

Internal control over Financial Reporting

Testing/Examination of three types of controls

1) Entity level controls

A)	Code of conduct	<p>i) Memorandum of Association</p> <p>ii) Articles of association</p> <p>iii) HR manual</p> <p>iv) Values, Vision and code of ethics</p>	<p>a) Certificate of commencement of business</p> <p>b) Certificate of incorporation</p> <p>c) Liability of members/Subscribers to the memorandum</p> <p>d) Registered office of the company/any change in registered office</p> <p>e) Objects clause/any change in objects clause</p> <p>d) Number of shares held by subscribers to the memorandum</p> <p>a) Rules and regulation/ change in rules and regulation in the company</p> <p>b) Inclusion of any additional matters in AOA during the year</p> <p>c) Approval for change/amendment in AOA by all members in private company</p> <p>d) Approval for change/amendment in AOA by special resolution in public company</p> <p>e) Regulation of model articles if adopted by the company</p> <p>a) Policy governing employees</p> <p>b) Review of hierarchical structure in the organisation, top, middle and lower level</p> <p>c) Overview and employment relationship, contractual/temporary/permanent</p> <p>d) Information about status and position in the organisation</p> <p>e) Workplace professionalism</p> <p>f) Payroll structure information</p> <p>g) Employee benefits information about gratuity, welfare fund, VRS</p> <p>a) Mission, vision and values of the company defined and demonstrated</p> <p>b) Code of ethics and code of conduct documented, explained and enforced</p> <p>c) Anti-bribery policy, self disclosure of conflicts and whistleblower policies introduced and explained</p>
B)	ISO guidelines International organisation for standardisation (ISO)	<p>i) ISO 9000-Quality management</p> <p>ii) Environmental Management</p>	<p>a) a set of requirements for quality system of supplier</p> <p>b) Review of product standards</p> <p>c) Final inspection and testing</p> <p>d) Guidelines for developing and implementing quality system principles, structure, auditing and review</p> <p>a) Review of ability to meet supplier requirements</p> <p>b) Review of environmental performance</p>

		<ul style="list-style-type: none"> c) Sustainability in day to day operations for saving money, improve brand reputation d) Ability to rapidly adapt to change e) Build resilience against uncertainty f) Evaluation of emergency response g) Meeting customer expectations h) Relationship with stakeholders and local community
	iii) Country code	<ul style="list-style-type: none"> a) Maintenance of various countries and their capital cities codes
	iv) Social responsibility	<ul style="list-style-type: none"> a) Social return on investments b) Global impact investing network c) CSR policy stated in companies Act,2013 d) CSR Rules under companies Act,2013 e) Review of socially responsible behaviour in the organisation f) Review of accountability, transparency, ethical behaviour g) Respect for rule or law, stakeholder interests, human rights
	v) Energy Management	<ul style="list-style-type: none"> a) Plan-do-check-act process for continual improvement b) Development of policy for efficient use of energy c) Fix targets and objectives to meet that policy d) Decision concerning energy use e) Scope for continual improvement of energy policy f) Compliance with energy audits g) Review of energy performance indicators
	vi) Risk Management	<ul style="list-style-type: none"> a) Effect of uncertainty on objectives b) Design of framework for managing risk c) Establishing the context d) Risk identification e) Risk analysis f) Risk evaluation g) Risk treatment
	vii) Food safety management	<ul style="list-style-type: none"> a) Compliance of FSSAI rules and regulation
	viii) Information security management	<ul style="list-style-type: none"> a) Information security policies b) Organisation of information security c) Human resource security d) Asset management e) Access control d) Cryptography e) Physical and environmental security f) Operations security g) Communication security h) System acquisition, development and maintenance i) Supplier relationships j) Information security incident management k) Information security aspects of business continuity management
	ix) Sustainable events	<ul style="list-style-type: none"> a) Choosing the venue b) Reducing waste before during and after the event c) Analyse and improve d) Records of contribution to benchmarking

C)	Risk Management policy	i) Risk Assessment and control	<ul style="list-style-type: none"> a) All points covered in point B (vi) above b) Strategic risk- threat of competitor c) Compliance risk-new legislation or regulation might change way of going business d) Financial risk- payment from the customer not received within time e) Operatinal risk-Human error, fraud and error, failure of information systems, problems related to personnel management, commercial disputes, accidents, fire, floods, natural calamities f) Environmental risk- ability to adapt to changing environment and it's costs g) Employee risk-high employee turnover rate, loss of key managerial person h) Political risk- trade barriers domestic or international, monetary policy, impact of change in international taxation on the business i) Society- change in needs of the society and meeting it's requirements, social obligations of CSR, cost of adapting to change
D)	HR Policy	<ul style="list-style-type: none"> i) Management policy ii) Hiring iii) Employee benefits iv) Safety and security 	<ul style="list-style-type: none"> a) HR goals in line with the organisation b) Identification of work timings, offs, c) Review of communication with the HR department a) Verification of job description b) Documentation verification c) References of applicants d) Employee turnover rate control e) Selection processes used with reference to uniform guidelines f) Signing of application form by all candidates g) Use of consultants for manpower h) Salary structure defined i) Selected candidate informed j) Documentation after selection has been sent to the candidate a) Information to employees about benefits of gratuity, VRS, PF, ESIC b) Summary plan descriptions provided to participants c) Leave encashment benefit is provided employees d) Review of Insurance premiums and claims paid to employees a) Review of safety hazards b) Workplace accidents, injuries, illnesses, reported and investigated c) Measures in place to prevent intruders from entering the grounds or buildings d) Measures for access badges, traffic control, to keep unauthorised persons outside e) Response system in place for alarm f) Encouragement of employees to promptly report incidents and suggest ways to reduce or eliminate risk

E)	Related party transactions	i) Control activities	<ul style="list-style-type: none"> a) Assessing related party transactions and relationships b) Board approval for affiliations and related party transactions c) Compiling related party transactions d) Assessing investment statements, accounts payable ledger, investor listings, board meeting minutes e) Related party compliance under companies Act, 2013, Income tax Act, 1961, or any other law required as specified therein f) Incorporating certain detective controls to identify related party transaction from ERP system g) Report on related party transaction reviewed by legal and finance department h) Related party relationship can also be verified from procedures prescribed when hiring for individual and contractor employee i) Establishment of authority, committee to approve related party transactions j) Performing procedures when previously undisclosed related party transactions are identified k) Transactions involving significant risk
F)	Business continuity plan	i) Control activities	<ul style="list-style-type: none"> a) Assessing resources for the business b) Evaluation and rating of suppliers, customers, stakeholders c) Comparison of profits trends of past five years d) Evaluation of dividends paid over previous five years e) Review of net worth of the company f) Review of reserves and surplus funds available with the company g) Review of proposed expansion, diversification plan
G)	Organisation structure and division of work and responsibilities	i) Control activities	<ul style="list-style-type: none"> a) Clarity of role of the board b) Regularity of meetings c) Timely recording of minutes d) CFO empowered and independent to ensure full and fair reporting e) Clearly defined, updated organisation chart f) Well defined roles, responsibility and authority structure g) Formal delegation of powers h) Segregation of duties and functional roles across the company to improve internal controls i) Written policy for financial statements closure with assigned responsibilities j) Basis for making financial estimates and approval authority for it defined k) Ensuring employee empowerment and growth
H)	Disaster recovery plan	i) Control activities	<ul style="list-style-type: none"> i) Ensuring documented disaster recovery plan (DRP) ii) Testing of backups periodically iii) Communication of DRP to all employees iv) Identification of mission critical activities for effective DRP

I)	MIS and other controls	<p>i) MIS Control activities</p> <p>ii) Other control activities</p>	<p>v) Data recovery plan is established and operational</p> <p>vi) Assessing time required to recover from the disaster and it's impact on business</p> <p>vii) Alternative plans, substitute plans</p> <p>viii) Evaluation of business loss in terms of money, goodwill, human resources and capital assets</p> <p>ix) Develop contingency planning policy statement</p> <p>x) Conduct business impact analysis (BIA), it helps to identify and prioritize critical IT systems and components</p> <p>xi) Indetify preventive controls. These measures reduce the effects of system disruptions and contingency life cycle costs</p> <p>xii) Preventive controls can increase system availability</p> <p>xiii) Ensure recovery strategies are developed to recover quickly and effectively</p> <p>xiv) Develop IT contingency plan for restoring a damaged system</p> <p>xv) Plan testing, training and exercising</p> <p>xvi) Testing plan identifies gaps, training prepares recovery personnel for plan activation.</p> <p>xvii) Plan maintenance. It should be living document updated regularly with system enhancements</p> <p>a) Budgetary controls</p> <p>b) Performance review by management, with deviation analysis</p> <p>c) Well structured MIS generated from IT system used for financial reporting</p> <p>d) Periodic analysis to identify aberrations, exceptions and unusual trends</p> <p>e) System of internal audit for periodic review of controls</p> <p>f) Periodic review of adequacy of processes and controls by functional heads and departments</p> <p>a) Management's philosophy on IT usage, compliance and employee policies</p> <p>b) Emphasis of IT enables processes and automation</p> <p>c) Compliance framework and compliance reporting to management</p> <p>d) Employee policies and performance appraisal process</p> <p>e) Commitment, integrity and competency</p> <p>f) proposed action, remedial action for frauds and errors with responsibility</p>
----	------------------------	--	--

2) Process level controls/Transaction level controls/Operational level controls

A)	Receivable and sales	i) Control activities	<p>a) Sales orders prenumbered</p> <p>b) Credit approval</p> <p>c) Credit and sales department independent</p> <p>d) Sales order and sales invoice preparation</p> <p>e) Review of sales invoices</p> <p>f) Control over returned merchandise</p>
----	----------------------	-----------------------	---

			<ul style="list-style-type: none"> g) Matching of credit period and receiving reports h) Scrap sales and sales to employees i) Reconciliation of sales with cash receipts and accounts receivables and inventory j) Periodic preparation of aging schedule k) Control over collections of written-off receivables l) Receivables more than 180 days and less than 180 days report m) Independence of sales, receivables, receipts, billing and shipping personnel
B)	Accounts payable	i) Control activities	<ul style="list-style-type: none"> a) Designation of responsibility and it's independence from purchasing, cashier, receiving functions b) Periodic comparison of detail and control c) Control over purchase return d) Clerical accuracy of vendor's invoices e) Matching of purchase order, receiving report and vendor invoice f) Reconciliation of vendor statements with accounts payable details g) Advance payments and debit memos h) Review of discounts and debit balances i) Aging schedule of accounts payable and reasons for penal interest cost due to delay
C)	Payroll	i) Control activities	<ul style="list-style-type: none"> a) Authorisation to pay and personnel data records b) Review of time cards and payroll calculations c) Comparison of time cards to job sheets d) Imprest payroll account e) Responsibility for payroll records, Compliance with labour statutes f) Distribution of payroll checks and control over unclaimed wages g) Review of tax records for form 16, 12b, 12bb, ITR h) Comparison of pay slips with payroll structure
D)	Fixed Assets	i) Control activities	<ul style="list-style-type: none"> a) Detailed property records b) Periodic comparison with control accounts c) Proper authorisation for acquisitions and written policy for acquisitions d) Capital budgeting calculation and expected benefits of asset predefined e) Use of work orders and individual asset identification plates f) Written authorisation for sale and retirement g) Physical safeguard for theft h) Depreciated assets and disposal documentation i) Capitalisation, revenue expenses appropriation j) Depreciation adjustment for sales and retirements k) Inter-company transfer of asset documentation l) Adequacy of insurance m) Revaluation of fixed assets at the year end n) Hypothecation, charge, mortgage over fixed assets o) Physical verification of fixed asset
E)	Inventory management	i) Control activities	<ul style="list-style-type: none"> a) Periodic inventory counts by noncustodial b) Use of Count tags and inventory adjustment

			<ul style="list-style-type: none"> c) Periodic comparison of general ledger records and perpetual record d) Investigation of discrepancy e) Consignment inventory and inventory stored at warehouses f) Control over returnable containers left with customers g) Preparation of receiving reports, independence of custodian from record keeping h) Adequacy of insurance i) Physical safeguards against theft, fire j) Adequacy of cost system k) Cost system tied into general ledger l) Periodic review of overhead rates m) Use of standard cost and action on variances n) Inventory requisitions and authorisation over it o) Valuation of inventory as per accounting standard p) Method of valuation of inventory used such as FIFO, LIFO, Weighted average q) Valuation of waste and scrap items
F)	Treasury	i) Control activities	<ul style="list-style-type: none"> a) Imprest system and authorisation over it b) Amount of budget, spent and deviation in amount of cash fund c) Completeness of vouchers and custodian responsible for fund d) Reimbursement checks to order of custodian e) Physical checks and surprise audits f) Daily deposit and bank accounts authorisation g) Comparison of deposit slips with cash book and account receivables h) Cash received from other sources i) Separation of cashier personnel from accounting duties j) Use of cash registers and daily reconciliation of cash k) Control over bearer cheques and post dated cheques, authorisation to sign cheques l) Control over interbank transfers m) Inclusion of treasury controls in board policy n) Involvement of senior management in treasury
G)	Record to report	i) Control activities	<ul style="list-style-type: none"> a) Accounting policies adapted b) Accounting standards used c) Use of ERP system accounting packages and control over it d) Review of accounting system and integration with IT system e) Procurement, sales, administration, payroll mapped with accounting package used f) Internal audit and periodic review of transactions g) Risk control matrix (RCM) preparation for material risk of each process h) Review of organisational chart of defined responsibilities i) Review and use of standard journal entries j) Rotation of accounting personnel k) Record retention and display at appropriate level
H)	Duties and Taxes	i) Control activities	<ul style="list-style-type: none"> a) ERP system or tax software implementation b) Integration between compliance and tax provision c) Material weaknesses/significant deficiency or borderline assessments d) Compliance with tax law changes e) Causes of penalties, interest for the delay

			<ul style="list-style-type: none"> f) Internal audit review over statutory returns filed g) Contingent tax liability over the period h) Provision made for estimated tax liability i) Subsidy or Government grant or any scheme benefit to the company j) Communication with accounting and tax department k) Tax auditor's compliances and control over reporting as per tax laws l) Record of documentation and it's maintenance for specific period of years m) Compliances with statutory departments and cost involved in it
--	--	--	---

3) General IT controls

A)	General IT Controls	<ul style="list-style-type: none"> i) IT policy and department structure ii) IT procurement and outsourcing iii) Physical security and access to IT resources iv) Logical access controls v) Data security vi) Business continuity and 	<ul style="list-style-type: none"> a) Well documented IT policy explaining the company's philosophy and IT vision b) IT department's structure with clear identification of the roles and responsibilities c) Policy on anti-piracy, preferred platforms and mode of development a) Policy for procurement of IT hardware and software b) IT outsourcing policy clearing indicating the activities that need to be done in-house and those that may be outsourced c) Vendor KYC and due diligence policy d) Policy on access rights to outsourced vendors and control on data security e) Review of service level agreements (SLA) at pre-defined periodicity a) Physical control on access to IT servers and data rooms b) Safeguarding of IT hardware c) Custody and safekeeping of archived data and source code files d) Software licence management a) Access rights allocation, approval and periodic review b) "Need to know" basis of access right allocations c) Log reports for detection of threats and penetration d) Blocking and de-blocking of access rights e) Password change policy f) Controls on sharing of passwords a) Back-up polciy b) Data archival and access policy c) Choice of media for data storage d) Firewalls for safety from unauthorised access e) Protection of data stored on third party servers and on the cloud a) Documented BCP/DRP
-----------	----------------------------	--	--

	disaster recovery plan (BCP & DRP)	<ul style="list-style-type: none"> b) Testing of backups periodically c) Communication of DRP to all employees d) Identification of mission-critical IT activities for effective BCP/DRP
	vii) IT Manuals and source code	<ul style="list-style-type: none"> a) Availability of manuals for all IT applications and systems in use b) All modifications to IT systems duly updated in IT manuals c) For customised software, availability of source code for future modifications and for fixing bugs
	viii) Change management process for modification to IT applications	<ul style="list-style-type: none"> a) Tracking of IT change requests b) Modifications only in test server c) User acceptance test and technical test for all changes prior to go live d) Process for ensuring seamless data processing pre and post changes to the software
	ix) IT audit, log monitoring	<ul style="list-style-type: none"> a) Periodic IT security management audits b) Ongoing generation of log reports and effective review c) System based alerts for all security threats and unauthorised access
	x) Review of IT controls of significant outsourced vendors	<ul style="list-style-type: none"> a) For all significant outsourced activities, assessment of IT systems used and related controls implemented by the vendor e.g. outsourced payroll processing