Chap 1 :

1) **Evaluating IT Governance Structure and Practices by Internal Auditors**
   Internal audit while evaluating the IT governance structure can evaluate several key components that can lead to effective IT governance. These are briefly explained here.
   - **Leadership :** Assess the involvement of IT leadership in execution of the organization's strategic goals & Determine how IT will help organization to achieve goals.
   - **Organizational Structure :** Review how management and IT personnel are interacting and communicating across the organization & also include understanding of their roles and reporting to appropriate authorities.
   - **Processes:** Evaluate What processes are used by the IT organization to support the IT environment.
   - **Risks :** Review the processes used by the IT organization to identify, assess, and mitigate risks within the IT environment;
   - **Controls :** Assess key controls that are defined by IT to manage its activities.
   - **Performance Measurement/Monitoring:** Evaluate the framework and systems in place to measure Role of IT in organization outcome.
2) **Sample Areas of GRC for Review by Internal Auditors**
   Sample areas of Governance, Risk and Compliance which can be reviewed by internal auditors are as follows:
   - **Scope :** Internal audit activity must evaluate and improve governance, risk management, and control processes using a systematic approach.
   - **Governance :** Internal audit activity must assess and make recommendations for improving the governance process.
   - **Evaluate Enterprise Ethics :** Internal audit activity must evaluate the design, implementation, and effectiveness of the organisation's ethics and whether it is related to organisation's objectives.
   - **Interpretation :** Internal audit activity must determine whether risk management processes are effective, Significant risks are identified and assessed, and Appropriate risk responses are selected which are within organisation's risk appetite.
   - **Risk Management Process :** Internal audit activity may gather several information's during visits. The results of these visits, when viewed

together should provide an understanding of the organisation's risk management processes and their effectiveness.

- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization with regards to strategic objectives; Reliability of financial and operational information and Compliance with laws, regulations, policies, procedures, and contracts.
- **Evaluate Fraud and Fraud Risk :** Internal audit activity must evaluate the potential for the occurrence of fraud .
- **Address Adequacy of Risk Management Process :** Internal auditors must address risk which are consistent with business objectives and also alert for other significant risks.

3) **Sample Areas of Review of Assessing and Managing Risks**
   - Risk management ownership;
   - Different kinds of IT risks (technology, security, continuity, regulatory, etc.);
   - Defined and communicated risk tolerance profile;
   - Risk mitigation measures;
   - Quantitative and/or qualitative risk measurement;
   - Risk assessment methodology, and
   - Risk action plan and timely reassessment.

4) **Management Practices for Assessing and Evaluating the Internal Controls System in an Enterprise As per COBIT 5 :**
   - **Monitor Internal Controls:** Continuously monitor, set benchmark and improve the IT control environment to meet organisational objectives;
   - **Review Business Process Controls Effectiveness :** Review the operation of controls to ensure that controls within the business processes operate effectively.
   - **Perform Control Self-assessments :** Encourage management for self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts and for improvements;
   - **Identify and Report Control Deficiencies :** Identify control deficiencies and analyze the reason for deficiencies and report to management;

Chap 1 :

- **Ensure that Assurance Providers are Independent and Qualified:** Ensure that the independent entities are performing assurance activities and adhere to codes of professional standards;
- **Plan Assurance Activities :** Assurance activities should be planned based on enterprise objectives, strategic priorities, and sufficient knowledge of the enterprise;
- **Scope of Assurance Activities :** Define and agree with management on the scope of the assurance activities, based on the assurance objectives;
- **Execute Assurance Activities:** Execute the planned assurance activity. Provide opinion & recommendations for improvement where seems appropriate.