Global Information Security Society for Professionals of Pakistan

Certified Information System Auditor-CISA

Trainer: Ali Nouman

How to use Zoom Client

If you are using Zoom for the first time than these points will be useful for you .

- If you are unable to hear audio than you need to connect via device audio . Look at the bottom left corner .
- Kindly turn off your camera while connecting to Zoom as we respect your privacy .
- The Speaker will keep you muted during the session however if you want to ask any question during QA session ,you can click on the three dots and “raise hand” so that the speaker can unmute you .
- You can click on the participants tab to chat with host or to send a member to all participants
- If you are attending the session while doing some other work ,kindly mute yourself in case if the host unmutes all users during QA session

Trainer Profile

- Ali Nouman is Working as Manager IT Security in one of the top Bank, based in Qatar. Over 15 years of IT experience and focus on Information Security for the last 10 years. He is CISA, CISSP, CISM, COBIT-5, IRCA registered Lead Auditor of ISO ISMS, AWS and ITIL certified as well as founding member of (ISC)² Qatar Chapter. He is visiting faculty member and CISA Trainer at SKANS, ISACA Lahore Chapter and Audit General of Pakistan, He has previously worked in Teradata, ABL, BOP and Samba Bank. He is a Corporate trainer of different area of information security, governance and CISA. LinkedIn :
- https://www.linkedin.com/in/ali-nouman-cissp-aws-cisa-cism-isms-itil-ba3a8225/

Welcome!

- This program is designed to prepare you for success on the CISA exam, one step in the process of becoming certified.
- The program will include:
  - Information about the CISA exam and certification
  - Detailed coverage of the body of knowledge required by CISA
  - Activities, exam discussion questions, and group discussions
  - Real-world examples of CISA subject matter

Domain 1

The Process of Auditing Information Systems

Domain 1

The Process of Auditing Information Systems

Discussion Question-1

Due to resource constraints of the IS audit team, the audit plan as originally approved cannot be completed. Assuming that the situation is communicated in the audit report, which course of action is **MOST** acceptable?

A. Test the adequacy of the control design.
B. Test the operational effectiveness of controls.
C. Focus on auditing high-risk areas.
D. Rely on management testing of controls

Domain 1

The Process of Auditing Information Systems

Discussion Question-2

Although management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should **FIRST**:

A. include the statement from management in the audit report.
B. verify the software is in use through testing.
C. include the item in the audit report.
D. discuss the issue with senior management because it could have a negative impact on the organization.

Domain 1

The Process of Auditing Information Systems: Task 1

Task 1.2:

Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.

Domain 1

The Process of Auditing Information Systems: Task 1

Key Terms

Key Term	Definition
Audit plan	A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion; includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work and topics such as budget, resource allocation, schedule dates, type of report and its intended audience, and other general aspects of the work
Audit risk	The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred

Domain 1

The Process of Auditing Information Systems: Task 1

Key Terms

Key Term	Definition
Audit universe	An inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process
Reasonable assurance	A level of comfort short of a guarantee but considered adequate given the costs of the control and the likely benefits achieved

Domain 1

The Process of Auditing Information Systems: Task 1

Audit Planning

The first step in performing an IS audit is satisfactory planning.

To plan an audit, the following tasks must be completed:

List all the processes that may be considered for the audit.

Evaluate each process by performing a qualitative or quantitative risk assessment. These evaluations should be based on objective criteria.

Define the overall risk of each process.

Construct an audit plan to include all of the processes that are rated “high” which would represent the ideal annual audit plan.

When To Audit

- Audit planning includes short-term and long-term planning.
  - Short-term planning involves all audit issues that will be covered during the year.
  - Long-term planning takes into account all risk-related issues that might be affected by the organization's IT strategic direction.

When To Audit (cont'd)

- In addition to a yearly analysis of short-term and long-term issues, individual audits may be conducted based on the following:
  - New control issues
  - Changes in risk environment, technologies and business processes
  - Enhanced evaluation techniques

Audit Planning Steps

- In order to plan an audit, the IS auditor must have an understanding of the overall environment under review. To accomplish this task, the IS auditor should:
  - Gain an understanding of the business's mission, objectives, purpose and processes.
  - Understand changes in business environment of the auditee.
  - Review prior work papers.
  - Identify stated contents, such as policies, standards and required guidelines, procedures and organization structure.

Audit Planning Steps (cont'd)

- Also, to plan for an audit, the IS auditor should:
  - Perform a risk analysis to help in designing the audit plan.
  - Set the audit scope and audit objectives.
  - Develop the audit approach or audit strategy.
  - Assign personnel resources to the audit.
  - Address engagement logistics.

Additional Considerations

- The audit plan should take into consideration the objectives of the IS audit relevant to the audit area and its technology infrastructure and business strategic direction. The IS auditor can gain this information by:
  - Reading background material, including industry publications, annual reports and independent financial analysis reports
  - Reviewing prior audit reports or IT-related reports (from external or internal audits, or specific reviews such as regulatory reviews)
  - Reviewing business and IT long-term strategic plans

Additional Considerations (cont'd)

- Other ways the IS auditor can gain this information include:
  - Interviewing key managers to understand business issues
  - Identifying specific regulations applicable to IT
  - Identifying IT functions or related activities that have been outsourced
  - Touring key organization facilities
- The IS auditor must also match available audit resources, such as staff, with the tasks defined in the audit plan.

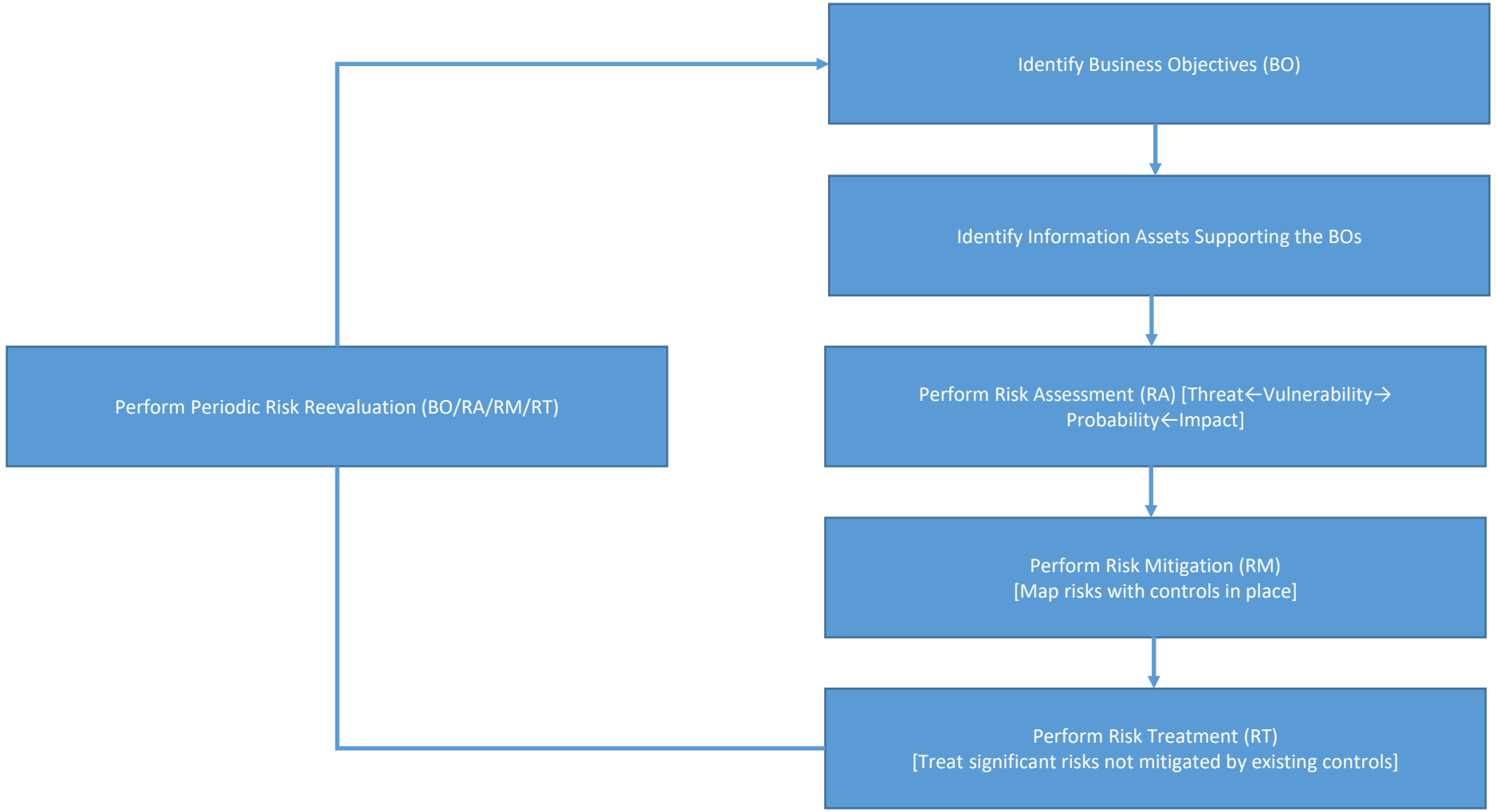
Risk Analysis

- During audit planning, the IS auditor must perform or review a risk analysis to identify risks and vulnerabilities in order to determine the controls needed to mitigate those risks.
- The IS auditor's role is to:
  - Understand the relationship between risk and control.
  - Identify and differentiate risk types and the controls used to mitigate the risk.
  - Evaluate risk assessment and management techniques used by the organization.
  - Understand that risk exists as part of the audit process.

Risk Analysis (cont'd)

- IS auditors are often focused on high-risk issues associated with confidentiality, integrity and availability of sensitive and critical information.

Risk Management Process



Risk Response

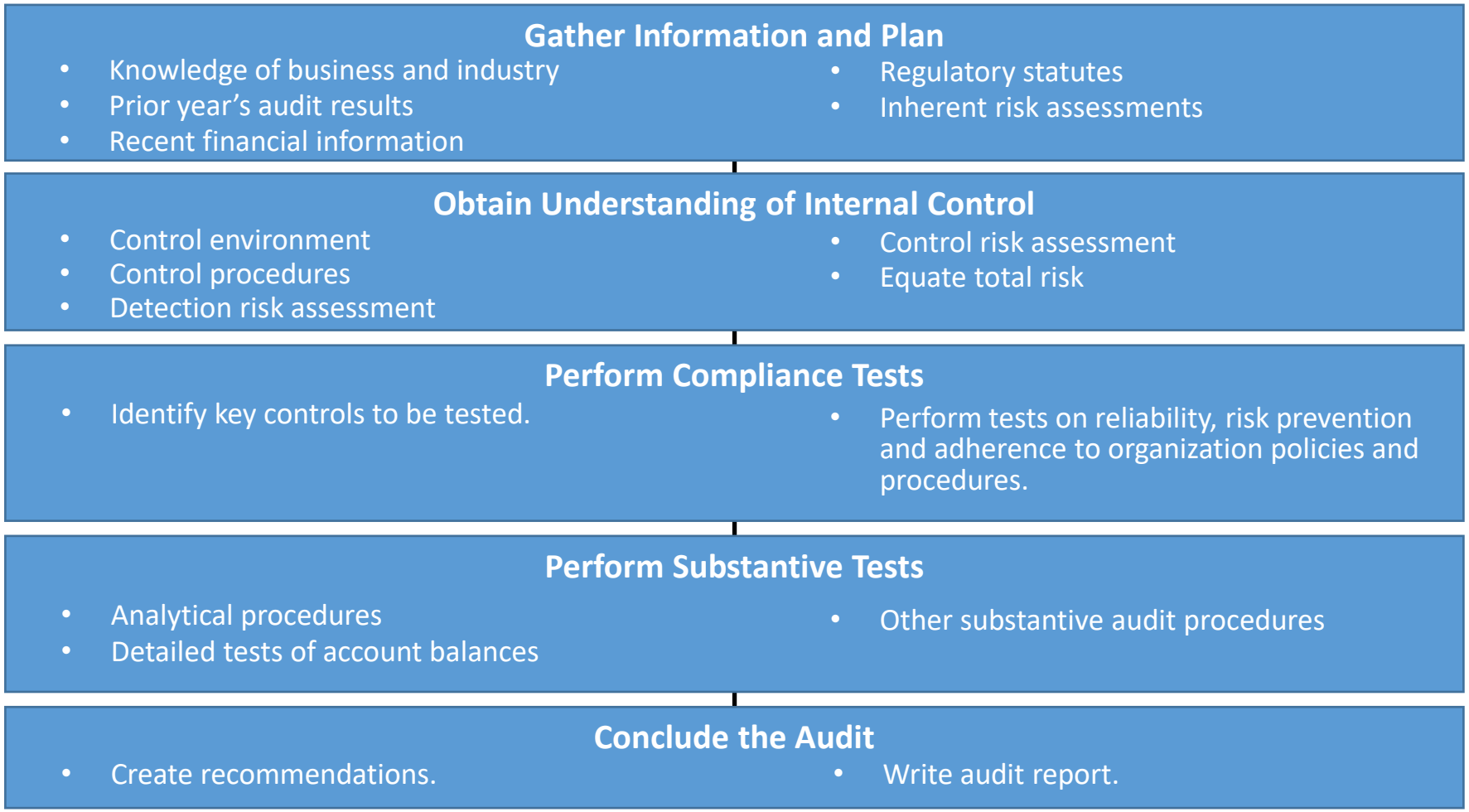
Risk Response Options

- **Risk mitigation** – Applying appropriate controls to reduce the risk
- **Risk acceptance** – Knowingly and objectively not taking action, providing the risk clearly satisfies the organization's policy and criteria for risk acceptance
- **Risk avoidance** – Avoiding risk by not allowing actions that would cause the risk to occur
- **Risk transfer/sharing** – Transferring the associated risk to other parties

Risk Assessment

- A risk assessment assists the IS auditor in identifying risk and threats to an IT environment and IS system, and it helps in the evaluation of controls.
- Risk assessments should identify, quantify and prioritize risk against criteria for risk acceptance and objectives relevant to the organization.
- It supports risk-based audit decision making by considering variables, such as:
  - Technical complexity
  - Level of control procedures in place
  - Level of financial loss

Risk-based Auditing



Internal Controls

- Internal controls are normally composed of policies, procedures, practices and organizational structures that are implemented to reduce risk to the organization.
- Internal controls should address:
  - What should be achieved?
  - What should be avoided?

Control Classification

Class	Function
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors).
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.

Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.5

IS Control Objectives

- IS control objectives are statements of the desired result achieved by implementing controls. They provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented, detected or corrected.

IS Control Objectives (cont'd)

- IS control objectives may also include:
  - Safeguarding assets
  - System development life cycle (SDLC) processes are established, in place and operating effectively
  - Integrity of general operating system (OS) environments
  - Integrity of sensitive and critical application system environments
  - Appropriate identification and authentication of users
  - The efficiency and effectiveness of operations
  - Integrity and reliability of systems by implementing effective change management procedures

General Controls

General controls include:

- Internal accounting controls that concern the safeguarding of assets and reliability of financial information
- Operational controls that concern day-to-day operations, functions and activities
- Administrative controls that concern operational efficiency in a functional area and adherence to management policies
- Organizational security policies and procedures to ensure proper usage of assets
- Overall policies for the design and use of adequate documents and records
- Access and use procedures and practices
- Physical and logical security policies for all facilities

IS Specific Controls

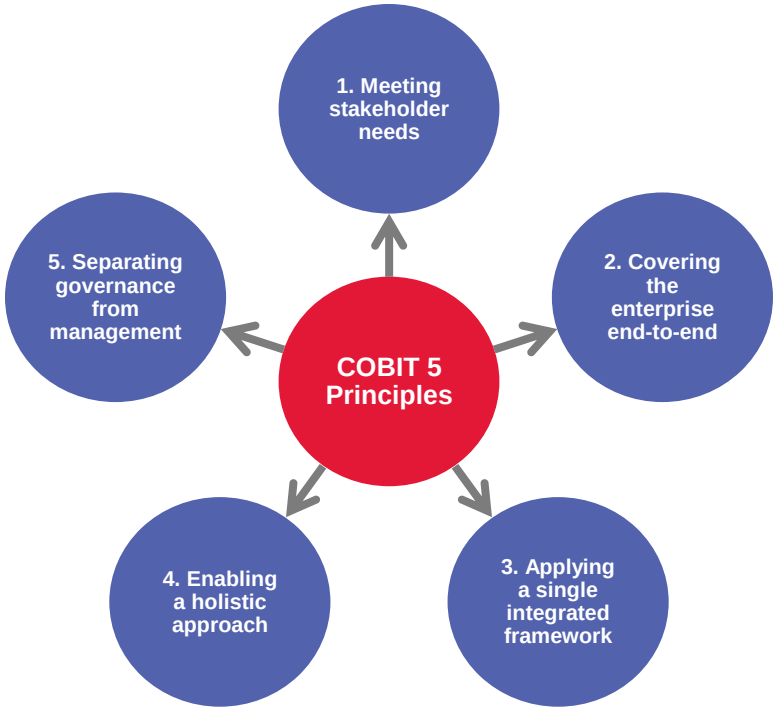
- Each general control can be translated into an IS-specific control. The IS auditor should understand IS controls and how to apply them in planning an audit.
- IS control procedures include:
  - Strategy and direction of the IT function
  - General organization and management of the IT function
  - Access to IT resources, including data and programs
  - Systems development methodologies and change control

IS Specific Controls (cont'd)

- Additional IS control procedures include:
  - Operations procedures
  - Systems programming and technical support functions
  - Quality assurance (QA) procedures
  - Physical access controls
  - Business continuity planning (BCP)/disaster recovery planning (DRP)
  - Networks and communications
  - Database administration
  - Protection and detective mechanisms against internal and external attacks

COBIT 5

- ISACA's COBIT 5 provides a comprehensive framework for governance and management of enterprise IT. It helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.



Source: ISACA, COBIT 5, USA, 2012, figure 2

Types of Audits

Type	Description
Compliance audits	Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. Examples include Payment Card Industry Data Security Standard (PCI DSS) audits for companies that process credit card data and Health Insurance Portability and Accountability Act (HIPAA) audits for companies that handle health care data.
Financial audits	The purpose of a financial audit is to assess the accuracy of financial reporting. It often involves detailed, substantive testing, although increasingly, auditors are placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.

Types of Audits (cont'd)

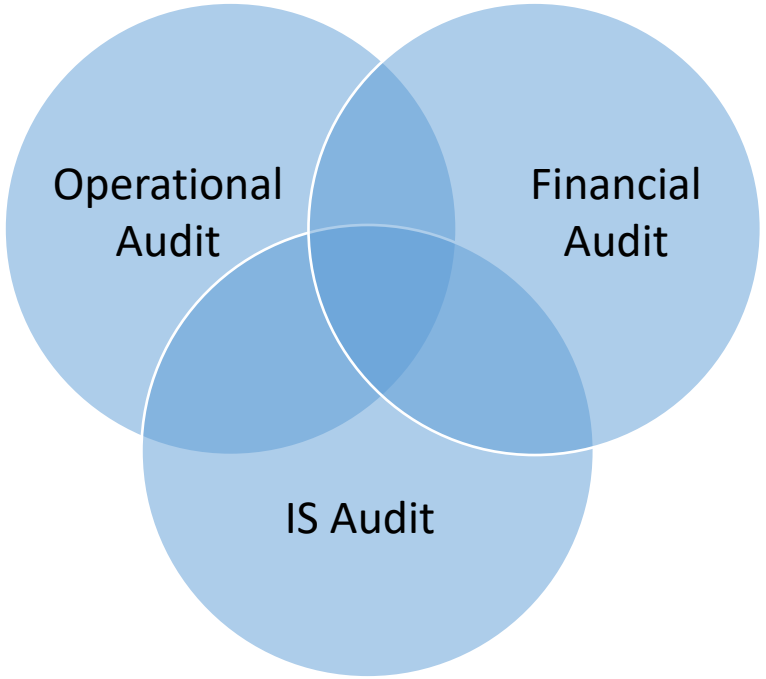
Type	Description
Operational audits	An operational audit is designed to evaluate the internal control structure in a given process or area. Examples include IS audits of application controls or logical security systems.
Administrative audits	These are oriented to assess issues related to the efficiency of operational productivity within an organization.
IS audits	This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, and consume resources efficiently. Also, do they have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner.

Types of Audits (cont'd)

Type	Description
Forensic audits	Forensic auditing has been defined as auditing specialized in discovering, disclosing and following up on fraud and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities.
Integrated audits	An integrated audit combines financial and operational audit steps. It is performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance.

Integrated Audit

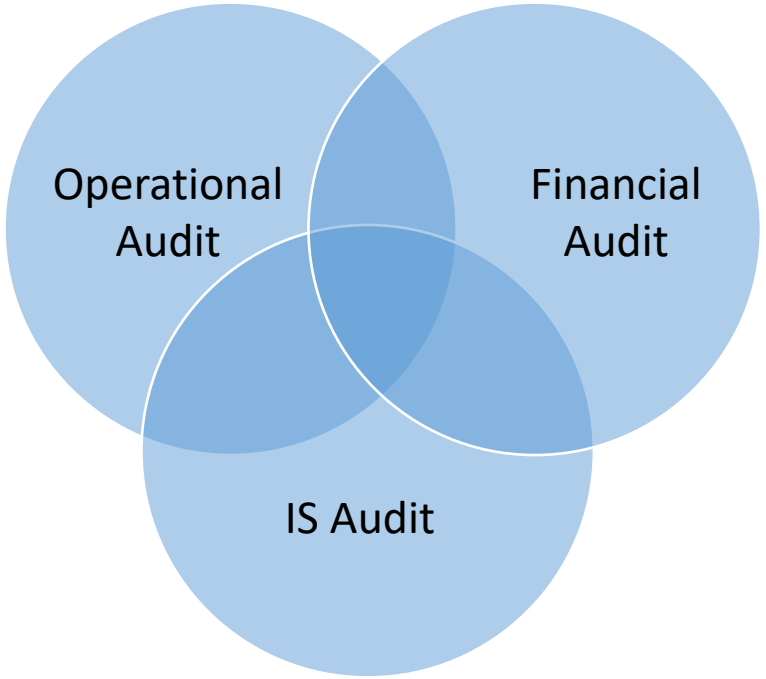
- An integrated audit focuses on risk. It involves a team of auditors with different skill sets working together to provide a comprehensive report.



Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.13

Integrated Audit (cont'd)

- The process typically involves:
  - Identification of risk faced by the organization for the area being audited
  - Identification of relevant key controls
  - Review and understanding of the design of key controls
  - Testing that key controls are supported by the IT system
  - Testing that management controls operate effectively
  - A combined report or opinion on control risk, design and weaknesses



Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.13

Continuous Auditing

- Continuous auditing is characterized by the short time lapse between the audit, the collection of evidence and the audit reporting.
- It results in better monitoring of financial issues, such as fraud, ensuring that real-time transactions benefit from real-time monitoring.
- Continuous auditing should be independent of continuous controls and continuous monitoring.

Continuous Auditing (cont'd)

- This process must be carefully built into the business applications and may include IT techniques such as:
  - Transaction logging
  - Query tools
  - Statistics and data analysis (CAAT)
  - Database management systems (DBMS)
  - Intelligent agents

Continuous Auditing (cont'd)

- For continuous auditing to succeed, it needs to have:
  - A high degree of automation.
  - Alarm triggers to report timely control failures.
  - Implementation of highly automated audit tools that require the IS auditor to be involved in setting up the parameters.
  - The ability to quickly inform IS auditors of the results of automated procedures, particularly when the process has identified anomalies or errors.
  - Quick and timely issuance of automated audit reports.
  - Technically proficient IS auditors.
  - Availability of reliable sources of evidence.
  - Adherence to materiality guidelines.

Audit Methodology

- An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit programs.
- Each audit department should design and approve an audit methodology that is formalized and communicated to all audit staff.
- An audit program should be developed to serve as a guide for performing and documenting all of the audit steps, and the extent and types of evidential matter reviewed.

Audit Phases

Audit Phase	Description
Audit subject	• Identify the area to be audited.
Audit objective	• Identify the purpose of the audit.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review, such as functional flow charts, policies, standards, procedures and prior audit work papers. • Identify locations or facilities to be audited. • Develop a communication plan at the beginning of each engagement that describes who to communicate to, when, how often and for what purpose(s).

Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.7

Audit Phases (cont'd)

Audit Phase	Description
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	• Identify methods (including tools) to perform the evaluation. • Identify criteria for evaluating the test (similar to a test script for the IS auditor to use in conducting the evaluation). • Identify means and resources to confirm the evaluation was accurate (and repeatable, if applicable).

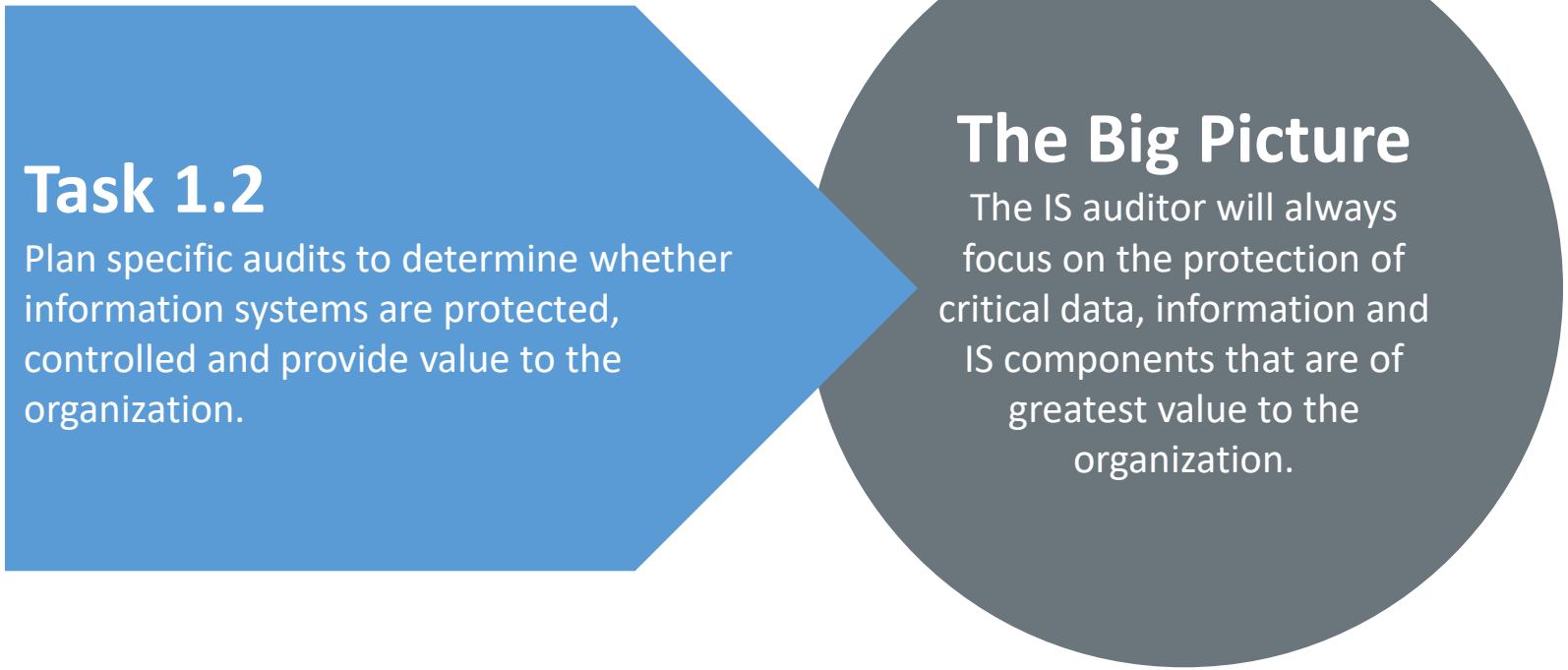
Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.7

Audit Phases (cont'd)

Audit Phase	Description
Procedures for communication with management	• Determine frequency of communication. • Prepare documentation for final report.
Audit report preparation	• Disclose follow-up review procedures. • Disclose procedures to evaluate/test operational efficiency and effectiveness. • Disclose procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

Source: ISACA, *CISA Review Manual 26th Edition*, figure 1.7

In the Big Picture



GISSP

THANK YOU!

Certified Information System Auditor-CISA

Trainer: Ali Nouman