Technical Guide on Revised Directions issued by CAG under Section 143(5) of the Companies Act, 2013

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Technical Guide on Revised Directions issued by CAG under Section 143(5) of the Companies Act, 2013

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Edition	:	February 2026
Committee	:	Auditing and Assurance Standards Board
Email	:	aasb@icai.in
Website	:	www.icai.org
Price	:	Rs. 200/-
Published by	:	The Publication and CDS Directorate on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002.

Foreword

Section 143(5) of the Companies Act, 2013 empowers the Comptroller and Auditor General of India (CAG) to issue specific directions to the auditors of Government companies and other Government-owned/controlled companies. Exercising these powers, the CAG issued directions under this section, and now the CAG has issued a revised set of directions vide letters dated 23rd May 2025 and 17th October 2025. These directions, inter alia, require the auditor to cover fair valuation of investments made for post-retirement employees' benefit, IT-based processing and controls over accounting transactions including cyber security/IT controls, proper accounting and utilization of Government grants/subsidies, formulation of risk management policy including identification/valuation of data assets, and compliance with applicable legal and regulatory requirements.

Given the expanding scope and increasing complexity of audit responsibilities in Government and public sector audits, these revised directions assume significant importance in strengthening accountability, transparency, and governance. Considering the systemic relevance of these directions which are required to be responded by auditors, the Auditing and Assurance Standards Board (AASB) of the Institute of Chartered Accountants of India (ICAI) undertook the important task of developing guidance on these directions.

I am pleased to note that AASB has issued this "Technical Guide on Revised Directions issued by CAG under Section 143(5) of the Companies Act, 2013", to assist the members in understanding and complying with the revised directions. The Technical Guide provides guidance on the reporting requirements and includes illustrative examples of auditor's reporting for each requirement. In developing this Technical Guide, AASB has closely consulted the CAG officials with a view to ensure its relevance and usefulness.

I express my sincere gratitude to the CAG officials and place on record my appreciation for CA. Sripriya Kumar, Chairperson, CA. Ravi Kumar Patwa, Vice Chairman, and all the members of the Auditing and Assurance Standards Board for their dedication and efforts in bringing out this Technical Guide.

I am confident that the members and other stakeholders will find this Technical Guide immensely useful.

CA. Charanjot Singh Nanda
President, ICAI

Preface

Government companies and other Government-owned/controlled companies constitute an important segment of the national economy due to their strategic relevance and public interest responsibilities. Recognising their distinctive nature, the audit framework for such companies is specifically prescribed under section 143(5) of the Companies Act, 2013, which enables the Comptroller and Auditor General of India (CAG) to ensure that audits of such companies address areas of significance from the perspective of governance, accountability and stewardship of public resources.

In terms of section 143(5), the CAG is empowered to issue directions to the auditors of such companies regarding the manner in which the accounts of such companies are required to be audited. In exercise of these powers, the CAG issued a revised set of directions vide letters dated 23rd May 2025 and 17th October 2025. These revised directions require the auditors to specifically focus on certain high-impact thematic areas, inter alia:

- Fair valuation of investments made for post-retirement employees' benefits.
- IT-based processing of accounting transactions, with emphasis on IT controls and cyber security-related controls.
- Accounting and utilisation of Government grants/subsidies.
- Risk management policy for key risk areas, and identification & valuation of data assets.
- Compliance with the applicable legal and regulatory requirements.

Given the specialised nature of the above requirements, auditors may face practical challenges in interpreting the directions, aligning audit procedures, and drafting appropriate reporting responses while ensuring full compliance with the applicable Standards on Auditing and relevant legal and regulatory framework. In this

backdrop, the Auditing and Assurance Standards Board (AASB) of the Institute of Chartered Accountants of India (ICAI) undertook the initiative to develop a Technical Guide to provide guidance on these directions.

We are pleased to present this "Technical Guide on Revised Directions issued by CAG under Section 143(5) of the Companies Act, 2013", published by the Auditing and Assurance Standards Board. This Technical Guide aims to assist the members by providing direction-wise guidance on audit approach and reporting considerations, along with illustrative reporting formats/examples to promote clarity, consistency and quality in auditors' responses. It is, however, clarified that this Technical Guide is intended to supplement and not substitute the requirements of the Companies Act, 2013, and the applicable Standards on Auditing, which continue to remain fully applicable in audits of such companies.

We express our sincere thanks to CA. Charanjot Singh Nanda, President, ICAI and CA. Prasanna Kumar D, Vice President, ICAI, for their guidance and support to the activities of the Board.

We wish to place on record our sincere gratitude to all members of the study group *viz.* CA. Archana Bhutani, CA. Mohit Bhuteria, Mr. K T Saravanabhava, CA. Vivek Newatia, CA. Deepa Agarwal, CA. Kamal Mour, CA. Lalit Kumar, and CA. Puneet Nanda for their valuable contribution in developing this Technical Guide. We also wish to place on record our sincere gratitude to the CAG officials for their valuable support and contribution at various stages in finalising this Technical Guide.

We wish to place on record high appreciation of all Board members and special invitees to the Board viz. CA. Jay Chhaira, CA. Piyush Sohanrajji Chhajed, CA. Chandrashekhar Vasant Chitale, CA. Vishal Doshi, CA. Arpit Jagdish Kabra, CA. Durgesh Kabra, CA. Purushottamlal Khandelwal, CA. Priti Paras Savla, CA. Babu Abraham Kallivayalil, CA. Dayaniwas Sharma, CA. Sridhar Muppala, CA. Sanjib Sanghi, CA. Abhay Chhajed, CA. (Dr.) Anuj Goyal, CA. Satish Kumar Gupta, CA. Gyan Chandra Misra, CA. Pankaj Shah, CA. Pramod Jain, CA. Rajesh Sharma, CA. (Dr.) Sanjeev Kumar Singhal, Shri Manoj Kumar Sahu, Shri Naveen

Singhvi, Justice (Former) Shashi Kant Gupta, CA. Vinay Mittal, CA. Jagdeesh Vishwanath Dhongde, CA. Devendra Kumar Somani, CA. Manish Agarwal, CA. Heneel Kamleshkumar Patel, CA. Prabhakar P S, CA. Ranganathan P K, CA. Rajeesh Gupta, CA. Sandeep Sharma, CA. Chinnasamy Ganesan, CA. Narasimhan J, CA. Mahesh Krishnan, CA. Bhavani Balasubramanian, CA. Raghuram K, CA. Nachiappan SP, CA. Dhananjay Gokhale, CA. Sumant Chadha, CA. Rajesh Arora, CA. Sonika Burman, CA. Vijay Kumar, CA. Nachiket Ratnakar Deo, CA. Shrenik Mehta, CA. Rajesh Guraria, CA. Pinaki Chowdhury, CA. Sanjay Agarwal, CA. Jayanta Mukhopadhyay, CA. Ratna Rachita Mohanty, CA. Jitendeep Singh, CA. Nilanjan Paul, CA. Himanshu Sarpal, CA. Pranav Jain, CA. Himanshu Kumar Agarwal, CA. Vivek Agarwal, CA. Sumit Mahajan, CA. Jyoti Prakash Gadia, Shri Pranay Nahar, Shri Deep Mani Shah, CA. Prateek Maheshwari and CA. Sanjay Vasudeva for their valuable contribution in various activities of the Board.

We also wish to express our sincere thanks to all the Council Members for their suggestions, support and guidance in various activities of the Board. We also thank CA. Megha Saxena, Secretary, AASB and other staff of AASB for their contribution in finalising this Technical Guide.

We are confident that this Technical Guide will be well received by the members and other interested readers.

CA. Ravi Kumar Patwa
Vice Chairman, AASB

CA. Sripriya Kumar
Chairperson, AASB

Contents

Background to this Technical Guide

1. Section 143(5) of the Companies Act, 2013 ("the Act") empowers the Comptroller and Auditor General of India ("CAG") to issue specific directions to the auditors of certain classes of companies, as prescribed in the section. These directions are mandatory in nature, and auditors are required to comply with and report on them as part of the independent auditor's report addressed to the shareholders of the company.

   Section 143(5) states as under:

   "In the case of a Government company or any other company owned or controlled, directly or indirectly, by the Central Government, or by any State Government or Government, or partly by the Central Government and partly by one or more State Government, the Comptroller and Auditor-General of India shall appoint the auditor under sub-section (5) or sub-section (7) of section 139 and direct such auditor the manner in which the accounts of the company are required to be audited and thereupon the auditor so appointed shall submit a copy of the audit report to the Comptroller and Auditor-General of India which, among other things, include the directions, if any, issued by the Comptroller and Auditor-General of India, the action taken thereon and its impact on the accounts and financial statement of the company."

2. The CAG vide their letters dated 23rd May 2025 and 17th October 2025 have issued a revised set of directions under section 143(5) of the Act **("Directions")**. The directions will be applicable for compliance by the Statutory Auditors of Government Companies/ Government owned/ controlled other companies where accounts are finalised after date of issue of the said letter dated 17th October 2025. The directions are given as **Appendix** to this Technical Guide.

3. The reporting required under the directions is supplemental to the audit of financial statements of the company and forms an integral part of the auditor's report on the financial statements.

Hence, the procedures required to be performed by the auditor for reporting under the directions would generally be expected to be within the framework of the principles enunciated in the Standards on Auditing (SAs) prescribed under Section 143(10) of the Act. In addition, the specific requirements of the directions may also require other specific audit procedures to be performed which could be in addition to the audit procedures required to express an opinion on the financial statements.

4. The purpose of this Technical Guide is to assist statutory auditors of companies to which the directions apply, in discharging their additional responsibility pursuant to the directions. The auditors are advised to exercise their professional judgment, due diligence, and prudence while using this Technical Guide in specific client engagement contexts and should ensure compliance with all the applicable Standards on Auditing in the conduct of their audit engagements. The auditors may note that this Technical Guide is not a substitute for the authoritative text of all the applicable Standards on Auditing.

5. The auditor should consider whether any adverse or non-affirmative comments in response to the directions have a bearing on the true and fair view presented by the financial statements and whether the same would warrant a modification in the main audit report under sub-sections (2) and (3) of section 143 of the Act. If the auditor is of the opinion that such comments warrant a modification in the main audit report, the manner of reporting would be in accordance with the principles enunciated in SA 705(Revised), “Modifications to the Opinion in the Independent Auditor’s Report”.

6. The auditor should also consider whether the circumstances require an emphasis of matter paragraph to be incorporated as required under SA 706(Revised), “Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor’s Report”.

7. It should not, however, be assumed that every adverse or non-affirmative comment under the directions would necessarily result in a modification in the main audit report.

8. Firstly, the adverse or non-affirmative comment may be regarding a matter which has no relevance to a true and fair view presented by the financial statements. Secondly, while the non-compliance may be material enough to warrant an adverse or non-affirmative comment under the directions, it may not be material enough to affect the true and fair view presented by the financial statements. In deciding, therefore, whether a modification in the main audit report is necessary, the auditor should use their professional judgement in the facts and circumstances of each case.

9. This Technical Guide also includes illustrative formats of reporting under various clauses of the directions. Auditors are advised to suitably modify the reporting as per the specific facts and circumstances of their audit engagements, using their professional judgment and ensuring inclusion of relevant information and explanation as applicable.

Clause I – Fair Valuation of Investments for Post Retirement Benefits

10. **Clause I. Assess the fair valuation of all the investments, both quoted and unquoted, made directly by the Company or through Trusts, for Post retirement benefits of the employees. This includes verifying valuation methodologies, ensuring consistency with Ind AS and reviewing supporting documentation. The auditor shall provide a brief note on the valuation approach, its reasonability, and compliance with applicable regulations, reporting any material deviations or misstatements.**

11. The above clause requires auditor to do the following:

    a. Assess the fair valuation of all the investments both quoted/unquoted, made directly by the company or through trusts, for post retirement benefits of the employees.

    b. Verify the valuation methodologies.

c. Ensure consistency with relevant Ind AS/AS (as applicable) to the company.

d. Review of supporting documentation.

e. Provide a brief note on the valuation approach, its reasonableness and compliance with applicable regulations.

f. Report material deviations or misstatements, if any.

12. Post-employment benefits are defined as employee benefits (other than termination benefits and short-term employee benefits) that are payable after the completion of employment. This definition captures retirement benefits (e.g. pensions and lump sum payments on retirement) and other post-employment benefits (e.g. post-employment life insurance and access to medical care). If an entity provides such benefits, the requirements of Ind AS 19, "Employee Benefits"/AS 15, "Employee Benefits" (as applicable) apply irrespective of whether a separate entity is established to receive contributions and to pay benefits.

13. The auditor should first critically assess whether the retirement plans of an entity are in the nature of defined contribution plans or defined benefit plans (Please refer Ind AS 19/ AS 15 for definitions of these terms) and are appropriately categorised based on the plan.

14. Defined benefit plans may be unfunded, or they may be wholly or partly funded by contributions by an entity, and sometimes its employees, into an entity, or fund, that is legally separate from the reporting entity and from which the employee benefits are paid. Given the focus of the reporting requirement on fair valuation of investments, the clause is primarily relevant for post-retirement benefits which are in the nature of defined benefit plans.

15. In accordance with the principles of Ind AS 19/ AS 15, it should be assessed whether the investments made by the company, or the trust qualify as plan asset.

- The fair value of any plan assets is deducted from the present value of the defined benefit obligation in determining the deficit or surplus.
- If the criteria for plan assets is not met, the company should consider whether the assets intended to fund its obligations should instead be recognised as its own assets in its balance sheet, either because they are held directly by the entity or by an entity that is consolidated by it.

16. If the investments qualify as plan asset, then its fair value should be determined as per the applicable financial reporting framework (Ind AS 19/ AS 15).

17. It is management's responsibility to establish processes that ensure compliance with the requirements of the applicable financial reporting framework. This will include fair valuation of the investments accounted for as plan assets involving selection of appropriate methods, use of appropriate assumptions and data.

18. SA 540, "Auditing Accounting Estimates, including Fair Value Accounting Estimates, and Related Disclosures" deals with auditor's responsibilities in relation to accounting estimates. It expands on how other relevant Standards on Auditing e.g. SA 315, "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment", SA 330, "The Auditor's Responses to Assessed Risks" and SA 500, "Audit Evidence" are to be applied to the audit of accounting estimates. It also includes requirements and guidance on the evaluation of misstatements of individual accounting estimates, and indicators of possible management bias.

19. SA 540 explains that the auditor's objectives are to obtain sufficient appropriate audit evidence about whether accounting estimates in the financial statements are reasonable, and the related disclosures are adequate, in the context of the applicable financial reporting framework.

20. There are three main components of the process for determining fair value as an accounting estimate:

1. Methods (including models)
2. Assumptions
3. Data

21. The measurement of fair value can be subject to judgement and estimation uncertainty giving rise to inherent subjectivity and variation in outcomes. The auditor should assess the design and implementation of internal controls relating to fair valuation of investments. Since fair value is an accounting estimate, the auditor should comply with SA 540 with respect to audit of fair value measurement.

22. The following aspects of SA 540 need to be considered in the context of audit of fair value accounting estimates:

    a. Risk Assessment Procedures and Related Activities
    b. Identifying and Assessing the Risks of Material Misstatement
    c. Responses to the Assessed Risks of Material Misstatement
    d. Further Substantive Procedures to Respond to Significant Risks
    e. Evaluating the Reasonableness of the Accounting Estimates, and Determining Misstatements
    f. Disclosures Related to Accounting Estimates
    g. Indicators of Possible Management Bias
    h. Written Representations
    i. Documentation

23. The auditor may employ or engage an expert ('Auditor's expert') with expertise in fair valuation. In such a case, the auditor should comply with SA 620, "Using the Work of an Auditors' Expert", which establishes requirements and provides guidance in determining the need to employ or engage an auditor's expert and the auditor's responsibilities when using the work of an auditor's expert. The auditor should evaluate

whether the auditor's expert has the necessary competence, capabilities and objectivity for the auditor's purposes.

24. When using the work of an auditor's expert, the auditor as per the requirements of SA 620, should evaluate the appropriateness of the expert's work. In evaluating such work, the nature, timing and extent of the further audit procedures are affected by the auditor's evaluation of the expert's competence, capabilities and objectivity, the auditor's understanding of the nature of the work performed by the expert, and the auditor's familiarity with the expert's field of expertise.

25. Where the auditor identifies a material misstatement in the valuation of these investments and such material misstatement remains uncorrected, the auditor should consider the impact on the audit opinion.

26. **Written Representations:** The auditor should consider the disclosures made in the financial statements in respect of reporting under this clause. Additionally, the auditor should also consider to obtain written representations from management as may be appropriate e.g. management accepts their responsibility for the fair valuation of investments, valuation methods used, including the related assumptions, are appropriate and consistently applied, all financial records, related data, and relevant information have been made available to the auditor, key assumptions used in fair value measurements are reasonable and reflect market participant perspectives, subsequent events in terms of SA 560, "Subsequent Events", that may require adjustments to fair value measurements have been considered by the management and disclosed to the auditor, any knowledge of fraud or suspected fraud that could affect the fair value measurements has been disclosed to the auditor.

    The auditor may consider to obtain written representations from management covering, inter alia, the following aspects:

    a. Statement of investments stating separately:

        (i) Investments held directly by the company

(ii) Investments held through a Trust

b. Basis of valuation

(i) Quoted

(ii) Unquoted

c. Valuation approach

d. Reasonableness of valuation

e. Compliance with applicable regulations

f. Report of material deviations or misstatements, if any

27. The auditor should maintain adequate audit documentation as per the requirements of SA 230, “Audit Documentation” with respect to the procedures performed, evidence obtained and the conclusions reached.

28. **Illustrative reporting**

Illustrative reporting under this clause is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement.

i. All the investments, made directly by the Company or through Trusts, for Post-retirement benefits of the employees have been valued appropriately in accordance with the applicable financial reporting framework and applicable regulations. The valuation approach and valuation methodologies applied by the company for these investments is appropriate. Brief note on the valuation approach is attached.

OR

ii. The investments, made directly by the Company or through Trusts, for Post-retirement benefits of the employees have been valued appropriately in accordance with the applicable financial reporting framework and applicable regulations. The valuation approach and valuation methodologies applied by the company for these investments is appropriate, except as mentioned below.

(Give details of cases of material deviations or misstatements)

Brief note on the valuation approach is attached

OR

iii. Any other as relevant

Clause II–Accounting Transactions and IT systems

29. **Clause II. Whether the Company has a system in place to process all the accounting transactions through IT system? If yes, whether review of this system and controls that are significant to the Companies' financial reporting process as well as cyber security has been done and material discrepancies found, if any, have been suitably reported? The implications of processing of accounting transactions outside IT system on the integrity of the accounts along with the financial implications may also be reported.**

30. Under this clause, the auditor needs to comment on the following:

a. Whether the company uses an IT system for processing all accounting transactions

b. If all accounting transactions are not processed through the IT system, the implications of processing accounting transactions outside the IT system on the integrity of the accounts and the financial implications, if any

c. If an IT system has been used by the entity, whether a review of systems and controls that are significant to the financial reporting process has been done and material discrepancies, if any, have been suitably reported

d. Whether any cyber security review has been done and material discrepancies, if any, have been suitably reported

Note 1: For the purpose of this clause, the wordings "implications of processing accounting transactions outside IT system on the integrity of the accounts" may be interpreted as

financial or disclosure implications which cause/may cause a material misstatement of the financial statements.

Note 2: The auditor's response to the directions would be based on the procedures carried out by the auditor during the course of the audit engagement including reviews of other relevant reports, if any, in accordance with the Standards on Auditing and does not envisage the performance of cyber security audits or reviews by the auditor.

31. **The guidance relating to this clause is organised into the following three parts:**

    Part A: Guidance in Respect of IT systems and transactions processed outside the IT System

    Part B: Guidance in Respect of IT systems reviews and material discrepancies, if any

    Part C: Guidance in Respect of cyber security reviews and material discrepancies, if any

Part A: Guidance in Respect of IT systems and transactions processed outside the IT System

Whether the Company has a system in place to process all the accounting transactions through IT system? The implications of processing of accounting transactions outside IT system on the integrity of the accounts along with the financial implications may also be reported.

32. SA 315, "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment" requires the auditor to identify and assess the risks of material misstatement, whether arising from fraud or error, at both the financial statement level and the assertion level. This is achieved through obtaining an understanding of the entity and its environment, including the entity's internal control. Such understanding provides an appropriate basis for designing and implementing audit responses that are responsive to the assessed risks, thereby enabling the auditor to reduce audit risk to an acceptably low level.

33. An understanding of the entity's internal control assists the auditor in identifying and assessing the risks of material misstatement at the financial statement and assertion levels. By understanding how internal control is designed, implemented and maintained by management, the auditor is able to identify areas where misstatements may arise and to evaluate whether the controls are capable of preventing, or detecting and correcting, material misstatements on a timely basis.

34. Such an understanding also enables the auditor to determine which controls are relevant to the audit and to assess whether those controls have been implemented. This forms the basis for designing further audit procedures that are responsive to the assessed risks, including determining the nature, timing and extent of substantive procedures and, where appropriate, testing the operating effectiveness of controls.

35. Further, understanding internal control helps the auditor to identify risks arising from the use of information technology, the complexity of transactions, and the susceptibility of financial statements areas to fraud or error. It also provides insight into the reliability of information produced by the entity that the auditor intends to use as audit evidence.

36. SA 315 prescribes five interrelated components of internal control, namely: (1) control environment, (2) the entity's risk assessment process, (3) the information system, including the related business processes, relevant to financial reporting, and communication, (4) control activities relevant to the audit, and (5) monitoring of controls.

37. For the purposes of reporting under this Clause, the auditor's understanding is primarily focused on the information system used for processing accounting transactions. Where accounting transactions are processed outside the IT system, the auditor is required to consider and report the implications of such processing on the integrity of the accounts along with the financial implications, if any.

38. An entity's business processes are the activities designed to

develop, purchase, produce, sell and distribute an entity's products and services; ensure compliance with laws and regulations; and record information, including accounting and financial reporting information. Business processes result in the transactions that are recorded, processed and reported by the information system.

39. The auditor should obtain adequate understanding of the entity's business processes, which include how transactions are originated, recorded, processed, and reported. This will also enable the auditor to obtain an understanding of the entity's information system relevant to financial reporting in a manner that is appropriate to the entity's circumstances. In this context, an entity may use a single integrated IT system for financial reporting or may use multiple IT systems (for example, specialised systems may be used for payroll, property, plant and equipment management etc. in addition to the main ERP system)

40. SA 315 requires that the auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas:

    (a) The classes of transactions in the entity's operations that are significant to the financial statements.

    (b) The procedures, within both information technology (IT) and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, transferred to the general ledger and reported in the financial statements.

    (c) The related accounting records, supporting information and specific accounts in the financial statements that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form.

    (d) How the information system captures events and conditions, other than transactions, that are significant to the financial statements.

(e) The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

(f) Controls surrounding journal entries, including non-standard journal entries used to record non-recurring, unusual transactions or adjustments.

41. Based on the above, the auditor would be able to identify IT systems and manual systems and processes which are adopted by the entity in respect of their accounting transactions. Risk assessment procedures, tests of controls and substantive audit procedures would enable the auditor to further confirm their understanding of the extent of usage of IT systems as complete or partial.

42. The entity (auditee) may also use service organizations as defined in SAE 3402, "Assurance Reports on Controls at a Service Organization". A service organisation is a third-party organization (or segment of a third party organization) that provides services to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting. The auditor would also need to gain similar understanding of the business processes and the extent of use of IT systems in respect of accounting transactions processed through such service organisations to determine impact, if any, for the purpose of reporting under this clause.

43. Exceptions where accounting transactions are processed outside the IT system should be reported by the auditor under this clause. For example, if payroll processing is carried out manually using spreadsheets and resulting entries are then recorded in the IT system, the same may be identified and reported as an exception while reporting under this clause. Similarly, where records relating to property, plant and equipment, including depreciation computations, are maintained in spreadsheets and form the basis for recording transactions in the entity's IT system, the same may also be reported as an exception under this clause.

44. In case of preparation of group financial statements (divisions, branches or units) or consolidated financial statements (subsidiaries, associates, joint ventures), the auditor may specifically enquire whether adjustment entries made for the purpose of consolidation are maintained in an IT system. In case record of such entries are maintained in spreadsheets, the same may also be highlighted while reporting under this clause.

45. In case where accounting transactions are not processed through an IT system, the auditor should also comment on whether the same have any impact on the integrity of the financial statements.

46. **Written Representations:** The auditor should also consider to obtain written representations whether the company has a system in place to process all the accounting transactions through IT system(s) and whether all the accounting transactions have been processed through such IT system(s) and exceptions, thereto.

47. **Illustrative reporting under this part of the Clause**

    Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement and indicate that the reporting is based on procedures as performed by the auditor.

    i. The Company has a system in place to process all the accounting transactions through IT system(s).

       OR

    ii. The Company has a system in place to process all the accounting transactions through IT system(s) except as mentioned below.

       ……

       (Instances, if any, which could affect the integrity of the accounts and financial implications, if any to be stated here).

       OR

    iii. Any other as relevant

Part B: Guidance in Respect of IT systems reviews and material discrepancies, if any

Where transactions of the company have been processed in IT systems, whether review of this system and controls that are significant to the Companies' financial reporting process has been done and material discrepancies found, if any, have been suitably reported?

Note: For the purpose of this clause, the term "material discrepancies" refers to "material weakness"

"A 'material weakness' is a deficiency, or a combination of deficiencies, in internal financial control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis."

[Paragraph 128 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

48. SA 315 requires the auditor to obtain an understanding of those control activities that are relevant to the audit, being the controls the auditor judges it necessary to understand in order to assess the risks of material misstatement at the assertion level and to design further audit procedures responsive to the assessed risks.

    Accordingly, the audit requires an understanding of only those control activities that relate to significant classes of transactions, account balances, and disclosure in the financial statements and the related assertions identified in the risk assessment process.

    Control activities are the policies and procedures established by management of the entity to help ensure that management's directives are carried out. Such control activities may be implemented through IT-based or manual systems, have varying objectives, and operate at different organisational and functional levels.

49. In understanding the entity's control activities, the auditor is required to obtain an understanding of how the entity has responded to risks arising from IT. IT also poses specific risks to an entity's internal control, including, for example:

    a. Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.

    b. Unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions or inaccurate recording of transactions. Particular risks may arise when multiple users access a common database.

    c. The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby breaking down segregation of duties.

    d. Unauthorised changes to data in master files.

    e. Unauthorised changes to systems or programs.

    f. Failure to make necessary changes to systems or programs.

    g. Inappropriate manual intervention.

    h. Potential loss of data or inability to access data as required.

[Paragraph IG 4.6 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

50. For the purpose of reporting under this clause, the auditor may rely on the work performed by them or by auditor's experts. The auditor may also consider reviews conducted by the management or by other specialists, engaged by the management, where such reports are available.

51. As required by the clause, the emphasis is on IT systems and controls and cyber security reviews which are significant to the company's financial reporting process.

52. The use of IT influences the manner in which control activities are designed and implemented. From the auditor's perspective, controls over IT systems are considered effective when they ensure the integrity of information and the security of the data processed by such systems. Controls over IT systems comprise effective general IT controls and application controls.

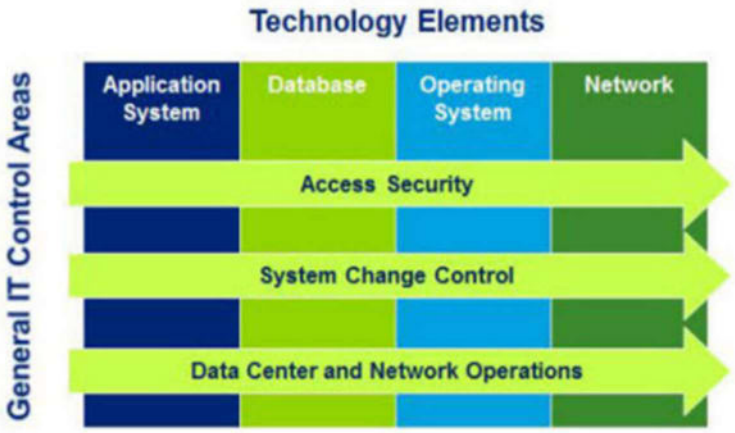
General IT Controls

53. General IT controls (GITCs) are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, miniframe, and end-user environments. General IT controls that maintain the integrity of information and security of data commonly include controls over the following:

- Data centre and network operations.
- System software acquisition, change, and maintenance.
- Program change.
- Access security.
- Application system acquisition, development, and maintenance.

[Paragraph IG 4.7 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

54. GITCs include controls in the three areas of access security, system change control, and data centre and network operations. GITCs also include controls over each of the relevant technology elements within the entity's IT environment, including the application systems, databases, operating systems, and networks. As depicted in Figure below, GITCs are typically structured such that there are similar controls in place for each of the GITC areas across each of the technology elements.



[Paragraph IG 4.8 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

Access security

55. GITCs related to access security include logical access controls to prevent or detect unauthorised use of, and changes to, data, systems, or programs, including the establishment of system-based segregation of duties.

[Paragraph IG 4.9 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

56. An entity will typically have numerous controls in place to address logical access security, such as implementing user authentication to its systems through the use of unique user IDs and passwords; controlling the process for assigning, modifying, and terminating user access; monitoring the use of privileged-level access; and periodically reviewing user access privileges for appropriateness.

[Paragraph IG 4.10 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

57. Entities also control access to their systems through establishing segregation of duties controls. From an IT perspective, the auditor typically considers segregation of duties as it relates to each of the following types of users:

a. End user system access — End users may be defined as entity personnel outside of the IT department who use the entity's application system (e.g., to process transactions or perform controls related to significant accounts and disclosures).

   For example, a control over end-user access that prevents a single user from having access to both enter and approve journal entries may address risks of material misstatement related to the recording of fictitious or fraudulent journal entries for various significant accounts and disclosures.

b. IT personnel system access — IT personnel may be defined as entity personnel responsible for administering the entity's IT systems (e.g., system administrators, security administrators). Segregation of duties controls over IT personnel system access are typically controls that address IT risks. It is typically appropriate for the auditor to test segregation of duties whenever testing user access to the entity's IT systems.

   For example, a control over IT personnel system access that prevents a single IT system administrator from having access to both make changes to systems and promote those changes to the production environment may address an IT risk related to the promotion of unauthorised changes into the production environment, resulting in inappropriate modifications to systems or data.

[Paragraph IG 4.11 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

System change control

58. System change controls address implementation and integration of programs or systems within the IT environment to verify the integrity of processing, performance, and controls over the computerised application systems that it supports.

[Paragraph IG 4.12 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

59. GITCs related to system change control include controls within the following categories:

    a. Program change: Controls to provide assurance that changes to the application systems and database management systems are implemented in a controlled manner.

    b. System software acquisition, change and maintenance: Controls to provide that network and communication software, systems software, and hardware are effectively acquired, changed, and maintained.

    c. Application system acquisition, development, and maintenance: Controls to provide that application systems and database management systems are effectively acquired, developed, implemented, and maintained.

[Paragraph IG 4.12 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

Data centre and network operations

60. GITCs related to data centre and network operations include controls to provide for the integrity of information as it is processed, stored, or communicated by the relevant aspects of the IT infrastructure.

[Paragraph IG 4.13 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

Application Controls

61. Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Timely, accurate and reliable information is critical to enable informed decision making. The timeliness, accuracy and reliability of the information are dependent on the underlying application systems that are used to generate, process, store and report the information. Application controls are those controls that achieve the business objectives of timely, accurate and reliable information. They consist of the manual and automated activities that ensure that information

conforms to certain criteria that is referred to as business requirements for information. Those criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

[Paragraph IG 7.1 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

62. Many control activities in an entity are partially or wholly automated using technology. These procedures are also known as automated control activities or automated controls. Automated controls include financial process-related automated transaction controls, such as a three-way match performed within an ERP system supporting the procurement and payables sub-processes, and computerised controls in operational or compliance processes, such as checking the proper functioning of a power plant. Sometimes the control activity is purely automated, such as when a system detects an error in the transmission of data, rejects the transmission, and automatically requests a new transmission. Other times there is a combination of automated and manual procedures. For example, the system automatically detects the error in transmission, but someone has to manually initiate the re-transmission. In other cases, a manual control depends on information from a system, such as computer-generated reports supporting a budget-to-actual analysis.

[Paragraph IG 7.2 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

63. Most business processes have a mix of manual and automated controls, depending on the availability of technology in the entity. Automated controls tend to be more reliable, subject to whether technology general controls are implemented and operating, since they are less susceptible to human judgement and error, and are typically more efficient.

[Paragraph IG 7.3 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

64. Application controls relate to the transactions and master file, or standing data pertaining to each automated application system, and are specific to each application. They ensure the

accuracy, integrity, reliability and confidentiality of the information and the validity of the entries made in the transactions and standing data resulting from both manual and automated processing.

[Paragraph IG 7.4 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

65. The objectives relevant for application controls generally involve ensuring that:

    - Data prepared for entry are authorised, complete, valid and reliable.
    - Data are converted to an automated form and entered into the application accurately, completely and on time.
    - Data are processed by the application accurately, completely and on time, and in accordance with established requirements.
    - Data are protected throughout processing to maintain integrity and validity.
    - Output is protected from unauthorised modification or damage and distributed in accordance with prescribed policies.

[Paragraph IG 7.5 of the "Guidance Note on Audit of Internal Financial Controls Over Financial Reporting" issued by ICAI]

66. **Written Representations:** The auditor should also consider to obtain appropriate written representations from management confirming that the entity has designed, implemented and maintained controls (including IT related controls) that are significant to the financial reporting process. Such written representations may, inter alia, include confirmations that the controls identified by management as significant to financial reporting were in operation during the year under audit, that no material weaknesses or deficiencies in such controls exist other than those disclosed to the auditor, and that any deficiencies identified during the year have been appropriately evaluated and remedial actions initiated.

Illustrative reporting under this part of the clause

67. Illustrative reporting is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement.

    Whether review of this system and controls that are significant to the Companies' financial reporting process has been done and material discrepancies found, if any, have been suitably reported

    i. Based on the audit procedures performed by us, reports of reviews conducted by the management (if any), reports of reviews conducted by specialists engaged by the management (if any), there are no material weakness in such IT systems and controls, which may result in material misstatement of the financial statements of the entity.

       OR

    ii. Based on the audit procedures performed by us, reports of reviews conducted by the management (if any), reports of reviews conducted by specialists engaged by the management (if any), there are no material weakness in such IT systems and controls, which may result in material misstatement of the financial statements of the entity except as stated below:

       ……..

       OR

    iii. Any others as relevant and necessary.

Part C: Guidance in respect of cyber security reviews and material discrepancies, if any

Where transactions of the company have been processed in IT systems, whether review of cyber security has been done and material discrepancies found, if any, have been suitably reported?

68. Cyber Security reviews refer to a systematic and independent assessment of an organization's security controls, policies, and procedures to evaluate their effectiveness in protecting

information systems and data from cyber threats. A cyber threat is a potential cyber related event or condition that could exploit a vulnerability and result in harm, disruption, or damage to a system, organization, or its assets.

69. The objective of a cyber security review is to systematically assess an entity's cyber security posture, identify vulnerabilities, evaluate control design and operating effectiveness of such controls, and provide recommendations to protect information assets against threats such as breaches, ransomware, and disruptions and to enhance cyber resilience of the entity.

70. ISA 315(Revised), "Identifying and Assessing the Risks of Material Misstatement" (Appendix 5: Considerations for Understanding Information Technology (IT)) - The auditor's consideration of unauthorized access may include risks related to unauthorized access by internal or external parties (often referred to as cybersecurity risks). Such risks may not necessarily affect financial reporting, as an entity's IT environment may also include IT applications and related data that address operational or compliance needs. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the IT application, database and operating systems that affect the preparation of the financial statements. Accordingly, if information about a security breach has been identified, the auditor ordinarily considers the extent to which such a breach had the potential to affect financial reporting. If financial reporting may be affected, the auditor may decide to understand, and test the related controls to determine the possible impact or scope of potential misstatements in the financial statements or may determine that the entity has provided adequate disclosures in relation to such security breach.

71. For the purpose of this clause, the auditor is required to:

- Obtain an understanding of the cyber security reviews undertaken by the entity and consider the reports, if any,

of such cyber security reviews, conducted by the management and / or specialists engaged by the management; and

- Report the results of such cyber security reviews, based on the reports and information furnished to the auditor.

72. The auditor may ascertain whether the entity's risk assessment process considers cyber security risks and reviews thereof and whether the entity has a process to periodically review their cyber security posture (e.g. Vulnerability Assessment, Penetration Testing). Organisations, based on their internal policies or based on regulatory mandates may undertake cyber security audits and reviews such as the following:[1]

    i. Compliance Audits- Evaluation of an organization's security practices to ensure they adhere to relevant industry standards, regulations, and policies.

    ii. Risk Assessments- The process of identifying and evaluating risks arising from cyber threats, vulnerabilities, and potential cyberattacks that could impact organizational operations, organizational assets, individuals, and connected entities. This involves assessing the likelihood and impact of various cybersecurity incidents.

    iii. Vulnerability Assessments- Examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

    iv. Penetration Testing- A security testing methodology in which individual components or the application as a whole are actively tested to identify and exploit potential

[1] Comprehensive Cyber Security Audit Policy Guidelines (Version 1.0 dated 25th July 2025) issued by the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India: https://www.cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf).

vulnerabilities. The objective is to determine whether these vulnerabilities can be exploited to compromise the application, access sensitive data, or affect the underlying infrastructure and environment.

v. Network infrastructure Audits- Comprehensive review of network components, including hardware devices such as firewall, end point devices, servers, router, network switches, IPS / IDS etc., software, configurations, access controls, and security measures, to identify vulnerabilities, inefficiencies, and areas for improvement.

vi. Operational Audits- Evaluation of an organization's cyber security operations, processes, and controls to assess their efficiency, effectiveness, and alignment with security objectives.

vii. IT security policy review and assessment against security best practices.

viii. Information Security Testing- The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.

ix. Source Code Review- Examining an application's source code to identify security vulnerabilities, coding errors, and inefficiencies, ensuring adherence to best practices, coding standards, and regulatory requirements to improve code quality and security.

x. Process Security Testing- Evaluating the security measures and controls within an organization's operational processes to identify vulnerabilities and ensure that sensitive information, systems, and applications are protected from security threats.

xi. Communications Security Testing- Evaluating the security measures implemented on communication channels to identify vulnerabilities and ensure that information transmitted over those channels is protected from unauthorized access, interception, modification, or disruption.

xii. Application security testing (including web applications, mobile applications and APIs)- Assessing an application’s architecture, components, and configuration to identify security vulnerabilities.

xiii. Mobile Application Security Auditing – A structured evaluation of mobile apps to identify security vulnerabilities, assess data protection, and ensure compliance with secure development practices.

xiv. Wireless Security Testing- Evaluating the security measures of a wireless network by simulating attacks to identify potential vulnerabilities and ensure the network is protected against unauthorized access and data breaches.

xv. Physical Security Testing- assessing and evaluating the physical security measures that protect an organization's assets, including its facilities, equipment, and personnel, from unauthorized access, theft, damage, or other physical threats.

xvi. Red Team Assessment- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

xvii. Digital Forensic Readiness Assessment- Evaluating an organization's preparedness to effectively collect, preserve, and analyze digital evidence in the event of a security incident.

xviii. Cloud Security Testing- Evaluating and assessing the security measures, configurations, and vulnerabilities of cloud-based systems, applications, and infrastructures.

xix. Industrial Control Systems/ Operational Technology Security Testing- Evaluating the cyber security posture of industrial control systems (ICS) and operational technology (OT) networks, specifically designed to identify vulnerabilities and potential threats that could disrupt critical industrial processes, impacting safety,

production, and overall system availability within a facility.

xx. Internet of Things (IOT)/ Industrial Internet of Things Security Testing (IIOT) - Evaluating and validating the security posture of connected devices within an IoT network, particularly in industrial settings, by identifying vulnerabilities and potential attack vectors.

xxi. Log Management and Maintenance Audit - Assessing the effectiveness and completeness of system and security log generation, retention, integrity, and monitoring practices, ensuring that logs are maintained in accordance with organizational policies and regulatory requirements to support detection, investigation, and response activities.

xxii. Endpoint Security Assessment - Evaluating the security posture of endpoint devices (e.g., desktops, laptops, mobile devices) by assessing configurations, patching, malware protection, encryption, access controls, and monitoring mechanisms to ensure robust protection against endpoint based threats.

xxiii. Artificial Intelligence (AI) System Audits – Evaluation of AI systems for security, ethical alignment, transparency, data integrity, and resilience to adversarial manipulation.

xxiv. Vendor Risk Management Audits – Assessment of third-party and vendor cybersecurity practices to identify supply chain risks and ensure alignment with organizational security policies.

xxv. Blockchain Security Audit – A structured assessment of blockchain systems, including smart contracts and infrastructure, to identify vulnerabilities, verify cryptographic integrity, evaluate access controls and consensus mechanisms, and ensure compliance with security best practices and regulatory requirements.

xxvi. SBOM (Software Bill of Materials), QBOM (Quantum Bill of Materials), and AIBOM (Artificial Intelligence Bill of

Materials) Auditing – Evaluation of the Software Bill of Materials (SBOM), Quantum Bill of Materials (QBOM), and Artificial Intelligence Bill of Materials (AIBOM) to ensure transparency, traceability, and integrity of components used in software, quantum computing, and AI systems. This audit focuses on identifying known vulnerabilities, licensing issues, and supply chain risks associated with open-source and third-party components, and verifies adherence to secure development lifecycle practices and regulatory compliance.

73. For the purpose of reporting under this clause, with specific reference to cyber security reviews, the auditor may obtain information and reports, from the management, relating to:

    a. List of cyber security audits / reviews as conducted for the year under audit along with the details of the service providers.

    b. The reports issued and the key findings and recommendations of such audits/reviews.

    c. The impact of issues, if any, on the financial statements of the entity.

74. **Written Representations:** The auditor should also consider to obtain written representations from management regarding cyber security reviews. Such representations may include confirmations as to whether any cyber security audits or reviews were conducted during the year, the scope and nature of such reviews, the material findings or vulnerabilities identified, if any, and the status of remediation of such findings. Confirmation may also be obtained that there were no cyber incidents during the year that had, or could reasonably be expected to have, an impact on the integrity of accounting records or financial reporting, except as disclosed to the auditor.

Illustrative reporting under this part of the clause

75. Illustrative reporting is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement.

    The Company has undertaken a cyber security assessment / review / audit in respect of the following areas.

Cyber Security Review Report	Report date	Deficiencies reported (High / Medium / Low)

Clause III – Grants and Subsidies

76. **Clause III. Whether funds (grants/ subsidy etc.) received/ receivable for specific schemes from Central/State Government or its agencies were properly accounted for as per the applicable accounting standards or norms and whether the received funds were utilised as per its terms and conditions? Whether accounting of interest earned on grants received has been done as per terms and conditions of the Grant. List the cases of deviation.**

77. This clause requires the auditor to comment whether funds (grants/ subsidies) received / receivable for specific schemes from Central/State Government or its agencies have been properly accounted for as per the applicable Accounting Standards or norms and whether the received funds were utilised as per its terms and conditions. Further, whether accounting of interest earned on grants received has been done as per terms and conditions of the grant. In this context, the auditor may consider the guidance set out in the following paragraphs:

78. The relevant Accounting Standards which deal with accounting of government grants are Ind AS 20, “Accounting for Government Grants and Disclosure of Government

Assistance", or AS 12, "Accounting for Government Grants" (as may be applicable).

79. The auditor should identify and understand the applicable financial reporting framework applied by the entity (AS 12 or Ind AS 20). This determination forms the basis for the timing of recognition, measurement, presentation and disclosure requirements.

80. *Understanding of the terms and conditions of grant:* The auditor needs to review the terms and conditions on which grants have been sanctioned to the entity. This includes the purpose of grant, criteria for utilisation of grant, refund of grant/ interest clauses, reporting requirements etc.

81. *Understanding of the internal control framework over grants:* The auditor needs to walk through the internal control framework over grants to review how grants are received, coded, monitored and reported. Deficiencies identified in controls which raise the risk of non-compliance with terms and conditions of grants, should be documented by the auditor. In this regard, the auditor may consider the following key risks and assess the controls in respect of such risks:

Key risk	Description
Premature recognition	Grants booked on memorandum of understanding or budget allocation rather than on "reasonable assurance".
Misclassification of capital vs. revenue	Common classification where ERP chart of accounts lacks grant-specific codes.
Diversion or delayed utilisation	Repeated inter-fund transfers, large advances to unrelated vendors.
Interest incorrectly dealt with	Interest earned parked in general revenue instead of scheme account or refund.

82. The illustrative audit procedures in respect of grants would include the following:

Audit assertion	Illustrative procedures
Existence & completeness	- Reconcile grants sanctioned totals with General Ledger balances. - Obtain third-party confirmation from the granting authority for material schemes.
Accuracy & valuation	- Re-perform amortisation or asset-cost offset calculations as per AS 12 / Ind AS 20. - Verify subsidy amounts with scheme notifications.
Cut-off	- Trace year-end receipts to bank statements. - Ensure no post-year receipts are recorded prematurely.
Compliance/ utilisation	- Vouch sampled expenses to scheme purpose. - Inspect progress reports, and, where practical, physical verification of assets created.
Compliance/ utilisation	- Detailed inspection of utilisation certificates furnished by the entity to the concerned ministry / office from which grant has been received.
Interest and refunds	- Recompute interest on unspent grant. - Check whether the treatment, recognition as income, liability or refund, matches the terms of grant and the requirements of relevant accounting standard.
Disclosure	- Cross-check notes to the financial statements for each grant: nature, outstanding conditions, contingencies and refunds due.

The auditor may apply attribute sampling, for testing compliance-related attributes and monetary-unit sampling for testing high-value schemes. It may be noted that materiality for grants is often set lower than overall performance materiality because the possibility of misuse of public funds is qualitatively significant.

83. **Written representations:** The auditor should consider the disclosures made in the financial statements in respect of reporting under this clause. The auditor should also consider to obtain management representation that all grants and related conditions have been disclosed; grants have been accounted for as per the applicable accounting standards or norms; funds have been used exclusively for sanctioned purposes; interest/refund obligations have been fully recognised or remitted; and accounting of interest earned on grants received has been done as per terms and conditions of the grant.

84. **Illustrative Reporting**

Illustrative reporting under this clause is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement

i. The Company has properly accounted for funds (grants / subsidy etc.) received/ receivable for specific schemes from Central/ State Government or its agencies, as the case may be, as per the applicable accounting standards or norms. The received funds were utilised as per its terms and conditions. Further, accounting of interest earned on grants received has been done as per terms and conditions of the grant.

OR

ii. The Company has properly accounted for funds (grants / subsidy etc.) received/ receivable for specific schemes from Central/ State Government or its agencies, as the case may be, as per the applicable accounting standards or norms. The received funds were utilised as per its terms and conditions. Further, accounting of interest earned on grants received has been done as per terms and conditions of the grant, except as mentioned below.

(Give details of cases of deviations)

OR

iii. No funds (grants/subsidy etc.) were received or are receivable for specific schemes from the Central/State government or its agencies during the year.

OR

iv. Any other as relevant

Clause IV(a)–Risk Areas and Risk Management Policy

85. **Clause IV(a). Whether the Company has identified the key Risk areas? If yes, whether the Company has formulated any Risk Management Policy to mitigate these risks? If yes, (a) whether the Risk Management Policy has been formulated considering global best practices?**

Risk Areas and Risk Management Policy

86. The auditor's responsibilities under this clause are to be understood in the context of the powers and duties of the auditor as specified by Sections 143(1) to (4) of the Act, read together with the Standards on Auditing ("SAs"), particularly SA 315, and SA 330.

87. As per SA 315, the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement. The auditor, therefore, performs risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. Identification of the risks by the auditor is followed by development of appropriate audit response to respond to such risks. This is required to achieve the objective with which an audit of financial statements is performed i.e., to express an opinion on whether the financial statements are prepared, in all material respects,

in accordance with the applicable financial reporting framework.

88. Hence, the auditor's primary objective under SA 315 is to identify and assess business risks that may result in a risk of material misstatement in the financial statements rather than evaluation of the entity's enterprise-wide risk management framework. Hence, the auditor is concerned specifically about those risks and controls that have a bearing on the audit.

89. Although most controls relevant to the audit are likely to relate to financial reporting, SA 315 clarifies that not all controls that relate to financial reporting are relevant to the audit. It is a matter of the auditor's professional judgment whether a control, individually or in combination with others, is relevant. Therefore, in the context of this clause, the auditor's responsibility is to evaluate the design and implementation of those internal controls that are deemed relevant for the purpose of the audit, rather than performing an exhaustive review of all risk management policies and controls that an entity might have put in place.

90. In the context of the above, the auditor needs to distinguish between their work on internal controls relevant for the purposes of the audit and the entirety of the controls that a company might have implemented as part of its enterprise-wide risk management framework. While auditor tests the design and implementation of controls that might be relevant for the audit, they are not required to do so for all controls within the entity's risk management framework.

91. Therefore, the procedures designed by the auditor should be aimed at gathering sufficient appropriate evidence to provide factual answers to the specific questions laid out in this clause.

Risk Management Policy

92. The auditor should determine whether a documented and formally approved risk management policy exists within the company, typically evidenced through minutes of board or audit committee meetings. Such policy should, at a minimum,

articulate the company's approach to identifying, assessing, prioritising, and mitigating business risks that may result in a risk of material misstatement in the financial statements.

93. Therefore, the auditor should examine relevant documentation, including the formally documented risk register, to confirm the explicit linkage between identified risks and corresponding risk mitigation strategies articulated in the risk management policy.

Obtain and Review the Risk Management Policy and Risk Register

94. The auditor should obtain a current and formally documented copy of the company's risk management policy and the related risk register, as formally approved by those charged with governance. The auditor should carefully read and analyse these documents to understand the company's formal approach towards identification, categorisation, assessment, and mitigation of business risks.

Identification of Key Risks

95. The auditor's objective under this clause is not to provide assurance on the completeness of company's risk register. Instead, the objective is to evaluate whether the company has an established process for identifying key risks and whether the output of that process appears reasonable. The primary benchmark for this evaluation is the auditor's understanding of the company, its environment, and its business risks, as obtained through risk assessment procedures performed under SA 315. To achieve this, the auditor should consider performing procedures such as inquiring of management and those charged with governance to understand their risk identification process; reviewing the company's documented risk register and policies; examining minutes of meetings of the board and its committees; and, most importantly, comparing the risks identified by the company against the key business risks and potential risks of material misstatement identified by the auditor during the audit.

96. The auditor's conclusion should be based on the factual

evidence. If the company has a documented process and its identified risks are consistent with the auditor's understanding of the entity and its environment, the auditor may be able to report in the affirmative. However, if the auditor identifies a significant risk (for example, a critical new environmental regulation or a major cyber security vulnerability) that is absent from management's assessment, such omission will form a factual basis for reporting that the company may not have identified all its key risk areas as required under this clause.

Risk Management Policy - Global Best Practices

97. The scope of audit of financial statements as envisaged in the Standards on Auditing does not require the auditor to evaluate whether the risk management policy of the company is benchmarked against global best practices.

98. Accordingly, for the purpose of this clause, the auditor may ascertain from the management, the benchmark, if any, adopted by the company in framing the risk management policy and report appropriately. Global benchmarks may include COSO's Enterprise Risk Management ("ERM") Framework (2017) or ISO 31000:2018 – Risk Management Guidelines. If management represents that any such benchmark has been applied, the same may be referred to in the auditor's response, based on management's note and / or written representation in this regard.

99. **Written Representations:** The auditor should also consider to obtain written representation whether the company has identified the key risk areas, and the company has formulated risk management policy to mitigate these risks. Further, the risk management policy has been formulated considering global best practices.

100. **Illustrative Reporting**

Illustrative reporting under this clause is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement

i. The company has identified the key risk areas and has

formulated a risk management policy to mitigate these risks. The said policy has been duly approved by the Board of Directors and, as represented by management, the same is stated to be based on global best practices, namely (…….)

OR

ii. The company has identified the key risk areas and has formulated a risk management policy to mitigate these risks. As informed by management, the policy has not been specifically benchmarked against any global framework; however, it incorporates principles considered appropriate to the company's operations and risk profile.

OR

iii. The company is yet to formally identify and document the key risk areas. Accordingly, the company has not yet formulated a risk management policy to mitigate these risks.

OR

iv. Any other as relevant

Clause IV(b)- Data Assets

101. **Clause IV(b). Whether the Company has identified its data assets and whether it has been valued appropriately?**

102. *Meaning of data asset:* For the purpose of this clause, a data asset refers broadly to organisational resources comprising information datasets—both structured and unstructured—generated, acquired, or retained by the entity, whether tangible (stored physically or digitally on hardware) or intangible (knowledge assets, intellectual property, customer data, market insights).

103. *Identification of data assets:* In determining the scope of reporting under this clause, the auditor should first ascertain whether the entity has recognised any data-related intangible assets in its financial statements, in accordance with the

applicable financial reporting framework i.e., Ind AS 38, “Intangible Assets” /AS 26, “Intangible Assets”. The auditor should identify whether such data assets are explicitly inventoried by management, appropriately documented within an Information Technology Asset Management ("ITAM") system, or Information Security Management System ("ISMS"), or equivalent inventories.

104. *Valuation of data assets:* This clause also requires auditor to comment on valuation of data assets. The auditor’s primary responsibility in this context is to perform necessary audit procedures to obtain reasonable assurance that the amounts recorded as intangible data assets in the financial statements are in accordance with the applicable financial reporting framework (Ind AS 38/AS 26) i.e., valuation of data assets is free from material misstatement.

105. Where no data asset has been recognised by management in the financial statements in accordance with the applicable financial reporting framework, the auditor is not required to perform further procedures under this Clause.

106. However, in situations where data assets have been recognised as intangible assets in the financial statements, the auditor should critically assess whether the prescribed criteria for recognition and measurement under the applicable financial reporting framework have been appropriately applied by management. This assessment should involve confirming compliance with Ind AS 38/AS 26 regarding initial recognition criteria, subsequent measurement, amortisation methods, and, where applicable, impairment testing requirements pursuant to Ind AS 36, “Impairment of Assets”/ AS 28, “Impairment of Assets”. The auditor should perform procedures to evaluate the appropriateness of the valuation methodology adopted by management and perform procedures to determine whether the carrying amounts of such data assets reflect their recoverable amounts, as mandated by the applicable financial reporting framework.

The auditor should also check the consistency, appropriateness, and reasonableness of valuation methodologies used by management. Where necessary, the auditor may consider using work of an expert in line with SA 620 in complex or material scenarios. Any findings or exceptions arising from these procedures should be clearly documented in the audit working papers and appropriately reported as part of compliance with this clause.

107. **Written Representations:** The auditor should also consider to obtain written representation that the Company has identified its data assets and data assets have been valued appropriately in accordance with the applicable financial reporting framework.

108. **Illustrative Reporting**

Illustrative reporting under this clause is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement.

i. The company has identified its data assets in accordance with the applicable financial reporting framework. The data assets have also been valued in accordance with the applicable financial reporting framework.

OR

ii. The company has identified its data assets in accordance with the applicable financial reporting framework. However, no data assets have been valued by the company.

OR

iii. The company has not identified any data assets and consequently these have not been subject to valuation.

OR

iv. Any other as relevant

Clause V – Compliance with Specified Laws and Regulations

109. **Clause V. Whether the Company is complying with the Securities and Exchange Board of India (SEBI) (Listing Obligations and Disclosure Requirements) Regulations, 2015, and other applicable rules and regulations of SEBI, Department of Investment and Public Asset Management, Ministry of Corporate Affairs, Department of Public Enterprises, Reserve Bank of India, Telecom Regulatory Authority of India, CERT-IN, Ministry of Electronics and Information Technology and National Payments Corporation of India wherever applicable? If not, the cases of deviation may be highlighted.**

110. This clause requires the auditor to examine whether the company has complied with the various laws and regulations specified therein, and to report appropriately on any cases of deviation.

111. SA 250, "Consideration of Laws and Regulations in An Audit of Financial Statements" provides the framework for the auditor's consideration of various laws and regulations in an audit of financial statements.

112. The Standard provides that the management, with the oversight of those charged with governance, is responsible to ensure that the entity's operations are conducted in accordance with the provisions of laws and regulations, including compliance with the provisions of laws and regulations that determine the reported amounts and disclosures in an entity's financial statements.

113. The Standard distinguishes the auditor's responsibilities in relation to compliance with two different categories of laws and regulations as follows:

    (a) The provisions of those laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements. The Standard provides that the auditor's responsibility is to obtain sufficient appropriate audit evidence about compliance with the provisions of those laws and regulations.

(b) Other laws and regulations that do not have a direct effect on the determination of the amounts and disclosures in the financial statements, but compliance with which may be fundamental to the operating aspects of the business, to an entity's ability to continue its business, or to avoid material penalties; non-compliance with such laws and regulations may therefore have a material effect on the financial statements. The Standard provides that the auditor's responsibility is limited to undertaking specified audit procedures to help identify non-compliance with those laws and regulations.

114. The Standard is intended to assist the auditor in identifying material misstatement of the financial statements due to non-compliance with laws and regulations. However, the auditor is not responsible for preventing non-compliance and cannot be expected to detect non-compliance with all laws and regulations.

115. However, this clause requires auditor's comments with regard to compliance with certain specific laws and regulations as specified in this clause and not limited to only those laws and regulations which could result in material misstatement in the financial statements due to non-compliance. In this context, the auditor may consider the guidance set out in the following paragraphs.

116. Section 134(5)(f) of the Act requires that the Directors' Responsibility Statement (referred to in Section 134(3)(c) of the Act) shall specifically state that the directors had devised proper systems to ensure compliance with the provisions of all applicable laws and that such systems were adequate and operating effectively.

117. In this context, the auditor should first obtain from management a list of the laws and regulations specified in this clause that are applicable to the company. The auditor should then, through inquiry and other appropriate audit procedures, satisfy himself that the list is complete, and that any laws or regulations excluded by management are indeed not applicable to the company.

118. The auditor should consider obtaining from management or those charged with governance a "Legal and Regulatory Compliance Statement" (prepared for the purpose of compliance with the CAG Directions), covering all laws and regulations applicable to the company as specified in this clause. The illustrative contents of such a statement may include, inter alia, the following:

Name of the Law / Regulation / Guideline and issuing authority	List of Key Compliances	Type (One time, Annual, Continuous, Event based)	Applicable for financial year 20XX-XX	How the compliance is ensured and demonstrated?	Status (Complied / Not complied)	Consequences of non-compliances (Fines/penalties/ others)
Companies Act 2013 (MCA)	Annual Financial statements and Audit					
	Composition of the Board					
	Meetings of the Board					
	Related Party Transactions					
	Loans to Directors					
	…					
SEBI LODR Regulations 2015 (SEBI)						

119. The auditor should, based on such test checks as considered relevant and necessary, verify the accuracy of the above statement, and report any deviations identified as required under this clause.

120. Section 205 of the Act outlines the functions of the company secretary, which include reporting to the Board about compliance with the provisions of the Companies Act, 2013 and the Rules made thereunder, and other laws applicable to the company. Accordingly, the auditor may also consider to obtain copies of the compliance reports / certifications submitted by the company secretary to the Board. Reference to such reports may also be made in the auditor's response under this clause, where appropriate.

121. **Written representations:** The auditor should also consider to obtain written representation regarding compliance / non-compliance by the company with the various laws and regulations specified under this clause.

122. **Illustrative Reporting**

Illustrative reporting under this clause is given below. Auditors may suitably modify the reporting as appropriate to reflect the specific facts and circumstances of the engagement

i. Based on the information and explanations given to us, secretarial audit report of the company (where applicable), and audit procedures carried out by us, the company is complying with the Securities and Exchange Board of India (SEBI) (Listing Obligations and Disclosure Requirements) Regulations, 2015, and other applicable rules and regulations of SEBI, Department of Investment and Public Asset Management, Ministry of Corporate Affairs, Department of Public Enterprises, Reserve Bank of India, Telecom Regulatory Authority of India, CERT-IN, Ministry of Electronics and Information Technology and National Payments Corporation of India wherever applicable.

OR

ii. Based on the information and explanations given to us, secretarial audit report of the company (where applicable) , and audit procedures carried out by us, the company is complying with the Securities and Exchange Board of India (SEBI) (Listing Obligations and Disclosure Requirements) Regulations, 2015, and other applicable rules and regulations of SEBI, Department of Investment and Public Asset Management, Ministry of Corporate Affairs, Department of Public Enterprises, Reserve Bank of India, Telecom Regulatory Authority of India, CERT-IN, Ministry of Electronics and Information Technology and National Payments Corporation of India wherever applicable, except as mentioned below.

(Give details of cases of deviations)

OR

iii. Any other as relevant

Appendix
Revised Directions issued by CAG under Section 143(5) of the Companies Act, 2013

CAG's revised directions for Statutory Auditors under Section 143(5) of Companies Act, 2013

I. Assess the fair valuation of all the investments, both quoted and unquoted, made directly by the Company or through Trusts, for Post retirement benefits of the employees. This includes verifying valuation methodologies, ensuring consistency with Ind AS and reviewing supporting documentation. The auditor shall provide a brief note on the valuation approach, its reasonability, and compliance with applicable regulations, reporting any material deviations or misstatements.

II. Whether the Company has a system in place to process all the accounting transactions through IT system? If yes, whether review of this system and controls that are significant to the Companies' financial reporting process as well as cyber security has been done and material discrepancies found, if any, have been suitably reported? The implications of processing of accounting transactions outside IT system on the integrity of the accounts along with the financial implications may also be reported.

III. Whether funds (grants/ subsidy etc.) received/ receivable for specific schemes from Central/State Government or its agencies were properly accounted for as per the applicable accounting standards or norms and whether the received funds were utilised as per its terms and conditions? Whether accounting of interest earned on grants received has been done as per terms and conditions of the Grant. List the cases of deviation.

IV. Whether the Company has identified the key Risk areas? If yes, whether the Company has formulated any Risk Management Policy to mitigate these risks? If yes, (a) whether the Risk Management Policy has been formulated considering global best practices? (b) whether the Company has identified its data assets and whether it has been valued appropriately?

V. Whether the Company is complying with the Securities and Exchange Board of India (SEBI) (Listing Obligation and Disclosure Requirements) Regulations, 2015, and other applicable rules and regulations of SEBI, Department of Investment and Public Asset Management, Ministry of Corporate Affairs, Department of Public Enterprises, Reserve Bank of India, Telecom Regulatory Authority of India, CERT-IN, Ministry of Electronics and Information Technology and National Payments Corporation of India wherever applicable? If not, the cases of deviation may be highlighted.

Note: The above directions will be applicable for compliance by the Statutory Auditors of Government Companies/ Government owned/ controlled other companies where accounts are finalised after date of issue of Hqrs letter dated 17.10.2025.