UNIT-3: GOVERNANCE

DEFINITION: Combination of processes & structures implemented by board to inform, direct, manage & monitor activities of organization towards achievement of objectives.

INTERNAL MECHANISMS		EXTERNAL MECHANISMS	
1. Corporate charter	3. IA	1. LAWS	3. GOVT. REGULATORS
2. By laws	4. Board	2. REGULATIONS	

⇒ Effective governance considers risk while setting Strategy
Risk management relies on effective governance

⇒ Effective governance relies on controls to manage risks

GOVERNANCE

STRATEGIC DIRECTION
- Business model
- Overall objectives
- Risk Apetite
- Limits of org. conduct

OVERSIGHT
- Risk mgmt performed by Sr. mgmt & RISK OWNERS
- Internal & External Assurance Activities

BOARD has ultimate responsibility of OVERSIGHT

DUTIES

1. AUDIT COMMITTEE
2. RISK COMMITTEE
3. COMPENSATION COMMITTEE
4. DIVIDENDS
5. CAPITAL STRUCTURE
6. Selection & removal of officers
7. Adding, amending or repealing BYLAWS
8. Initiate fundamental changes

RISK COMMITTEE

1. Identify risks
2. Connect to Risk Mgmt. processes
3. DELEGATE to RISK OWNERS
4. TOLERANCE LEVEL compared to RISK APETITE

SENIOR MANAGEMENT

1. WHERE ? 2. WHO? 3. HOW?

RISK OWNERS

1. DESIGN testing
2. OE testing
3. Implementation testing [Establishing monitoring activities]
4. REPORTING

★ ORGANIZATION CULTURE affects CONTROL ENVIRONMENT

Risk Aggressive ⟶ Low importance of control

Risk Averse ⟶ HIGH importance of control

★ SENIOR MANAGEMENT is responsible for establishing & maintaining ORG. CULTURE.

GOVERNANCE SYSTEM

LESS MATURE	MORE MATURE
– IA emphasizes on COMPLIANCE	– IA emphasizes on OPTIMIZING Structure & PRACTICES
– BASIC Risks addressed	

ROLE OF INTERNAL AUDITORS

⇒ Board & Sr. mgmt. responsible for D&I of Governance

⇒ IA must assess & make appropriate recommendation to improve Governance process

⇒ IA must assess whether I.T. Governance of org. Supports strategies & objectives..

★ Design & practice of effective governance vary with :-

1. Size, Complexity & LIFE-CYCLE maturity of org.
2. STAKEHOLDER Structure
3. LEGAL & CULTURAL requirements.

★ IA PLAN should define :-

1. NATURE of WORK
2. GOVERNANCE process
3. NATURE of ASSESSMENTS

★ IA should consider LEGAL COUNSEL both BEFORE audit & BEFORE issuing FINAL REPORT.

CORPORATE SOCIAL RESPONSIBILITY

CSR refers to :

① Social responsibility ② Sustainable Development

③ CORPORATE CITIZENSHIP

⇒ CSR IS VOLUNTARY PRACTICE

ISO 26000 Definition: "Willingness of an org to incorporate Social & environmental considerations in its decision making & be accountable for the impacts of its decisions & activities on Society & environment"

Archie B. Carroll

1. Economic responsibility
2. Legal — " —
3. Ethical — " —
4. Philanthropic — " —

CSR FRAMEWORKS

GLOBAL REPORTING INITIATIVE (GRI)

- Reporting framework that provides specific guidance on measuring CSR performance against predefined criteria

ISO 26000

- Emphasizes on how to IMPLEMENT & MANAGE a CSR initiative.

RESPONSIBILITY OF CSR

BOARD : OVERSIGHT

MANAGEMENT : ESTABLISHING CSR objectives

INTERNAL AUDITOR : EVALUATE CSR controls

EMPLOYEES : All employees responsible for Success of CSR.

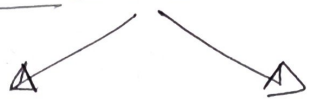
CSR STRATEGIES

1. REACTION : Deny responsibility & maintain STATUS QUO
2. DEFENSE : Use LEGAL ACTION
3. ACCOMODATION : Assume addional responsibility when PRESSURED
4. PROACTION : Org. takes INITIATIVE in implementing CSR

CSR RISKS

1. Loss of REPUTATION
2. NON-COMPLIANCE
3. LAWSUITS
4. OPERATIONAL FAILURES
5. SALES DECLINE (Customers)
6. STOCK Mkt. (Investors)
7. Employment mkt. (EMPLOYEES)

CSR AUDIT APPROACHES



By ELEMENT

1. Governance
2. Community Investment
3. Environment
4. Ethics
5. Health, Safety
6. Working condition & human rights

By STAKEHOLDER GROUP

1. Customers
2. Employees
3. Shareholder
4. Suppliers
5. ENVIRONMENT
6. NEIGHBOURING Communities

CSR REPORTING

Every Org. must make a business decision to:

1. COST OR BENEFIT of CSR report
2. What info to include in report?

REPORTING METHODS :-

1. Standalone report
2. Integrate CSR report + Annual financial report
3. CSR info booklet on Specific TOPICS.

UNIT-4: RISK MANAGEMENT

RISK: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of IMPACT & LIKELIHOOD.

RISK MANAGEMENT: A process to identify, assess, manage & control potential events or situations to provide reasonable assurance regarding the achievement of organisation's objectives.

RISK MANAGEMENT PROCESS

1) Identification of context
2) Risk identification
3) Risk assessment & prioritization
4) Risk Response
5) Monitor Risks

1. Identification of context

1. Capital projects
2. Laws & regulation
3. Business processes
4. Technology
5. Market risks
6. Organisation

2. RISK IDENTIFICATION

External risk factors @ Entity level

1. Technology changes
2. Customer wants & expectation changes

Internal risk factors @ entity level

1. Interruptions in automation systems
2. Quality of personnel hired
3. Level of trainings

1. Event Inventories
2. Questionnaires & Surveys
3. Leading Event Indicators & Escalation Triggers
4. Facilitated workshops
5. Process Flow analysis
6. Loss Event Data Methodology
7. SWOT
8. What-if (Sensitivity Analysis)
9. Brainstorming

3. Risk Assessment & Prioritization

Qualitative Methods

1. List all risks
2. Risk rankings
3. Risk maps

Quantitative Methods

1. Probabilistic models

Risk Modeling

IMPACT \ LIKELIHOOD	Remote	Possible	Likely
Critical	Risk A	Risk B	
Major			Risk D
Minor		Risk C	

Risk B & D ⇒ Professional judgement

4. Risk Response

Control: Actions taken by mgmt. to manage risks & ensure risk responses are carried out.

Control Risk: Risk that control FAILS to effectively manage CONTROLLABLE Risk.

RESIDUAL RISK : Risk remains after risk responses are executed

=> All personnel must be aware of importance of risk response appropriate to their levels of entity

5. RISK MONITORING

1. Track identified risks
2. Evaluate risk response
3. Monitor residual risk
4. Identify new risks.

Two Sources of information for ongoing assessment of adequacy of risk responses are :-

1. Manager of operating units.
2. Audit function
   ↳ especially if managers designed response strategy.

IMPLEMENTATION STANDARD 2120.A1

IA must evaluate RISK EXPOSURES relating to organisation's governance, operations & INFORMATION SYSTEMS regarding :

1. Achievement of org. strategic objectives
2. Reliability of financial & operational information
3. Effectiveness & efficiency of operations & programs
4. SAFEGUARDING OF ASSETS
5. Compliance with laws, policies, procedures, & contracts.

RESIDUAL RISK : Risk remains after risk responses are executed

⇒ All personnel must be aware of importance of risk response appropriate to their levels of entity

5. RISK MONITORING

1. Track identified risks
2. Evaluate risk response
3. Monitor residual risk
4. Identify new risks.

Two Sources of information for ongoing assessment of adequacy of risk responses are :-

1. Manager of operating units.
2. Audit function
   ↳ especially if managers designed response strategy.

IMPLEMENTATION STANDARD 2120.A1

IA must evaluate RISK EXPOSURES relating to organisation's governance, operations & INFORMATION SYSTEMS regarding :

1. Achievement of org. strategic objectives
2. Reliability of financial & operational information
3. Effectiveness & efficiency of operations & programs
4. SAFEGUARDING OF ASSETS
5. Compliance with laws, policies, procedures, & contracts.

⇒ IA must evaluate potential for occurrence of FRAUD & how org. manages FRAUD RISK

RISK MANAGEMENT MATURITY MODEL

① Initial ③ Defined ⑤ OPTIMIZED
② Repeatable ④ Managed

FOR CONSULTING ENGAGEMENTS

⇒ IA must address risk consistent with engagement's objectives

⇒ Incorporate knowledge of risks gained from consulting engagements

⇒ REFRAIN from assuming any mgmt. responsibility while assisting in establishing or improving processes.

COSO FRAMEWORK (ERM)

Provides basis for coordinating & integrating org.'s risk mgmt. activities. Effective integration (1) improves decision making & (2) enhances performance.

⇒ The culture, capabilities & practices integrated with strategy setting & objectives, that org. relies on to manage risk, in creating, preserving & realizing value.

⇒ CULTURE consists of attitudes, behaviour & understanding risk (+ve & -ve), that influence the decisions of mgmt. & personnel & reflect the mission, vision & core values of the org.

INHERENT RISK : In absence of mgmt. actions

ACTUAL RESIDUAL RISK : Remains AFTER mgmt. actions

RISK RESPONSE : Action taken to bring identified risks within org.'s RISK APETITE

RESIDUAL RISK PROFILE : Includes RISK RESPONSES

TARGET RESIDUAL RISK : Risk entity prefers to assume knowing mgmt. has acted or will act to alter its severity

VALUE is

1. CREATED → Benefits > Cost
2. PRESERVED → SUSTAINABLE
3. REALIZED → Benefits transferred to stakeholders
4. ERODED → Expected results not achieved

ERM ROLES & RESPONSIBILITIES

BOARD: OVERSIGHT
e.g. Audit Committee, Risk Comm., Governance Comm.
Compensation Committee

MANAGEMENT: OVERALL Responsibility for
① Day to day governance
② Implementation & development of COSO

CEO: ULTIMATE responsibility for ERM & achievement of strategy & objectives

RISK OFFICER OR Centralized Coordinator
↳ Facilitate risk management

3 LINES OF DEFENSE

1. Principal owner of risk.
2. RISK OFFICER
3. INTERNAL AUDIT

ERM COMPONENTS

SUPPORTING ASPECT: ① Governance & Culture (5)
② Information, Communication & Reporting (3)

COMMON ASPECT: ③ Strategy & objective setting (4)
④ Performance (5)
⑤ Review & Revision (3)

① Governance & Culture

1. Board exercise RISK OVERSIGHT
2. OPERATING STRUCTURE — LEGAL
   — Management
3. Define Culture
4. CORE VALUES
5. Attracts, develops & retains capable individuals

② STRATEGY & Objective Setting

1. Business Context — Dynamic
   — Complex
   — Unpredictable
2. RISK APETITE
3. ALTERNATIVE STRATEGY ← SWOT ANALYSIS
   COMPETITOR ANALYSIS
   SCENARIO ANALYSIS
4. Business objectives align with & support Strategy.
   ↳ (1) Specific (2) Measurable (3) Observable (4) Obtainable.
   ↳ TOLERANCES are established.

③ PERFORMANCE

1. Identify RISKS
2. Assessment of RISK
   - QUALITATIVE : Less costly
   - QUANTITATIVE : More precise
     - ↳ Decision tree, modeling,
     - Monte Carlo Simulation
3. Prioritize risks
   - (i) Agreed-upon criteria
   - (ii) Risk apetite
   - (iii) importance of affected business objective
   - (iv) Org. level.

AGREED-UPON CRITERIA [To evaluate characteristics of risk & determine entity's capacity to respond]

(1) Complexity (2) Velocity
(3) Persistence (4) Adaptability (5) Recovery

4. RISK RESPONSE
   - (1) Acceptance (Retention)
   - (2) Avoidance
   - (3) Pursuit
   - (4) Reduction
   - (5) Sharing/Transfer

FACTORS in selecting & implementing risk responses:

(1) Business Context (3) Cost & benefits
(2) Compliance (4) Risk Apetite <> Tolerance
(5) Risk response should reflect SEVERITY

5. DEVELOP & EVALUATE PORTFOLIO VIEW OF RISK
   - (1) RISK VIEW (minimal integration)
   - (2) RISK CATEGORY VIEW (LIMITED integration)
   - (3) RISK PROFILE VIEW (PARTIAL Integration)
   - (4) PORTFOLIO VIEW (FULL Integration)

④ REVIEW & REVISION

1. Identify & assess CHANGES
2. Review performance
3. Improvement of ERM

⑤ INFORMATION, COMMUNICATION & REPORTING

1. Leverage INFORMATION SYSTEMS to support ERM
2. Communication Channels
3. REPORTING

PURPOSE of reporting

(1) Understand relationship btw RISK, CULTURE & PERFORMANCE
(2) Decision making related to
   (i) Setting strategy & objective
   (ii) Governance
   (iii) Day-to-day operations

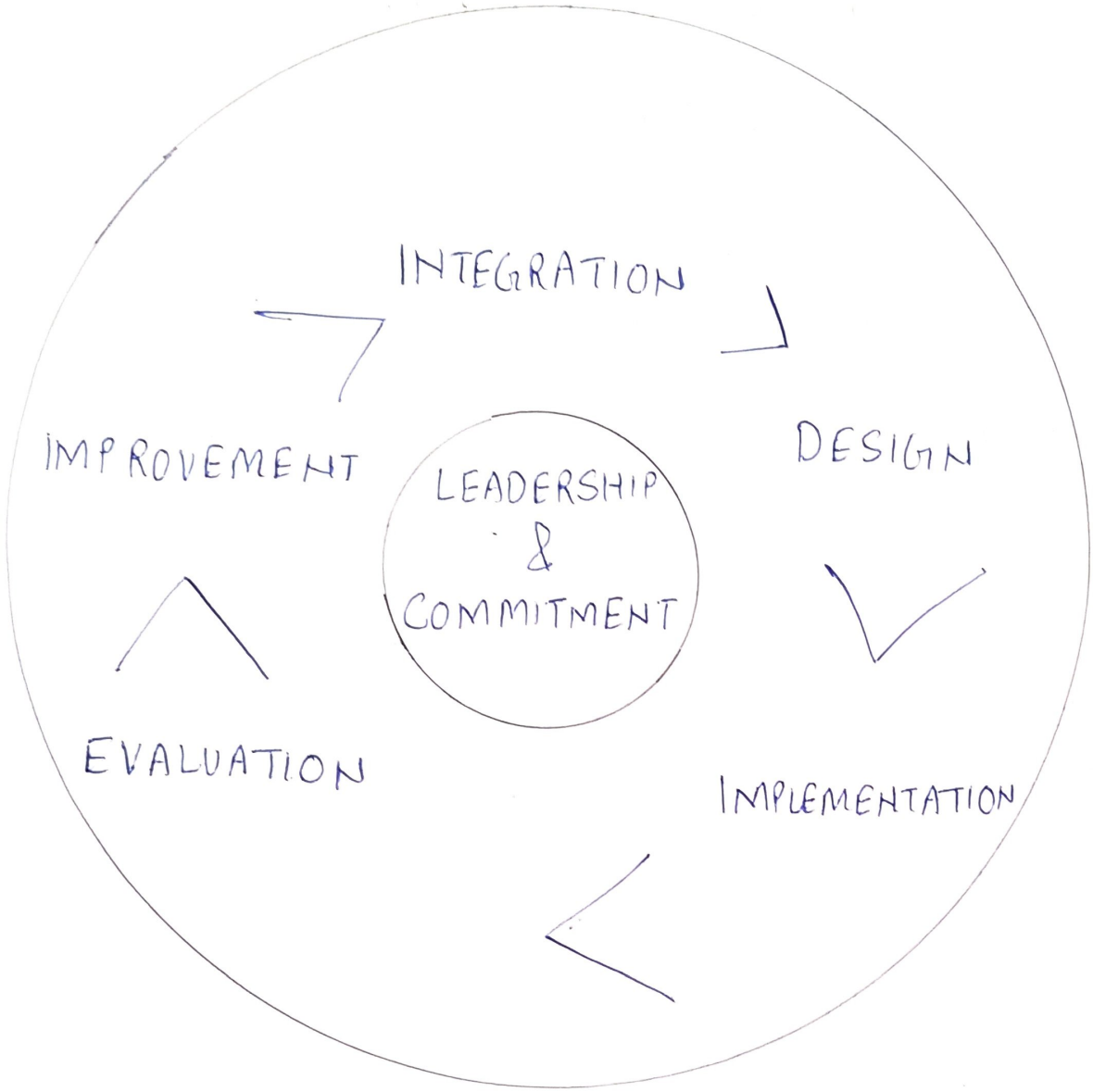
ASSESSING ERM

1. PRESENT: Components, principles & controls exist in D&I of ERM
2. FUNCTIONING: Components, principles & controls continue to OPERATE to achieve objectives

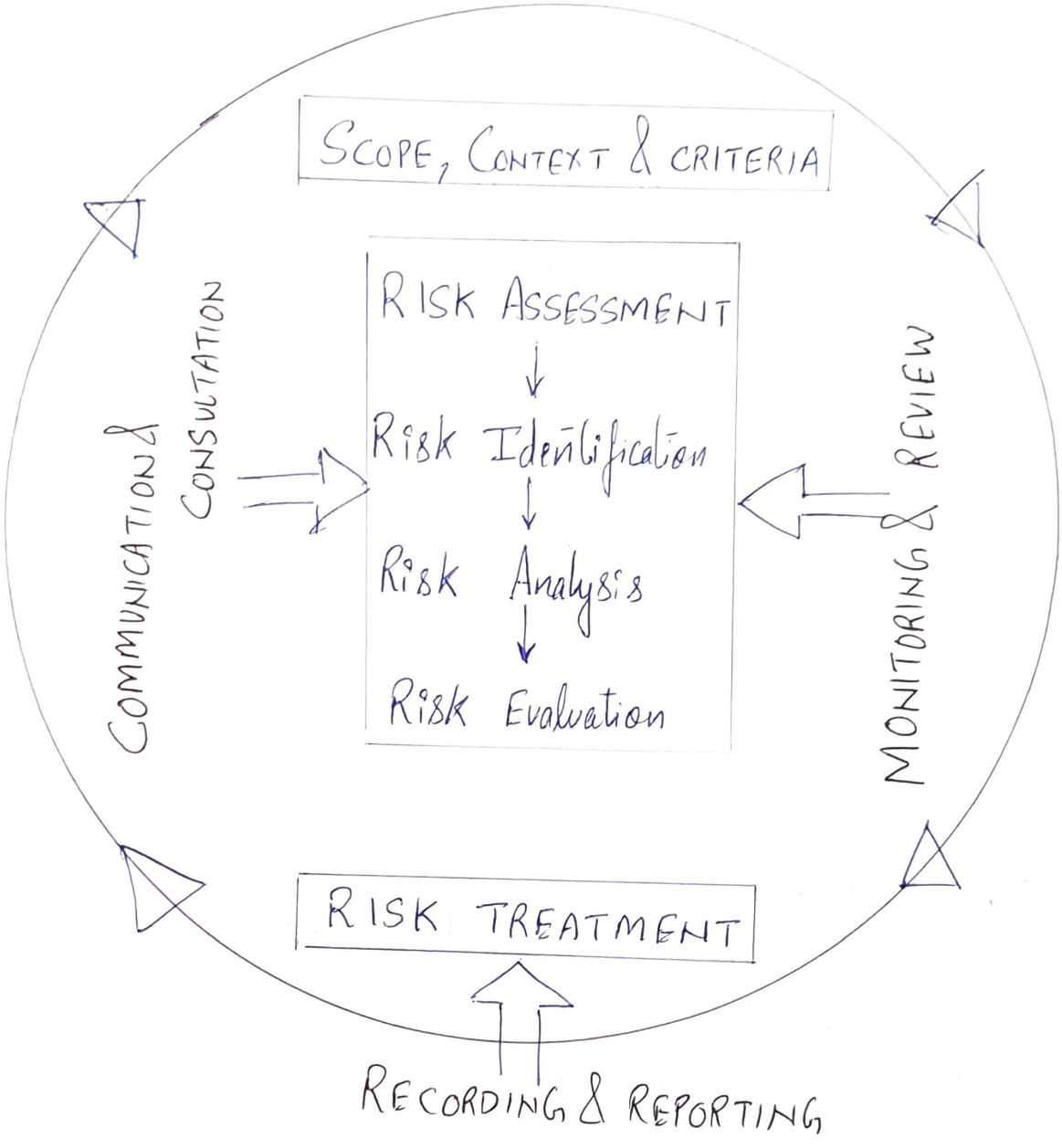
ISO 31000 : Risk Management Framework

⇒ Principle based approach.

PRINCIPLES


INTEGRATION
DESIGN
IMPLEMENTATION
EVALUATION
IMPROVEMENT
LEADERSHIP
&
COMMITMENT

FRAMEWORK


SCOPE, CONTEXT & CRITERIA
RISK ASSESSMENT
Risk Identification
Risk Analysis
Risk Evaluation
COMMUNICATION & CONSULTATION
MONITORING & REVIEW
RISK TREATMENT
RECORDING & REPORTING

PROCESS

✱ ISO 31000 – RESPONSIBILITIES for RISK MANAGEMENT

BOARD	MANAGEMENT	IA
⇩	⇩	⇩
OVERSIGHT	Set RISK ATTITUDE	Provide assurance regarding ERM

✱ ISO 31000 – ASSURANCE APPROACHES

1. KEY PRINCIPLES
2. PROCESS ELEMENT
3. CAPABILITY MATURITY MODEL : This approach determines where the risk mgmt. process is on MATURITY CURVE & evaluates whether :-
   (1) progressing as expected
   (2) Adds value (3) Meets org. needs.

LEVEL 0:	INCOMPLETE → Whether work can be completed, not known
LEVEL 1:	INITIAL → Work will be completed. NOT ON TIME & BUDGET
LEVEL 2:	REPEATABLE (MANAGED) → Projects planned, implemented, managed & monitored.
LEVEL 3:	DEFINED → Standards defined.
LEVEL 4:	QUANTITATIVELY MANAGED → Quantify performance improvement
LEVEL 5:	OPTIMIZING

✱ TURNBULL RISK MANAGEMENT FRAMEWORK : Emphasis on INTERNAL CONTROL

UNIT 5: CONTROL

CONTROL: Any action taken by mgmt., board & other parties to manage risks & increase likelihood that established objectives & goals will be achieved. Management plans, organises & directs the performance of sufficient actions to provide reasonable assurance that objectives & goals will be achieved.

CONTROL PROCESSES: Polices, procedures & activities that are part of control framework, designed & operated to ensure that risks are contained within RISK APETITE.

CONTROL ENVIRONMENT: Attitude & actions of board & management regarding the importance of control within the organisation.

INHERENT LIMITATIONS of INTERNAL CONTROL

1. HUMAN JUDGEMENT is FAULTY
2. MANAGEMENT may inappropriately OVERRIDE internal control.
   e.g. fraudulently achieve revenue projections OR hide liabilities
3. COLLUSION
4. COST should not be > BENEFITS

IMPLEMENTATION STANDARD 2130.A1

IA must evaluate the adequacy & effectiveness of controls in responding to risks within the org.'s governance, operations & INFORMATION SYSTEMS regarding the:

1. Achievement of org.'s strategic objectives
2. RELIABILITY & INTEGRITY of financial & operational info
3. Effectiveness & EFFICIENCY of operations & programs
4. SAFEGUARDING OF ASSETS
5. Compliance with laws, regulations, policies, procedures & contracts.

⇒ IA must incorporate knowledge of controls gained from consulting engagements into evaluation of org.'s control processes

⇒ Adequate criteria are needed to evaluate GRC.

IA MUST ASCERTAIN the EXTENT to which mgmt/BOARD has established adequate criteria.

If ADEQUATE ?

YES → IA should use this criteria

NO → IA to identify appropriate evaluation criteria

TYPES OF CONTROLS

1. PRIMARY CONTROLS

① PREVENTIVE CONTROLS

② DETECTIVE

③ CORRECTIVE e.g. Vasiances shadd be explained

④ DIRECTIVE
- ↳ Policies & procedures
- ↳ Trainings
- ↳ Job descriptions

2. SECONDARY CONTROLS

⑤ COMPENSATORY (MITIGATING)
e.g. NEXT morning SUPERVISOR RECONCILES count to CASH Registes.

⑥ COMPLEMENTARY CONTROLS
e.g. Separating Acctg. & custody of cash receipts is COMPLEMENTED by obtaining deposit slips validated by bank.

BATCH PROCESSING ⇒ MEMO POSTING ⇒ OLTP

3. ITGC

OBJECTIVE: (1) To ensure appropriate development & implementation of applications

(2) INTEGRITY of data files & computes opexations

① LOGICAL ACCESS

② SDLC

③ Program Change mgmt.

④ Physical Security over data center

⑤ System & data backup & Recovery

4. APPLICATION CONTROLS

OBJECTIVE :

INPUT data is accurate, complete, authorized & correct
↓
PROCESSING is done in acceptable time period
↓
STORE
↓
OUTPUT
↓
AUDIT TRAIL

⇒ When designing data input controls, primary consideration is given to AUTHORIZATION, VALIDATION & ERROR NOTIFICATION

a) BATCH INPUT CONTROLS

1. Financial Totals
2. Record Count
3. Hash Totals

(b) ONLINE INPUT CONTROLS

1. PREFORMATTING
2. FIELD/FORMAT
3. VALIDITY
4. LIMIT
5. CHECK DIGIT
6. SEQUENCE Check
7. ZERO BALANCE Check

(c) PROCESSING CONTROLS/ CONCURRENCY CONTROLS

(d) OUTPUT CONTROLS

(e) INTEGRITY

(f) MANAGEMENT TRAIL

5. Entity level, Process level & Transactional level

1) ENTITY LEVEL GOVERNANCE CONTROLS
   e.g. IT policies, code of conduct, oversight, Setting Risk Apetite

2) ENTITY LEVEL MANAGEMENT OVERSIGHT
   e.g. ITGC
   Period-end controls

3) PROCESS LEVEL
   e.g. Physical inventory count,
   Review of revenue center report,
   Performance assessment.

4) TRANSACTIONAL LEVEL
   e.g. SOD,
   Application controls
   Exception Reports.

6. TIME BASED CLASSIFICATION

1) FEEDBACK CONTROLS
   e.g. Inspection of goods followed by variance analysis,

2) CONCURRENT CONTROLS
   e.g. Close Supervision of production-line workers

3) FEEDFORWARD CONTROLS → long-term perspective
   e.g. Policies & procedures

7. Financial Vs. Operating Controls

Financial Controls should be based on relevant accounting principles

Objective: ① Proper Authorization
② Record keeping
③ Safeguarding of assets
④ Compliance

Operating Controls apply to production & support activities
↳ Lack established criteria or standards, etc, should be based on mgmt. principles & methods.
↳ Should be designed with mgmt. functions of PODC.

8. People Based vs. System Based

Control Frameworks

① 1973-74: WATERGATE investigations

② 1977: FCPA

③ 1985: NCFFR or, Treadway Commission
↳ Funded by 5 professional actg. org.
↳ COSO ⇒ Group of 5 orgs.

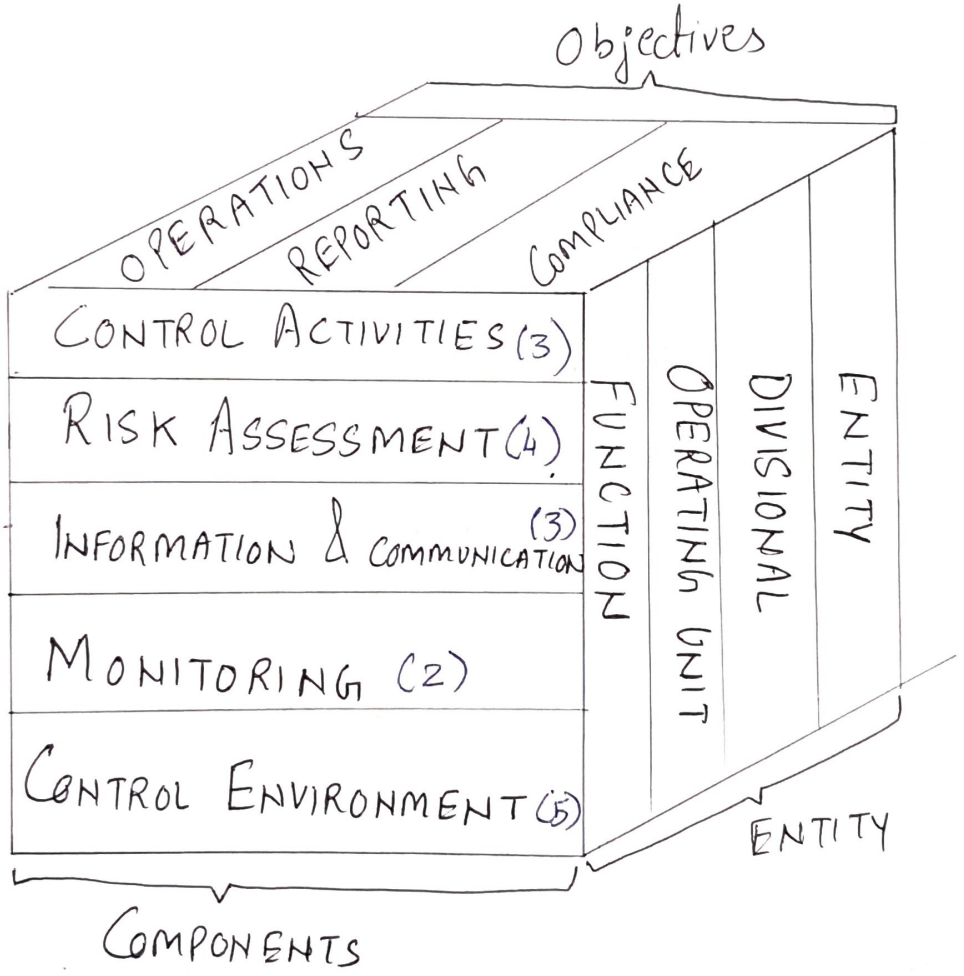
④ COSO 1992, 1994 & 2013

⑤ COBIT

⑥ VAL IT ⑦ eSAC

COSO FRAMEWORK

⇒ IC is a process, effected by an entity's BOD, mgmt. & other personnel to provide reasonable assurance regarding the achievement of objectives relating to ORC



(1) CONTROL ENVIRONMENT

1. Commitment to integrity & ethical values
2. Board exercises OVERSIGHT of IC
3. Structures, reporting lines, & appropriate authority & responsibility
4. Attract, develop & retain talent
5. Hold individuals ACCOUNTABLE

② Risk Assessment

1. Specify Objectives
   (1) Operations (2) External financial reporting
   (3) Internal Reporting (4) External non-financial - " — (5) Compliance
2. Identify Risks & Analyze Risks
3. Assessing Fraud Risks
4. Identify & Assess Changes

③ Control Activities

1. Risk Mitigation 2. Technology 3. Policies & Procedures

④ Information & Communication

1. Relevant, & valid Information
2. Internal Communication 3. External Communication

⑤ Monitoring

1. Ongoing or Separate evaluations
2. Evaluates & communicates deficiencies

Stages in an Effective Monitoring Program

1. Control baseline
2. Change Identification
3. Change Management
4. Control revalidation

COCO MODEL

① Purpose ② Commitment ③ Capability ④ Monitoring & Learning

COBIT 5

⇒ Best known control & governance framework for IT

COBIT-5 GOALS CASCADE

STAKEHOLDER DRIVERS

↓

STAKEHOLDER NEEDS

↓

VALUE CREATION

↳ Realization of benefits
↳ Optimization of Risks
↳ Optimal use of resources

↓

ENTERPRISE GOALS

↓

IT - Related GOALS

↓

ENABLERS

- Policies, frameworks
- Processes — People
- Org. Structures — Infrastructure, Applications
- Culture, Ethics
- Information

① Meeting Stakeholder needs

② Covering Enterprise end-end

③ Single, Integrated framework

④ ENABLING HOLISTIC Approach

⑤ Separating Governance from Mgmt.

COBIT 2019

I GOVERNANCE SYSTEM PRINCIPLES

① STAKEHOLDER VALUE
② HOLISTIC APPROACH
③ DYNAMIC
④ Governance DISTINCT from Mgmt.
⑤ ENTERPRISE NEEDS
⑥ END to END ENTERPRISE

II GOVERNANCE FRAMEWORK PRINCIPLES

① Based on CONCEPTUAL MODEL
② OPEN & FLEXIBLE
③ Aligned with MAJOR STANDARDS

COBIT PERFORMANCE MANAGEMENT (CPM)

① CAPABILITY LEVELS ② MATURITY LEVELS

VAL IT (Complements COBIT)

Objective : VALUE CREATION

① VALUE GOVERNANCE ② INVESTMENT Mgmt. ③ PORTFOLIO Mgmt.

↓

Maximizes quality of BUSINESS CASES

BUSINESS CASES must include answers for

1. Doing right things?
2. Doing right way?
3. Org. getting them done well?
4. Org. getting benefits?

eSAC Model (Influenced by COSO)

Objectives: ① Operating effectiveness & efficiency
② Reporting
③ Compliance
④ SAFEGUARDING of ASSETS

eSAC's IT BUSINESS ASSURANCE OBJECTIVES

↳ Availability
Capability
Functionability
Protectability
Accountability

GUIDES TO ASSESSMENT OF IT RISKS (GAIT)

↳ Consistent with COSO

FOUR PRINCIPLES

1. Identification of RISKS should be a combination of TOP-DOWN & RISK BASED approach
2. ITGC risks identified affect CRITICAL IT functionality
3. ITGC risks identified EXIST
4. Risks of ITGC processes are MITIGATED by achieving IT control's objectives & not individual controls.

SOFT CONTROLS

One approach to auditing Soft controls is CONTROL SELF ASSESSMENT

$$\text{Vulnerability} = \underset{\text{of occurence}}{\text{Probability}} \times \underset{\text{of occurence}}{\text{Significance}}$$

UNIT - 7 : FRAUD RISKS & CONTROLS

FRAUD: Any illegal act characterised by DECEIT, CONCEALMENT, or violation of TRUST.

① To obtain money, property or services.
② To avoid payment or loss of services
③ To secure personal or business advantage

FRAUD RISK: Possibility that fraud will occur & potential effects to org. when it occurs.

CHARACTERISTICS OF FRAUD

1. PRESSURES or, INCENTIVES
2. OPPORTUNITY
   ↳ Low-level employee fraud
   ↳ Insufficient SOD
   ⇒ Org. can influence MOST
3. RATIONALIZATION
   ↳ Feeling UNDERPAID is rationalization for a LOW LEVEL Emp. fraud

TYPES OF FRAUD

1. Asset Misappropriation [Concealed by adjusting RECORDS]
2. SKIMMING [Before Recording]
3. Payment fraud
4. Payroll fraud
5. Expense Reimbursement fraud
6. Financial Statement Misrepresentation

7. Information Misrepresentation

8. Corruption → Involves 2 ← 9. Bribery

Purchasing

10. Wrongful Use 11. Conflict of Interest

12. Diversion 13. Related party fraud 14. Tax Evasion

Low-Level Fraud

↳ Benefits individuals

↳ e.g. Lapping A/R

Executive Level Fraud

↳ Benefits Org.

↳ e.g. FS misrepresentation

Symptoms Of Fraud

① Document ② Lifestyle ③ Behaviour

Indicators of Fraud

1. Lack of employee rotation
2. Inappropriate combination of duties
3. Unclear lines of reporting
4. Unrealistic Sales & production goals
5. Employee refuses to go on vacation
6. Established controls not operating
7. High profits, when competitors are suffering
8. High turnover in Supervisory position
9. Sole-Source procurement
10. ↑SALES >> ↑COGS
11. CONTRACT ≠ BIDS

TYPES OF FRAUDULENT PROCESSES

(1) LAPPING OF RECEIVABLES

- ↳ Access to customer payments & A/R records
- ↳ Steals customer's payment.
- ↳ Shortage in one customer's A/c is covered from another customer's payments

Process continues until:

1. Customer complaints 2. Perpetrator is on leave / absent
3. Perpetrator COVERS the amount stolen

(2) CHECK KITING

- ↳ only for MANUAL CHECKS
- ↳ Delay b/w (a) depositing check in one bank
  (b) clearing check through bank it was drawn
- ↳ Check is KITED when (a) kiter writes check with insufficient funds in his bank
  (b) deposits check in another bank

ROLE OF INTERNAL AUDITORS

- ↳ Evaluate INDICATORS of FRAUD
- ↳ Decide if further action reqd. OR, RECOMMEND INVESTIGATION

FRAUD CONTROLS

FRAUD MANAGEMENT PROGRAM

1. Company's Ethics Policy
2. FRAUD RISK AWARENESS
3. FRAUD RISK ASSESSMENT
4. Ongoing Reviews
5. Prevention & Detection
6. INVESTIGATION

⇒ COSO IC FRAMEWORK can be applied to fraud context to promote environment to effectively manage fraud.

1. Control Environment : Code of conduct, Ethics Policy Fraud Policy
2. FRAUD RISK ASSESSMENT :
3. Control Activities : ↳ Policies & procedures
   ↳ SOD
4. Information & Communication : Fraud Awareness Trainings
5. MONITORING : Independent evaluations

⇒ Preventing Fraud : - Instill strong ethical culture
- Tone @ the top

⇒ Detecting Fraud : → HOTLINE
- Employee feedback

FRAUD INVESTIGATION

FORENSIC AUDITING : Uses accounting & auditing knowledge & skills having CIVIL & LEGAL implications.

⇒ FRAUD POLICY addresses :

1. Rights of individuals
2. Qualification of investigators
3. Relevant laws
4. Discipling employees & includes LEGAL measures

⇒ Authority & responsibility of investigator & legal counsel Should be CLEAR

⇒ Internal communications about ongoing investigation Should be MINIMIZED

⇒ Mgmt. decides whether to NOTIFY others/outside authorities

⇒ RESPONSIBILITY of IA for investigations Should be defined in CHARTER & FRAUD POLICY

INTERROGATION of EMPLOYEES

1. PURPOSE :- Seeking Confirmation.
   - Facts are already gathered
2. DON'T ACCUSE employee
3. Use evidence to obtain confession
4. Correctly document interrogation
5. 2 ppl should be present. 1 witness & 1 for notes

⇒ Employee should not be allowed to return to his/her normal work area

FRAUD REPORTING

⇒ Formal communication to include :

- Time frame — Conclusion — Corrective Action
- Observation — Resolution

⇒ DRAFT to be submitted for LEGAL COUNSEL's review

⇒ Significant fraud to be reported to BOARD & Senior Mgmt.

⇒ If FS for 1 or more years affected, inform BOARD & SM

UNIT-1: FOUNDATIONS OF INTERNAL AUDITING

DEFINITION: IA is an INDEPENDENT, OBJECTIVE ASSURANCE & CONSULTING activity designed to ADD VALUE & IMPROVE the org.'s operations. It helps an org. to achieve its objectives by bringing a SYSTEMATIC, DISCIPLINED approach to EVALUATE & IMPROVE the effectiveness of GRC processes.

CORE PRINCIPLES

1. Demonstrates INTEGRITY
2. Competence & Due Professional Care
3. Objective & free from UNDUE INFUENCE
4. Aligns with strategies, objectives & risks
5. Appropriately positioned & adequately resourced
6. Quality & Continuous improvement.
7. COMMUNICATES Effectively
8. RISK BASED Assurance
9. Insightful, proactive & future-focussed
10. Promotes organisational improvement

PURPOSE, AUTHORITY & RESPONSIBILITY of IA

Purpose: Same as Definition Responsibility: Same as definition

	ASSURANCE SERVICES	CONSULTING SERVICES
NATURE & SCOPE:	IA determines	– Agreement with Engagement Client
PARTIES INVOLVED:	① Process Owner ② IA ③ User	– ① Engagement Client ② IA
e.g.	Due Diligence engagements Financial — " — Performance — " — Compliance — " —	– e.g. ADVICE TRAININGS COUNSEL FACILITATION

AUTHORITY of IA

- Defined in CHARTER
- Charter approved by BOARD

CODES OF ETHICAL CONDUCT for Professionals

PURPOSE: To promote an ethical culture

1. Communicating acceptable value to others
2. Establish OBJECTIVE Stds. for MEASURING performance
3. Communicate ORG.'s value to OUTSIDERS

ASPECTS OF CODE

- MERE EXISTENCE of code does not ensure anything
  1. Measure of COHESION & PROFESSIONALISM ∝ Voluntary Compliance
  2. Code worded to reduce likelihood of members being Sued for Substandard work DOES NOT earn public confidence
- Establishes MIN. Std. of COMPETENCE, but IMPOSSIBLE to require EQUALITY of Competence
- PROVIDE for DISCIPLINARY ACTION

Components of Code of Ethics

(1) Integrity (2) Objectivity

(3) Confidentiality (4) Competence

Rules Of Conduct — Integrity

1. Shall perform work with HONESTY, DILIGENCE & Responsibility
2. Observe the LAW & make disclosures expected by law & profession
3. Shall NOT KNOWINGLY be part of any ILLEGAL activity, OR engage in any ACT DISCREDITABLE to the profession
4. Respect & contribute to legitimate & ethical objectives

Behaviors that are DISCREDITABLE, but not illegal

1. Noncompliance with Stds. & other IPPF
   - Performing IA services for which one is not competent
   - —— " —— with undeclared impairments to objectivity & independence
   - Disclosing confidential info without AUTHORIZATION
   - Stating IA is operating in CONFORMANCE with stds. when assertion is not supported by QAIP

Conformance to Integrity

1. QAIP 2. Acknowledgement forms 3. Diligent Supervision & CSA

Rules Of Conduct - Objectivity

1. Don't participate in any activity that IMPAIRS or is PRESUMED to IMPAIR (objectivity) unbiased assessment.
2. Don't ACCEPT anything that impairs or presumed to impair
3. Disclose facts, which IF NOT disclosed, may distort reporting

- IA can't assure ANONYMITY.

Conflict Of Interest Policy

- Prohibits transfer of benefits b/w employee & those who org. deals with.

Conformance With Objectivity

- CAE provides evidence of relevant P&P, requirement of IA to attend training related to objectivity
- Documentation of research into potential COI
- Engagement w/Ps

Rules Of Conduct – Confidentiality

1. Be PRUDENT in use & protection of information
2. Don't use information for personal gain

⇒ Org. generally uses INFORMATION SECURITY Policies to protect data

⇒ To better understand IMPACT of legal & regulatory requirement CAE should CONSULT with LEGAL COUNSEL

Conformance With Confidentiality

- CAE provides evidence of trainings
- Release of engagement results
- Document DISTRIBUTION RESTRICTIONS
- No reports on IA regarding violation ⇒ CONFORMANCE

Rules Of Conduct – Competency

1. Necessary knowledge, skills & competencies
2. Accordance with IPPF Stds.
3. CPE

Conformance with Competency

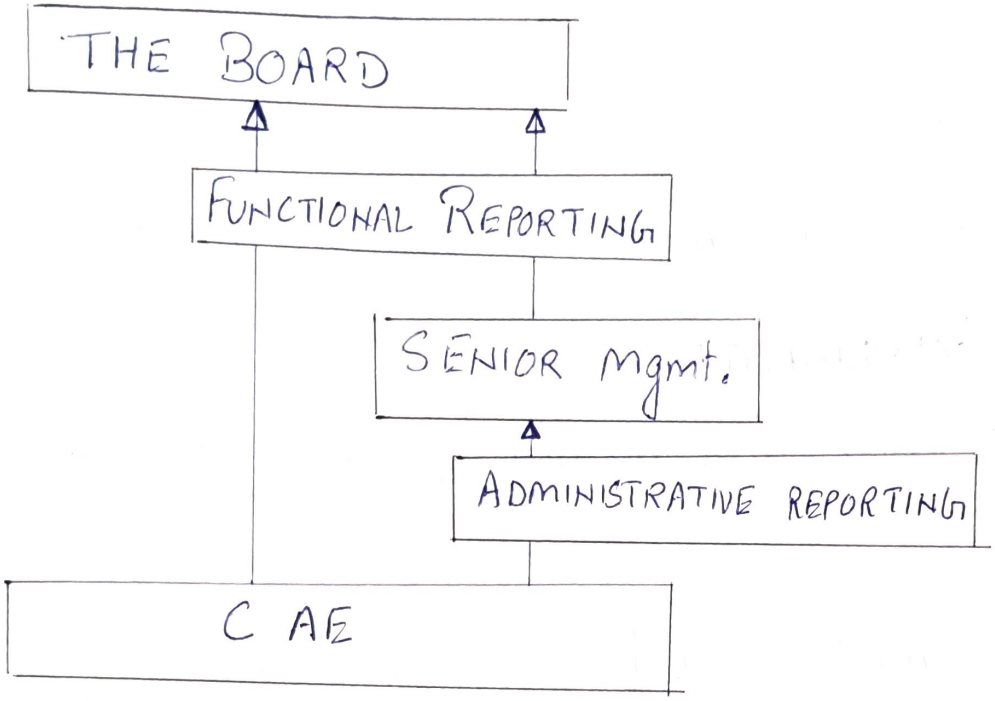
- Properly resourced & supervised engagements
- QAIP
- Qualification of IAs
- Self Assessment documents
- CPE
- Evidence of experiences gained

Internal Audit Charter

- Defines Purpose, Authority & Responsibility of IA
- Scope Limitation: Auditee refuses access to records, personnel & physical properties
- MOM of board meeting serves as approval of charter
- CAE must periodically review charter & seek approval from Board

INDEPENDENCE, OBJECTIVITY, PROFICIENCY, CARE & QUALITY

STUDY UNIT-2



↳ CAE must CONFIRM to BOARD, the organisational Independence of IA, at least ANNUALLY.

→ MOM ⇒ CAE communicated to BOD

⇒ INDEPENDENCE is an attribute of IA activity. At org. level.

⇒ OBJECTIVITY is an attribute of individual IA.

MAINTAIN INDIVIDUAL OBJECTIVITY

↳ Responsibility to maintain objectivity rests with CAE & individual IAs

ASSESS INDIVIDUAL OBJECTIVITY

↳ CAE to establish P&P to assess objectivity of individual IA

→ e.g. Periodic review of COI P&P

IMPAIRMENT TO INDEPENDENCE & OBJECTIVITY

⇒ If I or O is impaired in fact OR appearance, then details of impairment MUST be DISCLOSED to appropriate parties.

Nature of disclosure depends on type of impairment.

INDEPENDENCE IMPAIRMENTS

1. CAE conducts audit in a function, for which he/she is functionally responsible
2. CAE conducts audit in a function, which his Supervisor is responsible for
3. No DIRECT ACCESS to BOD
4. BUDGET is Reduced

OBJECTIVITY IMPAIRMENTS

- Providing Assurance Services to an activity which he was previously working with < 1 year.
- Assume/Presume without evidence that area being audited is effectively managing risks.
- Audit an area in which close friend/relative works
- Modify plan upon undue influence of others, without justification

COMMUNICATION APPROACH

1. CAE believes impairment is NOT REAL, but recognises there could be PERCEPTION of impairment, then CAE may discuss & document these concerns. Disclose this in FINAL ENGAGEMENT Communication / report.
2. CAE believes its REAL => Disclose to SM & BOD.
3. Impairment found after Completion of AUDIT, & impacts RELIABILITY (or, Perceived Reliability) of results, then disclose to SM & BOD.

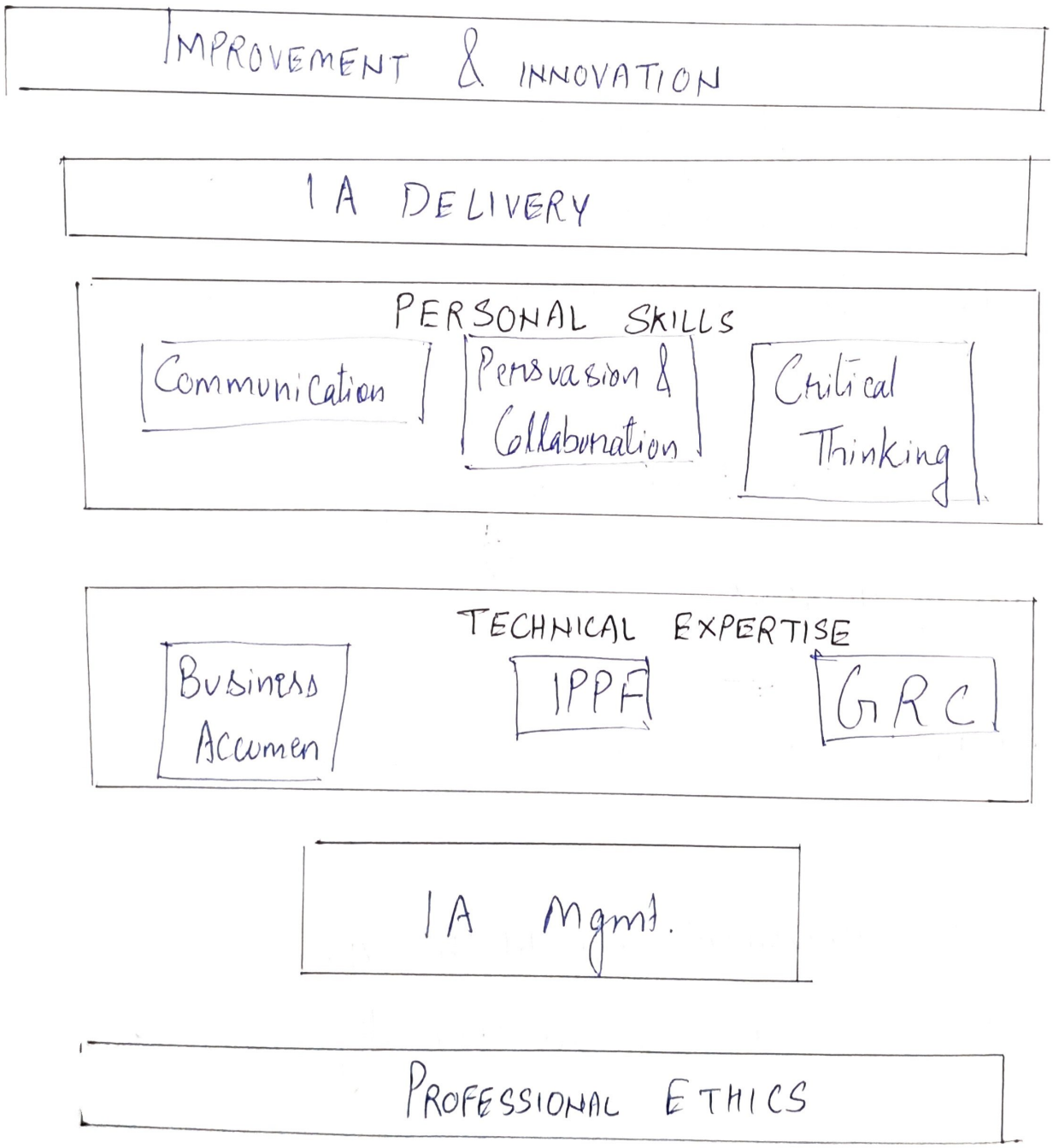
Recommending Stds. of Control
Performing reviews
→ NO IMPAIRMENT

DRAFTING Procedures → PRESUMED to IMPAIR ○

⇒ Assurance engagements for which CAE is functionally responsible, MUST be OVERSEEN by party outside IA.

PROFICIENCY

1. IAs must possess knowledge, skill & other competencies to perform their individual responsibilities.
2. IA must COLLECTIVELY possess K, S & Competency.



IIA COMPETENCY FRAMEWORK

Quality Assurance & Improvement Program

* Five Components

1. Internal Assessment.
2. External " .
3. Communication of QAIP Results.
4. Conformance Statement
5. Disclosure of non-conformance

* Requirement of QAIP: Must include Internal & External assessment.

Internal Assessment

1. Ongoing Monitoring
   - Engagement planning, Supervision,
   - W/P procedure & Signoffs,
   - Report reviews
2. Periodic Self Assessment
   ↳ Validates Ongoing Monitoring

External Assessment

- Uses an Independent Assessor
- At least once in 5 years
- Self-assessment allowed in lieu of full external assessment IF, it is validated by external asso

Deming Cycle

Plan: Formal documentation of stds.

Do: Develop activities to define quality

Check: Various forms of assessment & Review to measure quality

Act: Undertake improvement initiatives