ROHAN

Governance: (BCCI = Governance)	**IT Governance (CISA= CA(Govrnance)+IT)**	**Governance of Enterprise IT (GEIT) (IPL = GEIT)**
The term **"Governance"** is derived from the Greek verb meaning **"to steer".** (Now in a cricket, multiple stakeholder of IPL enable to say that Evraj singh is option due to dhoni's directional setting and mohit sharma's complete performance. Whatever, Dhoni is Satisfied because of he has achieved his Specific Objective) A governance system typically - refers to all the means and mechanisms - that will **enable** multiple **stakeholders** in an enterprise - to have an **organized mechanism** for **evaluating** options, setting **direction** and **monitoring** compliance and performance, - in order to satisfy specific enterprise **objectives.**.	(CISA Department's **BOD and executive Mgmt** has made available set of responsibilities and practices to CISA student , with goal of providing starategic direction in study and ensuring that passing % objectives are achieved as well as failure risk are managed) 'The **set of responsibilities and practices** - exercised by the **board** and executive **management** - with the goal of providing strategic direction, - ensuring that objectives are achieved, - ascertaining that risks are managed appropriately - and verifying that the organization's resources are used responsibly.	**IPL = BCCI (Enterprise/Governance) + I(international)T(teams)** IPL is Subset of BCCI and facilitating implementation of International Standered control within India as relevant.) **Governance of Enterprise IT** is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas.
Benefits of Governance (BCCI = Governance)	**Benefits of IT Governance (CISA= CA+IT)**	**Benefits of GEIT (IPL=GEIT)) (BCCI=Enterprise / Governance)**
(BCCI achieved objective (Won Worldcup) by ensuring msission, strategy are assigned and transport decion framework. In press conference they told that their secrets , they defined and desirable behaviors in use of International Teams coach and execution of Iternational Teams Outsourcing Arrnagement. Implementing & Integrating desired Batting Practice into the team,) 1 . Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clearly understood and transparent decisions rights and accountability framework.	(CA auditors value increased through CISA degree also their user(client) satisfaction increased with CISA auditor because they have to pay low fees and they can do better cost performance. Auditors can bring improvement in supporting business needs like accounting, taxation hence company can do compliance with relevant laws and optimum utilization of IT Resources.) Increased value delivered through enterprise IT; Increased user satisfaction with IT services Improved agility in supporting business needs	IPL ensure that International Team-related decisions are made in line with the BCCI's strategies and objectives. IT Ensure that that International Team-related processes are overseen effectively and transparently. IPL confirms compliance with legal and regulatory requirements of Indian Lwas It ensures. that the BCCI requirements for board members are met It provides a consistent approach integrated and aligned with the enterprise governance approach. It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.

ROHAN

2. Defining and encouraging desirable behavior in the use of IT and in the execution of ITOutsourcing arrangements; 3. Implementing and integrating the desired business processes into the enterprise 4. Providing stability and overcoming the limitations of organizational structure 5. Enabling effective and strategically aligned decision aking for the IT Principles that define the role, architecture, Infrastructure of IT	Better cost performance of IT Improved management and mitigation of IT-related business risk IT becoming an enabler for change rather than an inhibitor More optimal utilization of IT resources Improved compliance with relevant laws, regulations and policies	It ensures that IT-related processes are overseen effectively and transparently It confirms compliance with legal and regulatory requirements. It ensures that the governance requirements for board members are met
Good corporate governance requires **(Audit Committee has conflict of Interest in Philips (Sound) Co. Internal Departments Control; Hence they failed to comply with relevant laws and regulations & Corporate disclosure requirements.)** - segregation of incompatible functions, elimination of conflict of interest, - establishment of Audit Committee, - risk management and compliance with the relevant laws and -standards including corporate disclosure requirements.	**Critical Ensure of Defined Benefit of IT Goverence (CISA =IT Govn)** **(CISA Exam's ownership is defined and agreed. It is relevant and link to ICAI's Strategy.** **Risk, Assumption and passing (relisation) benefits are understood, correct and current.** **Timely and accurate result data of CISA Exam are easy to obtain or available on website.)** • Ownership is defined and agreed; • It is relevant and links to the business strategy; • The timing of its realization of benefit is realistic and documented; • The risks, assumptions and dependencies associated with the realization of the benefits are understood, correct and current; • An unambiguous measure has been identified; and • Timely and accurate data for the measure is available or is easy to obtain.	**Best practices of corporate governance** **(After "SATYAM" Fraud case, many co. introduce corporate governance system which include assignment of responsibilities and decision-making authorities, Establishment of a mechanism for the interaction and cooperation among the board of directors, Implementing strong internal control systems Special monitoring of risk exposures where conflicts of interest)** • Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors; • Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors; • Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks

ROHAN

		and balances; • Special monitoring of riskexposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g.traders); • Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition.
Key Governance Practices of Risk Management **Evaluate = Identify/Analyse Effects / WHO,HOW, WHAT question relating to decision** **Direct = Estalbilish/Assure /Guide** **Monitor = Monitor Goals/result/ matrics/performance** **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.	**Key practices to determine status of IT Governance** **Evaluate = Identify/Analyse Effects / WHO,HOW, WHAT question relating to decision** **Direct = Estalbilish/Assure /Guide** **Monitor = Monitor Goals/result/ matrics/performance** • Who makes directing, controlling and executing decisions? (Evaluate) • How the decisions are made? (Evaluate) • What information is required to make the decisions? (Evaluate) • What decision-making mechanisms are required? (Evaluate) • How exceptions are handled? **(Direct)** • How the governance results are monitored and improved? (Monitor)	**Key Governance Practices of GEIT** **Evaluate = Identify/Analyse Effects / WHO,HOW, WHAT question relating to decision** **Direct = Estalbilish/Assure /Guide** **Monitor = Monitor Goals/result/ matrics/performance** **Evaluate the Governance System:** - Continually identify & engage with the enterprise's stakeholders, document an understanding of requirements - make judgment on the current and future design of governance of enterprise IT; **Direct the Governance System**: - Inform leadership and obtain their support, buy-in and commitment. - Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. - Define the information required for informed decision making.

ROHAN

		Monitor the Governance System: - Monitor the effectiveness and performance of the enterprise's governance of IT. - Assess whether the governance system and implemented mechanisms are operating effectively and provide appropriate oversight of IT.
key management practices, which need to be implemented for evaluating 'Whether business value is derived from IT', **Evaluate = Identify/Analyse Effects / WHO,HOW, WHAT question relating to decision** **Direct = Estalbilish/Assure /Guide** **Monitor = Monitor Goals/result/ matrics/performance** **Business Value = IT Enabled investment, Investment Claimed Benefits, Expected Benefits, Realized Benefits** **-Evaluate Value Optimization** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. **-Direct Value Optimization** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle. **-Monitor Value Optimization.** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services.	**Key Management Practices for Aligning IT Strategy with Enterprise Strategy** **(CU CU AD relating to IT service, strategy, enterprise environment)** **Understand enterprise direction:** understanding of the enterprise environment and requirements. **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. **Assess the current environment, capabilities and performance** Assess the performance of current internal business and IT capabilities and external IT services and develop an understanding of the enterprise architecture in relation to IT. **Conduct a gap analysis** between the current and target environments **Understand enterprise direction** Consider the current enterprise environment and also consider the external environment of the enterprise. **Communicate the IT strategy** and direction (Create awareness and understanding of the business and IT objectives and direction)	**Key Management Practices of Risk Management** **(MAD CAR related to IT Risk)** **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting. • **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors. • **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities. • **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response. • **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio. • **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

ROHAN

Key Management Practices of IT Compliance **(IOCO related to Compliance Requirement)** **Compliance = Internal & External Laws, Regulation, Agreement, Reports, Working Practice, Review Updates, Fine Penalties**	**key management practices for assessing and evaluating the system of internal controls in an enterprise are** **(MRP Independent & Qualified IPS)**	**key functions of the IT Steering committee** **(Set, Ensure, facilitate, Review Make ,Report)**
COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. **Identify External Compliance Requirements -** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective **Optimize Response to External Requirements** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. **Conform External Compliance and** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements **Obtain Assurance of External Compliance -** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	• **Monitor Internal Controls:** Continuously monitor, benchmark and improve the control environment and control framework to meet organizational objectives. • **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate ffectively. • **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of selfassessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts • **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders. • **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. • Plan Assurance Initiatives: Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise. • **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative,	• To sets priorities according to size and scope of IT function within its scope; • To ensure plans of the IT department are aligned with enterprise goals and objectives; • To facilitate implementation of IT security within enterprise; • To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and • To approve and monitor key projects by measuring result of IT projects in terms of ROI, etc. • To review and approve major IT deployment projects in all their stages; • To review and approve standards, policies and procedures; • To review the status of IS plans and budgets and overall IT performance; • To make decisions on all key aspects of IT deployment and implementation; • To report to the Board of Directors on IT activities on regularly

ROHAN

	based on the assurance objectives.	
Key Metrics for Assessing Compliance Process **Metrics = Cost, Percentage, Number, Frequency** **Compliance = Internal & External Laws, Regulation, Agreement, Reports, Working Practice, Review Updates, Fine Penalties** • **Compliance with External Laws and Regulations:** These metrics are given as follows: - Cost of IT non-compliance, including settlements and fines; - Number of IT related non-ompliance issues reported to the board or causing public comment or embarrassment; - Number of non-compliance issues relating to contractual agreements with IT service providers; and - Coverage of compliance assessments. • **IT Compliance with Internal Policies:** These metrics are given as follows: - Number of incidents related to non compliance to policy; - Percentage of stakeholders who understand policies; - Percentage of policies supported by effective standards and working practices; and - Frequency of policies review and updates.	**key metrics For Evaluation of Business value from use of IT** **Metrics = Cost, Percentage, Number, Frequency** **Business Value = IT Enabled investment, Investment Claimed Benefits, Expected Benefits, Realized Benefits** • Percentage of IT enabled investments where benefit realization monitored through full economic life cycle; • Percentage of IT services where expected benefits realized; • Percentage of IT enabled investments where claimed benefits met or exceeded; • Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits; • Percentage of IT services with clearly defined and approved operational costs and expected benefits; and • Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.	**Metrics of Risk Management** **Metrics = Cost, Percentage, Number, Frequency** **Risk Management = Critical Business Process, IT Services, Significant IT Related Incidents, IT Related Risk, Risk Profile Assessment** • Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment; • Number of significant IT related incidents that were not identified in risk Assessment; • Percentage of enterprise risk assessments including IT related risks; and • Frequency of updating the risk profile based on status of assessment of risks.
COBIT 5 Business Framework – Governance and Management of Enterprise IT **(Manage IT Risk, Policy Development, Increase User Satisfaction, For All Business)** COBIT 5 helps enterprises to manage IT related risk and ensure compliance, security and privacy. Cobit % enables clear policy development and good	**Integrating COBIT 5 with Other Frameworks** **COBIT 5** builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including	**Customizing COBIT 5 as per Requirement** **(Co. require Women Director (GIRL)Assure the Activities of CSR Reporting)** COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture.

ROHAN

practice for IT management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not for profit or in the public sector.	**-GEIT** **-ISO 27001** **-ITIL** **-Risk IT** **-Val IT** **-TOGAF (The Open Group Architechture)** **-ISO 38500** The **framework and resulting enablers should be** aligned with and in harmony with (amongst others) the: **• Enterprise policies, strategies, governance and business plans, and audit approaches;** **• Enterprise risk management framework; and** **• Existing enterprise governance organization, structures and processes.**	Because of its open design, it can be applied to meet needs related to: • Information security, • Risk management, • Governance and management of enterprise IT, • Assurance activities, • Legislative and regulatory compliance, and • Financial processing or CSR reporting.
Need for Enterprises to Use COBIT 5 **(Increase Value Creation using UID card. In future support compliance with relevant laws & regulation of UID will be increased)** • Increased value creation from use of IT • User satisfaction with IT engagement and services; • Support compliance with relevant laws, regulations and contractual requirements; • Development of more business-focused IT solutions and services; and • Increased enterprise wide involvement in IT-related activities	***Components in COBIT5*** **(PM CM on FC Road for purchasing mobile components)** • **Framework** - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements • **Process Descriptions** - A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor. • **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process. • **Management Guidelines** - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes • **Maturity Models** - Assess maturity and capability per process and helps to address gaps.	Benefits of COBIT 5 (Combine answer **of Benefit of IT Governance** and **Cobit GEIT Framework**) • A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT. • The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. • Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders. • COBIT 5 helps enterprises to manage IT related risk and ensures

ROHAN

		compliance, continuity, security and privacy. • COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction. • The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit - or in the public sector. • COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.
Five Principles of COBIT 5 **Co. ne stakeholder ki meeting bulai, meeting mein sare chair end to end full (cover) ho gaye, Sabne milk ek single plan banaya ki hum Holi ko Mathura Jayenge but management and governance separate jayenge** Principle 1: Meeting Stakeholder Needs Provides all of the required processes and other enablers to support business value creation through the use of IT. An enterprise can customize COBIT 5 to suit its own context & creates value for its stakeholders through the use of IT Principle 2: Covering the Enterprise End to End It does not focus on IT function, it considers all IT related governance and management enablers to be enterprise-wide & end to end including each & everything Principle 3: Applying a Single Integrated Framework There are many IT related standards and best practices, each providing guidance	**Seven Enablers of Cobit 5** **Ek origination ne aisa decision liya ki hum principles and policies for day to day management ke liye banayenge ki agar koi staff co. ki process ko wrong cultural , ethical and behavior se follow karta hai to use next month se service desk pe shift karenge aur uskee skill and competence sudharne ke liye training denge (correct Action). Aur aise staff ki information dene wale ko inam denge.** **Principles, policies and Frameworks** are the vehicle to translate the desired behaviour into practical guidance for day-to-day management. **Processes** describe organized set of practices and activities to achieve certain objectives & produce a set of outputs in support of achieving overall IT-related goals. **Oraganisation structure** are the key decision-making entities in an enterprise **Culture, ethics and behaviour** Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.	**Cobit 5 Reference Model** It defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities providing a common reference mode understandable to operational IT and business managers **Govenance Process -** **-Evaluate direct monitor practices (EDM) – 5 Processes** **Management Process -** **-Audit , Plan , Organise – 13 Process** **- Build, Acquire and implement**

ROHAN

on a subset of IT activities. COBIT 5 framework aligns with them at a high level & serve as an overarching framework to simplify complexity. Principle 4: Enabling a Holistic Approach COBIT 5 defines a set of 7 enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Principle 5: Separating Governance from Management Cobit 5 Make Clear Dstinction between Governance and management. The COBIT 5 recognizes that these two disciplines (governance and management)are involved in different types of activities, serve different purposes and requires different organizational structures to fulfil their individual needs.	**Service, Infrastructure and application** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services. **People, Skill and Competence** Are linked to people and are required for successful completion of all activities and for making correct decision and correct action. **Information** Information is required for keeping the oraganisation ruuning and well goverened . Perational level information is key product of the enterprise itself.	**– 10 processes** **-Deliver, Service Support – 6 Process** **-Monitor, Evaluate, Accesses -3 Processes**
IT Compliance Review in Cobit 5 **(SOX, Clause 49, PCAOB, CARO, IT act ye cobit mein compliance Review ke tarike hai.)** **SOX** - Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made. **Clausre 49 of SEBI** – Mandates implantation of ERM & Internal Controls as appropriate for Company **CARO** – Compulsory to report on internal control & Separate annexure to audit report **Public Company Accounting Oversight Board (PCAOB)** has come out with detailed guidelines on Compliance by Auditors and Companies under the Act.	**Risk Management by Cobit 5** **(COBIT mein Risk Mgmt karne k liye Governance Risk ki Planning aur monitoring karte hai and Management Risk Ko identify, analyze and reduce karte hai)** Organisation can manage risk without COBIT also, but it would not be effective. Cobit 5 provide detailed guideline, framework, standered and practices, which developed by experts across the globe, to treat IT related Risk. That is why organization follow COBIT 5 to reduce level of Risks. **Governance Domain** of Cobit focus on shareholder risk related objective . **EDM 03** Process – Ensure risk optimization. Ensure the IT Risk doesnot exceed risk appetite and Risk tolerance. Direct how risk faced by organization will be treated. **Management Domain** of Cobit 5 – **APO 12 – Manage Risk Process-**	**Using Cobit 5 Best Practice for GRC (Governance , Risk and Compliances) programme implementation Requires Following Steps** **(GRC Co. Ka best practice award dene liye audit shuru kiya and COBIT ke ye step follow kiye , first GRC co. ki applicable requirement define ki, 2nd compliances identify ki, bad mein uske current status review kiya and thereafter hamne most optimal approach determine kiya, Report mein success parameter set karne ke liye kaha aur suggestion mein Global best practices adopt karne ke liye kaha)** • Defining clearly what GRC requirements are applicable; • Identifying the regulatory and compliance landscape;

ROHAN

In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements **IT ACT** – It provide legal recognition for electronic records & mandate for respnsibilites for protecting information. Identifies cyber crimes & impose specific responsibilities on corporate. **IT Compliance in Cobit 5** **(Monitor, Evaluate, Assess, Cobit, Coso ye cobit mein Compliance ke tarike hai)** **Monitor, Evaluate and Assess (MEA)** - contains a compliance focused process: "**MEA03 Monitor, Evaluate and Assess Compliance with External Requirements**". This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. COBIT 5 - COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance /management structures (RACI charts) for each process, which also include a compliance-related role. GRC - The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities Risk Mgmt Process- The Risk	Continuously Identify, assess and Reduce IT related Risks within tolerance levels. Integrate of IT related Enterprise Risk with overall ERM & Balance the Cost benefit of Managing IT related Enterprise Risk **Combination** of both domains ensure that IT Risk management covers entire life cycle & Both Governance. COBIT Suggest Accountabilities, Responsibilities & Risk Related Roles at each level of Mgmt. Risk Management Steps- 1. Risk identification 2. Risk Analysis 3. Risk Prioritazation 4. Risk Reduction 5. Risk Planning 6. Risk Monitoring	• Reviewing the current GRC status; • Determining the most optimal approach; • Setting out key parameters on which success will be measured; • Using a process oriented approach; • Adapting global best practices as applicable; and • Using uniform and structured approach which is auditable.

ROHAN

management process and supporting guidance for risk management across the GEIT space meet the compliance need of regulations such as SOX and other similar regulations across the world COSO - COBIT combined with COSO has been the most widely used framework for implementing IT controls as part of enterprise risk management to meet governance requirements.		
Using Cobit 5 For IS Assurance **(IS Assurance naam ki co. ne hame best director ka award diya, and hame success ke tarika batane ko kaha, then we told that first understand business process & expectation of multiple stakeholder which can be meet by allocating job responsibilities to IT staff & written policies in non technical language which can by understand by senior mgmt personnel, employee & not only the IT professional or consultants.** **Award ka benefit internal stakeholder and bod, employee mein deliver kar di.)**	**Evaluating & Assessing the System of Internal Control as per Cobit 5 Process** **(IIM, PMO's Continuously internal control environment ko evaluate and monitor karte hai through self assessment and assurance reviews.**	**Sources of GRC Programme Measured by Following Goals & Metrics** **(GRC co. Ke source of income wale goal / metrics ko badhane ke tarike - Reduction in legal exp, reduction in required time of audit , reduction in production time through automation control, reduction in compliance exp through timely reporting)**
1. Auditor to understand bisuness process, policy and organization objective by effectively 2. Proper Job Responsibilities to IT Staff, Proper internal Control Structure **3.** COBIT 5 has been engineered to meet expectations of multiple stakeholders. **4.** deliver benefits to both an enterprise's internal stakeholders, such as the board, management employees, etc. as well as external stakeholders - customers, business partners, external auditors,	• Continuously monitor and evaluate the control environment, including self assessments and independent assurance reviews; • Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions; and • Plan, organize and maintain standards for internal control assessment and assurance activities.	• The reduction of redundant controls and related time to execute (audit, test and remediate); • The reduction in control failures in all key areas; • The reduction of expenditure relating to legal, regulatory and review areas; • Reduction in overall time required for audit for key business areas; • Improvement through streamlining of processes and reduction in time through automation of control and compliance measures; • Improvement in timely reporting of regular compliance issues and remediation measures; and

ROHAN

shareholders, consultants, 5. It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers;		• Dashboard of overall compliance status and key issues to senior management on a realtime basis as required.
Evaluating IT Governance Structure & Practices by Internal Auditors **(Internal Auditors Evaluating IT Governance RCM POLicy)** • **Leadership:** The following aspects need to be verified by the auditor: o Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel. o Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals. o Determine how IT will be measured in helping the organization achieve these goals. o Review how roles and responsibilities are assigned within the IT organization and how they are executed. o Review the role of senior management and the board in helping establish and maintain strong IT governance. • **Organizational Structure:** The following aspects need to be assessed by the auditor: o Review how organization management and IT personnel are interacting and communicating current and future needs across the rganization . o This should include the existence of	**Sample Area of GRC for Review of Assurance & Managing Risks** **(Sample invoice payment of GRC vendors review karte waqt following cheese notice kiye, Different kinds of IT risk security related item purchase kiye the, invoice mein raw material ownership and accountability ke term define the , risk tolerance in delivery Communicated and defined thi.** **Risk Timely reassess karke hamne payment ka action plan bana liya and yahi risk assessment methodology for any root cause analysis ke liye follow karne ke liye kaha .)** • Risk management ownership and accountability; • Different kinds of IT risks (technology, security, continuity, regulatory, etc.); • Defined and communicated risk tolerance profile; • Root cause analyses and risk mitigation measures; • Quantitative and/or qualitative risk measurement; • Risk assessment methodology; and • Risk action plan and Timely reassessment.	**Sample Areas of GRC for Review of Internal Auditors** **(Internal Auditors verify the sample area of FIRE PAGES)** • **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach. • **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives: o Promoting appropriate ethics and values within the organization; o Ensuring effective organizational performance management and accountability; o Communicating risk and control information to appropriate areas of the organization; and o Coordinating the activities of and communicating information among the board, external and internal auditors, and management. • **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.

necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. • **Processes:** The following aspects need to be checked by the auditor: o Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems. o What processes are used by the IT organization to support the IT environment and consistent delivery of expected services? • **Risks:** The following aspects need to be reviewed by the auditor: o Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment. o Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met. • **Controls:** The following aspects need to be verified by the auditor: o Assess key controls that are defined by IT to manage its activities and the support of the overall organization. o Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity. • **Performance Measurement /Monitoring:** The following aspects need to be verified by the auditor:		• **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes. • **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that: o Organizational objectives support and align with the organization's mission; o Significant risks are identified and assessed; o Appropriate risk responses are selected that align risks with the organization's risk appetite; • **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. • **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the: o Achievement of the organization's strategic objectives; o Reliability and integrity of financial and operational information; o Effectiveness and efficiency of operations and programs; o Safeguarding of assets; and o Compliance with laws, regulations, policies, procedures, and contracts. • **Evaluate Fraud and Fraud Risk:** The internal audit activity must

ROHAN

o Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.		evaluate the potential for the occurrence of fraud and how the organization manages fraud risk. • **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.
Role of IT in Enterprises **(IT Not only data proceesing but for strategic advantage, MIS decision support, transformed the way of business process, Innovative services)** IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to decision support systems to online transactions/services IT has not only automated the business processes but also transformed the way business processes are performed Implementing IT has to consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage. Senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services	**Internal Control** **(RRP of financial statement as per gaap and policies for ensuring RAPP)** internal control over financial reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting & Preparation of financial statement as per GAPP & Policies Procedure that ensure - recording of all transaction - proper authorization - accurate recoed of asset - prevention or timely detection of unauthorized acuisation, use or disposition of company's asset that have material effect on the Financial Statement. **company's annual report must include "an internal control report of management that contains** • A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company	**Internal Control as per COSO** **(COSO CRIME related to business process)** • **Control Environment:** For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process. • **Risk Assessment:** must include an assessment of the risks associated with each business process. • **Control Activities:** Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process • **Information and Communication:** Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

ROHAN

	• A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting • A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting	• **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.
ERM (Enterprise Risk Management) -Integrated framework published by COSO -It is **Process**, Effected by an entity's **BOD , Mgmt and Other Personnal , applied in** strategy setting across the enterprises -Designed To identify potential events that effect entity. -Manage risk to be within risk appetite. -to provide reasonable assurance to achieve enterprise objective -IT security & control are sub set of the overall ERM strategy.	**Responsibility for implementing Internal Control as per SOX** -SOX hold CEO/CFO personally and criminally liable for the quality and effectiveness of their organization's internal controls -Internal controls can be expected to provide only a reasonable assurance, not an absolute assurance. -An organization must ensure that its financial statements comply with **Financial Accounting Standards (FAS)** and **International accounting Standards (IAS)** or local rules -must be a system of checks and balances of defined processes that lead directly from actions and transactions reporting to an organization's owners, investors, and public hosts.	**Clause 49** - Clause 49 of the listing agreements issued by SEBI in India - similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls - holds the senior management legally responsible for such implementation. it also provides for certification of these aspects by the external auditors.
Risk Related Terms **Asset** Asset can be defined as something of value to the organization; ex- information in electronic or physical form, software systems, employees. **Characteristics –** • They are recognized to be of value to the organization.	**Sources of Risk** **(Naturally har event mein human behavior dusre ke Legal relationship , Economic circumstances, Political circumstances, technical issue ko dekhata hai, aise tendency se hi risk creat hota hai)** • Commercial and Legal Relationships,	**Characteristics of Risks** • Loss potential that exists as the result of threat/vulnerability process; • Uncertainty of loss expressed in terms of probability of such loss; and • The probability/likelihood that a

ROHAN

• They are not easily replaceable without cost, skill, time, resources or a combination.
• They form a part of the organization's corporate identity, without which, the organization may be threatened.
• Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

Vulnerability

Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components.

Some examples of vulnerabilities are given as follows:

• Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
• Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

vulnerability is a state in a computing system (or set of systems), which must have at least one condition out of following –

• 'Allows an attacker to execute commands as another user' or
• 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
• 'Allows an attacker to pose as another entity' or
• 'Allows an attacker to conduct a denial of service'.

Threat

Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction,

• Economic Circumstances,
• Human Behavior,
• Natural Events,
• Political Circumstances,
• Technology and Technical Issues,
• Management Activities and Controls
• Individual Activities

Risk Management Strategies

(T5)

• **Tolerate/Accept the risk** - accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low

• **Terminate/Eliminate the risk** – possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors

• **Transfer/Share the risk** – A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure bybeing more capable and having access to more highly skilled staff than the primary organization.

Risk also may be mitigated by transferring the cost of realized risk to an insurance provider

• **Treat/mitigate the risk** – suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

• **Turn back** –
Where the probability or impact of the risk is very low, then management may decide to ignore the risk

Risk Analysis / Assessment Includes

threat agent mounting a specific attack against a particular system.

Risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by

(use of technology, constraint space and time, external factors such as legal, devolution of mgmt control)

• Widespread use of technology;
• Interconnectivity of systems;
• Elimination of distance, time and space as constraints;
• Unevenness of technological changes;
• Devolution of management and control;
• Attractiveness of conducting unconventional electronic attacks against organizations; and
• External factors such as legislative, legal and regulatory requirements or technological developments.

New risk areas that could have a significant impact on critical business operations, such as

• External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information;
• Growing potential for misuse and abuse of information system affecting privacy and ethical values; and
• Increasing requirements for availability and robustness.

ROHAN

modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. **Exposure** An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For **example** - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources **Likely Hood** Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring **Attack** An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system **Risk** risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and etermining their magnitude and impact on an organization **Counter Measure** An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system	**(Identity of threat, vulnerability, control and potential impact that loss of CIA)** • Identification of threats and vulnerabilities in the system; • Potential impact or magnitude of harm that a loss of CIA, and • The identification and analysis of security controls for the information system.	

ROHAN

is referred as Counter Measure For **example**, well known threat 'spoofing the user identity', has two countermeasures: • Strong authentication protocols to validate users; and • Passwords should not be stored in configuration files instead some secure mechanism should be used. **Residual Risk** An organization's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk		
IT Strategy Planning **(Decide in advance, Direction to deployment of IS, & Communication, Feedback relating to business process)** Planning is basically deciding in advance 'what is to be done', 'who is going to do' and 'when it is going to be done'. IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and Implementation Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties in enterprises. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of	**IT Strategy Planning Process** **(Establish, Modify the short & Long range IT Plan, Reguraly translated Long to short IT Plan, Resources allocate on basis of consistent, Reassessed and Amended short IT plan.)** Establish Policy to develop and maintain, IT long and short range plans Modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan short-range plans should be reassessed periodically and amended as necessary in	**Objective of IT Strategy** **(For playing Holi at strategically, we don't need it Planning, communicating accountiblities & direction to mitigate the environmental colors on skin)** The primary objective of IT strategy is to provide a holistic view of the current IT environment. Set future direction & take initiative required to mitigate to desired future environment. Align Strategic IT Plans with business objective, by communicating objective and associated accountibilites , so they understood by all.

ROHAN

long and short-range plans The feedback obtained should be evaluated and considered in future IT planning	response to changing business and IT conditions	
3 Level of Managerial Activity in Enterprises relating to IT strategy planning **(Manager define the controls of the SMOking level plan)** • **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. • **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives • **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.	**Business & IT Strategy - (To Devlope IT Strategy should know the business strategy)** Management strategy determine the overall path and methodology of rendering service Integration of IT Strategy with business strategy Auditor should be involved in providing assurance related to info system & control system Strategies and tactics of IT department to ensure effective day to day IT operations. Metrics & goals establish to measure IT perform on a Tactical basis. Internal Audit can measure progress of IT strategy & its alignment with business objective.	**Classsification of IT Strategy Planning** **(For classification of External & Internal Strategically Plan , We need IS control requirement plan & IS Control Application plan.)** IT Strategy planning in an enterprise could be broadly classified into the following categories • Enterprise Strategic Plan, • Information Systems Strategic Plan, • Information Systems Requirements Plan, and • Information Systems Applications and Facilities Plan **1)Enterprises Strategy Planning** The primary Plan prepared by Top mgmt that guide long run development of enterprises. It Provides overall **character** -Statement of mission -Specification of Strategic Objective -Assessment of environment & organization factors -constraints -a listing of priorities In an IT environment it is important to ensure that IT plan is aligned with the enterprise plan.

ROHAN

2) IS Strategic Planning The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. Some of the enablers of the IS Strategic plan are: **(For implementation of IS Strategic Plan NEED TIME)** • Enterprise business strategy, • Definition of how IT supports the business objectives, • Inventory of technological solutions and current infrastructure, • Monitoring the technology markets, • Timely feasibility studies and reality checks, • Existing systems assessments, • Enterprise position on risk, time-to-market, quality, and • Need for senior management buy-in, support and critical review	**3) Information System Requirements Plan** Every enterprise needs to have clearly defined information architecture. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information. The information architecture will determine information needs and flow in an enterprise. Based on the information architecture, the organization structure is determined. This in turn will lead to specific information systems, which include the relevant IT and related processes. Some of the key enablers of the information architecture are as follows: **(IS Require DADE business model plan)** • Automated data repository and dictionary, • Data syntax rules, • Data ownership and criticality/security classification, • An information model representing the business, and • Enterprise information architectural standards	**4) Information System Application & Facilities Plan** On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes: • Specific application systems to be developed and an associated time schedule, • Hardware and Software acquisition/development schedule, • Facilities required, and • Organization changes required.