CIA Part 1
Handouts

By

Arif Zaman
FCCA, CIA, CISA, CPA, CFE, CCSA, CRMA, CGA

Subscribe to YouTube Channel "**Stuployer**" for CIA Lectures
Link:

https://www.youtube.com/c/Stuployer

You can Connect with me via LinkedIn

https://www.linkedin.com/in/arifz/

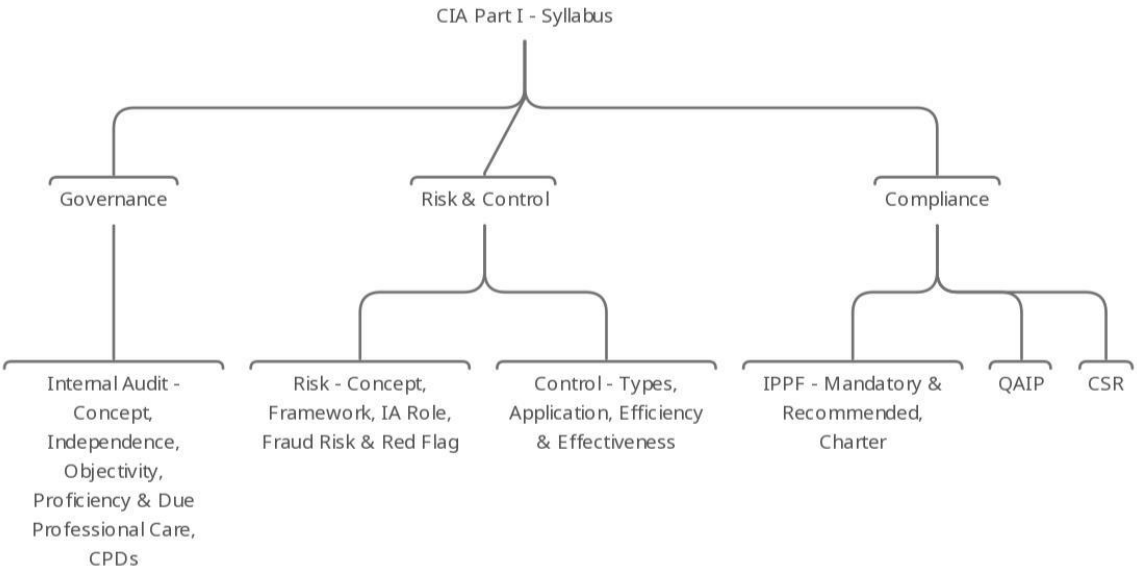
Contents

CIA Exam Overview

- 170K + Members
- Three Parts
- Exam duration 150 mins (2.5 hours)
- Exam questions 125 (1 hours – 50 MCQs, 30 Mins – 25 MCQs) – 1.2 Mins per MCQs
- The test assesses your knowledge, skills and abilities and align with IPPF (Standards; 1000, 1100, 1200 and 1300)
- Passing Score 600+ (250 – 750) : 100+ MCQ's need to pass
- Total 30 Topics (14 Basic & 16 Proficient)

Please Continue Next Page…

Part I – Syllabus



#	Area	%	MCQs
1	Foundation of IA	15%	19
2	Independence & Objectivity	15%	19
3	Proficiency & Due Professional Care	18%	23
4	QAIP	7%	9
5	Governance, Risk & Control	35%	44
6	Fraud Risk	10%	13
	Total	**100%**	**127**

I – Foundation of Internal Audit (15% -**19 MCQs**) – Completed – 3 January 2022

- **Section A – Proficient**
  - IA Mission
  - IA Definition
  - IA Core Principles
  - IA Purpose, Authority and Responsibility
- **Section B - Basic**
  - IA Charter (Components, Board Approval & Communication) etc.
- **Section C - Proficient**
  - Assurance Services
  - Consulting Services
- **Section D - Proficient**
  - IIA Code of Ethics

II – Independence & Objectivity (15% -**19 MCQs**) – Completed – 5 January 2022

- **Section A – Basic**
  - Organizational Independence (Importance and functional reporting etc.)
- **Section B – Basic**
  - **I**mpairment of Internal Audit Independence (Identify)
- **Section C - Proficient**
  - Individual Auditor's Impairment (Identify)
- **Section D – Proficient**
  - Policies to Promote Objectivity (Analyze)

III – Proficiency & Due Professional Care (18% - **23 MCQs**) - Completed – 5 January 2022

- **Section A – Basic**
  - I-A Knowledge, Skills & Competence (In-house or Acquire)
- **Section B – Proficient**
  - Technical Skills & Soft Skills
- **Section C - Proficient**
  - Due Professional Care
- **Section D – Proficient**
  - CPD'sw

IV- Quality Assurance & Improvement Program (7% - **9 MCQs**) – Completed – 7 January 2022

- **Section A – Basic**
  - QA (Internal & External Assessment)
- **Section B – Basic**
  - QA Results (Board / Governing Body)
- **Section C - Basic**
  - IPPF (Conformance vs. Nonconformance)

V – Governance, Risk Management & Control (35% - **44 MCQs**) – 27 January

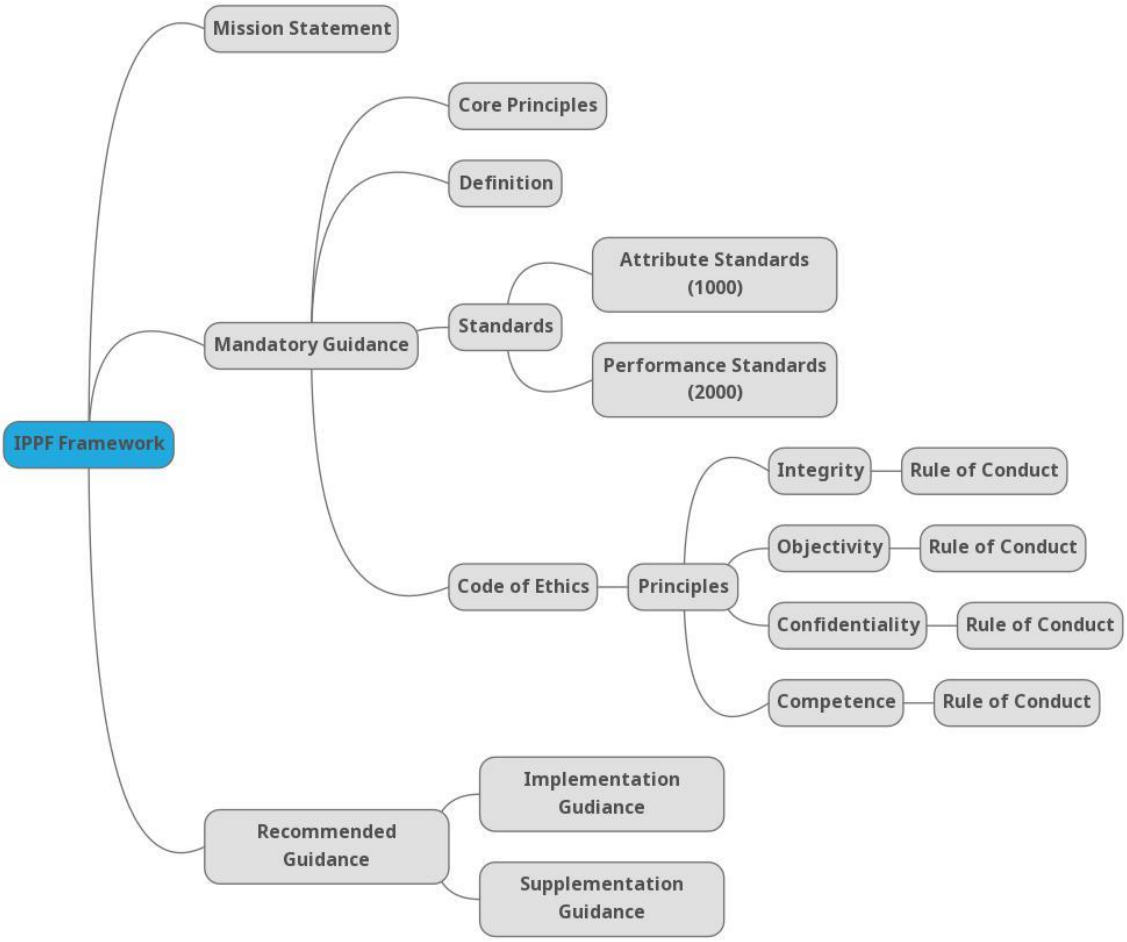
- **Section A – Basic**
  - Org Governance

- **Section B – Basic**
  - Org Culture Impact on Control Environment (Ind. Engagement)
- **Section C – Basic**
  - Ethics & Compliance Incident
- **Section D – Basic**
  - CSR
- **Section E – Proficient**
  - Risk Management Concept (Fundamental)
- **Section F – Basic**
  - RM Framework (COSO, ISO 31000 etc.)
- **Section G – Proficient**
  - Effectiveness of RM (Examine)
- **Section H – Basic**
  - Role of IA in RM
- **Section I – Proficient**
  - Types of IC
- **Section J – Proficient**
  - Application of IC Framework (COSO etc.)
- **Section K – Proficient**
  - Effectiveness and Efficiency of ICs

- **Section A – Proficient**
  - Types of Fraud Risk
- **Section B – Proficient**
  - Fraud Red Flags
- **Section C - Proficient**
  - Fraud Awareness & Control
- **Section D – Basic**
  - Forensic Auditing (IA Role)

Notes

1. Foundation of Internal Audit (15% -19 MCQs)



IPPF Framework

- The framework encompasses **Mission, Mandatory** and **Recommended** guidelines.
- Mandatory guidelines comprises of four elements; **Core Principles, Definition, Standards, Code of Ethics.**
- Recommended guidelines comprises of two elements; **Implementation** and **Supplemental Guidance.**

Mission Statement

The mission for internal auditing is to "Enhance and protect organizational value by providing risk-based and objective assurance, advice and insight."

1. Core Principles (Mandatory Guidelines)

1. Demonstrates integrity.
2. Demonstrates competence and due professional care.
3. Is objective and free from undue influence (independent).
4. Aligns with the strategies, objectives, and risks of the organization.
5. Is appropriately positioned and adequately resourced.
6. Demonstrates quality and continuous improvement.
7. Communicates effectively.
8. Provides risk-based assurance.
9. Is insightful, proactive, and future-focused.
10. Promotes organizational improvement.

2. Definition (Mandatory Guidelines)

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

3. Standards (Mandatory Guidelines)

- **Attribute Standards (1000)** – Purpose, Authority, Responsibility, Independence, Objectivity, Proficiency and Due Professional Care, Quality Assurance and Improvement Program.
- **Performance Standards (2000)** – Planning, Performing, Communicating and Monitoring audit activities.

4. Code of Ethics (Mandatory Guidelines)

The code of conduct include two essential components; **Principles** and **Rules of Conduct**.

Code of Ethics – Principals

1. **Integrity -** The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
2. **Objectivity -** Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.
3. **Confidentiality -** Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
4. **Competency -** Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

Code of Ethics - Rules of Conduct

(Interpreting behavior norms expected of internal auditors)

1. **Integrity**
   1.1. Shall perform their work with **honesty**, **diligence**, and **responsibility**.
   1.2. Shall observe the law and make **disclosures** expected by the law and the profession.
   1.3. Shall not knowingly be a **party to any illegal activity**, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
   1.4. Shall respect and contribute to the **legitimate and ethical objectives** of the organization.

2. **Objectivity**
   2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their **unbiased assessment**. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
   2.2. Shall not accept anything that may impair or be presumed to impair their **professional judgment**.
   2.3. Shall disclose all material facts known to them that, if not disclosed, may **distort the reporting** of activities under review.

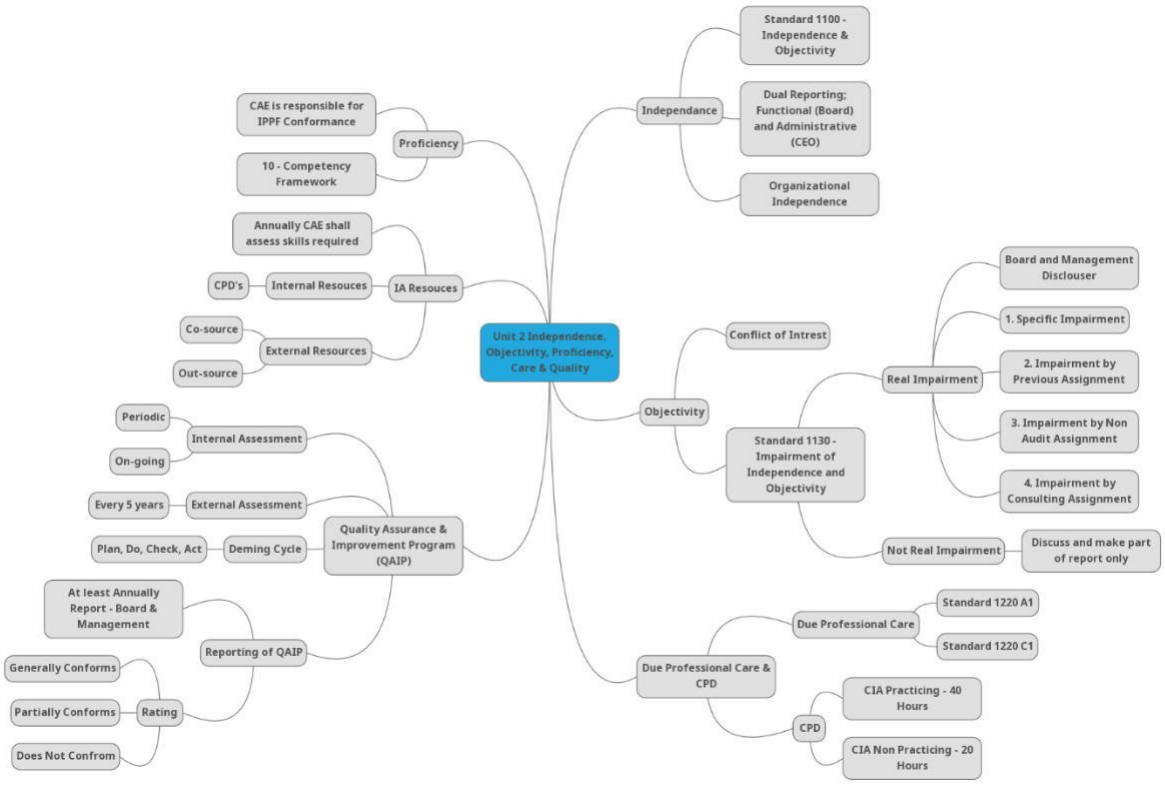
3. **Confidentiality**
   3.1. Shall be **prudent** in the use and protection of information acquired in the course of their duties.
   3.2. Shall not use information for any **personal gain** or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. **Competency**
   4.1. Shall engage only in those services for which they have the **necessary knowledge, skills, and experience**.
   4.2. Shall perform internal audit services in accordance with the **IPPF**.
   4.3. Shall continually **improve** their proficiency and the effectiveness and quality of their services.

5. Recommended Guidance

1. Implementation Guidance.
2. Supplementation Guidance

2. Independence, Objectivity, Proficiency, Care and Quality (40% - 50 MCQs)



Independence of Internal Audit

(Attribute Standard 1100 Independence & Objectivity)

- Freedom from conditions that threatens the ability of the internal audit activity to carry out in an unbiased manner. Disclose any interference to the Board (Imp. Standard 1110. A1).
- CAE direct and unrestricted access to Sr. Management and Board (Standard 1111).
- CAE dual reporting; functional to Audit Committee and administrative to Sr. Management.
- CAE MUST confirm annually Org. Independence of internal audit activity to the Board.

Functional Reporting

(Attribute Standard 1110 Org Independence)

Approving:

- Internal Audit Charter (IA Charter)
- Risk Based Internal Audit Plan
- Budget & Resource Plan
- Performance Appraisal
- Appointment and Removal of CAE
- Remuneration
- Scope Limitation
- Inquiries about Management

Administrative Reporting

- Report of CEO

Conformance

Standard 1110

- AC and IA Charter – Describe AC oversight duties
- CAE JD and Performance Evaluation – Note reporting relationship and supervisory oversight
- IA Policies – Addresses independence, board reporting reflecting in org chart

Standard 1111

- Board meetings agendas and minutes demonstrate CAE direct interaction with Board.

Objectivity

Standard 1100

- Independence – IA activity attribute
- Objectivity – Auditor attribute
- Objectivity is impartial and unbiased mindset, threats to objectivity must be management at internal auditor, engagement, functional and organizational level.

Standard 1120

- Auditor must have an impartial, unbiased attitude and avoid conflict of interest.
- Conflict of Interest (CoI) – not in the best interest of the org and prejudice in performing duties.
- CoI exists even if no unethical or improper act results.
- IA Policies shall demonstrate expectation and requirement for unbiased mindset.

Impairment of Objectivity

- Personal CoI
- Scope limitation
- Restriction to access records or personnel or property
- Resource limitation (such as funding)
- Self-review
- Self-interest
- Familiarity
- Bias
- Undue Influence

Independence Issue led to Objectivity Impairment

- CAE broader responsibility
- Auditor Supervisor broader responsibility
- No direct communication with Board
- Budget is reduced

Reporting

- Impairment is not real – Discuses the concern with management and document engagement planning meeting with explanation and make such disclosures in report.
- Impairment is real – Discuss with Board and Sr. Management and seek support to resolve it.

Scope Limitation

- Restriction place on internal audit activity

Reporting

- Report to the Board and its likely impact on the overall engagement, preferably in writing.

- If potential impairment, disclosure should be made before the acceptance of the engagement.

Auditor Proficiency – Standard 1200

Proficiency is a collective term that refers to the knowledge, skills and other competencies required of internal auditor to effectively carry out their professional responsibilities such as fraud risk and IT risks.

IA become proficient by experience, CPD and certifications.

- Engagement shall be performed with due professional care and proficiency.
- Every internal Auditor is responsible to ensure this.
- Internal auditors are considered proficient if collectively possess competencies needed
- CAE decline if lack knowledge, skills and other competencies to perform consulting engagement.

Competency Framework

- Competency – Ability to perform job properly based on knowledge, skills and behavior.
- Competency Framework is the tool that defines IPPF requirements are met.

10 Independent Competencies

1. Professional Ethics
2. IA management
3. IPPF
4. Governance, Risk & Controls
5. Business Acumen
6. Communication
7. Persuasion and Collaboration
8. Critical Thinking
9. IA delivery
10. Improvement & Innovation

Internal Audit Resources

Internal Resources

- CAE shall review periodical (at least annually skill assessment)
- Carry out staff performance review
- Ensure CPDs
- Recorded the IA background Information such as skills, completed projects, training and developments need.
- If CAE loose in-house expertise can outsource or co-source audit activity from external sources.

External Resources

- IA can be outsourced or sourced all audit activities.

- The oversight rest with the organization.
- The audit activity shall be performance as per IPPF.
- Engagement client is unacceptable.
- External source can recruited from audit firm, consultancy or university.

Due Professional Care and CPD

- Reasonably prudent and competent internal auditor
- Reasonable care not absolute care
- Conformance with the IIA Code of Ethics and IPPF
- IA SOP are systematically provide disciplined approach towards audit cycle.

In assurance engagement, the auditor need to exercise due professional care by: extend of work needed, risk maturity and governance of the org, cost benefit analysis and probability of error, fraud or noncompliance.

IA shall use technology and data analytics tool.

In consultancy engagement, the auditor need to exercise due professional care by; need and expectation by the client, complexity of the work, cost benefit analysis.

CPDs

- Auditor can use self-assessment tools such as competency framework
- On job training, coaching, mentoring, external training, conference, seminar, research, study plan etc.
- A practicing CIA must obtain 40 hours and non-practicing 20 hours of CPDs annually.

Quality Assurance & Improvement Program (QAIP)

- CAE MUST develop QAIP and is responsible to covers all aspect of audit activity.
- CAE should encourage Board oversight in QAIP
- QAIP shall be in both Assurance and Consulting engagements.
- Carry out internal periodic, ongoing and external assessment.
- QAIP consist of five components; internal and external assessment, communication of results, conformance and non-conformance disclosures.
- Performance metrics (KPIs); accomplishment of audit plan, cycle time, accepted recommendation, customer satisfaction.
- CAE must have thorough understanding of mandatory element of IPPF.
- CAE as required shall periodically evaluates and update QAIP.
- External – Every 5 years.
- CAE can use Demining Cycle; Plan, Do, Check and Act.
- Plan – Establish standards
- Do – Establish process
- Check – Compare actual results
- Act – Provide feedback

Internal & External Assessment

Internal Assessment

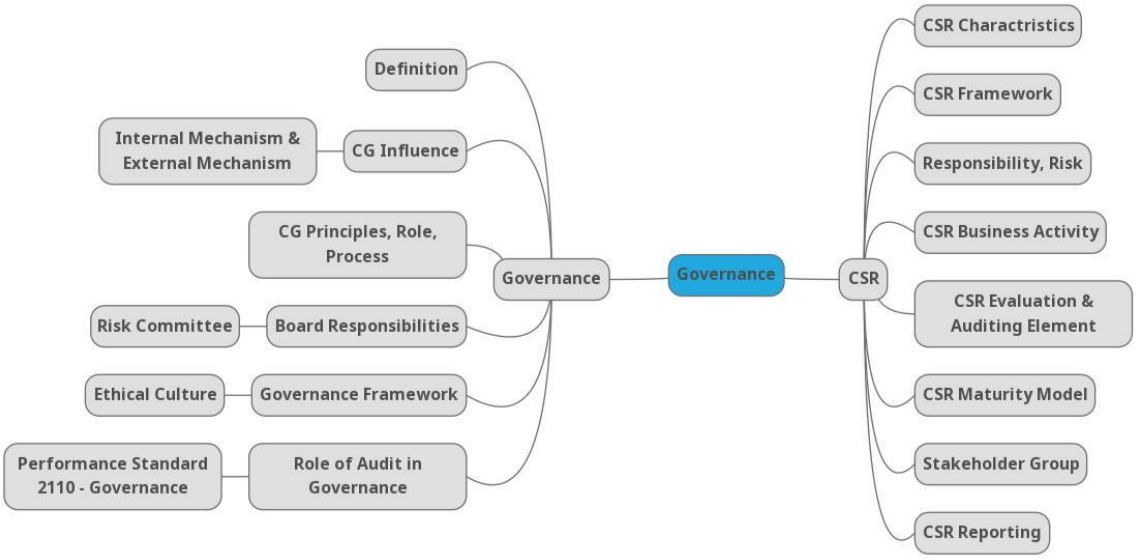
- On-going (engagement level, planning, supervision, working papers, report, reviews, KPIs, feedback)
- Periodic (Sr. Auditor or CIA, Conformance with Standards, Code of Ehtics)
- The CAE shall report the results to Board and Management.

External Assessment

- Once every 5 years
- Qualified Independent Assessor or Team
- CAE discuss with the Board – Form and Frequency of External Assessment and Independence of Assessors)
- External Assessment Two Approaches:
    - Full External Assessment
    - Self-Assessment with Independent External Validation (SAIV)*
- External Assessor shall be competent in (1) IPPF (2) External Assessment Quality Processes
- External assessor shall not have CoI, former employee related party, former company employee.
- **Peer Review** of unrelated organization (but not between two) may satisfy organization independence.
- **One of more Independent Individuals** may provide separate validation.

***** The CAE to complete the self-assessment work performed with the same level of due professional care found in performing other internal audit engagements. The independent external validation team validates the work of the internal assessment team through review of assessment planning documentation, re-performing a sample of assessment work program steps, conducting interviews with key stakeholders, and assessing the conformance conclusions reported by the internal assessment team.

3. Governance (10% - 12 MCQs)



Governance Principles

Definition

- IPPF – The combination of the **Processes** and **Structured** implemented by the **Board** to INFROM, DIRECT, MANAGE, and MONITOR the activities of the org toward the achievements of its objectives.
- OECD – CG involves a set of **Relationships** between a company's management, board, shareholders and other stakeholders. CG also provide **Structure** through which the **Objectives** of the companies are set and the **Means** for attaining and monitoring **Performance** are determined.

CG is influenced by

- Internal Mechanism – Charters, Bylaws, Board, IA
- External Mechanism – Laws, Regulations

Governance Principles

- Interrelated GRC (consider risks and relies on controls)
- Effective Board
- Operating Structure
- Organization Strategy
- Governing Policy, Compensation Policy, Risk Management Policy,
- DOA
- Disclosers and Reporting
- Oversight
- Ethical Culture, Related Party Transaction, Conflict of Interest
- Internal & External Auditor

Governance Process & Roles

- The board is ultimate responsible for oversight.
- Governance has two major components; Strategic Direction & Oversight
- Board could be Supervisory Board, Board of Governors, Committee or Trustees.
- The board shall manage the stakeholder expectation.

Board Responsibilities

- Selection and removal of officers
- Capital structure i.e. debt, equity
- By laws
- Fundamental Change i.e. mergers, acquisition etc.
- Management compensation
- Evaluating risk and coordinating audit activities
- Dividends

Risk Committee

- Identify, Analyze, Manage/ Treated, Report and Follow-up Risk

Governance Framework

- Governance applies to all organizational level
- Governance practice reflects organizational unique culture
- Sr. Management responsible for establishing and maintaining organizational culture
- Organization culture affects overall control environment
- Governance practice may use various forms.

Ethical Culture

- The board oversees the ethical culture
- The management promotes and set examples
- Each person should be an ethics advocate
- Code of Conduct (CoC) and Vision Statement
- Org could have Chief Ethics Officer
- IA may play a active role in support of ethical culture, the role depends on:
    - Less mature system; IA emphasis on compliance
    - Mature system; Optimizing the structure and systems
- IA can evaluate the ethical culture by ensuing:
    - Formal CoC
    - Demonstration of leader attitude and behaviors
    - Org strategies support ethical behavior
    - Confidential reporting
    - Employees' declaration
    - Surveys
    - Employee reference and background checks

Role of IA in Governance

- It's part of IA definition.
- The board and the management are responsible for design and implementation of governance process.

Performance Standard 2110 – Governance

IA assess and make improvement recommendation to improve governance by:

- Governance systems varies by entity (law, size, complexity, life cycle, stakeholders)
- Strategic and operational decisions
- Overseeing risk and control framework and activities
- Promoting ethical values
- Ensuring organization performance management and accountability
- Effective communication of the information
- **IA ultimately responsible to evaluate and improve Governance.**
- CAE may improve governance through consulting services.
- IA should consider consulting legal counsel before audit or before issuing audit report.

Corporate Social Responsibility (CSR)

CSR Characteristics

- Stakeholders expects organization (1) management social and environmental impact (2) engagement stakeholders (3) report results to public.
- CSR refers to (1) social responsibility (2) sustainable development (3) corporate citizenship.
- ISO 26000 definition of CSR.
- IIA Practice Guide definition of CSR.
- Archie B. Carroll four responsibility of social responsibilities; economic, legal, ethical, philanthropic.
- CSR is largely **voluntary** practice.

CSR Framework

- Global Reporting Initiative (CGI) – Emphasize on Reporting – Specific guideline on measuring CSR performance against predefined criteria.
- ISO 26000 – emphasize on Implementing and Managing a CSR initiative.
- ISO 14000 – Certification of Environmental Management Systems; waste management, consumption of resources (energy, material), distribution cost, corporate image.

CSR Responsibilities

- Board – responsible for overseeing
- Management – Setting objectives, assessing and managing risks, measuring performance, monitoring and reporting activities.
- IA – Evaluating controls towards achievement of objectives
- Employees – Success of CSR initiative.

CSR Risks

- Loss of reputation
- Non-compliance
- Law suites
- Operational failure (environmental effects)
- Stock market
- Employment market
- Sales (consumer behavior)

CSR Business Activity

- SOPs
- Strategies, Objectives and Performance Goals
- CSR Principles integrating in Business Decision Making
- Monitoring and Benchmarking
- Engaging Stakeholders
- Auditing

Internal and External Reporting

CSR – Evaluation and Auditing

- Provide advice on design and implementation
- Facilitate management in CSR Controls Self- Assessments
- IA shall ensure its competence while performing CSR audit
- CAE consider CSR Risks, adequacy of controls to achieve objectives

CSR Audit Element

- Governance
- Communality Investment
- Social & Environmental Impact
- Anti-corruption Culture
- Health, Safety and Security
- Transparency
- Human rights and working condition

CSR Maturity Model

- Compares the maturity level with the organization desire to achieve
- Level 1 is initial and level 5 is optimizing.

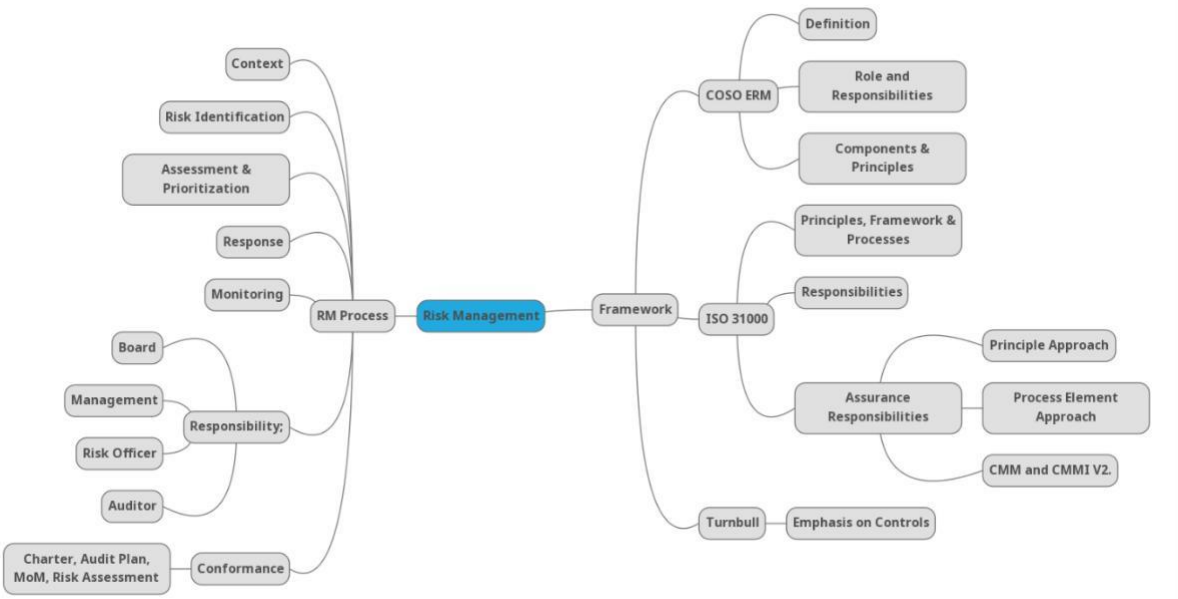
Stakeholders Group

- Customers
- Employees
- Environment
- Communities
- Shareholders
- Suppliers

CSR Reporting

- Cost benefit analysis
- What information to include
- Verification and assurance process
- Reports
- Types of distribution (booklet, online, press release, regulatory fillings)

4. Risk Management (10% - 12 MCQs)



Risk Management Process

Risk

- Possibility of an even occurring that have an impact on organization
- Risk is measured in terms of Impact and Likelihood
- RM – A process to Identify, Assess, Manage & Control potential events to provide reasonable assurance regarding achievement of organizational objectives.
- Standard 2120 – RM – IA Evaluate the effectiveness and Contribute to the improvement of RM process.
- RM could be formal or informal process.

RM Process

1. **Identification of Context** (Laws, regulation, capital projects, business process, tech, market risk, etc.)
2. **Risk Identification** (Ext & Int Risk, Past & Future Event – Event Inventory, Questionnaire, Escalation Trigger, Work Shop, Interviews, Process Flows, Loss Event etc.)
3. **Risk Assessment & Prioritization** (Likelihood & Impact – Qualitative and Quantitative, Risk Modeling)
4. **Risk Response** (Risk Appetite, Control, Control Risk, Residual Risk & Risk Committee)
5. **Risk Monitoring** (Track, Evaluate Risk Response Plan, Monitor Residual Risk, Identify New Risk)

Responsibility for Aspect of Org RM

- RM is the key responsibility of management and Board
- IA review and recommend improvement (Assurance)
- IA Identify, Evaluate, Implement and Manage methods and controls (Consulting)
- Board determine IA role in RM based on Org Culture, Competence, Local Condition & Customs.
- IA role in RM shall be provided for in Charter.

IA Role in RM

- Standard 2120 . A1 – IA assess; org objective are align with mission, risk are identified and assessed, risk response according to risk appetite, communication and reporting.
- Standard 2120 . A2 – evaluate potential occurrence of fraud and how org manages.
- IG 2120 – Risk Management – Obtain understanding of org., RM framework and model use, characteristic of org, risk maturity process, plan audit and reporting of RM issues.

- -Implementing Standard 2120 – CAE speak with Board on RM, assess risk, perform its own risk assessment, carry out gap analysis, identify risk and responding responses, ensure adequacy and timeliness of remedial action, ensure timely communication by reviewing Board minutes, auditor perform its own audit activity risk assessment, and monitor corrective action.
- Conformance – Charter, Audit Plan, MoM, IA Risk Assessment.
- Risk Management in Consulting
    - **Standard 2120 – C1 –** Must address risk is consistent with engagement's objectives
    - **Standard 2120 – C2 –** Incorporate knowledge gain from consulting engagements
    - **Standard 2120 – C3 –** Refrain from assuming any management responsibility.

COSO Framework – ERM Overview

COSO ERM Framework

- Integrating all RM activities for better Decision Making and enhanced Performance.
- Benefit of ERM are; increase opportunities, effectively manage risk, positive outcome, reduce performance volatility, improve recourse deployment and enhance resilience.

ERM – Definition and Concepts

- The culture, capabilities, and practices, integrating with strategy-setting and performance, that organization rely on to manage risk in creating, preserving and realizing value.

ERM – Role & Responsibilities

- Board – Oversight role, for which it forms certain committees e.g. audit, risk, remuneration, nomination, governance etc.
- Management – Day to day responsibility for managing risk and achievement of organizational objectives.
- Risk Officer – Centralized coordinating point to facilitate risk management across the entire enterprise.
- Three Line Model – First *Principle owner of risk, Second *Supporting business enabling functions e.g. Risk Officer, Third *Assurance function.

COSO Framework – ERM Component & Limitations

COSO ERM FRAMEWORK

The Framework itself is a set of principles organized into five interrelated components:

COSO ERM COMPONENTS

Assessing ERM

- When the components, principles, and supporting controls are present and functioning, ERM is reasonably expected to manage risk effectively and to help create, preserve, and realize value.

ERM Limitation

- Faulty human judgment, cost benefit consideration, simple errors or mistakes, collusion, and management override of ERM practices.

ISO 31000 Risk Management Framework

ISO 31000 – Principles, Framework & Processes

Principles

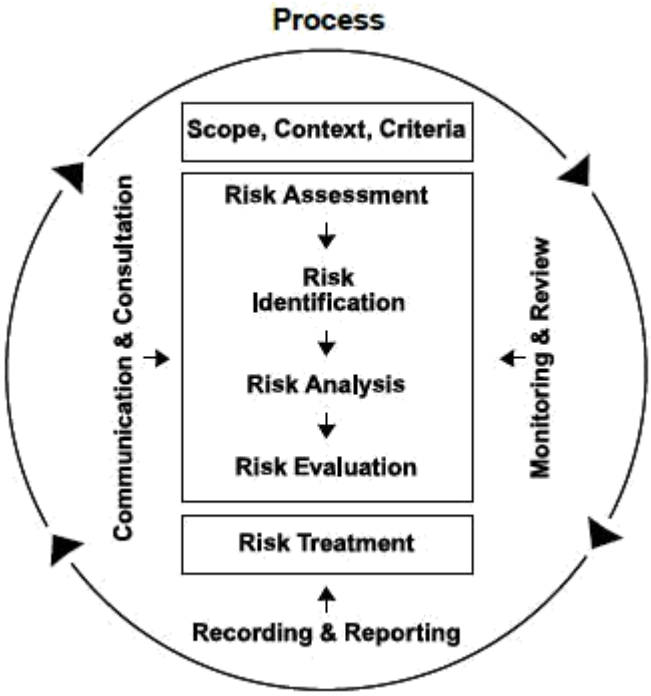
- **Integrated** – all organizational activities
- **Structured and comprehensive**
- **Customized** – customized to organizational objectives
- **Inclusive** – involvement of stakeholders
- **Dynamic** – react to change
- **Best available information** – past, present and future information
- **Human and cultural factors**
- **Continual improvement** – constantly improve risk management

Framework Components

- **Leadership and commitment** – policies, resources, responsibility, accountability and authority (Board and Management)
- **Integration** – all facet of organization
- **Design** - system
- **Implementation** – develop a plan, deploy if require make changes.
- **Evaluation** – measuring performance
- **Improvement** – monitoring and updating framework

Process

- **Communication and Consultation** – awareness and feedback
- **Scope, Context & Criteria**
- **Risk Assessment** – identifying, analysis and evaluation
- **Risk Treatment** – accept, avoid, reduce, share and pursue
- **Monitoring & Review** – improve quality and effectiveness
- **Recording & Reporting** – result should be communicated to stakeholders



ISO 31000 – Responsibilities for Risk

- **Board** – Oversight
- **Management** – Responsible for setting the organization Risk Attitude – approach to assess and eventually pursue, retain, take, or turn away from risks.
- **Auditor** - Assurance

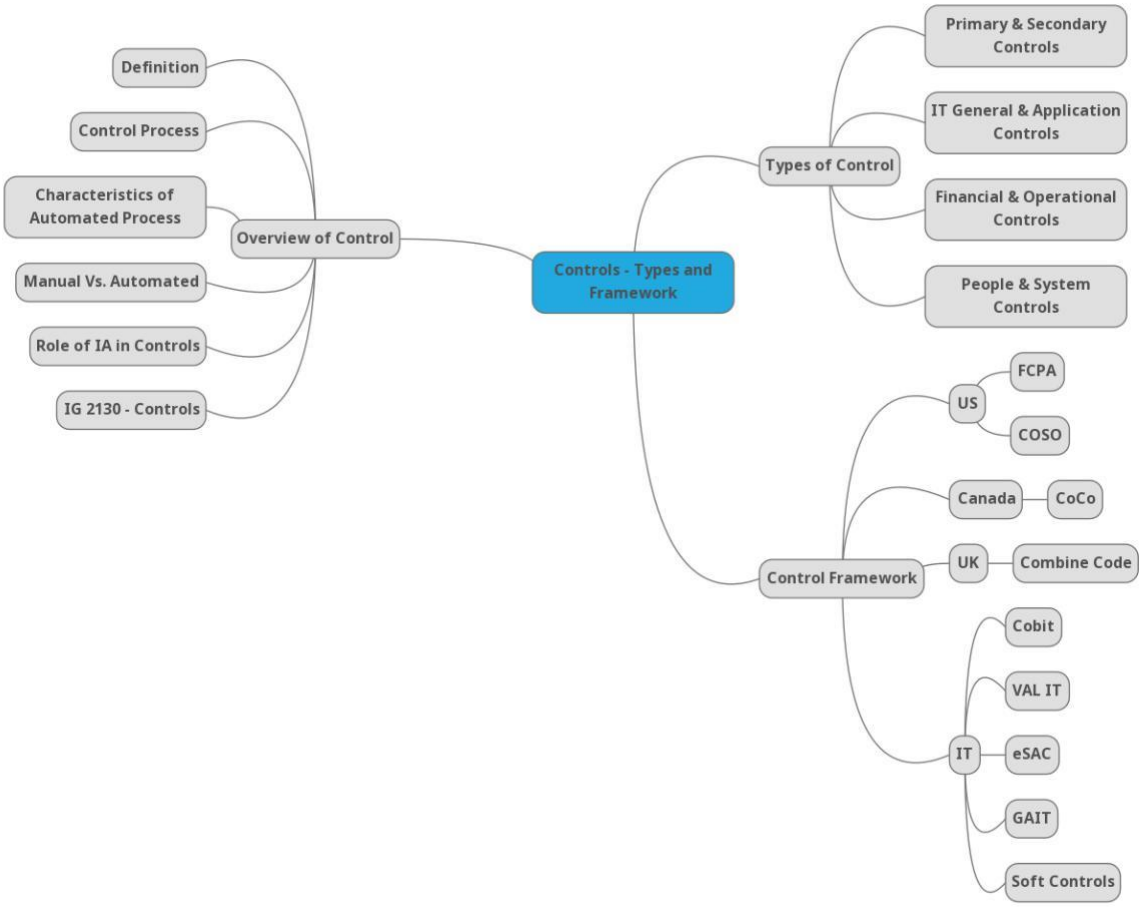
ISO 31000 – Assurance Approaches

- **Key Principle Approach** – RM principles are in practice
- **Process Element Approach** – RM elements are put in place
- **Maturity Model** – Capability Maturity Model (CMM) and CMMI Development V2.0

Trunbull Risk Management Framework

- Unlike ISO 31000, **emphasis on Controls**.

5. Controls: Types and Frameworks (5% - 6 MCQs)



Overview of Controls

Definitions; Control, Control Process, Control Environment

The Control Process

- Standards, Measuring Performance, Examining & Analyzing, Corrective Action and Reappraising the Standards
- Encourage reward system to ensure compliance
- Provide reasonable assurance rather than absolute (human judgment, override of controls, collusion, cost benefit analysis)

Characteristics of Automated Processing

- Transactions trail
- Same (uniform) processing instruction (programming error)
- Segregation – could be concentrated in systems (compensatory controls required)
- Potential for Error and Fraud – unauthorized access to data (reduce human intervention lead reduce for potential for errors)
- Increase Management Supervision – by use of analytical and other tools.
- Computer generation (initiated) Transaction – automatically execute transaction - based on logics
- Computer Input/output and Manual Use - effectiveness of controls dependent on the computer processing.

Manual Control vs. Automated Controls

- Manual – unique transactions, misstatements are difficult to predict, changing circumstances, performance of automated controls.
- Automated – high volume, predictability, require high degree of accuracy.

Role of Internal Auditors in Controls

- Performance Standards – 2130, 2130. A1, 2130. C1
- Implementation Standards 2210.AE

IG 2130: Controls:

- Controls mitigate the risk at entity, activity (process) and transaction level.
- Sr. Manage responsible for establishment, Manager assess controls, and Auditors provide assurance.
- IA should – understand controls, risk appetite, risk tolerance, risk culture, critical risks, control frameworks and have proper planning while auditing and reporting control problems.
- Control can be assess by using risk and control matrix.
- Controls cost benefit analysis should be performed.
- CAE recommend and aim for promoting continuous improvement.

Types of Controls

Primary Controls – Preventive, Detective, Corrective, Directive

Secondary Controls – Compensatory (mitigate) Controls, Complementary Controls

Processing Mode – Batch and Online (Real Time) Processing

IT General Controls

- General Controls – logical access, system development, change management, security control, data backups
- Application Controls – pertain to specific process or application, Input Controls; (authorization, validation, error notification), financial totals, record counts, hash totals. Output Controls; Data entry screen, format checks, validity checks, range checks, sequence checks, digit checks, zero balance check. Processing Controls; concurrency checks (2 or more users attmpts same time). Integrity Controls; Information is store consistently and correctly. Management Trails; Tracking processing history.

Time Based Classification

- Feedback Controls – Improvement based on past performances
- Concurrent Controls – Ongoing to avoid deviating from standards
- Feed forward Controls – Provide long term perspective e.g. policies.

Financial vs. Operational Controls

People based vs. System based

Control Frameworks

Control Frameworks

- US – FCPA Act (Govt.), COSO (Private)
- Canada – CoCo (CICA)
- UK – Combined Code
- IT – Cobit 2019 (ISACA) – VAL IT (IT enable business investments), eSAC (IIA)

COSO Framework

- Definition; Internal control is a process , effected by an entity BoD, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations reporting and compliance.
- Control Objectives – improve and manage risk pertaining to Operations, Reporting and Compliance.
- IC Components – Control environment, risk assessment, control activities, information and communication, reporting.
- Control Environment – Integrity and ethical values, board oversight, management establishes structure and reporting lines – role and responsibilities, retain competent individual, ensure individual accountability.
- Risk Assessment – risk related to specific objectives (operations, financial reporting, nonfinancial reporting, internal reporting, and compliance), identify and analyses risks, assess fraud risks, identify and assess changes.
- Control Activities – mitigation of risks, control over technology, control activities through policies.
- Information and communication – Assess quality of controls, change that lead to changes in controls, control revalidation.
- Relationship of Objectives, Components and Organizational Structure

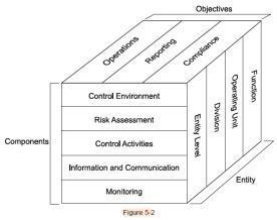


Figure 5-2

COCO Framework

- It has 4 components; Purpose, Commitment, Capability, Monitoring and Learning
- It has 20 criteria group in 4 components.

Cobit Framework

- It is specific to IT Processes
- IT supports the entire business operations

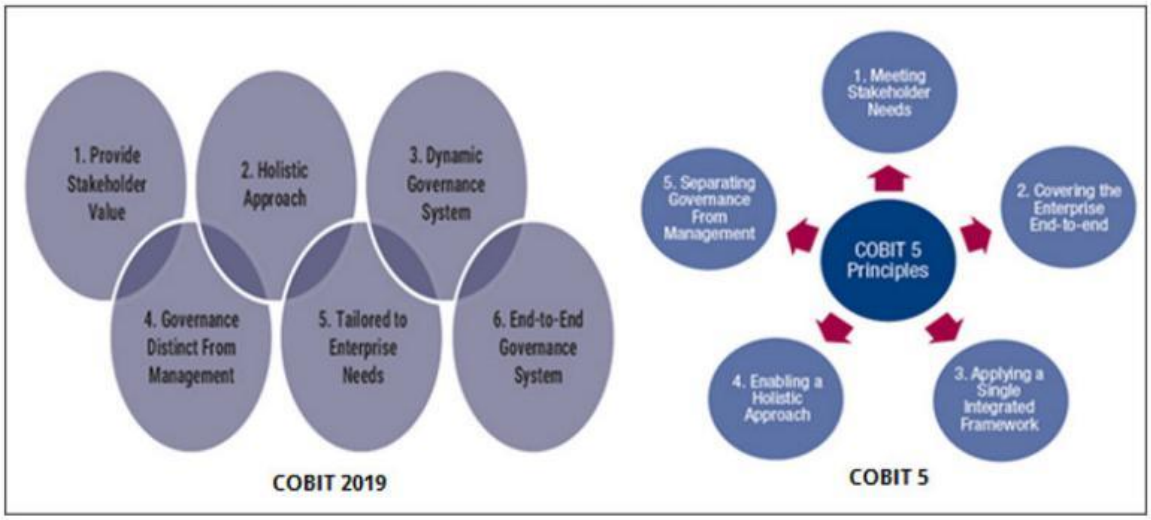
Cobit 5 Principles

1. Meeting Stakeholder Needs
   - Value creation is achieved by balancing three components; benefits, risk mitigation and optimal use of resources.
   - Stakeholders needs are not static it keep on change based on internal and external factors, collectively it called stakeholders drivers.
   - Also enterprise goals are also established
   - IT related goals are drawn up to address enterprise goals.
   - Enablers are identified to support IT related goals.
2. Covering the Enterprises End to End
   - All functions and process that manage information
3. Applying Single, Integrated Framework
   - One framework under which other standards can be applied
4. Enabling Holistic Approach
   - Principles, polices, and frameworks
   - Processes
   - Organizational Structure
   - Culture, Ethics and Behaviors
   - Information
   - Services, infrastructure, and applications
   - People, skills and competences
5. Separating Governance from Management
   - Governance (BoD) – Evaluate, Direct and Monitor
   - Management (CEO) – Plan, Build, Run and Monitor

Cobit 5 to Cobit 2019

1. Principals & Objectives – Increase governance principals from 5 to 6.

Figure 1—Governance Principles in COBIT 2019 and COBIT 5



2. Governance and Management Objectives – Similar in both model 40 Gov & Magm Obj organized in 5 domain.

Figure 2—Governance and Management Objectives in COBIT 5 and COBIT 2019

Source: ISACA, COBIT 2019, USA, 2018, and COBIT 5, USA, 2012.

3. Performance Management and Design Factors – Performance management in COBIT 2019 is based on the CMMI Performance Management Scheme.

Figure 4—Capability Levels of COBIT 2019 and COBIT 5

CoCo Model (Canadian)

- Most suitable for internal auditing purpose.
- It consist of 4 components (Purpose, Commitment, Capacity, Monitoring and Learning) under 20 criteria.

VAL IT

- VAL IT complements Cobit framework.
- It focus on value creation from business investment in IT.
- VAL IT framework consist of three domains; value governance, investment management, portfolio management.

eSAC Model

- The model is influenced by the COSO framework; operational effectiveness, reporting financial and other management reporting, compliance with laws and regulation and safeguarding of assets.
- eSAC IT business assurance are as following; Availability - of information at all time, Capability – reliable and timely completion of transaction, Functionality – fulfill business needs, Protectability – prevent unauthorized access, Accountability – data ownership, identification and authentication.

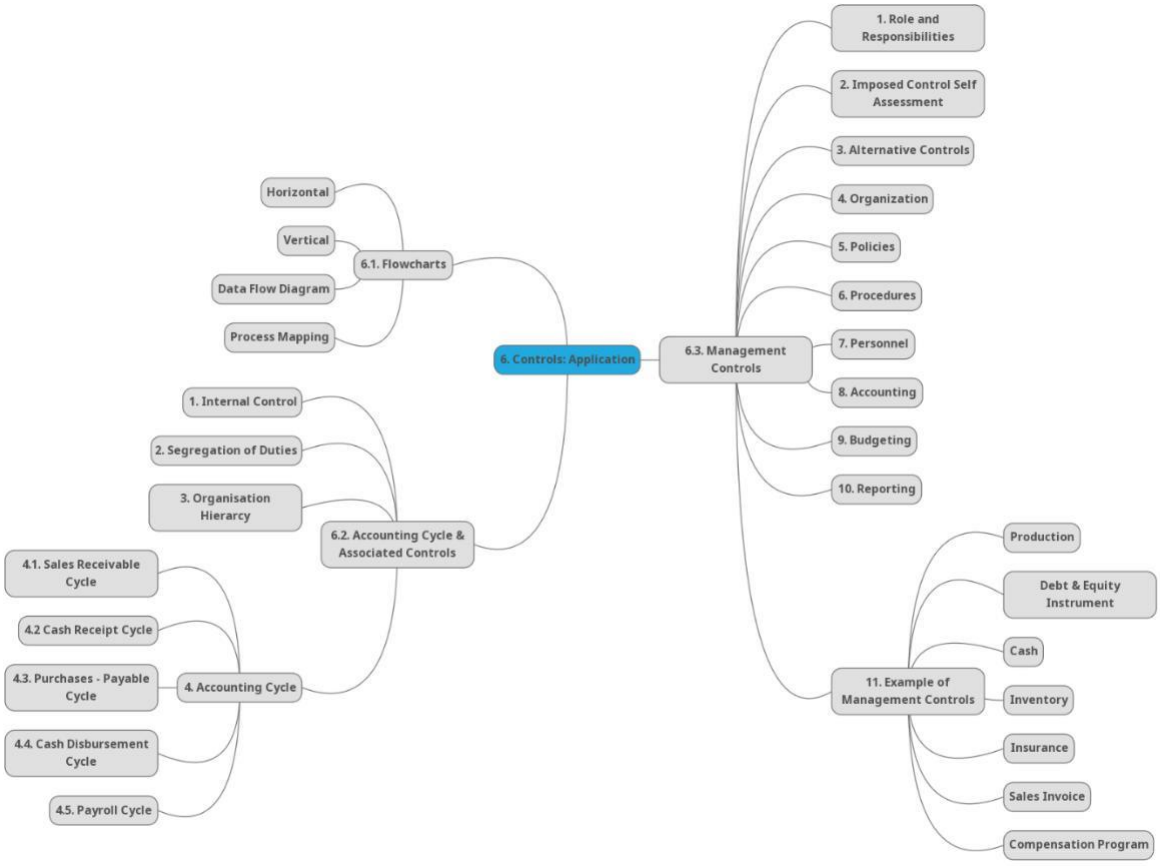
GAIT

- Provide auditors guidance for assessing the scope of IT general controls using TOP DOWN and RISK BASED approach.
- It has 4 principles; Identification of Risk, Risks that are more critical to core IT functionality, IT general controls pertaining to coding, network and operating system, focus on achievement of IT control objectives rather than individual controls.

Soft Controls

- COSO and COCO model emphasis on soft control.
- Soft control are part of the control environment.
- Soft control become more important than the hard control in the rapid changing environment.
- One approach could be use for assessing soft control is Control Self-Assessment.
- Hard and soft controls shall be associated with each risk and the impact and likelihood.

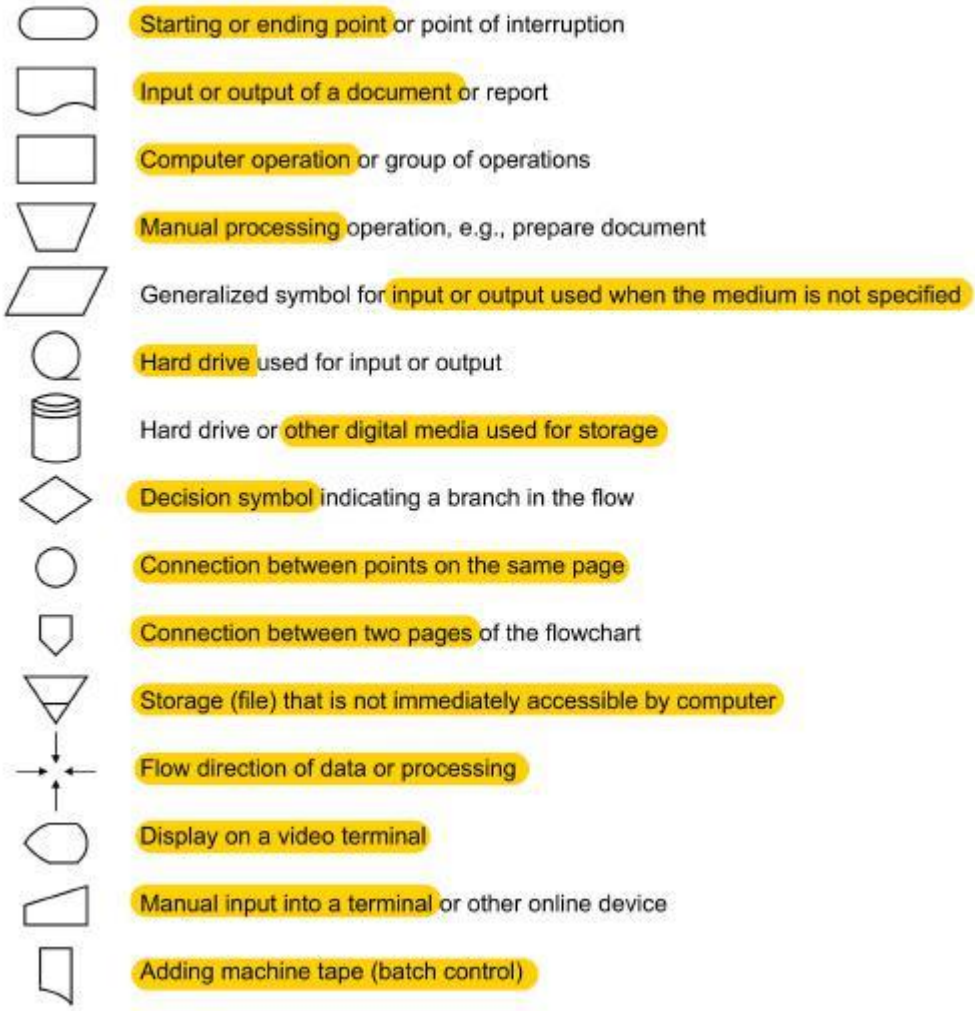
6. Controls: Applications (5% - 6 MCQs)



6.1 Flow charts

Flowchart – Graphical visual representations of step by step process.

Flowcharts Symbols



Types of Flowcharts

1. Horizontal – Depicts area of responsibility
2. Vertical – Depict specific action by a computer program, also known as program flowcharts.
3. Data Flow Diagram – Depicts data flow to, from and within information system with very few symbols.
4. Process Mapping – Depicts a client process.

6.2. Accounting cycles and associated controls

1. Segregation of controls
2. Organizational hierarchy
3. Accounting Cycles
    - Sales to debt
    - Collection to cash

- Purchases to credit
- Payment of cash
- Payment of employees

6.3. Management Controls

Role & Responsibilities:

- Management – CEO and CFO has crucial role to reflect ethical values and control consciousness.
- Board of Directors – BoD commitment to integrity and ethical values, need to have business acumen and role of board committees are important.
- Internal Audit – Provide assurance and consulting services, evaluate soundness of systems.
- Other Personnel – Everyone is responsible for their area of responsibility and associated controls to evaluate and report instances of poor controls.

Organization

- Organization is a means of controls.
- Role and responsibilities should be divided.
- Manger should have authority.
- Individual authority shall always be clearly define.
- Needs to have an effective system of follow-up.
- Individual shall be allowed to exercise their authority.
- People should report to their supervisors on responsibilities.
- Organization structure should be simple.
- Organization charts and manual shall be available.

Policies

- Guide or restricts action.
- Policies should be clearly written and systematically organized in a handbook.
- It shall be communicated to all level.
- Policies shall be in conformity with the local laws and regulation.
- It shall be periodically be reviewed.

Procedures

- Procedures shall be in conformity with policy.
- Procedure should have embedded controls for review and approval.
- It should be so detail that hinder the use of human judgment.
- It shouldn’t be overlapping, conflicting, or duplicative.
- It should be periodically reviewed and improved.

Personnel

- People should be qualified and properly supervised.
- People should be given training and information over their role and responsibilities.
- Performance of all employees shall be reviewed.

Accounting

- Accounting shall be used for proper reasoning and decision making.
- Accounting shall be based on line of responsibility.
- Controllable cost should be identified.

Budgeting

- Budget is expected results express in numerical terms.
- Budget owners shall be represented in the budget making process.
- Variance between actual and budget shall be identified and inquired.
- Subsidiary budget shall be in line with the parent's company budget.

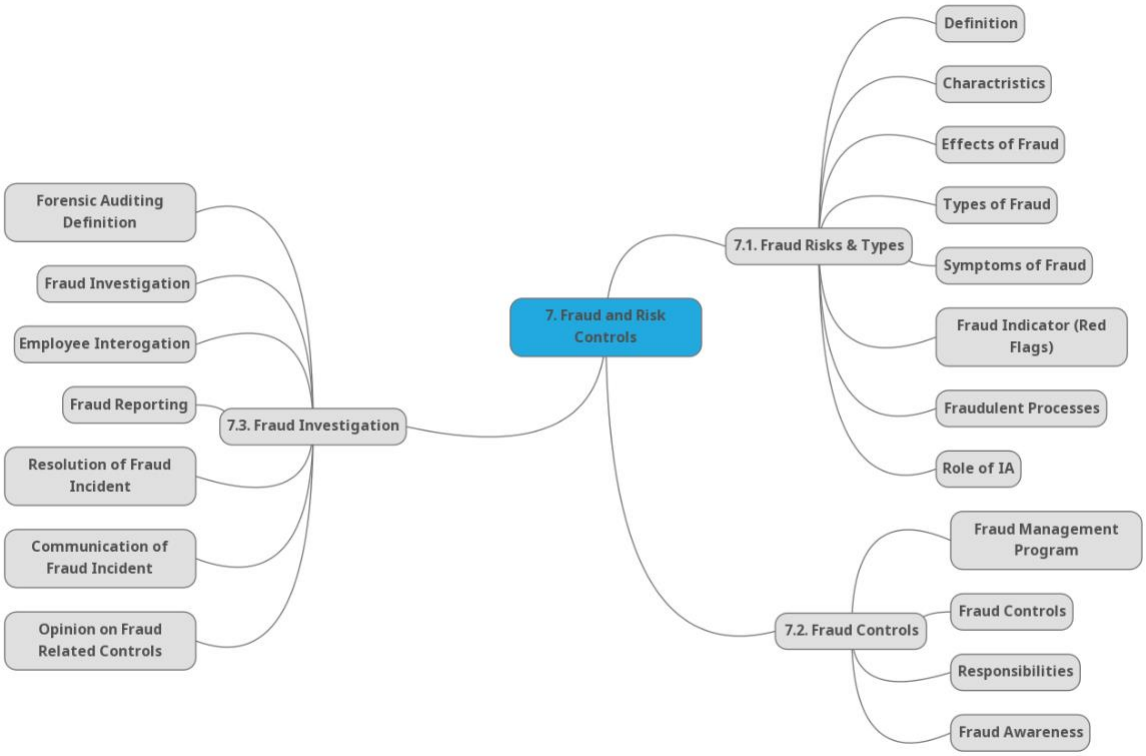
Reporting

- Report should be timely, accurate, meaningful, and economical.
- Report should be in accordance with the responsibilities.
- Cost benefit analysis shall be performed.
- Performance report shall show comparison.
- Report shall also emphasis on significant matters disclosure.
- Report recipient input shall be obtain for input.

Example of management control assertions

- Occurrence
- Existence
- Completeness

7. Fraud Risks & Controls (10% - 12 MCQs)



Fraud Risks and Controls

Fraud – Risks and Types

Fraud is “any illegal act characterized by deceit, concealment, or violation of trust

Characteristics of Fraud

- Pressure – satisfy personal needs by committing fraud.
- Opportunity – control deficiencies allow ability to commit fraud.
- Rationalization – ability to justify fraud.

Effects of Fraud

Full cost is immeasurable but generally cause significant monetary losses.

Types of Fraud

- Asset misappropriation – stealing cash or assets
- Skimming – Theft of cash before recorded
- Payment Fraud – Payment of fictitious goods or services
- Expense Reimbursement Fraud – Payment for fictitious or inflated expenses
- Payroll Fraud – False claim for compensation
- Financial Statement Misrepresentation – Overstate assets or revenues and understate liabilities and expenses.
- Information Misrepresentation – Provide false information.
- Corruption – Improper use of power.
- Bribery – Kickbacks
- Conflict of Interests
- Diversion – Redirect to an employee or outside transactions
- Wrongful Use – wrong use of information
- Related Party Fraud
- Tax Evasion

Low Level vs. Executive Fraud

- Low Level – theft of property by staff
- Executive Level – Misappropriation of statements

Symptoms of Fraud

- Documentary Symptoms – Fake documents
- Lifestyle Symptoms – Employee Social Status
- Behavioral Symptoms – Guilt and Stress

Fraud (Red Flag) Indicators

- Lack of employee rotation
- Lack of clear job responsibilities
- Lack of segregation of duties
- Ambitious sales or production goals
- Employee refuse to take vacation
- Control override
- High reported profit despite competitor or economic downturn
- Sole sourcing
- Disproportionate increase is sales vs. cost of sales
- Actual product differ from requisition
- Petty cash not handle through imprest account

Types of Fraudulent Processes

- Lapping receivable – employee steal customer payment and shortages pay by taking payment from other customers and follow the cycle.
- Check Kiting – Issue check without enough funds and replenished before it is being noticed, exploit delay in check clearing.

Role of Internal Auditors

- Auditors are not responsible for detection of all frauds but they alert the possibility of fraud.
- Auditor should have sufficient knowledge to evaluate the risk of fraud but not expect to have the expertise of investigator.
- Auditor should carry out fraud risk assessment, evaluate control design and choose audit procedures.
- Auditors should have sufficient knowledge to identify indicators.
- Auditors can recommend investigations.

Fraud – Controls

Fraud Management Control

- Company ethics policy
- Fraud awareness
- Fraud risk assessment
- Ongoing reviews
- Prevention and detection
- Investigation

Controls

- Can use COSO to apply in fraud context.

Responsibility for Controls

- Management is primarily responsible
- Auditor is responsible to evaluate and assess and recommend improvement

Fraud Awareness

- Periodic training, risk assessment and communication.

Fraud – Investigation

Fraud Investigation

- Forensic auditing uses audit and accounting skills
- These skills are important for civil and criminal legal implication
- Internal auditors, lawyers, and other specialists usually conduct fraud investigation
- Management implements control over the investigation (1) develop policies and procedures (2) preserving evidence (3) responding to the results (4) reporting (5) communication.
- Internal auditor role for fraud shall be define in charter and fraud policies and procedures.
- To be efficient fraud investing team must obtain sufficient knowledge of (1) fraud scheme (2) investigation methods (3) applicable laws.
- Lead investigator determines the knowledge, skills and competence required for the assignment.
- Obtain process to ensure no conflict of interest involved.
- All evidences shall be recorded chronologically
- Investigation should be coordinated with the management, legal counsel, and others.
- The evidence need to be secured and the chain of custody shall be follow.

Interrogation of Employees

- Fraud related interrogation differ from normal interviews.
- Internal audit lead the conversation from general to specific.
- In investigation the employee should be bar from his work till completion of investigation.

Fraud Reporting

- CAE is responsible for fraud reporting.
- A draft shall be submitted before final submission to the legal counsel for review.
- Any significant fraud, shall be timely reported to senior management and board.

Resolution of Fraud Incidents

- Management and Board is responsible for resolving fraud incident.
- Closure to person who were found innocent.
- Disciplining employees.
- Requesting voluntary financial restitution.
- Terminating contract with suppliers.
- Reporting the incident to law enforcement.
- Filling of civil suit.
- Filling insurance claim.
- Recommending control improvement.

Communication of Fraud Incidents

- The management and the board determine the communication of fraud incident to the outsider.

Opinion of Fraud-Related Controls

- The Board might ask the internal auditor on give opinion fraud related internal controls.