

भारत के नियन्त्रक-महालेखापरीक्षक का कार्यालय
9, दीनदयाल उपाध्याय मार्ग, नयी दिल्ली 110124
OFFICE OF THE COMPTROLLER & AUDITOR GENERAL OF INDIA
9, Deen Dayal Upadhyaya Marg, New Delhi 110 124

नीतिगत प्रबंधन इकाई
Strategic Management Unit

No. 1214-B/SMU/41-2019

2 December 2019

Subject: Standard Operating Procedure for conduct of Information System (IS) Audits

In the Senior Management meeting held in June 2019, CAG stated that a formalized arrangement where iCED and iCISA can be part of the audit process organically should instead be devised and knowledge sharing between the concerned audit offices and the two institutes institutionalized. Accordingly, the following Standard Operating Procedure (SOP) is instituted for conduct of IS Audit. This SOP will supersede the instructions for conduct of IT Audits issued earlier *vide* letters No. IT Audit/2005-06/Policy dated 22nd March 2006, No.120-16/SMU/2013 dated 3rd April 2013 and No.343/SMU/25-2017 dated 31st August 2017.

Risk Analysis and selection of topics for audits

1. In view of the fast evolving technology landscape, Chief Technology Officer (CTO)/ DG-iCISA will carry out, on a periodic basis, risk assessment in the areas of policy, strategy, governance, standards, security and implementation framework surrounding technology & its application to programme, activities, service design and delivery. The risk assessment exercise will involve effective stakeholder engagement (field offices, functional wings), research and survey of developments in above mentioned area and indicate **broad area of focus in audit**.
2. The risk assessment exercise by CTO/DG-iCISA will be supported by field offices and functional wings at HQ. A Risk Assessment Committee will be formed to lead the exercise, with DAI (Coord, Commn & IS) and DAI (CRA) as chair and co-chair. The Committee will be convened by CTO/DG-iCISA and comprise four representatives of State ADAs Committee, one representative of CRA wing, one representative of GA wing, DG (RC), DG (Railways), DG (Co-ordination), DG (Commercial),

DG/PD (SMU) and PD (P&T). CTO/DG-iCISA will frame the ToR of the Committee and evolve the mechanism for collaboration and timely feedback from field offices.

3. Incorporating the topics/areas communicated by field offices, the Risk Assessment Committee will arrive at priority areas for audit in the next two years in respect of all related functional wings at HQ. The topics/areas for the second year will be open to review in the next annual meeting of the Risk Assessment Committee.
4. An annual workshop, guided by the deliverables of the Risk Assessment Committee, attended by external experts/resource persons/HoDs of IAAD offices and members from Senior Management, will be held by CTO/DG-iCISA which will precede the annual audit plan exercise for the Department. The workshop will be scheduled latest by middle of September for the audit cycle commencing from the following April.
5. A two year rolling plan for the Department incorporating list of important topics/areas/subject matter, as per the scope of this SOP, will be prepared by Risk Assessment Committee. The risk associated with the topics and their priority will then be decided and depending upon the risk being national or local in character, it will be decided whether audit will be undertaken at State or All-India level. Association of experts, whether by field office or through CTO/DG-iCISA, will also be decided and enumerated at this stage.
6. In audit assignments of all-India nature, as decided at sl no 5 above, CTO/DG-iCISA will be involved as co-lead auditor to provide technical inputs, domain knowledge as well as consolidate further learnings from field experience.
7. The workshop will prepare a calendar for submission of guidelines/audit design matrix/audit questions etc., by audit offices to CTO/ DG-iCISA for in-depth review. A tentative schedule of holding of mid-term and end-term reviews will also be prepared in respect of each audit.
8. The two year rolling plan, incorporating actions listed at sl no 5,6 and 7 above, will be sent by CTO/ DG-iCISA to SMU and all functional wings, latest 15 October.

Audit Plans

9. On the basis of the two year rolling plan agreed in the workshop, audit offices will incorporate the topics/areas/subject matter in their annual audit plan. As per existing

practice, audit offices will send their annual audit plan to the concerned functional/regional wings by 15 November. Any variation between the topics/areas/subject matter agreed in the workshop and that incorporated in their overall annual plan by audit offices will be accompanied by an explanatory note. Audit offices should have progressed in preparation of guidelines by this time.

10. As per existing practice, SMU will obtain approval of the CAG for overall annual audit plan and communicate approval to audit offices, latest by 15 February. A final list of IS audit will be intimated to CTO/DG-iCISA by SMU after approval, for appropriate changes in their work plan for the year starting April.

Audit Planning and Execution

11. Mid & end term appraisals and review of audit guidelines (including pilot studies, evaluation etc.) undertaken by concerned functional wing will be required to involve CTO/ DG-iCISA.

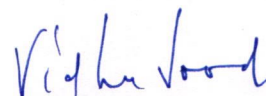
Audit Reporting

12. At the reporting stage, CTO/ DG-iCISA will participate in end term conference with lead auditors/audit offices of all/selected IS audits. These meetings may involve domain experts as previously co-opted (with due regard to maintaining confidentiality). The outcome of these meeting would be to agree on key messages/conclusions arising from evaluation of sufficiency and appropriateness of evidence in respect of audit objectives already set out in the guidelines. Drafting of reports would ideally commence from this stage.
13. CTO/DG-iCISA will assist the functional wings in examining the draft IS Audit Report from materiality and related angles. This would include Key Document (KD) verification (manual and electronic). The Audit Reports will then be processed for final approval by the respective functional wings for obtaining CAG's approval.
14. Where the draft audit material (e.g. a Performance Audit or a Theme-based Compliance Audit) includes both IS audit and non-IS Audit findings and recommendations, the draft report may be vetted by both CTO/ DG-iCISA and the functional wing. CTO/DG-iCISA will examine the relevant sections relating to IS audit keeping the concerned functional wing fully informed and will also conduct KD verification for the IS audit related findings.

15. The schedule of dispatch of the draft IS Audits from the field offices will be synchronized with that of the concerned Report of the respective functional wings so that undue delays are not experienced. Timelines between the CTO/DG-iCISA and functional wings will be accordingly worked out.

Review and Monitoring of SOP

16. CTO/DG-iCISA will submit a note on the functioning of the SOP for Senior Management review by March every year to SMU. The value chain and its effectiveness established by this SOP will be reviewed annually by Senior Management based on feedback from functional wings and CTO/DG-iCISA.
17. If during the operationalisation of SOP, it is felt that there exist skill/knowledge gaps, the concerned wing is encouraged to intimate the same to Training wing and iCISA.
18. The SOP will be implemented with effect from the Annual Audit Plan for the year 2020-21. For the AAP 2020-21, the Risk Assessment Committee may consider selecting appropriate activities as applicable and re-work the schedule, but within the overall timeline of concluding all activities by February 2020. From 2021-22, the activities and timelines will be as per the SOP.
19. For ongoing IS audits pertaining to AAP 2019-20, CTO/DG-iCISA will provide necessary support on request from the functional wings.



(Vidhu Sood)

Principal Director (SMU)