grievance Redressal

As per rule 5(9), the entity shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.

(B) Audit Assurance Program Assessment Parameters

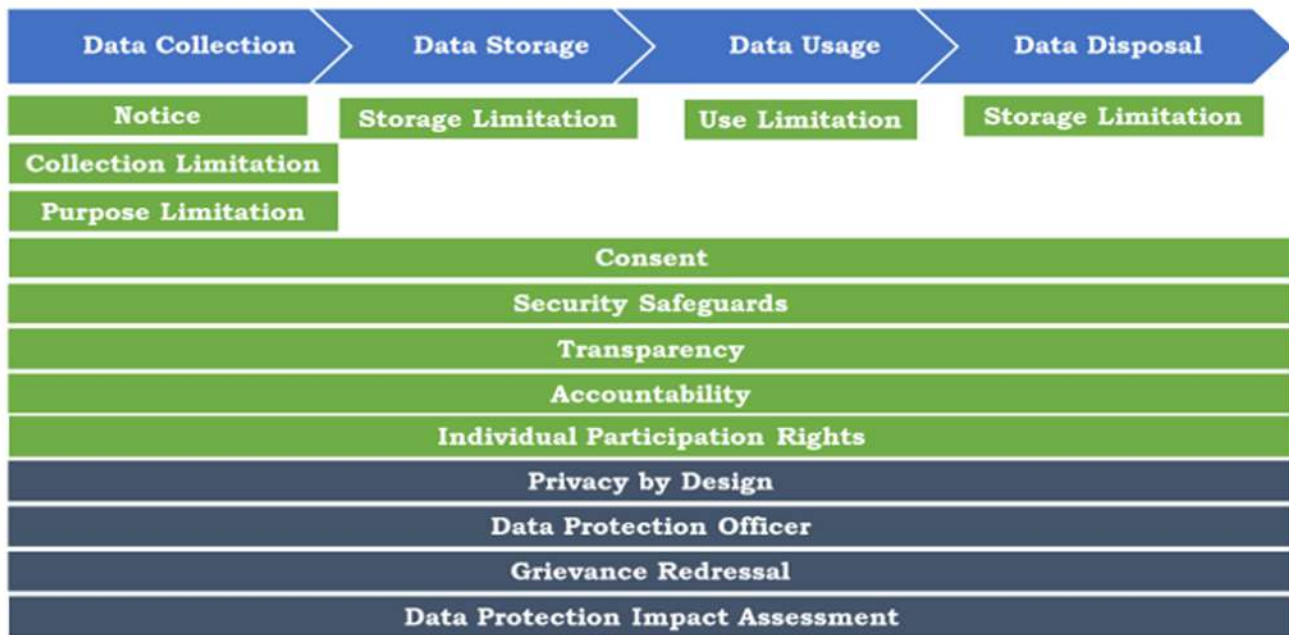


Image 16: Program Assessment Parameters

Privacy Principles for Assessment

The Privacy standard evaluates an e-Governance Project throughout its data collection lifecycle against fundamental privacy principles and best Practices – all of which have been derived from globally accepted principles of privacy and take into account some of the recent developments in this field.

Some of the key aspects of the chosen privacy principles are:

The Privacy principles cover the End to End Information Lifecycle from data collection to disposal. Each Privacy principle accounts for one or more stages of the information life cycle.

Recent developments around privacy and data protection have been taken into consideration to keep the standard contemporary and breathable at the same time.

Privacy principle notice, given its various dimensions of expression has been further categorized into logical Sub-categories. For e.g. Notice has been further divided into sections like Notice Availability, Content and Implementation. This ensures holistic evaluation of each principle

There are interdependencies between the privacy principles. Principles like transparency and accountability are manifested through other principles. i.e. aspects of Notice, Purpose limitation, Use limitation, as well Collection limitation. Data Security, which is a key aspect of Privacy, is covered in detail taking into account security of Personal Information during storage, transmission and disposal. Collectively considered, these Principles can help with the Comprehensive Privacy evaluation of an e-Governance Project.

To test for applicability and ensure robustness, the standards have been applied to and tested against some of the latest set of privacy related incidents pertaining to mobile apps and websites that have occurred in India and globally, as increasing e-Governance services are dispensed through these mediums.

Notice

Privacy notice is a public statement of how the entity applies data protection principles to processing Personal Information.

It is a statement that describes how the entity collects, uses, retains and discloses personal information of a data subject. Privacy notice ensures that data subjects are informed about what is going to happen to their Personal information once it is in the custody of the entity and it also provides the entity an opportunity to communicate its practices and intentions to stakeholders. A robust privacy notice can be considered an indicator of transparency and openness. Data subject can decide whether they want to avail the services provided by a digital product based on the notice. However, there are some challenges that have been observed during the scrutiny that the way entities have implemented notice. Some of these are listed below:

- Inadequate disclosure of the privacy intent and Personal Information usage objectives.
- Notice is complex, lengthy, difficult to understand & comprehend implications.
- There is a practice of transferring obligation to data subjects
- It is difficult to obtain the privacy notice as links are not available or are not working.
- Commitments made in the notice are not implemented in the entity.

Consent

Consent signifies any freely given, informed and unambiguous indication of the data subject's wishes by which they can signify agreement to the processing of their personal information referring. Consent can be obtained by a clear affirmative action.

However, consent maybe not be necessary in all instances of processing. There are certain kind of processing activities which necessitate that the data subject provides their personal data through non-consensual grounds such as function of state. This principle would not be applicable in its entirety in our assessment as the selected e-governance projects carry out collection of data for provision of schemes and services that may be deemed as falling under function of state. Keeping this in mind the assessment of this principle would be restricted to provision of 'optional data' or 'additional data', i.e.

data collection which is outside the scope of the purpose of provision of government services.

Purpose Limitation

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid 'function creep'. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public trust in how you use personal data.

There are clear links with other principles – in particular, the fairness, lawfulness and transparency principle. Being clear about why you are processing personal data will help you to ensure your processing is fair, lawful and transparent. If data is used for unfair, unlawful or 'invisible' reasons, it's likely to be a breach of both principles.

Collection Limitation

Entities collect personal information from user directly through application forms, registration/sign-up pages through applications and websites. In addition, the entity also indirectly collects online identifiers and other personal information residing on the users' device through permissions.

Privacy Law(s) require the entities to collect Personal information from user that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Mobile Apps and Websites can be intrusive and access Personal information like camera, contacts, microphone, location, external storage. The entity may need to access the above features to provide relevant functionality but, in many cases, it may not be relevant.

Use Limitation

Use Limitation principle states that entity may disclose, make available or otherwise use the

Personal Information collected from user solely for the purposes identified in the notice and for which the user has provided consent. Once the Personal Information has fulfilled/met the purpose, it must be destroyed as per the identified procedures for destruction and not be retained beyond the requisite time period.

Storage Limitation

Ensuring that erase or anonymise personal data when no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping to comply with the data minimisation and accuracy principles, this also reduces the risk of use of such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. It is unlikely to have a lawful basis for retention. From a more practical perspective, it is inefficient to hold more personal data than needed, and there may be unnecessary costs associated with storage and security. Remember that anyone to respond to subject access requests for any personal data. Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

Retention policies or retention schedules list the types of record or information held, what for it is used, and how long intend to keep it. This will to establish and document standard retention periods for different categories of personal data.

However, if there is no retention policy (or if exists and doesn't cover all of the personal data held) then a periodical review may be carried out to delete or anonymise anything which is no longer needed.

Security Safeguards

Entities should protect personal information that they collect or have in their custody with reasonable security safeguards against loss, unauthorised access, destruction, use, modification, disclosure or other reasonably foreseeable risks. Such safeguards should be proportional to the risk associated with the personal information misuse and the harms. Entity should also conduct periodic review and reassessment of the security measures deployed.

Transparency

Transparency principle is a fundamental piece of the assessment standard, it has cross cutting elements with other principle such As-Notice, purpose limitation, etc. It places an overarching responsibility on the state to maintain transparency over the processes and practices of the state while processing personal data of individuals for public service delivery.

Accountability

The principle states that an entity is accountable for complying with the privacy principles. Entity must have in place appropriate policies and procedures that promote privacy. Entity should be Transparent in its practices and should provide mechanism for data subject participation.

Accountability also implies the “Demonstration of Compliance”. The principle of Accountability for a mobile application or website is being tested from the perspective of an auditor and regulator.

Individual Participation Rights

The privacy regulations around the world aim to give users more control over the ways in which entities' process their personal information and this has led to the granting of new rights to users. Through these rights, users can make a specific request and be assured that their personal information is not being misused for purposes other than legitimate purpose.

GDPR has included new rights like right to erasure, restriction to processing and objection to automated decision making. Entities are trying to implement processes catering to these rights.

Entity should implement processes to receive and subsequently action upon requests from data subjects around their Rights from a PI perspective. The rights should be clearly communicated to the data subjects and also the process to exercise the rights. The rights could be around access and correction of PI to any other rights depending on the geography. The requests from Data Subjects should be resolved in a reasonable time.

Best Practices for Assessment

Privacy by Design

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after. Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, PbD begins within explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently e.g. preventing (internal) data breaches from happening in the first place. This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy – generally higher than the standards set out by global laws and regulation.
- A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.
- Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

Data Protection Officer

The designation of a specific individual or officer by a data controller to facilitate compliance through monitoring and advising as well as to act as a point of contact with a data protection authority is a crucial element of data protection laws. These individuals are often called data protection officers (DPOs).

Grievance Redressal

It is relevant to note that in the present Indian legal framework, a body corporate is required to designate a grievance officer for grievance redressal purposes with certain details of the same posted on the body corporate's website.

Data Protection Impact Assessment

A data protection impact assessment (DPIA) is a process centred on evaluating activities that involve high risks to the data protection rights of individuals.

The process can become necessary whenever a new project is taken up or a new policy is adopted by a data controller which may involve the use of a new technology or may have a significant impact on the data protection rights of individuals. A DPIA is aimed at describing the details regarding the processing activity, assessing the necessity and proportionality of such an activity, and helping manage the risks that are identified in relation to this activity. The DPIA is carried out before the proposed processing activity is initiated so that the relevant data controller can plan the processing at the outset itself.

Audit Assurance Standard

Minimum Requirements

- Privacy Policy in place
- Privacy Notice in place
- Consent capture mechanism in place, if applicable. In cases where consent is not the grounds used for Processing, a declaration would be obtained from the assessee entity listing the actual grounds used for processing.
- Grievance officer appointed
- Information Security Policy in place
- Cookie banner (website) is present

Some key points around the minimum criteria have been listed below.

1. Presence of a Privacy Policy and Notice are basic minimum criteria for any organization which is committed to Privacy. Privacy Policy is typically an internal document which states the entities' intent and key processes to maintain privacy. Privacy notice, on the other hand, is an external facing document, which talks about the key Personal Information collected and its uses, security posture and also point of contact in case of a grievance. Lack of policy and notice indicates a lack of cohesive planning towards Privacy.

2. A grievance officer is a single point of contact in an entity for the external world from a Privacy perspective. Lack of single point of contact reflects lack of ownership in an organization.

3. Data Security is one of the key areas within Privacy. Presence of information security policy indicates an entity wide approach to towards maintaining the Confidentiality, Integrity and Availability of the data.

Assurance Standard

1.	Notice	
	Availability	<p>Users shall have real time access to the Privacy Notice during the entire Lifecycle of their involvement with the service delivery system. The lifecycle would extend from the time of downloading/accessing the service from the Play store/AppStore/Web Portal, to Installation, registration, usage and any further Personal Information collection that happens during usage.</p> <p>Users shall be updated of any changes to the Privacy Notice.</p>
	Content	<p>Privacy Notice shall be updated if there are any changes to the purpose of processing the PI.</p> <p>Privacy Notice should be available in the local language of the user to ensure that the user full comprehends the terms of the Notice.</p> <p>Entity should provide a notice which clearly states the type of Personal Information being collected from the user, and specifically sensitive personal information like health information, financial information, etc. Notice should also mention the indirect sources of Personal information.</p> <p>Entity should provide a Notice which clearly states the purpose of collection of Personal Information from the User. The purpose should cover PI collected directly from the user as well as from indirect sources.</p>
		<p>Notice should list the 3rd Parties or Categories with whom the Personal Information is being shared, purpose of sharing and any mechanisms like contractual agreements that have been agreed to ensure User Privacy.</p> <p>Notice should communicate to the user if their Personal Information is being transferred to another country and also the purpose of the transfer.</p> <p>Notice should state the Information Security and safeguard mechanisms deployed to protect the Personal Information. Notice should state the Security obligations and expectations from the user.</p>
		<p>Notice should inform the users of the Personal Information retention mechanisms and duration for which Personal Information is retained and the criteria used to determine the retention period. This should cover the entire Lifecycle of product usage and post de-installation.</p>
		<p>Notice should provide details of Mechanism to report misuse/ breach and also the contact point of Grievance Officer for clarification/ recourse / query.</p>
		<p>Notice should mention the Standards followed by the entity.</p>
		<p>Notice should clearly mention organizational responsibilities towards Privacy of user and also mention scope and boundaries of their responsibilities. <i>(E.g. Clicking on Ads that appear on mobile app. Once the user clicks and gets directed to the Web page of ad, organizational boundary ends, and user needs to understand policies of the redirected site)</i></p>

		<p>Notice should clearly communicate to the user about their various rights from a PI perspective. The rights could be around Access and Correction of PI to any other rights (i.e. objection to processing, data portability, erasure) depending on the geography. The significance of the rights and process for availing the rights should also be clearly mentioned.</p>
		<p>Notice should inform the user about the Use of PI for legitimate interest of the entity and also for other lawful basis for processing. To ensure clarity to the user, examples of legitimate interest should be listed.</p> <p>Notice should clearly mention the right of user to file a complaint with the Supervisory Authority as well as the process for the same</p> <p>Notice should provide the user some basics of the entity like contact details and also details of the Notice like Last Updated date</p> <p>Implementation All the statements made in the Notice should have been implemented by the entity in terms of processes and procedures and the same should be verifiable. As other standards are evaluated as part of the Seal, a cross check on whether the details match with the statements in the Notice should be done. (E.g. In Collection Limitation, as the tester reviews the Personal Information collected from the user, one they should evaluate if the Personal Information collected is the same as what's mentioned in the notice).</p> <p>The implementation check would only be confined to the boundaries of the product</p>
2	Consent	<p>Entity should take consent from User for their agreement with the Privacy Policy/Notice for collection of optional/additional personal data which isn't necessary for providing the service.</p> <p>Entity should clearly demarcate mandatory and optional data when collecting data from the user. Optional data are those data points which are not critical for the service provided by the Entity.</p> <p>For optional/ additional personal data collected from the user, they should have the option to withdraw consent at any point of time and the process to withdraw consent should be easily available and communicated to the user in advance. The request should be respected within a reasonable amount of time.</p>
3	Purpose Limitation	<p>Personal data shall be processed only for purposes that are clear, specific and lawful.</p> <p>Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.</p>
4	Collection Limitation	<p>Entity would only collect Personal information (PI) from user which is Adequate and relevant to provide the services, done by lawful (Adhering to all relevant rules of law) and fair (Without intimidation or deception) means and in good faith and does not harm the data subject</p>

		The PI collected by the entity from the User is in line with the information provided in the Notice.
5	Use Limitation	The PI collected by the entity from the User is used for the same purposes and context as mentioned in the Notice.
6	Storage Limitation	Retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed.
		Undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession. Where it is not necessary for personal data to be retained, such personal data must be deleted.
7	Security Safeguards	Security controls would be deployed to protect and secure PI during various stages of the Information Lifecycle including collection, processing, transmission, storage & disposal
		Security controls would be deployed to protect the confidentiality, integrity and availability of PI during Storage. Entities will optimize the secure storage process by eliminating Transactional data which are past utility once the transaction is completed. (E.g. Personal Information stored in local storage is deleted once web site is closed)
		Security controls would be deployed to protect and secure PI during Data Transmission.
		Security controls should be there in place to manage the tracking mechanisms placed in the website
		Secure coding practice to be adopted in order to ensure only required permissions are requested from user. Root level access of device should not be requested from user. Passwords should not be hard coded.
		Security controls would be deployed to protect and secure PI during Data Disposal once the User has uninstalled the application.
		The Security Safeguards deployed by the entity to protect user PI is in line with the details provided in the Notice.
8.	Transparency	Reasonable steps to maintain transparency regarding its general practices related to processing personal data.
		Information with respect to categories of personal data generally collected and the manner of such collection, the purposes for which personal data is generally processed; any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm; available in an easily accessible form to the individual.
		Existence of and procedure for the exercise of individual participation rights.
9.	Accountability	Entity should be accountable for complying with measures that give effect to Privacy Principles. An accountable entity must have in place appropriate policies, procedures for privacy management.

		Entity should ensure Accountability by having clearly delineated roles and responsibilities around Privacy with at least single point ownership on customer grievances.
10.	Individual Participation Rights	<p>User should have the right to object to certain types of Processing on their PI. Entity should implement processes to receive and subsequently action upon these objections from users. The rights should be clearly communicated to the data subjects and also the process to exercise the rights.</p> <p>User shall have the right to receive their personal information collected by the entity in a structured, machine-readable format and have the right to transmit those PI to another entity. Entity should implement processes to receive and subsequently action upon these objections from users. The rights should be clearly communicated to the users and also the process to exercise the rights.</p> <p>User should have the right to request restriction of processing of their Personal Information by the organization. Entity should implement processes to receive and subsequently action upon these restrictions from users. The rights should be clearly communicated to the users and also the process to exercise the rights</p> <p>Users should be able to access and modify their Personal Information as and when needed. The process for access and correction should be clearly communicated to the user.</p>
11.	Privacy by Design	<p>Managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the individual.</p> <p>Privacy Principles have been embedded in organisational practices and processes.</p> <p>Technology used in the processing of personal data is in accordance with commercially accepted or certified standards.</p>
12.	Data Protection Officer	<p>The entity should have a data protection to oversee compliance with regulations and standards. The officer should monitor personal data processing activities of the entity to ensure that such processing is in concurrence with the regulation/standard.</p> <p>The Data Protection officer should be an individual of competence and integrity.</p> <p>The data Protection officer must develop internal mechanisms to maintain compliance with the principles set out in the standard.</p>
13.	Grievance Redressal	<p>Entity shall have in place proper procedures and effective mechanisms to address grievances of individuals efficiently and in a speedy manner.</p> <p>The mechanism should provide redressal in a defined time period. The Grievance officer/ Data Protection Officers' contact information should be displayed in the Privacy notice of the entity.</p>

14. Data Protection Impact Assessment

Data protection impact assessment should be undertaken, processing involving new technologies or large-scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to individuals.

Data protection impact assessment shall contain, detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed, assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed, measures for managing, minimising, mitigating or removing such risk of harm.

Thus, any e-Governance initiative may be examined on the above mentioned criteria and best practices to provides assurance that privacy of data of individuals are protected and also complying the set standard, if any.

Conclusion

An e-Governance Project should lay utmost

emphasis on drafting a privacy notice that clearly communicates the purpose of the collection and usage of personal data, in an easy to understand manner. This assessment revealed certain best practices that would assist projects around the world to comply with whichever privacy regulation they are subject to.



App watch

WHO mYoga App

Yoga has been found to be effective in promoting health and is useful in improving the conditions of patients with cardiovascular diseases, stroke, diabetes and mental disorders. It is recognized as a tool to promote physical activity by WHO also. WHO is developing a benchmark document for training in Yoga as part of its global strategy to strengthen the quality, safety and effectiveness of traditional and complementary medicine with support of the Ministry of Ayurveda, Yoga & Naturopathy, Unani, Siddha and Homoeopathy (Ministry of AYUSH), Government of India. This partnership has gone from strength to strength, most recently with the development of the mYoga app. This app is for the general public and yoga teachers for their daily life uses for persons aged 12-65 years and teaching. It includes WHO approved yoga teaching and practice sessions of different durations developed through extensive international expert consultation processes. It is available in all six UN languages and in Hindi.



Download link:

https://play.google.com/store/apps/details?id=org.who.APPMYOGA&hl=en_IN&gl=US

Secure Me

SecureMe is a new security app which can be used as app launcher. It has a single function of removing all the permissions of that app automatically. It's like a Bouncer (Google Play), but with a different approach. The app doesn't connect to the Internet and requires no special privileges or root to work. It's a pretty simple idea which seems to be executed well. The developers are still working out some bugs, so if you find one, leave some feedback and let them know.



Download link:

https://play.google.com/store/apps/details?id=com.zedsoft.secureme&hl=en_US&pcampaignid=pcampaignidMKT-Other-global-all-co-prtnr-py-PartBadge-Mar2515-1

Quiz corner

1. By auditing around the computer we mean

- (a) the inputs and the corresponding outputs are compared and checked for correctness
- (b) the programs and procedures are checked for correctness
- (c) special synthetic data is input and outputs checked for correctness
- (d) programs are written to check the functioning of the computer.

2. By auditing with a computer we mean

- (a) the inputs and the corresponding outputs are compared and checked for correctness
- (b) the programs and procedures are checked for correctness
- (c) special synthetic data is input and outputs checked for correctness
- (d) programs are written to check the functioning of the computer hardware

3. By auditing through the computer we mean

- (a) the inputs and the corresponding outputs are compared and checked for correctness
- (b) the programs and procedures are checked for correctness
- (c) special synthetic data is input and outputs checked for correctness
- (d) programs are written to check the functioning of the computer hardware

4. An audit trail is established in a system to

- (a) detect errors in a system
- (b) enable auditing of a system
- (c) localize the source of an error in a system
- (d) trail a program

5. Some audit and control procedures in a system

- (i) detect and correct errors in programs
- (ii) selectively print records in a system which meet certain criteria
- (iii) examine credit and debit balances in an accounting system and check if they balance
- (iv) provide a facility to trace a variable value through processing steps and print intermediate values when required

- (a) i and ii
- (b) ii and iii
- (c) i, ii, iii
- (d) ii, iii, iv

6. It is advisable for an auditor to require an operational information system to

- (i) keep logs of all system runs and people involved
- (ii) ensure that the programs and system operation are well documented
- (iii) ensure that no changes are allowed
- (iv) ensure that the inputs and batch controls are properly designed

- (a) i, ii, iii
- (b) ii, iii, iv
- (c) i, ii, iv
- (d) i, ii

7. In auditing with a computer

- (a) auditing programs are designed and used to check a system
- (b) the hardware of the computer is thoroughly checked for malfunctions
- (c) system software is thoroughly checked to ensure error free operations
- (d) auditors check system with a computer

8. Some of the features of audit package used to check systems are:

- (i) facility to total specified items based on some criteria
 - (ii) extracting items based on some criteria for checking
 - (iii) check-pointing and restart facility
 - (iv) Hardware faults recovery
- (a) i, ii
(b) i, ii, iii
(c) i, ii, iii, iv
(d) i, ii, iv

9. By information system testing we mean

- (a) testing an information system correctly
- (b) determining whether a system is performing as per specifications
- (c) determining whether a system is performing optimally
- (d) ensuring proper function of a system

10. The main objectives of testing are

- (i) when correct inputs are fed to the system the outputs are correct
 - (ii) when incorrect inputs are fed to the system they are detected and rejected
 - (iii) the requirement specifications are correct
 - (iv) verify that the controls incorporated in the system function correctly
- (a) i, ii (b) i, ii, iii
(c) i, ii, iii, iv (d) i, ii, iv

11. The scope of the system test includes

- (a) both computerized and manual procedures
- (b) only test of computer procedures
- (c) computerized procedures, manual procedures, computer operations and controls

- (d) mainly computerized procedures and operations controls

12. Program tests use test data to

- (i) exercise all paths taken by a program
 - (ii) test loop counters
 - (iii) test with values which change state of logical variables
 - (iv) comprehensively exercise program
- (a) i, ii
(b) i, ii, iii
(c) i, ii, iii, iv
(d) i, ii, iv

13. By string test we mean

- (a) a test which tests operations with strings
- (b) a string of tests on programs
- (c) Test on related programs
- (d) The output of a program is sent as input to related program(s) to see if data is transferred correctly

14. Parallel runs are used

- (a) during regular operation of an information system
- (b) when a system is initially implemented
- (c) whenever errors are found in a computerized system
- (d) whenever management insists

15. The purpose of parallel run is to

- (a) to see whether outputs of a newly computerized system matches those of currently running manual or legacy system
- (b) have redundancy for reliability
- (c) test an operational information system
- (d) test a system being newly designed

16. Security in the design of information system is used to

- (a) inspect the system and check that it is built as per the specifications
- (b) protect data and programs from accidental or intentional loss
- (c) ensure that the system processes data as it was designed to and that the results are reliable
- (d) ensure privacy of data processed by it

17. A relationship check

- (a) is concerned with checking a relation
- (b) uses an entity-relationship model for checking
- (c) finds out if a relationship is satisfied in computation
- (d) uses the fact that a known relationship exists between two data elements and checks if it is satisfied during computation

18. A check-point procedure

- (a) checks program correctness at certain points
- (b) divides a program into smaller parts
- (c) breaks a programs into portions at the end of each of which a check point program is executed
- (d) finds points in a program where it is convenient to check it

19. At each check-point

- (i) quantities such as control totals and proof figures are checked for correctness
 - (ii) process state is stored in secondary storage
 - (iii) a program halts for check by programmers
 - (iv) a self-checking system is invoked by the analyst
- (a) i and iv
 - (b) ii and iii
 - (c) i and ii
 - (d) i and iii

20. Audit in the design of information system is used to

- (a) inspect the system and check that it is built as per specifications
- (b) protect data from accidental or intentional loss
- (c) ensure that the system processes data as it was designed to and that the results are reliable
- (d) ensure privacy of data processed by it

Answer: 1(a) 2(c) 3(b) 4(c) 5(d) 6(c) 7(a) 8(b) 9(b) 10(d) 11(c) 12(b) 13(d) 14(b) 15(a) 16(b) 17(d) 18(c) 19(c) 20(a)

Answers of fifth issue: 1(c) 2(d) 3(d) 4(a) 5(d) 6(c) 7(d) 8(d) 9(d) 10(a) 11(a) 12(c) 13(b) 14(d) 15(b) 16(d) 17(d) 18(d) 19(c) 20(c)