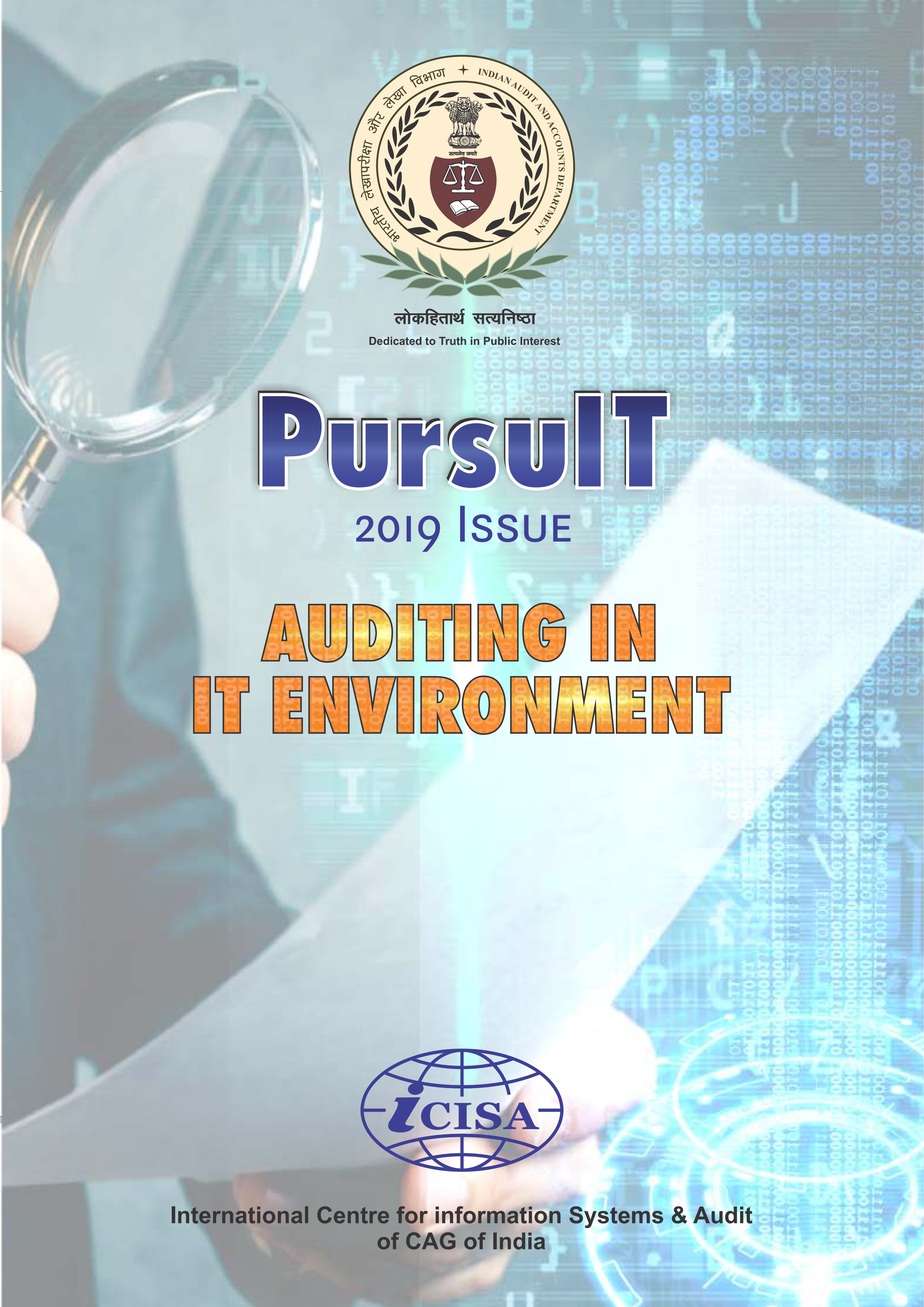


लोकहितार्थ सत्यनिष्ठा

Dedicated to Truth in Public Interest

PursuIT

2019 Issue

AUDITING IN IT ENVIRONMENT

International Centre for information Systems & Audit
of CAG of India

CONTENTS

PursuIT

2019 Issue-Auditing in IT Environment

About the Journal

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

Editorial Board

Submission of Articles

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

Feedback/Suggestions

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

Disclaimer

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

DG'S MESSAGE

With increasing use of technology in the field of Audit, the way three types of audit (Financial, Compliance and Performance) are being planned and conducted, could change dramatically in the future. We could visualise a situation where audit sampling is not necessary where end-to-end process automation is implemented and "100 percent" audit is feasible. In such a situation in the future, data analytics and Artificial Intelligence (Largely Machine Learning), available through cloud-hosted, secure platform, could form the foundation for audit risk assessment and planning. "Auditee units/ entities" may no longer form the primary basis for audit planning instead, and analytics platform, with substantial staff resources, could drive the identification of red-flagged/ anomalous transactions through a workflow pipeline for detailed examination and/ or direct intimation to the auditee. This is a technology enabled vision for IAAD.

Since its formation in 2002, iCISA has contributed to the world audit fraternity through its training programs. In the past, there has been a practice of sharing the latest developments in the Information Technology matters by way of an Online Journal PursuIT. This is the third e-Journal in this series with the theme "Auditing in IT Environment". Also to mention, one entire International Training Programme is dedicated to this theme of "Auditing in IT Environment", acknowledging the changing landscape of the audit process. There are articles in the e-Journal which talk about emerging technologies and also case studies with direct audit application within IAAD.

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

K R Sriram
Chief Technology Officer &
Director General (iCISA)

DG's Message contains excerpts from the Approach Paper of the AGs and DAGs Conclave concluded in November 2019 on the theme "Transforming Audit and Assurance in the Digital World". The full paper can be read at CoRE portal at https://cag.gov.in/core

Auditing In GMIS Environment

- Dr. Nanda Dulal Das, IA&AS

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.

Government process re-engineering, in the present parlance, has necessitated moving the essential government processes to electronic platform. In this context 'Auditing in GMIS Environment' holds significance for audit organisations. The term GMIS here refers to an integrated system of Geographic Information System (GIS) and Management Information System (MIS), both of which are by themselves two different Decision Support Systems (DSS) and amalgamation of which is expected to help develop a better DSS. Executives have been using both of these systems for better monitoring of social sector schemes and GMIS integration is visible in some major flagship schemes like MGNREGS, PMAY[i], NRHM[ii] etc. This article seeks to focus on selection of samples and an attempted audit observation based on the MIS and GIS data for one scheme, namely, MGNREGS with scope for similar analysis for other schemes like the Mid-Day Meal (MDM) Scheme, PMAY and NRHM.

Planning : Setting Audit Objectives and Sampling Using GIS and MIS

Let us start with the following audit objectives for auditing implementation of the MGNREGS in the state of Odisha:

1) To provide a picture of actual job availability among the needy sections of job-seekers in different rural areas, i.e. villages away from large urban centres, for example, in villages of Kandhamal district in Odisha and

2) To assess the difference in quality of assets, if any, built in different districts in the state of Odisha.

To address these selected objectives, data on the following items are needed (Table 1):

Table 1: Selection of Parameters and Data Sources

Sl. No.	Parameters for the purpose	Detailed Parameters	Source of Data
1	To find out villages away from urban centres	-Selection of villages located away from large urban centres (population weighted distance may be decided, to find out selected villages)	GIS-based extraction from the unit-wise Map of India/Odisha
2	To find out the extent of presence of needy sections	-Proportion of SC/ST population in the selected unit -Extent of literacy/illiteracy in the selected units -Proportion of marginal workers to the total workers in the selected unit -Proportion of marginal workers-cum agricultural labourers to the total marginal workers in the selected unit	Census Data, 2011
3	To bring out the status of actual job availability	-Proportion of household in the selected unit, demanded and provided with job under the MGNREGS -Average man-days of employment generated in the area	MGNREGS-MIS
4	To determine quality of assets built in the selected area	Intensity of expenditure on the assets selected (I.e. higher expenditure on one road in a village than a similar road in other nearby village in the same State would mean better uality, prima facie) Field visit and beneficiary	MGNREGS-MIS (expenditure data on assets) Household Survey

Since, MGNREGS seeks to promote rural wage-employment, the villages away from the influence of large urban centres would reflect the impact of MGNREGS in better way than the villages closer to the urban centre. Hence, GIS analysis would be very helpful to find out villages away from urban areas in a scientific manner. As per 2011 Census of India, there are nine cities with more than a lakh population (Table 2). Bhubaneshwar, with a population of 8.8 lakh, is the largest city and Baripada with 1.1 lakh, is the smallest among them. Hence, people from more distant areas would remain dependent on Bhubaneshwar when compared to similar dependency of people on Baripada. Hence, while selecting study villages more distance-weight can be assigned to Bhubaneswar and less weight to Baripada in the manner shown in the following table (Table 2).

Table 2: Cities in Odisha with more than one lakh population and assignment of distance-weights based on population

Rank	City	Population	Distance-weights (100 Km for 1 lakh)
1	Bhubaneswar	881,988	88
2	Cuttack	658,986	66
3	Raurkela	552,970	55
4	Brahmapur	355,823	36
5	Sambalpur	269,575	27
6	Puri	201,026	20
7	Balasore	177,557	18
8	Bhadrak	129,152	13
9	Baripada	116,874	12

Source: Provisional Population Table, Census of India, 2011

Selecting distance weights (assuming that people, within a radius of 100KM, would to large extent depend on the city which has one lakh population), buffer areas around the cities have been created. In other words, bigger cities would have larger area under their influence than smaller cities in the State. Now to see the impact of MGNREGS, sample villages are required to be selected from outside the city-buffer areas. Using techniques of GIS, distance buffer areas have been generated in the following diagram (Diagram 1).

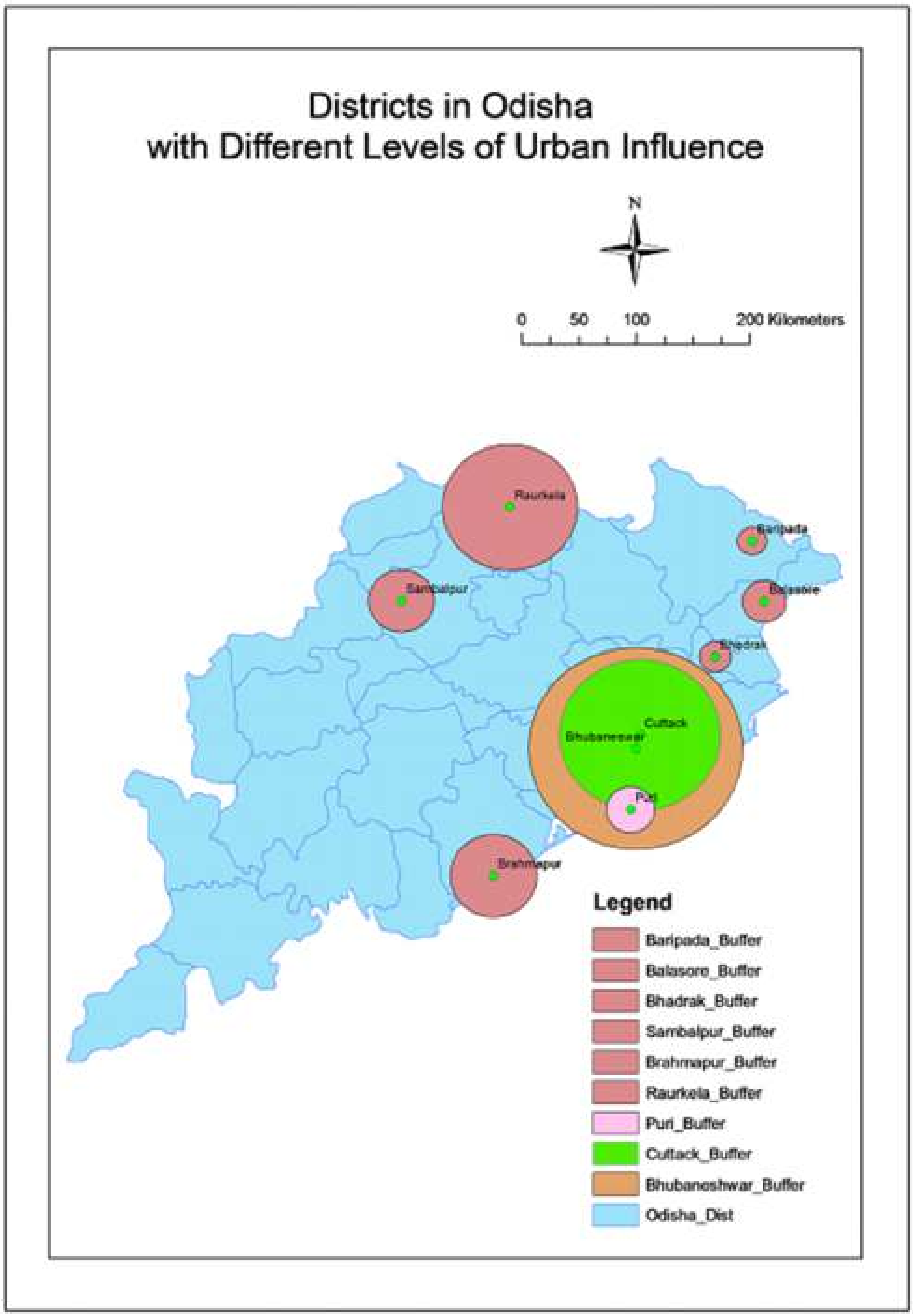


Diagram 1: **Buffer Areas around Large Cities in Odisha Overlapped on District Map of Odisha to show the area of Urban Influence**

At the next level, this study intends to find out presence of needy sections. To develop this point, four indicators, as detailed in serial number 2 in Table 1 above, have been selected to find out the areas with perceived higher requirement for wage employment. A composite index from these four indicators have been prepared using a simple method and result is produced below in Table 4[iii].

Interestingly, it can be seen that the indicators of needfulness show that the districts of Khordha (in which Bhubaneshwar city is located), Cuttack and Puri have the lowest need for wage-employment as per this analysis and have also been excluded from the samples by the distance-weighted buffer method using GIS, as detailed in the previous paragraphs. For the purpose of this study, sample villages can be selected using systematic random sampling method. For example, we select district with serial number 1, then every third, i.e. 4, 7, 10, 13, 16 and so on. So, following ten districts get selected for the audit, to be done using MGNREGS MIS data in this case as shown in table 3 below. Otherwise, if one wishes to study the regions with higher perceived need for wage employment, then the first five districts only can be selected and further selection of audit units/implementing units may be done downward (Judgemental Sampling).

Table 3: Selection of Audit Units using Random/ Judgemental Sampling

Sampling Method: 1		Sampling Method: 2	
Sl. No.	**Orissa Districts**	**Sl. No.**	**Orissa Districts**
1	Nabarangapur	1	Nabarangapur
4	Kandhamal	2	Malkangiri
7	Koraput	3	Rayagada
10	Debagarh	4	Kandhamal
13	Balangir	5	Mayurbhanj
16	Bargarh		
19	Sambalpur		
22	Dhenkanal		
25	Jajapur		
28	Cuttack		

Further, with similar set of indicators one can select audit units representing Blocks and Gram Panchayats.

[i] Detailed guidelines regarding integration between GIS and MIS under the Rajiv Awas Yojana (RAY)/ Pradhan Mantri AwasYojana (PMAY) was made for 2013 to 2022.

[ii] National Rural Health Mission: Presence of a good GIS-MIS system can be found in implementation of NHM in Assam (http://www.nrhmassam.info/).

[iii] Variable 1= (xi-mini)/(maxi-mini), since higher value for the selected indicators would mean higher demand for wage employment. The composite index has been derived by simply averaging other four indicators (Venkaiah, K. et.al. A. Development of composite index and ranking the districts using nutrition survey data in Madhya Pradesh, India. Indian J Comm Health. 2015; 27, 2: 204-210).

Table 4: Ranking of Districts in Odisha using Composite Index of Needfulness (Source mentioned in footnote on pre-page)

Sl. No.	Orissa Districts	% of SC/ST Pop	V1_SC-ST	%_Illiterates	V2_PC_Ill	% of Marginal Worker	V3_PC_MW	% of MW-AL to total Marginal Workers	V4_PC_MW_AL	Composite_Index
1	Nabarangapur	70	0.84	53.57%	1	54	0.97	77	0.98	0.95
2	Malkangiri	80	1	51.46%	0.95	42	0.63	71	0.84	0.86
3	Rayagada	70	0.84	50.24%	0.92	51	0.89	64	0.69	0.84
4	Kandhamal	69	0.82	35.87%	0.56	53	0.94	76	0.96	0.82
5	Mayurbhanj	66	0.77	36.83%	0.59	55	1	63	0.67	0.76
6	Kalahandi	47	0.47	40.78%	0.68	50	0.86	68	0.78	0.7
7	Koraput	65	0.76	50.79%	0.93	43	0.66	52	0.42	0.69
8	Nuapada	47	0.47	42.65%	0.73	50	0.86	63	0.67	0.68
9	Kendujhar	57	0.63	31.76%	0.46	42	0.63	78	1	0.68
10	Debagarh	52	0.55	27.43%	0.35	50	0.86	68	0.78	0.64
11	Gajapati	61	0.69	46.51%	0.83	42	0.63	47	0.31	0.62
12	Sundargarh	60	0.68	26.66%	0.33	39	0.54	73	0.89	0.61
13	Balangir	41	0.37	35.28%	0.55	47	0.77	57	0.53	0.56
14	Baudh	36	0.29	28.39%	0.38	44	0.69	70	0.82	0.55
15	Subarnapur	35	0.27	25.58%	0.31	41	0.6	73	0.89	0.52
16	Bargarh	39	0.34	25.38%	0.3	38	0.51	73	0.89	0.51
17	Anugul	33	0.24	22.47%	0.23	40	0.57	72	0.87	0.48
18	Ganjam	23	0.08	28.91%	0.39	40	0.57	71	0.84	0.47
19	Sambalpur	53	0.56	23.78%	0.26	33	0.37	61	0.62	0.45
20	Jharsuguda	49	0.5	21.14%	0.2	31	0.31	54	0.47	0.37
21	Baleshwar	33	0.24	20.21%	0.18	34	0.4	61	0.62	0.36
22	Dhenkanal	33	0.24	21.24%	0.2	36	0.46	55	0.49	0.35
23	Bhadrak	24	0.1	17.22%	0.1	30	0.29	63	0.67	0.29
24	Nayagarh	20	0.03	19.58%	0.16	33	0.37	55	0.49	0.26
25	Jajapur	32	0.23	19.87%	0.17	26	0.17	53	0.44	0.25
26	Kendrapara	22	0.06	14.85%	0.04	31	0.31	48	0.33	0.19
27	Jagatsinghapur	23	0.08	13.41%	0.01	28	0.23	51	0.4	0.18
28	Cuttack	23	0.08	14.50%	0.03	26	0.17	49	0.36	0.16
29	Puri	20	0.03	15.33%	0.05	28	0.23	48	0.33	0.16
30	Khordha	18	0	13.12%	0	20	0	33	0	0

Where: 1. PC= Percentage | 2. MW= Marginal Workers | 3. AL = Agricultural Laborer

Conducting: Audit Execution using MIS

Once the composite index was derived and sampling was conducted, following performance indicators of MGNREGS have been extracted from the MGNREGS-MIS:

i) Percentage of households issued with job-cards, to total number of households, in different districts

ii) Percentage of households provided with employment, to total number of households, in different districts

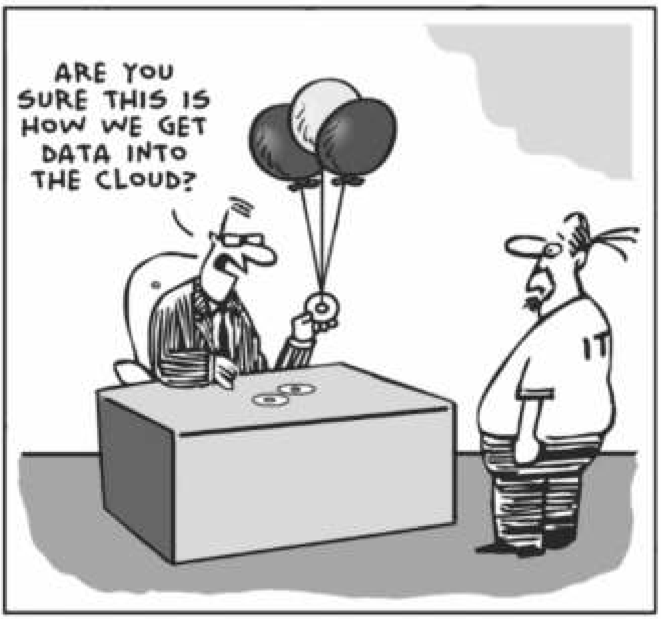
iii) Average person-days generated per household who were provided with employment

iv) Workers with age more than 60 years of age participating in MGNREGS

v) Average number of assets built per thousand households and

vi) Average expenditure on assets per thousand households.

These indicators are expected to show a positive correlation with the need-index developed in the previous section. In other words, higher the value of the composite index depicting higher need for employment, higher would be participation of the households in the wage-employment programme, higher would be the number of assets and expenditure incurred on those assets. This higher average investment may lead to better assets generation, or it could also be a result of inefficient use of resources. Either way this raises the flag of materiality for auditors, to be checked during field audits. Hence, in an IT environment, a simple correlation is tested between the composite indicator and individual MGNREGS performance indicators. It is found that in all the cases there remains a significant positive correlation between the composite indicator and individual MGNREGS performance indicators, except one indicator (workers with more than 60 years of age participating in the program, which is an encouraging social symptom), as detailed below in Table 5.



Reference: https://whatsthebigdata.com/2017/02/24/cloud-computing-cartoons/

Table 5: Correlation between the Composite Need-Index and Indicators Depicting Performance of MGNREGS

Correlation with Composite Indicator depicting need for wage-employment **(Pearson Correlation)**	
Percentage of households issued with job-cards, to total number of households	.706**
Percentage of households provided with employment, to total number of households	.779**
Average person-days generated per household who were provided with employment	.662**
Workers with age more than 60 years of age participating in MGNREGS	-.717**
Average number of assets built per thousand households	.804**
Average expenditure on assets per thousand households	.762**

**Correlation is significant at the 0.01 level (2-tailed).

This significant positive correlation between the selected indicators largely point to the fact that MGNREGS is catering to the needs of the wage employment, where they are needed the most. The number of assets and expenditure on assets are also pointers of success of MGNREGS in bringing in balanced regional development, to some extent.

However, despite this significant positive correlation, it is seen from the ranking of individual districts, as detailed in Table 6 below, that while Nabarangapur district is ranked one in the composite indicator, in terms of some of the performance indicators, this district is found to be quite down in the list.

Table 6: Comparison between Ranking of Districts in Composite Index and Performance Indicators of MGNREGS

Districts	Rank in Composite Index	Rank in_%HH_Jobcards_Total HH	Rank_%HH_ provided_emp	Rank_Avgpersondays generated per HH	Rank_>60 age worker as % of total employed	Rank_Average no. of assets per 1000 HH	Rank_Average exp. of assets per 1000 HH
NABARANGAPUR	1	2	26	28	18	11	10
MALKANGIRI	2	14	27	7	5	3	21
RAYAGADA	3	4	25	13	8	18	7
KANDHAMAL	4	5	11	2	10	9	17
MAYURBHANJ	5	13	23	15	16	5	9

Where **HH** indicates House Hold.

This observation also points to the fact that some of the comparatively well-off districts could manage to derive some of disproportionate benefits under the scheme, probably at the cost of other districts. However, quality of assets and nature of dynamics observed in the field can only be assessed properly when asset survey and beneficiary interviews are carried out at the field level. This also necessitates for selecting some of audit units further down to block and Gram Panchayat, particularly those which would explain the anomaly.

However, using the composite index is with the acknowledgement that this cannot be perfect in the real world, and has shortfalls. While drawing a correlation between the composite need index and MGNREGS Performance, the (implicit) assumption that the efficiency and effectiveness of implementation of MGNREGA is similar in the higher need index districts as in other districts may not be valid. This is perhaps the reason that Nabarangpur is not performing as well in MGNREGA despite being one amongst the poorest districts. Also, provision of employment is not the same as demand for employment; this is important as properly captured demand for MGNREGA would be closely correlated with the Need Index.

Conclusion:

This study mainly focused on highlighting the high risk areas pertaining to this audit by working in the GIS and MIS environment, which could largely facilitate the field auditing process before the audit team even charts out a field visit. Remote Sensing can also function as data source for basic analysis if one is interested in knowing the changes that took place in an area post introduction of some projects or to obtain a separate set of spatial statistics to substantiate what has been provided by the executives[iv]. GIS techniques further adds several analytical tools to it and thereby enhances the level of assurances that the audit process gives as it ensures that large areas and different parts of the audit units have been covered substantially to provide reasonable assurance on conclusion of the audit process.

References

1) Blanc, L. et. al. (2016). "Remote Sensing and Measuring Deforestation", Land Surface Remote Sensing, pp. 27-53, Copyright © 2016 ISTE Press Ltd. Published by Elsevier Ltd.

2) "Compliance Auditing Guidelines", (2016). Comptroller and Auditor General of India, New Delhi, India.

3) Duan, H. etl al. (2019). "Detection of illicit sand mining and the associated environmental effects in China's fourth largest freshwater lake using daytime and nighttime satellite images", Science of The Total Environment, Vol. 647, 10 January 2019, Pages 606-618, © 2018 Elsevier B.V.

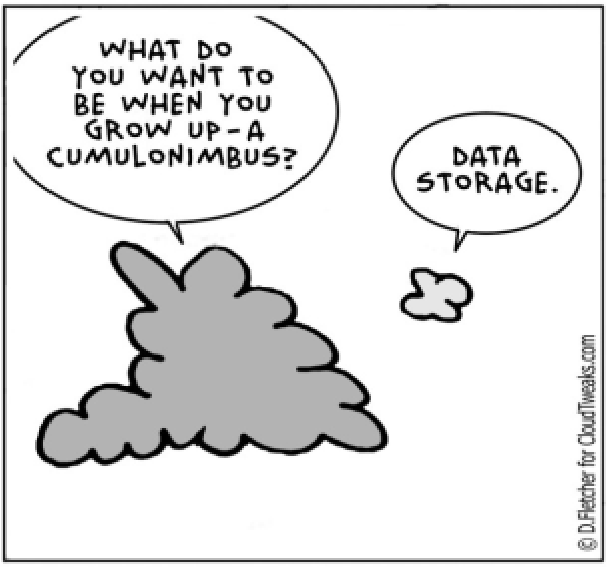
4) "GIS-based Municipal Information System (GMIS) for Improved Urban Planning" (2014), Cowater-Sogema, Ottawa, Canada. As viewed on 24th March, 2019 at https://cowatersogema.com/

5) "Integrating GIS and MIS: Database-level Integration for Watershed Development" (2017), GIM International, The Netherlands. As viewed on 24th March, 2019 at https://www.gim-international.com

6) "Rajiv Awas Yojana Guidelines for GIS, MIS, GIS & MIS Integration (2013-2022)", Ministry of Housing and Urban Poverty Alleviation, Govt. of India.

7) Suresh, M. and Jain, K. (2013). "Change Detection and Estimation of Illegal Mining using Satellite Images", Proceedings of 2nd International Conference on Innovations in Electronics and Communication Engineering (ICIECE-2013), Roorkee, India.

8) Voilini, S. (2013). "Deforestation: Change Detection in Forest Cover using Remote Sensing", Seminary – Master in Emergency Early Warning and Response Space Applications.Mario Gulich Institute, CONAE. Argentina


WHAT DO YOU WANT TO BE WHEN YOU GROW UP - A CUMULONIMBUS?
DATA STORAGE.
© D.Fletcher for CloudTweaks.com

Reference: https://whatsthebigdata.com/2017/02/24/cloud-computing-cartoons/

Restraining Risks In e-Governance/ ICT Based Projects: The Role Of Auditors

- Dr. Charru Malhotra[1]

Dr. Charru Malhotra, is presently working as an Associate Professor (e-Governance and Information & Communication Technology) at The Indian Institute of Public Administration (IIPA), New Delhi, INDIA. She is also Project Coordinator for a significant capacity building 'training of trainers' module under the prestigious Digital India Program of Government of India, India. She has undertaken impact assessment of several e-Government initiatives of GoI and has also been National ICT Consultant (India) for Asian Development Bank (ADB) in a rural e-Governance project and has served United Nations Development Program (UNDP), Winrock International as well as The World Bank as Short Term MIS/ GIS/ SmartCities Consultant. She has published more than 30 research studies in reputed international and national journals and has more than 28 years of experience in the field.

1. Introduction

Risks are situations that may have a negative effect on the goals and objectives of the project. These could surface due to uncertain factors that were either not anticipated or were not accounted for. This unpreparedness may negatively affect project costs or create dissatisfied customers or lead to schedule overruns thereby ruining the quality of the deliverables. Application of ICTs[2] assures improvements to the existing way of undertaking project activities. This becomes more relevant when the size and scope of the project expands to include the entire community or citizenry, such as in e-Governance[3] projects. However, the trends in ICTs evolve quite rapidly and therefore going online itself could entail several negative repercussions. The vast scope, criticality of public services and the delicate nature of citizens' data associated with e-Governance projects could further aggravate the risk-scenarios. Therefore, risks associated with e-Governance / ICT based projects, henceforth referred to as digital projects too in the study, need to be assessed and managed well to ensure timely, effective, and efficient deliverables. The proposed review paper is a systematic attempt to profile the risk landscape of e-Governance .

[1] Contact : IIPA, I.P. Estate, Outer Ring Road, New-Delhi-110002, Mobile: +91- 9818529298; 9318489364 ; charrumalhotra@gmail.com; charrumalhotra.iipa@gov.in

[2] Information Communication Technologies-ICTs, erstwhile referred as Information Technologies (IT), are electronic/digital computing and communications technologies that encompass desktops, networking, internet, mobile, cloud, websites, web- portals, social media, emerging technologies and so on. They are also referred as 'digital technologies' in this study.

[3] ICTs have been primarily deployed for the delivery of public services and information, popularly referred to as 'e-Government'. When ICTs are also used to include citizens' participation in the governance processes, then it is called 'e- Governance'. However, for popular consumption, both the terms could be used interchangeably, which is the instance in this study too.

1.1 Overview of the Paper

The first section titled 'Introduction' has already set the tenor of the paper where the need for undertaking such a study has been encapsulated. The next section encapsulates the learnings gathered from the review of literature undertaken on the key aspects of the study viz. 'types of risks' and the 'role of auditors'. This section establishes the background of the reader to identify and categorise the risks that digital projects are more specifically likely to face (section-3). Based on the learnings gleaned from the previous sections, the study moves on to specifically list the active role that the contemporary auditors (stressing the role of internal auditors) are expected to discharge to ensure the success of ICT based projects (section-4). The paper concludes (section-5) by asserting that in present digital times, the auditors cannot afford to stay only as reticent actors who are restricted to only 'control audits'; rather they must prepare themselves to be the 'active partners of growth' and 'agents-of-digital-change' in their organizations by imbuing ever evolving risk management strategies related to digital projects.

2. Review of Literature

The literature pertaining to three broad areas of immediate relevance viz. types of risks and their classification, risk management and role of auditors in risk management, were examined in order to understand the overall landscape of risks.

2.1 Types of Risks

Liu and Wang (2014)[4] emphasis that strategically important projects are more risky. ICT based projects are high-risk activities and they generally produce variable outcomes (Charette, 2005)[5]. The industry surveys (Aon Risk Solution, 2017)[6] report that only about a quarter of software projects succeed, i.e. they complete as scheduled, budgeted and specified and billions of dollars are spent on projects that either fail or do not deliver as promised. There are broadly two categories of risks encountered by ICT based projects in government viz. 'Generic risks' and 'Project specific' risks (Choudhary, Banwet & Gupta, 2007)[7]. Researchers Liu and Wang (2014)[8] proclaim that irrespective of type of risks or the project implementation strategy (in- house or outsourced), managing risks continues to be a central problem especially for ICT based projects. It was concluded after the primary survey of 77 in-house projects and 51 outsourced projects.

[4] Liu, S., & Wang, L. (2014). Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance. International Journal of Project Management, 32(8), 1494-1510.

[5] Charette, R. N. (2005). Why software fails [software failure]. Ieee Spectrum, 42(9), 42-49.

[6] Aon Risk Solution (2017), Global Risk Management Survey

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

[8] Liu, S., & Wang, L. (2014). Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance. International Journal of Project Management, 32(8), 1494-1510.

It was understood that the 'technical risks' (shortage of technically trained work force, new technology etc.) hamper in-house projects and the 'social risks' (too many requirement changes, unclear requirements, insufficient business knowledge etc.) assail the outsourced projects. Wallace, Keil and Rai (2004)[9] have classified risks in six dimensions viz. 'complexity', 'organizational environment', 'system requirement', 'planning and control', 'users' and 'development team'. Nagaraja (2016)[10] cautions that e-Gov projects are likely to confront 'project management risks', 'influence of ever changing global policy frameworks' and 'socio- cultural risks' specific to the context of country. Many other researchers too have delved into finding the types of risks. For instance, Bedi, Singh and Srivastava (2001)[11], attribute risk in e- Governance projects to factors such as 'limited technical knowledge', 'delayed processes', 'limited functionalities', 'budget overruns' and 'top down approach'. Subsequently, Tchankova (2002)[12] has proposed seven risk areas with two additional aspects viz. 'Legal' and 'Cognitive environment' to the list that had been put forth by Evangelidis (2004)[13]. The latter has squeezed this list to only five risk areas viz. 'social', 'technical/ operational', 'economic', 'political' and 'security/physical', which is incidentally quite similar to the generic Political, Economic, Sociocultural & Technological (PEST) framework suggested by Aguilar (1967)[14] . The present study takes cue from this list to classify risks restraining e-Governance / ICT based projects (section 3).

2.2 Role of Auditors in Risk Management

The role of auditors is changing from a traditional audit approach to a more proactive, value- added approach where auditors are expected to collaborate with the management whilst (re)designing its vision and action plans for their organisation. The most pertinent query raised by Froth (2003)[15], “How can auditors identify the practices that will add the most value given their own specific situation” is indeed quite relevant for auditors to define the expectations of their role in risk management. Auditors' objective evaluations and opinions are a valuable input for the new internal control review and disclosure requirements.

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

[10] Nagaraja, K. (2016). E-Governance in India: Issues and Challenges. IOSR Journal of Economics and Finance 7(5) Ver. IV, 50-54. DOI: 10.9790/5933-0705045054

[11] K. Bedi, P.J. Singh, S. Srivastava, (2001). Government net: new governance opportunities for India. SAGE.

[12] Tchankova, L. (2002). Risk identification–basic stage in risk management. Environmental Management and Health, 13(3), 290-297.

[13] Evangelidis, A. (2005). FRAMES–a risk assessment framework for e-services. Electronic Journal of e-Government, 2(1), 9

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

[15] Froth, J. (2003). How do internal auditors add value. Internal Auditor, 60(1), 33-37.

A study by Sarens and Beelde (2006)[16] suggests that auditors need to not just focus on the acute shortcomings indicated in the risk management process but also help to evolve strategies to overcome these pain points. Allegrini and D'Onza (2003)[17] undertook an empirical survey on risk assessment practices undertaken by auditors of large Italian companies by studying their audit documents. Their study revealed that a few companies (25% of the surveyed) carry out mainly traditional compliance activities and generally followed an audit-cycle approach (Milan & Dai, 1999)[18] for the annual audit planning. In most of the companies (67%), auditors had adopted the COSO model[19] (reference to COSO model can be seen in section 4.1) to perform operational auditing. Further, a very few large companies (8%) had been sighted in which auditors were applying a risk-based approach (McNamee, 1997)[20] both at macro and micro level. Another study (Mihret and Yismaw, 2007)[21] had been performed on an Ethiopian based public sector higher educational institution, where it was found that the internal audit quality, management support, organisational setting, and auditor attributes are the factors that play an important role in improving the effectiveness of auditing. Overall, this information about types of risk with special emphasis on role and expectations from auditors understood from the review of literature would be instrumental in assessing and managing risks in context of e-Governance/ ICT based projects.

3. Risks Pertaining To e-Governance / ICT Based Projects

The world has seen a growth in e-Governance projects, which promise greater efficiency and effectiveness of public sector operations. However, camouflaged behind these glowing advantages, lies a bitter fact that majority of these projects tend to fail either partially (50% of the projects) or completely (35% of the projects) (Table 1).

[16] Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. Managerial Auditing Journal, 21(1), 63-80.

[17] Allegrini, M., & D'Onza, G. (2003). Internal auditing and risk assessment in large Italian companies: an empirical survey. International Journal of Auditing, 7(3), 191-208.

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

[19] Committee of Sponsoring Organisation of the Treadway Commission. (1992). COSO Internal Control – Integrated Framework 2013. KPMG.

[20] McNamee, D. (1997). Risk-based auditing. Internal Auditor, 54(4), 22-27

[21] Getie Mihret, D., & Wondim Yismaw, A. (2007). Internal audit effectiveness: an Ethiopian public sector case study. Managerial auditing journal, 22(5), 470-484.

Table 1: e-Governance project failures- facts and reasons

Sno	Status	% of Projects	Reasons
1	Total failures (initiatives never implemented or abandoned immediately)	35% of total e-Government projects	● Initiatives not implemented ● Initiatives abandoned immediately
2	Partial failures (major goals not attained and/or significant undesirable outcomes)	50% of e-Government projects	● Main stated goals not achieved ● Initial success but failure after an year ● Success for one group but failure for another
3	Success most stakeholders attained major goals and didn't experience significant undesirable outcomes	15% of e-Government projects	● All stakeholders benefited ● No adverse effects

(Source: http://www.nisg.org/docs/539_Report.pdf)

Despite widespread use of advanced tools and technologies, project development all over the world suffer failure at one phase or the other due to several risks , some of the most popular being, in no particular order, shortage of technically trained manpower, rapid requirement changes insisted by the user-organisation, fast obsolesce etc. (Figure- 1).

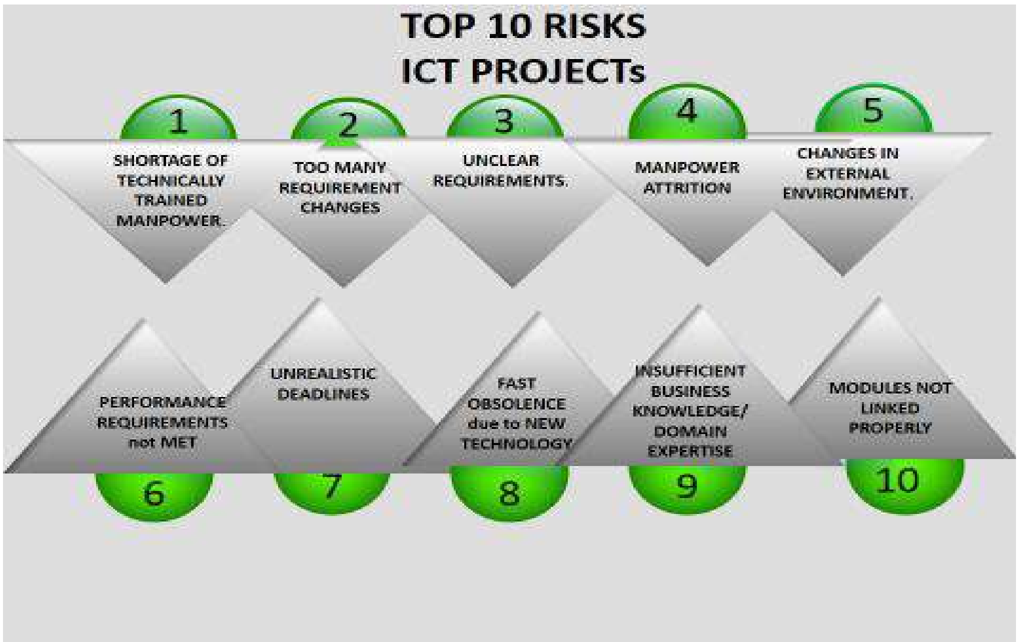

TOP 10 RISKS
ICT PROJECTs
1
SHORTAGE OF TECHNICALLY TRAINED MANPOWER.
2
TOO MANY REQUIREMENT CHANGES
3
UNCLEAR REQUIREMENTS.
4
MANPOWER ATTRITION
5
CHANGES IN EXTERNAL ENVIRONMENT.
PERFORMANCE REQUIREMENTS not MET
6
UNREALISTIC DEADLINES
7
FAST OBSOLESCENCE due to NEW TECHNOLOGY
8
INSUFFICIENT BUSINESS KNOWLEDGE/ DOMAIN EXPERTISE
9
MODULES NOT LINKED PROPERLY
10

Figure-1: 10 Top Risks that are likely to infest e-Governance/ ICT based projects

(A subjective list, in no particular order, based on experience/study only)

These failures come at quite a high price and Heeks (2003)[22] has classified the potential costs of e-Government failures under six heads. These six heads are 'Direct Financial Costs' (money that is invested in fixed assets, facilities, human resources, training programmes), 'Indirect Financial Costs' (money invested in time and effort of public servants involved), 'Opportunity Costs' (Better ways in which money could have spent had it not been spent on the e-Government failure), 'Political Costs' (loss of goodwill of an individual, organisations and nations involved), 'Beneficiary Costs' (The loss of benefits that a successful e-Government project would have brought) and 'Future Costs' (loss of morale of stakeholders and loss of credibility and loss of trust in e-Government). A large amount of money is lost on cancelled projects, late delivery, cost overruns, and poor quality of deliverables. A typical 'failed practice' is the case-study of new payroll system introduced for the employees of Queensland Health by State Government of Queensland, Australia in the year 2006 which five years down the line was touted to be the biggest failures in public administration of Australian history (Hamrouni, 2017)[23]. The initial contract was budgeted for around $6 million for the 80,000 employees of Queensland Health. The project was supposed to go live in six months after announcement, however till the year 2010 it didn't go live. An additional cost of $25 million was incurred and another 1,000 employees were hired to manually undertake the payroll, adding $1.15 billion over eight years. When the project reviewing commission completed its report, fault was found at every stage of project, including procurement, planning of the contract schedules, and vendor's management. The instances like this get further aggravated when the nature of digital technologies that are exercised for managing public service delivery go more ambiguous and disruptive. The burgeoning ICT technologies coupled with the risks posed by the emerging technologies (Blockchain, Artificial Intelligence etc) have led to a very precarious position for the e- Governance projects.

The most crisp and comprehending tool to list various types of risks confronting digital projects can be the PEST (Aguilar, 1967[24] ; Collins, 2010)[25] that broadly encompasses four categories of factors for understanding any ecosystem viz. political factors; economic factors; social factors and technological factors. Emulating PEST, risks can be broadly classified as Political risks, Economic risks, Social risks and Technical risks (Table-2).

[22] Heeks, R. (2003). Most e-Government-for-Development Projects Fail How Risks Can be Reduced? at http://unpan1.un.org/intradoc/groups/public/documents/cafrad/unpan011226.pdf, 2003, accessed in December, 2009.

[23] Hamrouni, W. (August 1, 2017). 5 of the biggest technology failures and scares. EXO Platform. Retrieved from https://www.exoplatform.com/blog/2017/08/01/5-of-the-biggest-information-technology-failures-and-scares

[24] Ibid 15

[25] Collins, R. (2010). A graphical method for exploring the business environment. Henley Business School.

Table 2- Suggested List of Risks faced by Digital projects (using PEST Analysis)

S.No	Risks	Some suggested examples
1.	P- Political risks	● Lack of trust on the service providing agencies ● Traditional mindset of leaders ● Political instability …
2.	E- Economic risks	● High implementation cost ● Poor maintenance facilities for digital services ● Repetitive or lack of timely technology upgrades …
3.	S- Social risks	● Varied needs of stakeholders ● Lack of awareness by the end-beneficiaries ● Lack of willingness to adapt by various stakeholders ● Digital divide / Gender Divide/ Geographical Divide …
4.	T-Technical risks	● Lack of Digital Standards ● Lack of CyberSecurity ● Privacy Concerns for personal sensitive data …

a. Political Risks - Reposing trust in the service delivery agencies has been identified as the top factor in the list of political risks. 'Trust' factor has two-pronged connotations - firstly, the trust of users on new software and secondly, trust in the government. The users of any type of software or technology must be confident and comfortable using it. Backus (2001)[26] also insists that the political stability and the nature of country's regime (dictatorial or democratic) and the preferences of its political head can affect the execution of the various e-Governance projects. Usually citizens also have an inherent fear that some fraudulent activities may occur leading to breach of their financial details or misuse of their personal sensitive information. Poor marketing by the government organizations and traditional mindset are some of the factors attributed to low use of portals. Even the level of IT literacy in a country can impede or facilitate the process implementation of e-Governance projects in a country like India (Mittal & Kaur, 2013)[27]. Education about the value of new system is one-step towards reducing some of this struggle.

[26] Backus, M. (2001). E-Governance and Developing Countries, 1-51.
[27] Mittal, P. & Kaur, A. (2013). E-Governance- A Challenge for India. International Journal of Advanced Research in Computer Engineering & Technology 2(3), 1-4.

b. Economic Risks - Economic risks can emanate from undue escalation of cost of implementation of operations as well as the cost of maintenance of technology. Maintenance of ICT based projects pose as a prominent risk because of continuous changes in technology landscape. Hence, maintaining both the new and old ones is a tedious and time consuming task which needs timely upgradation as well (Mansell, 1999)[28]. Any model developed by government should be reusable to provide the users with multi-channel operations and value-for-money implementation.

c. Social Risks – Social risk refers to the socio-cultural and contextual factors impeding the uptake of technology, where the 'usability' component plays a very important part. Usability aspect insists that the ICT based/ e-Governance services must be designed in accordance to the needs and aspirations of the citizens. However, in context of India, this citizen-centric approach for designing ICT based projects is tough to implement due to the size and diversity of Indian citizenry. Apart from this, lack of awareness and willingness to adapt on the part of citizens is another risk for e-Government projects that can be categorised as 'social risks' (Choudhari, Banwet & Gupta, 2014)[29]. 'Digital divide' too poses a risk for governance projects that can lead to failures. Marginalized communities without any access to digital tools might end up being left behind. Geographical difficulties too act as another hindrance in successful roll out of e-Services. Government networks have to go into all areas that are quite unfriendly for inhabitants and hence do not lend themselves easily for digital wiring up too. An auditor must carefully analyse the demography of such remote sites and propose better alternatives to enhance acceptance of digital initiatives in such areas. For instance, in such non-welcoming demography, e- Governance projects must try to use the wireless networks or supplement digital connectivity with other connectivity models using the existing cellular networks or other setups such as all-pervasive post offices.

d. Technical Risks - Erratic electricity and internet supply, and poor adaptability of technology usually retard the progress of e-Governance. Likewise, security and privacy are risks that each citizen takes while making online transactions (Bailey and Riffel, 2010)[30]. Any person or institution may misuse the valuable information. A risk of malicious users/ organisations invariably exists. Though, the digital/ e-signatures play a major role in providing authenticity, it is still expensive, require frequent maintenance and not very popular with majority of naïve users. Lack of interoperability becomes a major hurdle for processing and sharing of data, across modules, sections, departments, and ministries. The format in which the data is captured, stored, and shared seems to be a major concern assailing smooth Government to Government (G2G) interactions. Several of the technical issues can be resolved if the digital services should be 'standardized' to become 'interoperable' and 'portable' for popular acceptance; else the initiatives would stay non-sustainable.

[28] Mansell, Robin (1999) Information and communication technologies for development: assessing the potential and the risks. Telecommunications policy, 23 (1). 35-50 DOI: 10.1016/S0308-5961(98)00074-3

[29] Choudhari,R. D., Banwet, D. K., & Gupta, MP. (2014). Identifying Risk Factors in for E-Governance Projects: 1-9. Retrieved from https://www.researchgate.net/publication/237579298_Identifying_Risk_Factors_in_for_E-Governance_Projects

[30] Bailey, M. & Riffel, M. (2010). Understanding and Mitigating IT Project Risks. Government Finance Review.

Armed with the knowledge of the types of risks that an e-Governance project faces, the role of auditors begins in assessing/mitigating the risk and reducing the vulnerability for proper implementation of the objectives. The following section of the study elaborates on the role of auditors in detail.

4. Role of Internal Auditors

In 1947, the Statement of Responsibilities of Internal Audit defines internal auditing as “an independent appraisal function established within an organisation to examine and evaluate its activities”. Auditors - both internal and external, play a crucial role in identifying risks as well as in suggesting remedial measures/ putting forth action-plans/ guidelines. With the element of uncertainty ushered in by technology, the role and responsibilities of auditors too need to be revamped. Their style of working can no longer be the same as the conventional audit approach that had been followed by them in pre-digital technology times. It is more prudent for them to follow 'risk based auditing' and not 'internal control based auditing' approach. This implies that akin to managers, they have to be more determinedly involved in identifying risks and managing risks rather than to be just perceived as dictatorial control agents. For doing so, they must understand the culture of the organization. This would empower them to guide the employees in enhancing their understanding of the process under review, help them to do value-addition to these processes as well as facilitate them in developing action plans for future too. They must develop themselves in a manner that they can augment the organisation's value. Additionally, internal auditors must be able to proactively spread awareness about internal organisation's culture as well as stay abreast with external environment (global practices, national regulatory frameworks, competitors and their strategies) too. They also must possess a creative streak to innovate as well as adapt with emerging technologies. Persuasive skills of auditors, that could coerce both management and employees of the organisation to upgrade themselves as per the emerging trends, would be an additional boon. The presence of dynamic auditors in an organization can indeed help to manage better the anticipated disruptions caused by emerging digital technologies.

5. Concluding Remarks

e-Governance/ ICT based projects have become quite complex and volatile due to the transience of digital technologies employed. To bridle the risks infesting these projects, there is a need to develop collaborative risk management strategies in partnership with the auditors. Since the auditors have internal information about all the aspects of projects, it is their responsibility to provide a holistic picture of design-reality gap and support the organisation in incubating a risk resilient environment. However, for doing so the auditors of the organization must be well informed about the digital trends as well as about risk management techniques. As an illustration, they must be well equipped to decode what could go wrong and help to delineate various types of risks using PEST framework; they should be able to identify the design-reality gaps. Auditors also must collaborate with the management to prioritize the risks by calculating their exposure value; support the management to evolve agile strategies for mitigating these risks and then should regularly review the implementation processes to restrain the damaging repercussions of the risks. They are also expected to scout external opportunities and help their organisation to be prepared to confront it and utilize it. Such proactive consideration on the part of the auditors would help the organisation in successful uptake of e-Governance / ICT based project(s).

Summing up, the contemporary auditors have to be agile, receptive to digital technologies, and visionary so that they may serve as 'partners in the growth' and contribute substantially to organisation's organic evolution.

Acknowledgements:

I am very grateful to the entire Digital India team of IIPA – Ms. Nishtha Agarwal, Ms. Heeba Jamal, Ms. Rashmi Anand and Ms. Shilpa Yadav- all these officers have taken out time to discuss and enrich the content of this paper.

BEING A CLOUD WAS SUCH A CAREFREE EXISTENCE – NOW PEOPLE EXPECT SO MUCH FROM US!
© D.Fletcher for CloudTweaks.com

Reference: https://whatsthebigdata.com/2017/02/24/cloud-computing-cartoons/

Audit Execution in Digital Era

Ms Sangita Choure, IA&AS 1987, is a senior officer of the Department and has served in various capacities in the IA&AD in Maharashtra, Delhi and Goa and is currently posted as DG (Union Accounts). She has also served on deputations to SEBI and Department of Disinvestment, GOI.

-Ms. Sangita Choure, IA&AS

Considering the critical need of e-Governance, mobile Governance and Good Governance in the country, the approach and key components of **e-Kranti: National e-Governance Plan (NeGP) 2.0** have been implemented by GOI since March 2015 with the vision of **"Transforming e-Governance for Transforming Governance"**. All new and on-going e-Governance projects as well as the existing projects, which are being revamped, required to follow the key principles of e-Kranti namely 'Transformation and not Translation', 'Integrated Services and not Individual Services', 'Government Process Reengineering (GPR) to be mandatory in every MMP', 'ICT Infrastructure on Demand', 'Cloud by Default', 'Mobile First', 'Fast Tracking Approvals', 'Mandating Standards and Protocols', 'Language Localization', 'National GIS (Geo-Spatial Information System)', 'Security and Electronic Data Preservation'.

1. Re-orienting Audit strategy

There is a paradigm shift in utilisation of ICT in Government functions and services to citizens. Majority of Government departments are now using web-based services for improving government efficiency and transparency of transactions. This paradigm shift has not only opened lots of positive things but also exposed various challenges associated with it to the Executive as well the Auditors. Though auditing in digital era will allow the Auditor to examine more records, look at them in macro and micro manner, making it easy to quantify the audit outcomes but the challenges are also equally great. Ultimately, we may need to change the way we store the records and retrieve the information from Data Warehouse. We may even need to change the way we manage audit documents within our organization especially the way we use key audit evidence to support audit findings.

Any kind of Audit is a comprehensive exercise involving stages like **Audit planning, Audit execution** and **Audit reporting.** In digital era also, each of this stage needs to be given utmost and equal importance so as to get desired audit output and impact. With the advent of e-Governance at the Centre and the States, Audit planning and execution needs to be revamped.

Though the thrust of this article is "Audit execution in a digital era", let us discuss something about "Audit planning" in digital era since a job well-planned is half executed!!

Audit planning in digital era for Auditors can be seen in two stages.

- First stage, is identifying auditees which have largely shifted on to e-Governance platform in goods and service delivery to citizens. A comprehensive database needs to be built in each office for the projects/applications identified. Most offices may have captured this data for IT Audit purposes by now, since this was also being pursued by Office of the C&AG of India.
- We also need to identify the Data systems and data structure used by the auditee. Some of the data sources available in the department and the State government in centralized sources include (i) VLC data (ii) GR data and (iii) e-Procurement and some of system/ data are specific to the Audited entities such as Property tax and Water billing systems. Second stage is to properly store and maintain this data for audit warehousing activities.

An Audit Plan should identify the Application Systems/Portals for an Audit of the System by identifying parameters such as the functions computerized, size and outreach of the system and the time taken for rollout and status of its functionality etc. This can be easily achieved through a Pilot Study.

In IAAD there is enough literature available regarding these two sub-stages of Audit planning in the form of Data Analytics guidelines issued recently, IT Audit Vol I&II and various circulars issued by IS wing.

2. Present IT/Digital environment in IA&AD

We have been conducting all types of audit i.e., financial, compliance and performance audits. The present audit approach can be broadly categorized into following three categories, though these are not watertight compartments, and have overlaps:

(i) Use of CAATs: IT enabled Audit using Computer Assisted Audit Techniques (CAATs) are computer based tools, which help an Auditor in carrying out various automated tests to evaluate an IT system or data. These are very useful, where a significant volume of auditee data is available in electronic format. CAATs provide greater level of assurance as compared to other techniques, especially manual testing methods. Traditionally Excel, Access, IDEA and latter Qlikview are used for data extraction and analysis.

(ii) Use of Data Analytics: Data analytics method was introduced in 2015 and a Guidelines for Data Analytics was issued in 2017, institutionalizing the practice and use of data analytics in the Department. Data analytical tools such as KNIME and TABLEAU are in use for Data Analytics.

(iii) IT Audit/System Audit: IT Audit is taken up where Audit examines the economy, efficiency and effectiveness of the IT systems in the utilisation of resources to achieve the organizational goals in introduction of that IT System. It examines whether the IT assets are safeguarded and that appropriate controls are in place to ensure integrity of the system, reliability, availability and confidentiality of the data and information and compliance of the system to the business rules and procedures of the organization. Department has done number of system audit and IT audits. The IT Audit conducted by various field offices include (i) e-Tendering System in Government Departments (ii) e-Aushadhi System (iii) Government Receipt Accounting System (iv) Billing and Revenue Systems in Local Bodies (v) Individual SAP/ERP Systems in organizations and important Application Systems of Central Revenue Departments for Assessment and Collection of Taxes. This also makes use of above two categories at (i) & (ii).

3. Audit execution in digital environment: Opportunities and Challenges

(i) Access to IT systems and data

'Regulations on Audit and Accounts, 2007 enables the National auditor to access the IT systems, irrespective of the fact whether the systems are owned, maintained and operated by the auditable entity or by any other agency on behalf of the auditable entity. Also, the auditable entity is required to ensure that all requirements for the purpose of facilitation of audit are incorporated in the IT system.

Despite the available legal mandate, as auditors we face practical difficulties in getting access to the IT systems and this is a major serious challenge of auditing in a Digital Era. Very often only limited access is given to the system, which restricts our complete access to the data to do effective audit planning and sampling. For example the Revenue Departments both at the Centre and State give access only to the record of a particular assessee in the system. This is like just seeing an assessment record but in a soft copy. Such an access does not serve the purpose of audit analysis, planning and sampling especially for Performance and Theme/compliance Audits

So at the senior management level of field offices we need to engage with the auditee on a continuous basis and get the access to the complete data required in audit. **Access to IT system and data is the crucial aspect in audit execution stage. Repeated denials should be brought to the notice of the C&AG's office for remedial action.**

(ii) Data Dumps and Audit Information System Module

Traditionally we have been relying on the Data Dumps given by various auditee entity for performing various analytical tests. However we need to give equal importance to the data which can be accessed using Audit module or Audit Information Systems (AIS) of the auditee.

This issue can be seen in two ways; first, the absence of audit information system/ module in the systems used by auditee organization, reflects due importance not being given to this function and also the fact that we as auditors do not engage with auditee departments when the systems are being developed. Secondly mere incorporating the AIS module is not enough, the Auditee agencies need to make it live and accessible to users.

The ERP platforms like SAP and Google ERP have such kind of Audit information module. Government Oil marketing companies, various DISCOMS and big organization like Air India, BSNL have already shifted on the SAP-ERP platform. Even town planning authorities like CIDCO in Maharashtra have also shifted to SAP. In most of these ERP systems the challenge is restricted access given to the Auditors. While doing the audit of MH-GENCO, it was seen that so many reports (MIS) could be generated using the AIS and various audit trails and logs could be generated. Successful implementation of AIS modules will give audit lots of useful information.

(iii) Manual / guidelines and training

Manual of Information Technology Audit which is in use in the department since its release in 2006 needs updation in view of the changes in approaches of e-Governance projects, technology and risks.

Training: As most of the application systems being used in Government department are web based, they are exposed to several security threats. Audit of such system requires training to our staff in both security best practices and security technologies. Training should include demonstration of case studies of audits done in digital mode, in order to make it more relevant. Young IA&AS officers and Group B Officers should be encouraged to demonstrate in our Training Institutions, the modalities and nitty-gritties of the actual audit work done in an IT environment.

YOU NEED TO UPDATE YOUR FIREWALL.
PRIVATE DATA
KEEP OUT
OFFICE of PERSONNEL MANAGEMENT
TECH SQUAD

Reference: http://www.theeditorialcartoons.com/ store/add.php ?iid=29801

Case Study On Pahal

Introduction

PAHAL (DBTL) Scheme was introduced by Government of India in November 2014 for transfer of subsidy of Liquefied Petroleum Gas (LPG) directly to the consumers linking their ADHAR No., Bank Account and Consumer ID, i.e. direct transfer of benefits to the Beneficiary's Bank Account. The scheme is implemented by three Government of India owned Oil Marketing Companies viz. Indian Oil Corporation Limited (IOCL), Hindustan Petroleum Corporation Limited (HPCL) and Bharat Petroleum Corporation Limited (BPCL).

The scheme involved 19.26 crore domestic LPG consumers serviced by 16781 LPG distributors of the three Oil Marketing Companies.

The case study deals with how to audit various benefits transfer scheme such as PAHAL (DBTL) Scheme in Digital era. It also elaborates how various risk areas were identified, how samples were drawn, how the data was analysed and challenges involved in the process of data analysis.

Implementation Of The Pahal (DBTL) Scheme

The PAHAL (DBTL) Scheme is being implemented by the Oil Marketing Companies (OMCs) through its network of LPG distributors who constitute the interface with consumers. The distributors maintain the LPG consumer database (containing the particulars of the domestic LPG consumer, including a unique LPGID, name, address, date of birth, bank account details etc of the consumers) This is periodically synchronized with the Central system maintained by the OMCs.

The distributors deliver LPG cylinders in response to a request from the consumer at market prices and upload proof of receipt by the consumer (indicating completion of the transaction) to the central system. The action for reimbursement of subsidy to the consumer is initiated by the OMC (central system) which sends the advice to the sponsor bank (State Bank of India) and onward to the National Payment Corporation of India (NPCI) enabled payment platform for crediting the bank account of the LPG consumer. The information regarding transfer of subsidy to the consumer is received by the central system of the OMCs who then prefer a subsidy claim with the Government for reimbursement.

Audit Sample And Size

As on 31 October 2015, there were 16,781 LPG distributors in the country servicing 19.26 crore registered domestic LPG consumers. While selecting the distributors, due consideration was given to representation of geographical regions in the sample. The data relating to LPG Distributors of each OMC was ordered zone-wise (north, south, east and west) and a sample of the top 34 percent was selected. In the case of LPG consumers, audit examination was carried out on a sample of 11.89 crore domestic LPG consumers (comprising 9.94 crore active and 1.95 crore other than active consumers) coming under the selected 34 percent distributors out of a total population size of 19.26 crore consumers (61.73% of domestic LPG consumers). Selection of such a huge sample would not have been possible with manual procedures.

Audit Methodology – Use Of Idea Tool

The Data Dictionary of the three OMCs were obtained to ascertain the distinct tables utilized by them and to ascertain the fields contained therein. Out of the two major classes of tables i.e. the Master Table and the Transactional Table; the Consumer Master Table of each OMC was reduced to incorporate only fields deemed requisite for the conduct of the audit and were further standardized across the OMCs by allocation of common field heading names. Similarly, the fields contained in the numerous Transactional tables of each OMC were weeded out and 4 Transactional tables with desired fields were created. The three OMCs were requested to submit the data pertaining to the aforesaid master and transactional tables containing only desired fields requisite for audit in csv format with a "|" (pipe) separator.

The sample obtained was classified into data pertaining to "Active Consumers" and "Consumers other than Active Consumers". The sample of "Active consumers" was primarily used for all data analysis other than the duplicate detection analysis conducted on Aadhaar numbers and Bank Account Numbers for which data pertaining to both i.e. "Active Consumers" and "Consumers other than Active Consumers" was utilized.

The total size of Original data (Primary data) received from the 3 OMCs was 354.29 GB which comprised of 252.58 GB of Master data and 101.71 GB of Transactional data which on data analysis resulted in Secondary data of approximately 6312.39 GB in size.

This audit required the usage of laptops/desktops of higher configuration of a minimum i5 processor capacity and RAMs with a minimum of 8 GB capacity.

Audit checked the uniqueness and correctness of customer database, adequacy of systems put in place by OMCs to ensure de-duplication, and correctness of the transactions relating to release of Permanent Advances and refill subsidy to Cash Transfer Compliant customers.

What We Were Looking For In Audit

Risk Area 1: Removing Incentive for Diversion

Risk associated with higher consumption of domestic non-subsidized LPG cylinders since there is a significant price difference between the price of commercial and domestic non-subsidized LPG on account of additional duties and levies (i.e., customs duty, excise duty, and value added tax differentials). Table comprising the Consumer Master Data was joined with Table comprising the consumer refill off take data and filtered to capture only customers wherein consumption of refills was more than 24 and the consumption during the first seven months of 2015-16 (April to October 2015) exceeded the corresponding numbers for the entire year of 2014-15.

Risk Area 2: Fake/Duplicate Connections

The data received from the OMCs was filtered to identify consumers having multiple connections within the same OMC using the following distinct parameters viz. (i) 'Same Aadhaar number'; (ii) 'Same Bank account number and IFSC (code) (iii) 'Same Name and Same Address' and (iv) 'Same Name, Date of birth and Registered mobile number'.

Risk Area 3: Process of blocking and un-blocking connections

The data received from the OMCs vide Table which comprised Consumer-wise blocking and unblocking details was filtered to capture only consumers who were blocked and subsequently unblocked with major emphasis being laid on cases wherein reasons for blocking and subsequent unblocking, dates for blocking and unblocking were not ascertainable/not recorded.

Risk Area 4: Integrity of the consumer database

The data received from the OMCs vide Table which comprised Consumer details was filtered to capture instances wherein the consumer was less than 18 years of age, addresses bearing incorrect or incomplete PIN codes, inaccurate or incorrect Aadhaar numbers and IFSC codes associated with the Bank Accounts of consumers.

Risk Area 5: Consumer complaints redressal

The handbook of PAHAL (DBTL) prescribed that 98 percent of the consumer grievances had to be disposed of within seven days. The Scheme provided that a consumer can register a complaint through a toll free number of the respective OMC, or physically send their complaints to the LPG distributor through the web based OM C portal.

The data received from the OMCs was filtered to capture the complaint type based on stakeholder responsible (viz. OMCs, NPCI, UIDAI, Banks) and days taken for complaint resolution.

All above risk areas are illustrative in nature and not exhaustive.

Conclusion

This case study is a good example where various techniques were used for identifying various risk parameters, drawing appropriate samples and doing data analysis. The case study is also unique that the auditees filtered the data and provided it in the desired format of the Auditors. Else it would have been impossible for the audit to have mined the huge data given the constraints of time to produce the audit results.

Greater usage of such tools and techniques will deliver greater level of assurance in audit and may also reduce the time required for doing such audits, depending on the speed with which data is made available to us in the desired format and the size of the data to be analysed.

Note: The field audit of PAHAL was done and consolidated for others by MAB II, Mumbai and inputs for the case study courtesy Shri Ravi Ubale, IA&AS.

Case Study On Post-Matric Scholarship For Scheduled Caste Students

Introduction

The Post-Matric Scholarship Scheme for Scheduled Caste students (PMS-SC) is a Centrally Sponsored Scheme in operation since 1944. Its objective is to provide financial assistance to scheduled caste students studying at post matriculation or post-secondary stage to enable them to complete their education. 100 per cent central assistance is released to State Governments/UTs for expenditure incurred by them under the scheme over and above their respective committed liability. The committed liability of a State/UT is the total expenditure incurred by it under the scheme during the terminal year of the last plan period.

Salient features of the Scheme

Courses are categorized into four groups and one course for Commercial Pilot License Course for which the rates of financial assistance are prescribed The scheme includes the following components

- maintenance allowance,
- reimbursement of non-refundable compulsory fee charged by educational institutions,
- study tour charges
- thesis typing/printing charges for Research Scholars,
- book allowance for students pursuing correspondence courses,
- book bank facility for specified courses, and
- additional allowance for students with disabilities, for the complete duration of the course. (viz. reader allowance for blind scholars, transport allowance for disabled students, escort allowance for severely handicapped day scholars with low extremity disability)
- The scholarships are open to nationals of India for the study of all recognized post-matriculation or post-secondary courses pursued in recognized institutions and candidate who belongs to Scheduled Caste.
- Scholarships will be paid to the students whose parents/guardians' income from all sources does not exceed Rs. 2.5 lakh per annum w.e.f. academic session 2013-14. Income certificate is required to be taken only once i.e. at the time of admission to courses which are continuing for more than one year.

Implementation of the Scheme

Being a Centrally Sponsored Scheme at the Central level, the scheme is administered by the Ministry of Social Justice and Empowerment and implemented in the State Governments by the Social Justice Departments and their field functionaries in the districts.

Database and Portal

The Scheme has a web portal available to the candidates to apply for the scholarship and the application is processed by concerned college/institute. The data is stored in centralized database using SQL Server RDBMS. The data dump is divided in nine files with 83 GB size of all dump files. There is one dump file with all master tables, seven dump files with data relating to seven zones/regions each and one dump file containing summary data.

The details of scholarship from application, approval and disbursement are stored with the time stamp. Final payment of the scholarship is made to the eligible candidate direct to his bank account.

Scope of Audit

IT audit process involves analysis of data and studying the output for transactions/records indicator of unusual, duplicate, irrelevant payments or violating the norms of the scheme. The system level discrepancy in database and input controls are also to be checked.

Tools used for Data Analysis

The tables restored from the data dump were available in different region-wise database and master tables in separate database. The query tool of SQL Server RDBMS was used along with IDEA for data analysis.

WHAT WE WERE LOOKING FOR IN AUDIT

Risk Area 1: Whether all eligible candidates were covered

The details of SC students awarded the scholarship was available in the database. However, the database of all SC students enrolled in all the colleges/institutes was not prepared. Such database of eligible SC student was necessary to ascertain whether all eligible students were covered and the extent of non- coverage

Risk Area 2: Duplicate registration/ payment

The data received from the department was filtered for probable duplication of the student registration by checking the a) Name b) UID details c) Income Certificate numbers d) Secondary School Certificate (SSC) Seat numbers and payment of claims in bills across databases of seven regions. This showed duplicate beneficiaries and payments. The invalid / duplicate entries in UID numbers indicated lack of input control.

The web portal did not have the required input validation controls since it did not restrict invalid and duplicate entries at the time of initial data entry raising the risk of ineligible students availing the benefits under the scheme.

Risk Area 3: Acceptance of incorrect data by the System

The data received from the department was sorted and filtered to check the valid UID numbers with 12 digits. The data revealed that no validation was exercised on input of data in UID number column despite UID being an important validation source for the Scheme.

Risk Area 4: Unutilised/ undisbursed funds of scholarship

On verification of Bank Account details of the Assistant Commissioners in selected districts audit could find funds lying unutilised/undisbursed due to invalid bank account number, closed bank account, incorrect details of the beneficiary students and closure of e-portal

Risk Area 5: Income Eligibility criteria

The data received from the department was sorted and filtered for the Income greater than the eligibility criteria of two lakhs. The cases were found where beneficiaries with income above two lakhs were awarded the scholarship, which resulted in depriving the eligible student from the scholarship.

Conclusion

This case study demonstrates analysis of huge data of the e-portal which was possible using the data analytics tools available and various techniques were used to filter the data for ascertaining the risks and validation of data against the basic criteria of the scheme. With the use of powerful tools for data analytics of electronic data and systematic approach to the audit, a better insight in the data was possible which would not have been otherwise possible by auditing the manual records and the audit coverage would have also been limited.

Note: Case study is based on the field audit done by PAG (Audit) I, Maharashtra Mumbai for All India PA on PMS.

Reference:
https://timesofindia.indiatimes.com/humour/cartoons/itoons/photostory/62693898.cms?picid=68697579

Emerging Technologies & Involved Risks

Mr. Irfan Khan, heads Hypermine Technologies, a company building Cryptographic products for Access Security and Blockchains. He is also the Head of CAT Factory, a company building a telecommunications network to create data connectivity and financial inclusion products for rural areas. Lastly he is also the founder of Citadel Financial, a company involved in the research and development of Cryptocurrencies and related technologies. He has over a decade's experience in working with 30+ countries and governments across the globe to build security and data exchange infrastructures, from Telecommunication Networks, Access Control, Digital Passports, SecureIDs and Semiconductors.

- Mr. Irfan Khan

In January 2016, the Founder and Executive Chairman of the World Economic Forum, Klaus Schwab, stated that we are entering a fourth industrial revolution characterized by a range of new technologies that will fundamentally alter the way we live, work, and relate to one another. He mentioned that we are witnessing technological advances in areas such as AI, robotics, the Internet of Things, Blockchain, Autonomous Vehicles, 3D printing, nanotechnology, biotechnology, and Quantum Computing. With the rapid onset of technology overtaking every aspect of our work and personal lives, data breaches are becoming common place. Hacks, ransomware, leaky websites and databases pose considerable risk to businesses and to their owners' reputation. From LinkedIn to Wipro to Mariott to UIDAI; no one is safe. When such attacks occur, not only is the business accountable for this, they must also figure out what went wrong, who was responsible and offer compensation to those affected. No firm should find themselves in a position where they are unable to determine what occurred. A strong data audit trail which maintains a record of events carried out by the system, it's applications, and it's users is a necessity. Having such records allow firms to easily determine what went wrong post-attack and prevent future attacks from taking place. They also prevent downtime which can expose sensitive information through constant performance analysis for issues such as an unusually high number of queries being handled by websites. To achieve these security objectives, audit trails implement individual accountability, intrusion detection, and reconstruction of events to reduce threats, internal and external. Technology is playing a key role in our lives, and that goes for auditing as well. Understanding how key technologies such as Artificial Intelligence and Blockchain are transforming the way we think, live, work and play and also help us do better audit.

Data Transforms Life

The death of a pedestrian by an autonomous car in Arizona and the harvesting of personal data by Cambridge Analytica on Facebook in some way, both have highlighted the importance of data privacy, risk assessment and the role of trust and transparency. The two incidents, albeit separate, emphasize the need for the convergence of artificial intelligence and blockchain– the powerful emerging tech continuum.

Questions arise such as - ‘How would a technology enabled audit trail better suit these disaster scenarios?’

Data is only as good as its reputation. In any given environment, if the integrity of data is called into question by an incomprehensible or inaccessible audit trail, it will be perceived as a risk. Any recommendations based on that data will be disregarded.

Similarly, a key barrier in the adoption of AI as well as the trust of ecosystems created by Blockchains is based on the quality of data being fed into the AI algorithms and the secure Blockchains. Artificial Intelligence that runs on the black-box model will be restricted by mistrust. Blockchains that host and secure incorrect data will be regarded as compromised. Users are unlikely to have confidence in things they do not understand, and corporate leaders would not invest in AI applications that provide no evidence of their decision-making process.

The disclosure of Cambridge Analytica’s haul of Facebook data and the death of a pedestrian in Arizona in a collision with Uber’s test autonomous vehicle have ignited mistrust in what data is being used, how and by whom.

Artificial Intelligence as a solution?

AI Algorithms are, in crude form, opinions of what defines a successful outcome, embedded in code. An imperfect analogy: A teacher seeks to persuade a student to write two different essays for an exam. However, the student might not agree with this, but it's the teacher deciding that a two-essay-exam is the successful outcome.

Like people, algorithms can go wrong, or be born of good intentions yet generate undesirable outcomes. A badly designed car that crashes is open for public scrutiny, becomes part of the narrative that determines a product's or even a technology's success or otherwise. But a badly-designed algorithm can quietly wreak mayhem, and its flaws go undetected. So how can trust be engendered in something that is neither apparent nor understood?

The power of AI lies in machines conducting educated guesses on a precise scale that outperforms human ability. It is a probabilistic method, with the result being machines that are able to learn and make decisions based on what they determine to be the most likely reality. The more data available to the equation allows the AI to adjust the algorithm, with the aim of "improving" the outcome.

The Value of AI Today

Big data has transformed the approach to traditional AI. In the 80s and 90s, AI research was largely based in academia, generally consisting of a fixed dataset from which an algorithm was proposed and then distributed, often in a journal or conference setting.

Today, Data Scientist Jobs, dubbed as the sexiest job of the 21st century, are paid anything but modest salaries to ensure that the quality of data going into AI algorithms is credible. The black-box model of AI and its algorithms have increased concerns regarding data privacy and require increased attention to the audit trails for decision making.

The value of creating technology that mimics human cognition, is in augmenting human productivity rather than creating entirely new industries. Adding value to existing enterprises by detecting fraud, enhancing the resilience of supply chains and enabling managers to focus on analysis, are essential tools that the AI technology is providing to humans.

By automating processes that are too complex for legacy technologies, enhancing business value by identifying previously overlooked trends in historical data and strengthening human decision-making by articulating forward-looking intelligence, AI is now adding valuable support to human functions.

But organizations are facing increasing pressure from regulators and end-users to open their black boxes by making AI processes transparent, explainable, provable and testable. Vendors will need to share previously protected information, and previously incomprehensible AI will need to be explained by the creators of deep learning algorithms.

What is Blockchain?

In its simplest form, a Blockchain can be considered to be the Operating System to the 'one world supercomputer'. Instead of users keeping independent computers at their homes, offices and pockets; Blockchain can enable people to connect all the computing devices in the world onto one network; so, when people buy a new computer and connect to the network, they will simply be adding more computing power to the world super computer, rather than holding onto one individual separate computer at their desk.

Once everyone on the network is connected together on the Blockchain (Operating System) downloads a copy of the ledger or data to each and every computer on the network, thereby building a global 'distributed ledger' which contains the relevant details for every transaction that has ever been processed. The validity and authenticity of each transaction is protected by digital signatures (cryptography). In the ideal blockchain world, there is no central administration and anyone can process transactions using the computing power of specialised hardware (nodes/miners) and earn a reward in bitcoins for this service.

In private or enterprise type environments, small closed type ecosystems can be created with each branch or partner entity of the organization can join the network with their own hardware and custom blockchain software. This is done in order to avoid the decentralized, open and public networks, for multiple reasons ranging from privacy to security and creating custom features that would not be available on public networks by default.

Blockchain and the Audit Process?

Although blockchain promises highly secure transactions, fraud instances cannot be fully eradicated. In July 2017, a hacker managed to steal nearly $32 million USD worth of Ethereum.

The root cause of this fraud was not related to deficiencies in the blockchain technology but, rather, due to a vulnerability within the software that was used to manage Ethereum wallets (the place where cryptocurrency is stored). The fraud was quickly detected and vulnerability mitigated. Blockchain promises a world where all transactions can be logged, viewed and monitored in real time. There are potential implications for a wide variety of sectors, not least accountants and auditors.

The Ethereum breach suggests that the successful adoption of blockchain is highly dependent on the security of the underlying environment. In order to be in a position to provide the necessary level of assurance, the audit processes need to shift further towards the assessment of operating effectiveness of the internal IT controls.

To site some examples:

If an entity's employee accidentally or deliberately sends cryptocurrency to a wrong or an unauthorised recipient, there is currently no way to reverse that transaction. Auditors are therefore required to assess whether effective automated controls are in place to validate transactions before they are executed.

If an entity experiences a phishing attack, there is no such department to which reporting of such an incident can be done since in blockchain there is no central administration. This situation can also translate into a risk of fraud. When faced with such risk auditors will be expected to determine whether the existing internal controls that prevent and detect phishing attacks are in place and operating effectively.

If a private key is lost through a software or hardware malfunction, the virtual currency is lost. These coins will no longer be accessible to anyone on the network; they are effectively out of circulation. Effective disaster recovery procedures as well as backup and restoration procedures would help to prevent such situations from occurring. Such loss mitigation procedures are also expected to be assessed to verify whether controls that address the risks associated with blockchain can be relied upon.

Although blockchain technology offers inherently secure properties, it is humans who will be coding the necessary software to integrate and interface with blockchain. Humans are fallible and corruptible.

In adherence with the requirements driven by the International Standards on Auditing (ISAs), auditors are required to understand the specific risks to an entity's financial statements arising from IT, and how the entity is responding to these risks through implementation of IT controls. With the rising adoption of blockchain technology, auditors will need to raise the bar by providing increasingly complex assurance services in more agile business environments and in support of upcoming digital transformations. A different professional audit mind-set and additional expertise will be required to satisfy the expectations of stakeholders and business owners in this new world.

The Decentralized Intelligent Future

While an audit trail is a desirable trait in AI decision-making, the convergence of AI and Blockchain – may be able to reshape the entire process from scratch. Although adding further complexity to the digital eco-system, once established, can greatly reduce errors, increase confidence in recommendations and reduce copious amounts of time and resources.

Essentially, AI is the brain to Blockchain's body. Machine learning methods find opportunity and improve decision-making, adding intelligence and insight (albeit using guesswork), while blockchain automates the verification of the transactional process, providing the necessary integrity while providing security and decentralization (if required). The application of blockchain centres on the facts, while artificial intelligence is about the creative element.

Transactions are validated through a variety of mechanisms, but the connection of the blocks means that without network consensus, it is extremely difficult to modify any of the information established within the chain.

As opposed to traditional, clunky audit-trail software in computer security, blockchains have strengths. But technology-related obstacles and their origin in the technologically-outdated financial services sector mean that pairing blockchain with artificial intelligence will unleash the potential of both.

Conclusion

Blockchain and AI result in an intelligent and fully automated audit process that are inherently built into decentralized autonomous software; floating around on the one world supercomputer.

For one thing, we would seem to be approaching a paradigm clash between assurance and trust-less systems. Trust the algorithm, but who audits the algorithm?

Artificial intelligence will enhance blockchains in a number of ways: decentralizing the technology for increased scalability, economizing on energy consumption, enhancing security, democratizing privacy issues, increasing efficiency and enabling the capacity to track and sort the data.

Conversely, blockchain can have a profound impact on the development of machine learning systems by helping AI technology explain itself, cleaning and organizing personal data to lower market barriers, and also shrink the competitive advantage of incumbent tech giants. 'Artificial Trust' would consequently be increased.

The AI + Blockchain convergence is far from completion, given the number of companies actually working at their intersection. The focus appears to be on working on decentralized intelligence, and slightly lesser on conversational and prediction platforms and intellectual property. Technological concerns are building totally autonomous decentralized digital economies built on the blockchain and powered by Artificial Intelligence, leaving very little room for any human intervention. Audit trails are an essential part of such economies.

While blockchain's design seems sound from a security standpoint, the blockchain environment is still susceptible to various technology risks. AI will forever remain a technology that will be determined by the quality of data going into it and will be constantly required to justify its decisions. The efficiencies that will be gained through audit automation are likely to be balanced by the requirements for new procedures to address the risks associated with the blockchain environment.

In all cases, it is clear that these tools will enable auditors to consolidate a wide range of data from clients; they open up the possibility for the expansion of the auditor's assurance beyond financial statements. Although, auditors should not over rely on these tools. As powerful as these may be, or are expected to become, they will never be substitutes for the auditor's knowledge, judgment, and exercise of professional scepticism.

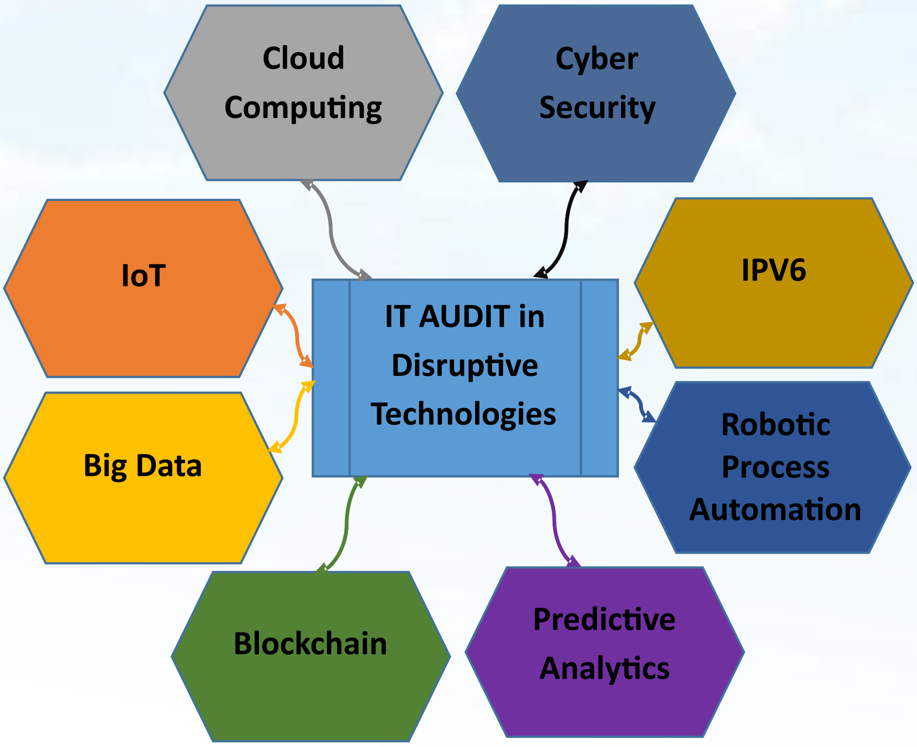
Auditors of the future will design the logic in these technologies to suit the appropriate reporting requirements and let the machines do all the heavy lifting. These developments will likely shape an audit culture where audit designed technology controls will play pivotal role in providing a reasonable assurance that the financial statements as a whole are free from material misstatement.

Reference: https://www.tes.com/lessons/p88ALFPajrnPlA/technology-and-privacy

IT Audit Transformation along with Converging and Disruptive Technologies

- Mr. Kaushlendra Singh Sisodia

Mr. Kaushlendra Singh Sisodia, an IIT Kanpur Alumni, is co-founder of UniConverge Technologies Pvt. Ltd (UCT). Prior to UCT, he played various key roles in Ericsson AB (Sweden), STMicroelectronics and other MNCs for over 18+ years. Under his leadership, UCT has been chosen by Nexus (University of Texas, USA Startup Hub) and collaborated with IIT Jodhpur and IIT Guwahati for commercialization of Security and Industrial IoT domain R&D projects. He is also prolific speaker on Industry4.0, Convergence of Technologies and Start-up eco-systems.



In this article, we will study the impact of various disruptive technologies on IT Audit one by one. Sometimes these technologies are companion and sometimes create challenges to IT Audit. So as per advancement of technologies, Audit and Assurance practices also need to be transformed with awareness and innovations.

1) Internet Of Things : Introduction

IoT is amalgamation of IT (Information Technology) and OT (Operational Technology). The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It is more in adoption now due to falling price of sensors and other electronics components, advancement in other companion technologies. IoT integrates technologies to enhance business information needs. IoT is not limited to a single industry or business process. IoT needs a skill set that is only going to grow in demand given the rapid deployment of connected devices throughout industry.

Audit scope

During audit, below points need to be checked:

- How is the IoT deployed in organization today, and who owns it or its respective components?
- This includes determining an organization's potential IoT inventory and IoT's business activity role.
- Do we know what data is collected, stored and analyzed, and have we assessed the potential legal, security and privacy implications?
- What is the threat environment for the device? What threats are anticipated and how will they be mitigated? What is the process for updating the device in the event of a published attack or vulnerability?
- Who is responsible for monitoring new attacks or vulnerabilities pertaining to the device? How will they perform that monitoring?
- Have all risk scenarios been evaluated and compared to anticipated business value?
- Who will have access to the device and how will their identities be established and proven?
- What personal information is collected, stored or processed by the IoT devices and systems?
- With whom will the data be shared/disclosed?

2) Cloud Computing : Introduction

According to National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud computing model is composed of five essential characteristics, three service models, and four deployment models."

As defined in the definition, cloud computing includes:

Five essential characteristics;

- On-demand self-service,
- Broad network access,
- Resource pooling,
- Rapid elasticity and
- Measured service.

Three service models;

- Software-as-a-Service (SaaS),
- Platform-as-a-Service (PaaS) and
- Infrastructure-as-a-Service (IaaS).

Four deployment models;

- Private cloud,
- Community cloud,
- Public cloud and
- Hybrid cloud.

The different characteristics, service models, and deployment models can be shaped and morphed into different resources depending on the needs of the organization.

Audit scope

Risk Assessment

- Inspect the company's documented risk assessment
- Inspect the risk assessment to determine whether mitigation activities are identified, as required

Monitoring Activities

- Inspect documentation which identifies system vulnerabilities
- Inspect system configurations to determine whether notifications are provided when vulnerabilities or failures are identified
- Inspect evidence that identified vulnerabilities are remediated

Systems Operation

- Inspect monitoring tools used to monitor traffic and alert on suspicious activity
- Inspect evidence that the tools successfully send alerts, as required
- Inspect evidence that notifications are followed-up on and remediated as necessary

Change Management

- Inspect evidence to confirm that changes are defined and documented, approved for development, tested, and approved for implementation

Deployments and Storage Management

- Out of four above given Deployment models, which has been adopted?

Service Model

- Out of three above given Service models, which has been adopted?

3) Cyber Security: Introduction

Cyber security has become a prevalent issue faced by most organizations- one that companies recognize as an enterprise-wide issue requiring thoughtful attention. Investments in controls are necessary to protect organizations from increasingly sophisticated and widely available attack methods. Intentional attacks, breaches and incidents can have damaging consequences.

Audit scope

- Organization’s network, software and licenses
- Cyber risk governance
- Data security
- Risk management : Categorization by risk level of each information system and set of information
- Policies and information security management system
- Business continuity and incident management
- Technical security controls
- Physical security controls
- Cloud systems, public-facing websites, third-party systems
- The security plan with security controls,

current policies and procedures and a general timetable for future control implementation

4) Internet Protocol Version 6 : Introduction

Internet Protocol IPv4 has now run out of space and deploying its replacement IPv6, is a challenging and daunting prospect for many businesses because the devices used by these businesses are not compatible with IPV6.

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communication protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. Devices on the Internet are assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available.

Audit scope

- Assessment of the effectiveness of the IPv6 network's architecture, security and alignment with the enterprise' networking and IT security policies and architecture.
- Evaluation of the IT function's preparedness in the event of an intrusion.
- Identification of issues that affect the security of the enterprise's network.
- Audit and analysis of the hardware and software version of all network equipment, and the Operating Systems running on any Desktop PCs or Servers can check needed upgrades to a full IPv6 compliant network.
- Not only the implications of migrating to IPv6 must be considered, but also need to understand how migration impact on existing infrastructure and legacy IPv4 applications.

5) Robotic Process Automation (RPA) : Introduction

Under RPA, computers perform the tasks normally performed by humans, and cut resource and time requirements for many repetitive activities.

With increased investment in RPA across all business sectors virtually, three key opportunities that come with employing intelligent automation:

1. Integrate governance, risk and controls considerations at the onset, as the organization creates and implements RPA programs
2. Identify opportunities where RPA should be recommended to apply to organization-wide processes
3. Begin to capitalize on RPA to increase the efficiency and effectiveness of its own activities with repeatable processes

Audit scope

- Improve efficiency of planning, testing, and reporting activities, creating more time for critical thinking activities
- Increase coverage and frequency of testing across the audit universe
- Move from limited sample testing to full population testing
- Manage labor capacity and geolocation constraints
- An impact of RPA on the following:
  - o Control matrices or monitoring mechanisms
  - o Standard operation procedures
- Assess changes to roles and responsibilities post RPA

- Incidents remediation in the RPA environment
- Controlling of privilege accounts for RPA environment.

Next below Technologies can be companion for audit process making it more efficient and error free.

6) Big Data, Predictive Analytics and Audit aspects

Big data improves the efficiency of overall data analytics, including descriptive, diagnostic, predictive, and prescriptive analytics. Audits can also get benefit from big data by utilizing more unstructured and nonfinancial information to control risks. The actual integration of big data into future audits will require further consideration.The rapid advancement in technology, and the development of data mining and data analytics techniques over the past decade, have led to the development of a methodology that can allow businesses to predict and prevent such anomalies before they occur.

The predictive analytics is a forward-looking approach that examines the validity of transactions before they are executed. It does so by comparing actual transactions to timely normative models, allowing managers to be alert to potentially problematic transactions before they occur. This gives senior staff the opportunity to investigate and resolve any issues before allowing flagged transactions to go through.

The predictive model can enhance the control environment of an organisation and also lead to improved feedback mechanisms for auditors. In particular, they can not only examine errors and irregularities that cause particular transactions to be flagged but can also ensure that prompt measures are taken to investigate and resolve them. Auditors have long used analytical methods to identify relationships between sets of data, and the predictive model builds on this to make specific predictions about certain business outcomes.

7) Blockchain and Audit Aspects

A Blockchain is a digital ledger created to capture transactions conducted among various parties in a network.

It is a peer-to-peer, Internet-based distributed ledger which includes all transactions since its creation. All participants (i.e., individuals or businesses) using the shared database are “nodes” connected to the Blockchain, each maintaining an identical copy of the ledger.

By eliminating the intermediary and harnessing the power of peer-to-peer networks, Blockchain technology may provide new opportunities to reduce transaction costs dramatically and decrease transaction settlement time.

Blockchain technology has the potential to impact all record keeping processes, including the way transactions are initiated, processed, authorized, recorded and reported.

A properly functioning Blockchain is immutable despite lacking a central administrator.

It has widely used cases as below:

- Land and Asset Records
- KYC records
- Financial, Investments & Insurance
- Employer or Business Records
- Medical Records
- Travel Records

References:

i. https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20 contro%20objectives%20for%20Cloud%20computing.pdf

ii. https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf

iii. https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2018_Geneva/PPTs/IoTPPTs/12_-_Eric_Cohen_-_IoT_CEFACT.pdf

iv. https://www.forbes.com/sites/insights-kpmg/2018/07/16/three-technologies-that-will-change-the-face-of-auditing/#6591ff427544

v. https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

vi. https://www.ey.com/Publication/vwLUAssets/EY-bmq-vol-9-big-data/$File/EY-bmq-vol-9-big-data.pdf

vii. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf

viii. https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-nternal-audit-role.html

We don't need to pay them. They'll sell data about our whereabouts
TAXI
TAXI
TAXI
TAXI
times@itoons.in

Reference:
https://timesofindia.indiatimes.com/humour/cartoons/itoons/photostory/62693898.cms?picid=68697579

1. Daywise

Daywise is a mobile application which allows the users to group their notifications application wise and contact wise so that they only receive them at certain times of the day. Users can also set exceptions for particular applications and contacts that they do not want to miss.

2. Blog Compass Google's Latest App

Blog Compass is a new application that aims to provide a one-stop shop for bloggers in the country, it is meant to help them track visitor information, engage readers, monitor search engine presence, and find new topics to write on regularly. The application is currently available in open beta and can be used by English and Hindi speaking users in the country. Google's Blog Compass connects with WordPress and Blogger.com, and can also access Google Analytics and Search Console when linked with an account.

Bloggers will be able to see statistics including viewer numbers, traffic sources, demographic information, Google Search status, and popular Google searches that lead to the specified blog, helping them make the right decision when it comes to content. Blog Compass also studies post history and blogger preferences, and extracts customised Google Trends data to help push relevant content on the blog. Google claims that its initial testing found out that a majority of bloggers improved their frequency when using Blog Compass.

Reference:
https://gadgets.ndtv.com/apps/news/blog-compass-for-bloggers-india-open-beta-google-play-bloggers-wordpress-blogger-com-1913129

www.getdaywise.com/

Reference:
https://www.financialexpress.com/opinion/data-privacy-towards-a-secure-and-connected-india/1063655/

Chris

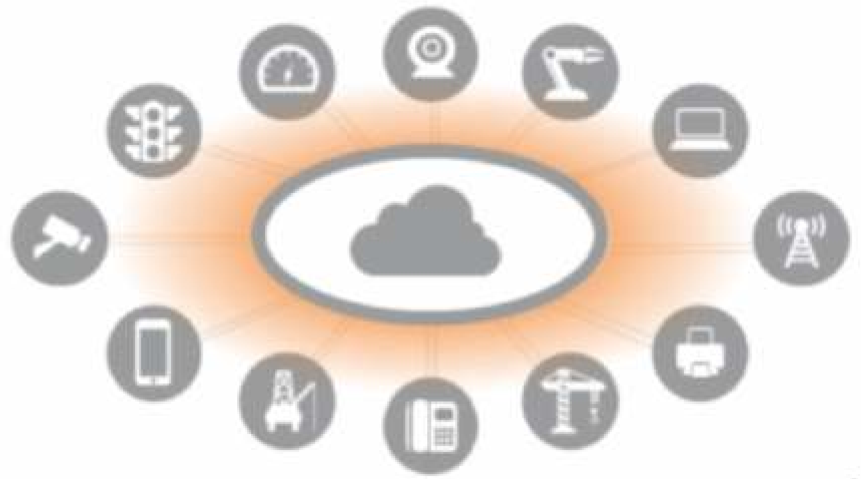
A Berlin-based startup, German Autolabs, has developed Chris, a standalone device that helps you to make calls, send messages and all the usual stuff that voice assistants do. It can process verbal commands in English and German, currently. It is special as, it has support for gestures so it's obviously helpful for the specially abled. Another big thing that makes it different from other available similar devices like: Google, Amazon, Microsoft and Apple's digital assistants, is that it can perform all of its functions without being connected to the Internet.

Reference:
https://www.slashgear.com/german-autolabs-chris-in-car-digital-assistant-hands-on-20527998

1. Fog Computing

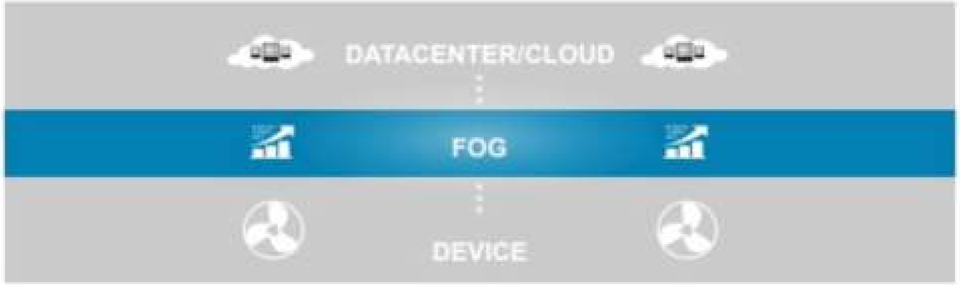
Fog Computing which will extend cloud services and Cloud Computing to the edge of the network. This will help in pulling the power of the cloud closer to the location where the data is stored and used. This method will be more efficient and reduce the amount of data transport and will be used in improving smart grids, smart cities, and smart buildings.

Figure 1. Connecting More and Different Kinds of Things Directly to the Cloud Is Impractical



Fog Computing is a decentralized computing infrastructure in which data, compute, storage and applications are located somewhere between the data source and the cloud. Like edge computing, fog computing brings the advantages and power of the cloud closer to where data is created and acted upon.

Figure 2. The Fog Extends the Cloud Closer to the Devices Producing Data



Reference:
https://www.outsource2india.com/software/articles/top-technology-trends-to-watch-out-for.asp
https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf
https://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging

Quiz corner

1. Which is not the purpose of Risk analysis?

A. It supports risk based audit decisions
B. Assists the Auditor in determining Audit objectives
C. Ensures absolute safety during the Audit
D. Assists the Auditor in identifying risks and threats

2. Which term best describes the difference between the sample and the population in the sampling process?

A. Precision
B. Tolerable error rate
C. Level of Risk
D. Analytical Data

3. Name one of the purposes of creating Business Continuity Plan

A. To maximise the number of decisions made during an incident
B. To minimise decisions needed during a crisis
C. To lower business insurance premiums
D. To provide guidance for federal regulations

4. Failing to prevent or detect a material error would represent which type of risk?

A. Overall Audit Risk
B. Detection Risk
C. Inherent Risk
D. Control Risk

5. Which is one of the bigger concerns regarding asset disposal?
A. Residual Asset Value
B. Employees taking disposed property home
C. Standing data
D. Environmental Regulations

6. Who should issue ogranisational policies?

A. Policies should originate from the bottom and move up to the middle management level for approval
B. The policy should be issued in accordance with the approved standards by the middle management level
C. Policy can be issued by any level of management based on a case to case basis
D. The policy should be signed and enforced by the highest level of management

7. A program check that ensures data entered by a data entry operator is complete, is an example of a

A. Detective Control
B. Preventive Control
C. Corrective Control
D. Redundancy Control

8. What is the primary objective in problem escalation?

A. Improve customer satisfaction
B. Optimise the number of skilled personnel
C. Ensure the correct response
D. Prove that the IT staff is competent

9. Which of the following is LEAST important when Auditors review Internal Controls?

A. The existence of an Audit Committee in the Organisation
B. The Organisational structure and the Management style used by the Organisation
C. The existence of a Budgeting System
D. The number of Personnel working for the Organisation

10. What is the best example of why plan testing is important?

A. To prove the plan worked the first time
B. To find the correct problems
C. To show the team that is not pulling their own weight
D. To verify that everyone shows up at the recovery site

11. Continuity planners can create plans without the Business Impact Analysis (BIA) process because

A. Business Impact Analysis is not required
B. Management already dictated all the key processes to be used
C. Not possible, critical processes continuously changes
D. Risk assessment is acceptable

12. What are the three competing demands to be addressed by the Project Management?

A. Scope, Authority and Availability of Resources
B. Time, Cost and Scope
C. Requirements, Authority and Responsibility
D. Authority, Organisational Culture and Scope

13. How should management act to best deal with emergency changes?

A. Emergency changes can not be made without advanced testing
B. All changes should still undergo review
C. The changes control process does not apply to emergency conditions
D. Emergency changes are not allowed under any condition

14. Which is the following is not an objective of a control?

A. Reduce expected losses from irregularities
B. Reduce the probability of an error occurring
C. Reduce the amount of loss if it occurs
D. Provide for all the failures and to ensure that business is protected fully from such failures

15. The objectives of IT audit include assessment whether systems are in place and working efficiently to

A. Ensure asset safeguarding
B. Ensure that the attributes of data or information are maintained
C. Both (a) and (b)
D. None of the above

16. Which among the following does not encompass Organisational and Management controls within the information processing facility (IPF)

A. Sound human resource policies and management practices
B. Methods to assess effective and efficient operations.
C. The regulatory framework within which the business is carried out
D. Separation of duties within the information processing environment

17. The essential aspect to be understood about the organisation subject to IT audit is

A. Organisation's business and its strategic goals and objectives
B. The number of operating units / locations and their geographic dispersion
C. Major pending projects in progress
D. All of the above

18. While understanding the type of software used in the organisation the IT auditor has to

A. See the policy decision on developing software inhouse or to buy commercial products.
B. Collect details of operating systems, application system and database management system
C. Collect information relating to network architecture and technology to establish connectivity.
D. All of the above

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

QUIZ

Q. NO	ANSWERS	Q. NO	ANSWERS
1	D	10	C
2	A	11	A
3	B	12	B
4	A	13	D
5	B	14	C
6	D	15	C
7	D	16	A
8	D	17	B
9	B	18	B

Digital Forensic Audit

Forensic audit inspects and evaluates the financial information of a firm or individual, to use it as an evidence that can be conducted to accuse it/him for fraud, scam or any other financial dues. Where, Digital forensics is the "process of identifying, conserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."

IT Forensic investigative skills can decrease occurrence of fraud; Increase the difficulty of committing fraud; Improve fraud detection methods; Reduce total fraud losses; Auditors trained in these skills are more valuable to the organization!

These six areas of inquiry are meant to begin a conversation and provide a framework of understanding to a computer forensics team conducting an investigation.

1. IT Standards, Policies and Procedures Acceptable use of policy in place, formally documented, formally communicated to all employees formally signed an acknowledgement of receipt and review of said policy; what behavior is acceptable and unacceptable; various methods of computing use, e.g. email, web surfing, social media use, etc. should be there in policy
2. User Access Monitoring – Both traditional user and privileged user access is subject to monitoring; mentioned layer access is monitored (e.g. database, application, network layers); type of activity is monitored (e.g. direct data access, etc.); monitoring also include a review of unsuccessful login attempts and a review of unusual access attempts (e.g. weekends, off-hours, etc.); inactive accounts should be disabled.
3. Web Access Monitoring –User activity on web surfing are tracked by computer or by user; web access filtered (blocked) by keyword and/or URL.
4. Password Controls – Password required for system access; a password policy in place and enforced; passwords required to be complex; password should be periodically changed.
5. Backup Procedures - Backups should be performed; Backup includes Application/ Database/ Configuration settings; Restore been performed to ensure backups operate as intended.
6. Audit Trails – Automatic logging of activity takes place or not? Gain an understanding of what activity is logged; Determine if audit trails are in place at the Operating System, Application or Database layer; Audit trails are periodically reviewed or not?

Reference:

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/overview-of-digital-forensics.aspx

https://digitalforensicsmagazine.com/blogs/?p=300

Disclaimer

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

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

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

Compiled & Designed By:

Abhay Singh, Dy. Director (R&I), *i*CISA
Manish Kumar, AAO (R&I), *i*CISA
Vijay Kumar, Sr. Auditor (R&I), *i*CISA

2019 Issue