Postgraduate Certificate in Internal Audit and Controls

# Governance and Compliance Auditing

Governance and Compliance Auditing

Governance and compliance auditing are crucial aspects of internal audit and controls within organizations. This glossary will provide a detailed explanation of various terms related to governance and compliance auditing in the context of the Postgraduate Certificate in Internal Audit and Controls.

1. Audit Committee
An audit committee is a subgroup of the board of directors responsible for overseeing the financial reporting and audit processes of an organization. The audit committee typically consists of independent directors who provide oversight and ensure the integrity of financial information.

2. Audit Plan
An audit plan is a detailed outline of the audit procedures and activities that will be conducted during an audit engagement. The audit plan includes the scope, objectives, resources, and timeline for the audit to ensure that all relevant areas are covered efficiently.

3. Compliance Audit
A compliance audit is an examination of an organization's adherence to laws, regulations, policies, and procedures. The purpose of a compliance audit is to assess whether the organization is operating within the legal and regulatory framework and to identify areas of non-compliance that require corrective action.

4. Control Environment
The control environment refers to the overall attitude, awareness, and actions of an organization regarding internal control. It encompasses the tone set by management, the ethical values of the organization, and the importance placed on internal control throughout the organization.

5. Control Testing
Control testing involves evaluating the design and operating effectiveness of internal controls within an organization. Control testing can be done through inquiries, observations, inspections, and re-performance of control activities to assess their reliability in achieving control objectives.

6. Corporate Governance
Corporate governance refers to the system of rules, practices, and processes by which a company is directed and controlled. It involves balancing the interests of various stakeholders, such as shareholders, management, customers, suppliers, financiers, government, and the community.

7. COSO Framework
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework is a widely recognized framework for designing, implementing, and conducting internal control and enterprise risk

management. The COSO framework consists of five components: control environment, risk assessment, control activities, information and communication, and monitoring activities.

8. Enterprise Risk Management (ERM)
Enterprise risk management (ERM) is a comprehensive approach to identifying, assessing, and managing risks across an organization. ERM integrates risk management practices into strategic decision-making processes to enhance the organization's ability to achieve its objectives.

9. Internal Audit
Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. Internal auditors evaluate the effectiveness of risk management, control, and governance processes and provide recommendations for improvement.

10. Internal Control
Internal control refers to the policies, procedures, and practices established by management to provide reasonable assurance regarding the achievement of organizational objectives. Internal controls are designed to mitigate risks, safeguard assets, ensure compliance, and promote operational efficiency.

11. Key Performance Indicators (KPIs)
Key performance indicators (KPIs) are quantifiable measures used to evaluate the success of an organization in achieving its strategic objectives. KPIs are used to monitor performance, identify trends, and make informed decisions to drive organizational success.

12. Risk Assessment
Risk assessment is the process of identifying, analyzing, and evaluating risks that may affect the achievement of organizational objectives. Risk assessment involves assessing the likelihood and impact of risks to determine the appropriate response strategies to mitigate or exploit them.

13. Sarbanes-Oxley Act (SOX)
The Sarbanes-Oxley Act (SOX) is a U.S. federal law enacted in 2002 to protect investors by improving the accuracy and reliability of corporate disclosures. SOX requires public companies to establish and maintain effective internal controls over financial reporting and enhance transparency and accountability in corporate governance.

14. Segregation of Duties
Segregation of duties is a fundamental internal control principle that involves dividing responsibilities among different individuals to prevent fraud and errors. Segregation of duties ensures that no single individual has control over all aspects of a transaction, reducing the risk of misappropriation.

15. Whistleblower Policy
A whistleblower policy is a set of procedures established by an organization to encourage employees to report misconduct, fraud, or unethical behavior without fear of retaliation. Whistleblower policies protect whistleblowers and promote transparency, accountability, and ethical conduct within the organization.

16. Audit Evidence

Audit evidence is the information gathered by auditors during the audit process to support their findings and conclusions. Audit evidence includes documents, records, observations, inquiries, and analytical procedures used to assess the reliability of financial information and internal controls.

17. Code of Conduct
A code of conduct is a set of ethical principles and guidelines that govern the behavior and actions of individuals within an organization. A code of conduct outlines expected standards of behavior, integrity, professionalism, and compliance with laws and regulations.

18. Compliance Risk
Compliance risk refers to the risk of legal or regulatory sanctions, financial loss, or reputational damage arising from non-compliance with laws, regulations, policies, or industry standards. Compliance risk management involves identifying, assessing, and mitigating risks to ensure adherence to legal and regulatory requirements.

19. Fraud Risk
Fraud risk is the risk of intentional deception or misrepresentation that results in financial loss, reputational damage, or legal consequences for an organization. Fraud risk management involves implementing controls, monitoring activities, and investigating suspicious behavior to prevent and detect fraud.

20. Information Technology (IT) Controls
Information technology (IT) controls are specific controls implemented to safeguard information systems, data, and technology infrastructure from unauthorized access, manipulation, or destruction. IT controls ensure the confidentiality, integrity, and availability of information assets to support business operations.

21. Risk Appetite
Risk appetite is the level of risk that an organization is willing to accept in pursuit of its strategic objectives. Risk appetite defines the boundaries within which management is comfortable taking risks and guides decision-making processes to achieve a balance between risk and reward.

22. Risk Management Framework
A risk management framework is a structured approach to identifying, assessing, mitigating, and monitoring risks across an organization. The risk management framework establishes the processes, tools, and methodologies for managing risks effectively and aligning risk management practices with strategic objectives.

23. Segregation of Duties (SoD) Matrix
A segregation of duties (SoD) matrix is a tool used to document and analyze the assignment of responsibilities within an organization to prevent conflicts of interest and fraud. The SoD matrix identifies critical control points, assigns roles and responsibilities, and ensures proper segregation of duties to enhance internal controls.

24. Stakeholder Engagement
Stakeholder engagement is the process of involving internal and external stakeholders in decision-making,

planning, and implementation processes to address their interests, concerns, and expectations. Effective stakeholder engagement fosters trust, collaboration, and transparency in governance and compliance activities.

25. Tone at the Top
Tone at the top refers to the ethical climate set by senior management and the board of directors within an organization. The tone at the top influences the organization's culture, values, and behavior, setting the standard for ethical conduct, compliance, and accountability at all levels.

26. Audit Trail
An audit trail is a chronological record of activities, transactions, and events that provides a documented history of changes and actions taken within a system or process. Audit trails are used to trace and verify information, detect errors, and investigate discrepancies for auditing and compliance purposes.

27. Business Continuity Planning (BCP)
Business continuity planning (BCP) is the process of developing strategies and procedures to ensure the continued operation of critical business functions during and after disruptions, such as natural disasters, cyber-attacks, or other emergencies. BCP aims to minimize downtime, protect assets, and maintain business resilience.

28. Control Self-Assessment (CSA)
Control self-assessment (CSA) is a process that involves employees assessing and evaluating the effectiveness of internal controls within their own areas of responsibility. CSA empowers employees to identify control weaknesses, gaps, and opportunities for improvement to enhance overall control environment and compliance.

29. Fraud Triangle
The fraud triangle is a model that explains the factors contributing to fraudulent behavior, including pressure, opportunity, and rationalization. According to the fraud triangle, individuals are more likely to commit fraud when they face financial pressures, have the opportunity to exploit weaknesses, and justify their actions morally.

30. Internal Control Framework
An internal control framework is a structured set of guidelines, principles, and standards established to design, implement, and assess internal controls within an organization. Internal control frameworks provide a systematic approach to managing risks, ensuring compliance, and achieving operational effectiveness.

31. Risk Mitigation
Risk mitigation is the process of reducing, avoiding, or transferring risks to minimize their potential impact on organizational objectives. Risk mitigation strategies may involve implementing controls, insurance, diversification, contingency planning, or other measures to manage risks effectively and protect the organization.

32. Sarbanes-Oxley Compliance

Sarbanes-Oxley compliance refers to the adherence to the requirements of the Sarbanes-Oxley Act (SOX) in establishing and maintaining effective internal controls over financial reporting. Sarbanes-Oxley compliance aims to enhance transparency, accountability, and integrity in financial reporting to protect investors and stakeholders.

33. Segregation of Duties (SoD) Policy
A segregation of duties (SoD) policy is a formal document that outlines the principles, rules, and procedures for assigning and segregating responsibilities within an organization. The SoD policy defines roles, access rights, and control mechanisms to prevent conflicts of interest, fraud, and errors in critical business processes.

34. Stakeholder Analysis
Stakeholder analysis is a systematic process of identifying, assessing, and prioritizing stakeholders based on their interests, influence, and impact on organizational decisions and activities. Stakeholder analysis helps organizations understand stakeholder needs, expectations, and relationships to effectively engage and manage stakeholders.

35. Training and Awareness Programs
Training and awareness programs are initiatives designed to educate employees, stakeholders, and partners about policies, procedures, and practices related to governance, compliance, and internal controls. Training programs enhance knowledge, skills, and awareness to promote ethical behavior, regulatory compliance, and risk management.

36. Audit Findings
Audit findings are the results of audit procedures and examinations that identify deficiencies, errors, weaknesses, or non-compliance with established criteria. Audit findings are documented in audit reports and communicated to management for corrective action, improvement, and resolution of issues identified during the audit.

37. Compliance Management System
A compliance management system is a structured framework of policies, processes, and controls established to ensure adherence to legal, regulatory, and ethical standards within an organization. A compliance management system aims to identify, assess, mitigate, and monitor compliance risks to prevent violations and promote ethical conduct.

38. Fraud Detection
Fraud detection is the process of identifying and investigating suspicious activities, transactions, or behaviors that indicate potential fraud within an organization. Fraud detection tools, techniques, and analytics are used to detect anomalies, patterns, and red flags that may signal fraudulent activities requiring further examination.

39. Internal Control Assessment
Internal control assessment is the evaluation of the design and operating effectiveness of internal controls within an organization to ensure compliance, risk mitigation, and operational efficiency. Internal control

assessments involve testing controls, identifying deficiencies, and making recommendations for improvement to enhance control environment.

40. Risk Register
A risk register is a documented list of identified risks, their likelihood, impact, and potential response strategies to manage risks effectively. A risk register provides a comprehensive view of risks facing an organization, facilitates risk assessment, prioritization, and monitoring, and guides risk management decisions and actions.

41. Segregation of Duties (SoD) Analysis
A segregation of duties (SoD) analysis is a detailed examination of roles, responsibilities, and access privileges within an organization to identify conflicts of interest, fraud risks, and control weaknesses. SoD analysis assesses the segregation of duties, identifies control gaps, and recommends corrective actions to strengthen internal controls.

42. Stakeholder Communication
Stakeholder communication is the process of exchanging information, feedback, and updates with internal and external stakeholders to ensure alignment, engagement, and transparency in decision-making processes. Effective stakeholder communication builds trust, fosters collaboration, and promotes shared understanding of goals, risks, and performance.

43. Audit Program
An audit program is a detailed plan outlining the audit procedures, objectives, scope, resources, and timeline for conducting an audit engagement. The audit program serves as a roadmap for auditors to follow, ensuring that all key areas are covered, risks are addressed, and objectives are achieved during the audit.

44. Compliance Monitoring
Compliance monitoring is the ongoing process of tracking, assessing, and verifying adherence to legal, regulatory, and internal policies within an organization. Compliance monitoring involves surveillance, reporting, and analysis of compliance activities to ensure that controls are operating effectively, risks are managed, and violations are detected and addressed.

45. Fraud Prevention
Fraud prevention refers to the proactive measures, controls, and strategies implemented to deter, detect, and mitigate fraudulent activities within an organization. Fraud prevention measures include segregation of duties, internal controls, employee training, ethical standards, and monitoring activities to minimize fraud risks and protect organizational assets.

46. Internal Control Review
Internal control review is the process of evaluating the effectiveness, efficiency, and reliability of internal controls within an organization to ensure compliance, risk mitigation, and operational effectiveness. Internal control reviews assess control design, implementation, and monitoring to identify weaknesses, gaps, and opportunities for improvement.

47. Risk Assessment Matrix
A risk assessment matrix is a tool used to categorize and prioritize risks based on their likelihood and impact on organizational objectives. A risk assessment matrix helps organizations identify high-priority risks, allocate resources, and develop risk response strategies to manage risks effectively and enhance decision-making processes.

48. Segregation of Duties (SoD) Report
A segregation of duties (SoD) report is a document that summarizes the findings, recommendations, and actions related to the segregation of duties within an organization. The SoD report provides insights into control weaknesses, conflicts of interest, and fraud risks identified through SoD analysis and suggests remedial measures to strengthen internal controls.

49. Stakeholder Engagement Plan
A stakeholder engagement plan is a strategic document outlining the objectives, strategies, and activities for engaging stakeholders in governance, compliance, and decision-making processes. A stakeholder engagement plan defines communication channels, responsibilities, and timelines to foster collaboration, participation, and mutual understanding with stakeholders.

50. Audit Sampling
Audit sampling is the process of selecting a representative sample of transactions, data, or activities to test the effectiveness of controls, identify errors, or assess compliance with established criteria. Audit sampling helps auditors draw conclusions about the population being audited based on the results obtained from the sample.

51. Compliance Reporting
Compliance reporting involves documenting and communicating the results of compliance assessments, monitoring activities, and control testing to management, stakeholders, and regulatory authorities. Compliance reports provide insights into compliance status, control effectiveness, and areas of non-compliance requiring corrective action to improve governance and risk management.

52. Fraud Risk Assessment
Fraud risk assessment is the process of identifying, analyzing, and evaluating fraud risks that may impact an organization's operations, financial integrity, and reputation. Fraud risk assessments help organizations understand fraud vulnerabilities, prioritize controls, and develop prevention and detection strategies to mitigate fraud risks effectively.

53. Internal Control System
An internal control system is the framework of policies, procedures, and practices established by management to ensure the achievement of organizational objectives, compliance with laws and regulations, and protection of assets. An internal control system aims to safeguard resources, mitigate risks, and enhance operational efficiency and effectiveness.

54. Risk Identification
Risk identification is the process of recognizing, documenting, and categorizing potential risks that may

affect organizational objectives, projects, or operations. Risk identification involves brainstorming, data analysis, scenario planning, and expert judgment to identify internal and external risks that require assessment, prioritization, and response planning.

55. Sarbanes-Oxley (SOX) Compliance Program
A Sarbanes-Oxley (SOX) compliance program is a structured set of policies, procedures, and controls established by public companies to comply with the requirements of the Sarbanes-Oxley Act. SOX compliance programs ensure the integrity of financial reporting, enhance transparency, and strengthen internal controls to protect investors and stakeholders.

56. Segregation of Duties (SoD) Tool
A segregation of duties (SoD) tool is a software application or system used to automate, monitor, and manage the segregation of duties within an organization. SoD tools help organizations identify control conflicts, assign roles, and enforce separation of duties to prevent fraud, errors, and unauthorized activities in critical business processes.

57. Stakeholder Mapping
Stakeholder mapping is a technique used to identify, analyze, and visualize the relationships, interests, and influence of stakeholders within an organization. Stakeholder mapping helps organizations understand stakeholder dynamics, prioritize engagement strategies, and align communication efforts to build positive relationships and support governance initiatives.

58. Audit Sampling Method
Audit sampling method refers to the approach used to select and evaluate a sample of transactions, data, or activities during an audit engagement. Audit sampling methods include statistical sampling, judgmental sampling, and random sampling techniques to assess the effectiveness of controls, detect errors, and provide reasonable assurance in audit findings.

59. Compliance Risk Assessment
Compliance risk assessment is the process of evaluating and prioritizing compliance risks that may impact an organization's ability to meet legal, regulatory, and industry standards. Compliance risk assessments help organizations identify compliance gaps, assess control effectiveness, and develop mitigation strategies to ensure adherence to laws and regulations.

60. Fraud Risk Management
Fraud risk management is the systematic process of identifying, assessing, mitigating, and monitoring fraud risks within an organization to prevent financial loss, reputational damage, and legal consequences. Fraud risk management involves implementing controls, training programs, investigations, and fraud detection tools to detect and deter fraudulent activities.

61. Internal Control Testing
Internal control testing is the process of evaluating the design and operating effectiveness of internal controls within an organization to ensure compliance, risk mitigation, and operational efficiency. Internal control testing involves assessing control activities, sampling transactions, and documenting results to

provide assurance on control reliability and effectiveness.

62. Risk Assessment Process
Risk assessment process is the systematic approach of identifying, analyzing, and evaluating risks that may impact an