CS4050 – WEEK2: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

DOMAIN 1: INFORMATION SYSTEMS AUDITING PROCESS

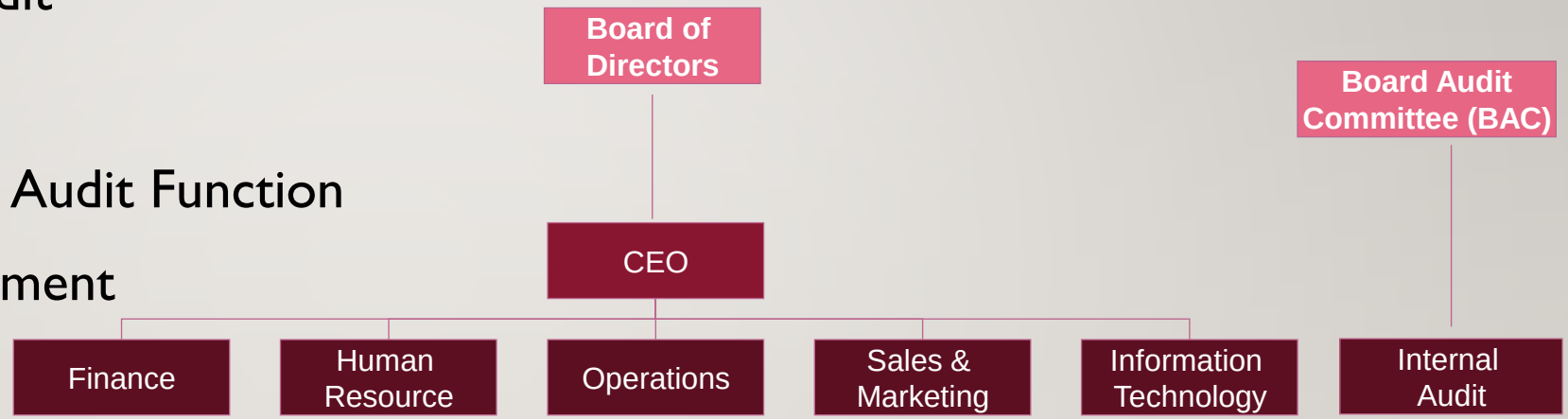
- **Part A: PLANNING**
  - 1.1 IS Audit Standards, Guidelines and Codes of Ethics
  - 1.2 Business Processes
  - 1.3 Types of Controls
  - 1.4 Risk-based Audit Planning
  - 1.5 Types of Audits and Assessments
- **Part B: EXCEUTION**
  - 1.6 Audit Project Management
  - 1.7 Sampling Methodology
  - 1.8 Audit Evidence Collection Techniques
  - 1.9 Data Analytics
  - 1.10 Reporting and Communication Techniques
  - 1.11 Quality Assurance and Improvement of the Audit Process

INFORMATION SYSTEMS AUDIT

- Information Systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines
- Information Systems and related processes comply with governance criteria and related and relevant policies and procedures
- Data and information have appropriate levels of confidentiality, integrity and availability
- IS operations are being accomplished efficiently and effectiveness targets are being met

INTERNAL AUDIT FUNCTION

- Role of IS Internal Audit
  - Audit Charter
- Management of the IS Audit Function
  - Resource Management
- IS Audit Planning
  - Audit Universe
  - Risk Assessment
  - Risk Rating
  - Risk-based Audit Plan

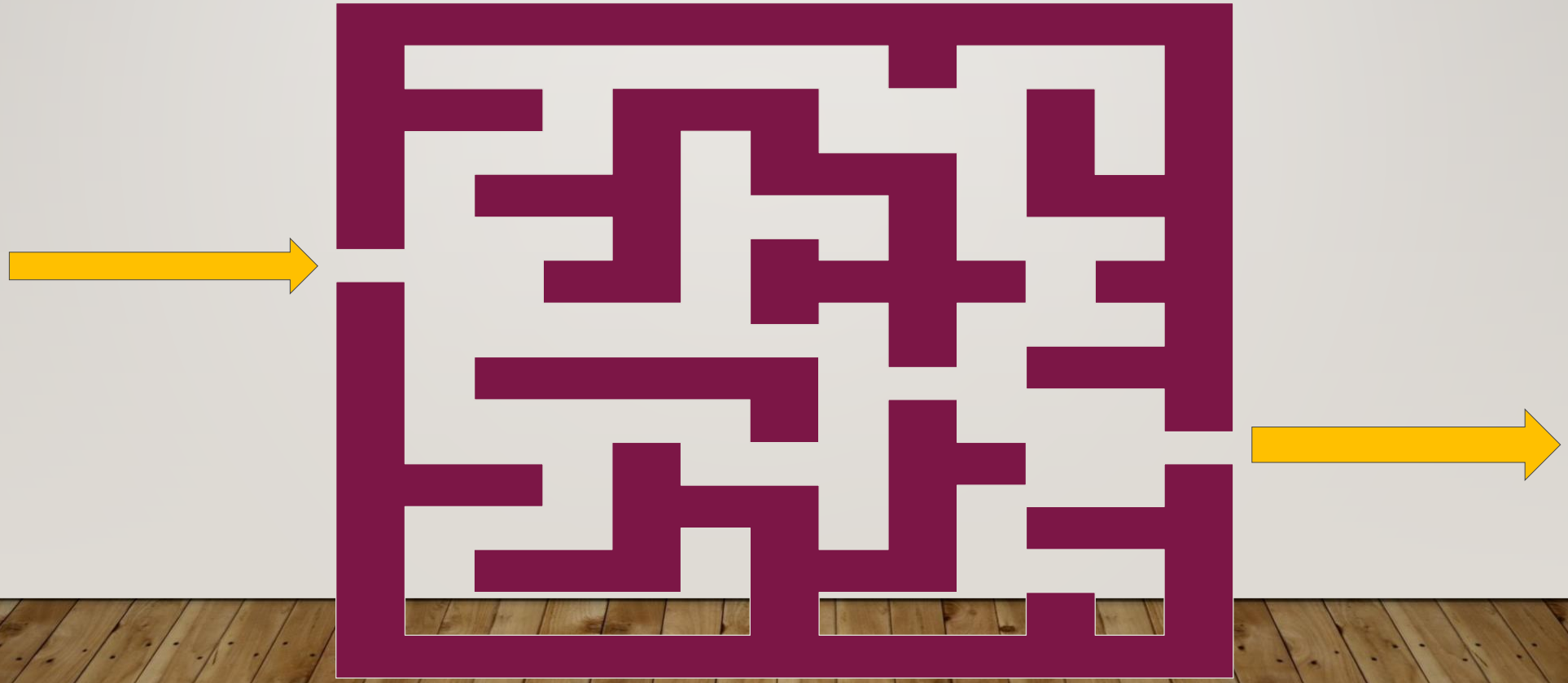


1.1 - IS AUDIT STANDARDS, GUIDELINES & CODES OF ETHICS

- ISACA IS Audit and Assurance Standards
  - General
  - Performance
  - Reporting
- ISACA IS Audit and Assurance Guidelines
- Code of Professional Ethics
- ITAF

1.2 - BUSINESS PROCESSES

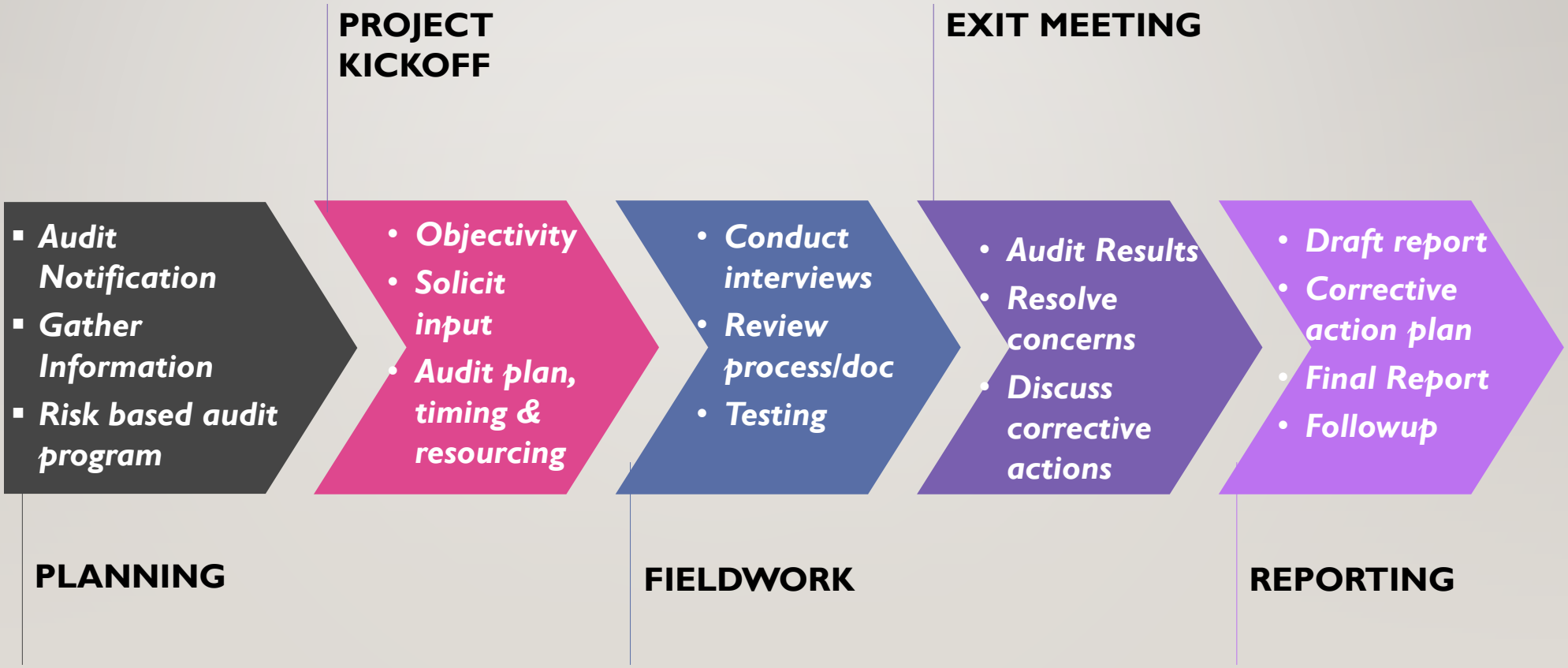
Collection of related, structured activities or tasks by people or equipment in which a specific sequence produces a service or product



Audit Charter

Approved by Top Management and Board	Authority & Responsibility of Audit Function	Static Document

TYPICAL AUDIT PROCESS



AUDIT PLANNING STEPS

- Understand organization's objectives, purpose & processes, including information & processing requirements
- Gain organization's governance structure and practices related to the audit objectives
- Understand changes in the business environment of the auditee
- Review prior work papers
- Identify stated contents such as policies, standards & required guidelines, procedures, and organogram
- 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 and address engagement logistics

EFFECT OF LAWS & REGULATIONS ON IS AUDIT

- Identify government or other relevant external requirements
- Assess whether the management of the organization and the IT function have considered the relevant external requirements in making plans and in setting policies, standards and procedures, as well as business application features.
- Determine adherence to established procedures that address these requirements.
- Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

E-Commerce

- CIA
- Authentication & Non-Repudiation
- Power Shift to Customers

EDI

- Unauthorized Access
- Deletion or Manipulation
- Loss or Duplication

Digital Banking

- Customer Authentication
- Segregation of Duties
- Integrity of Records & Transactions
- Confidentiality
- Maintaining Uptime

EFT & POS

- Personal Identification Number (PIN)
- Personal Account Number (PAN)
- Card Verificatoin Value (CVV)

Integration Manufacturing Systems

- Bill of Materials Processing (BOMP)
- Manufacturing Resource Planning (MRP)
- Computer Assisted Design (CAD)

CONTROL	FUNCTION	EXAMPLES
Preventive	• Identify problems before they arise • Monitor both operation and inputs • Attempt to predict potential problems before they occur and adjust • Prevent an error, omission or malicious act from occurring	• Employing only qualified personnel • Segregation of duties • Controlling access to physical facilities • Suitable procedures for authorization of transactions • Programmed edit checks • Use of access control software that allows only authorized personnel to access sensitive files • Use of encryption software to prevent unauthorized disclosure of data
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act	• Check points in production jobs • Error messages • Duplicate checking of calculations • Periodic performance reporting with variances • Review of activity logs to detect unauthorized access attempts • Secure code reviews • Software quality assurance
Corrective	• Minimize the impact of a threat • Remedy problems discovered by detective controls • Identify the cause of a problem • Modify the processing system(s) to minimize future occurrences of the problem	• Contingency/continuity of operations planning • Disaster recovery planning • Incident response planning • Backup procedures • System break/fix service level agreements

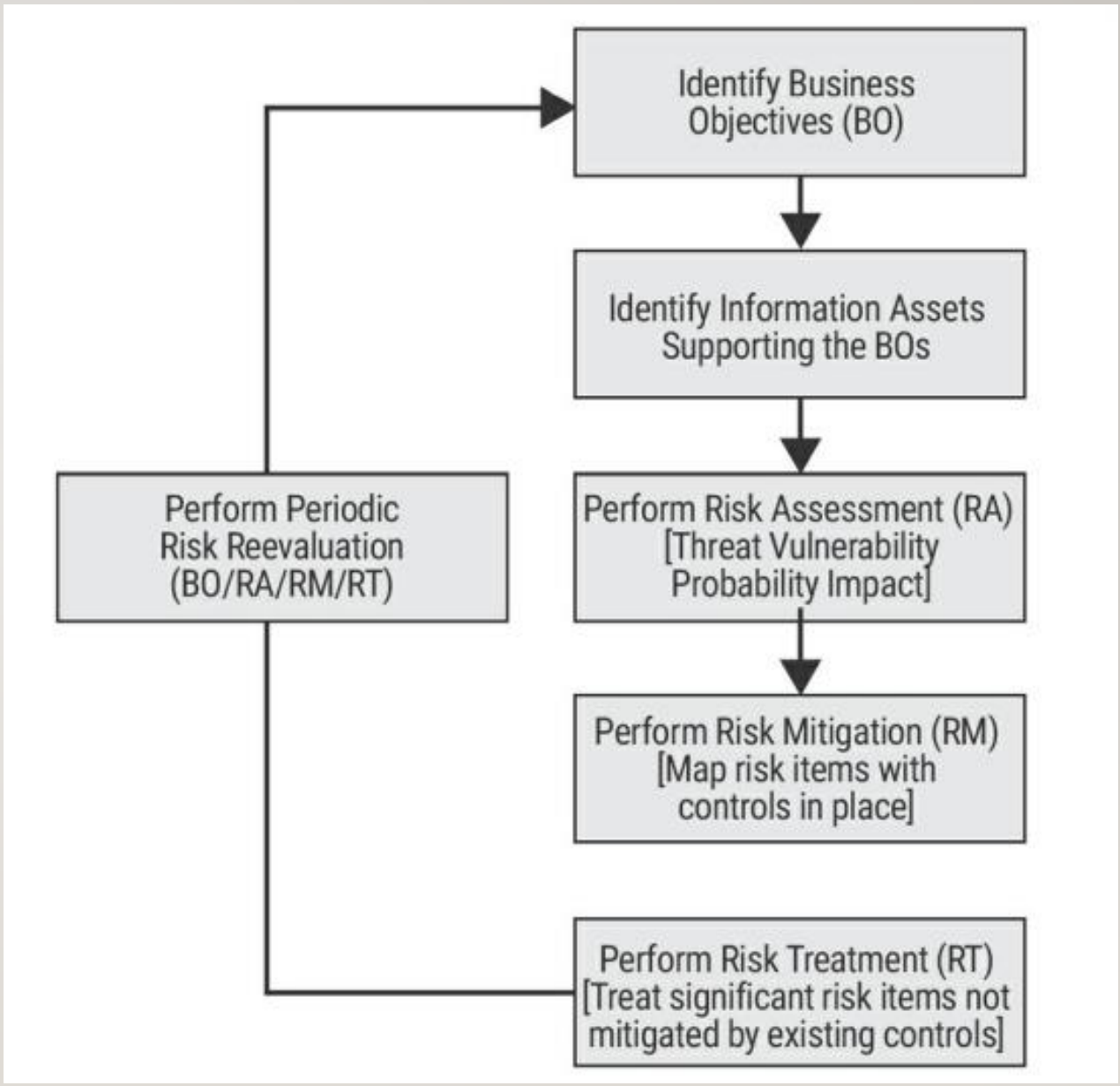
INFORMATION SYSTEMS CONTROLS

- 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
- Operations procedures
- Protection and detective mechanisms against internal and external attacks
- Systems programming and technical support functions
- Quality assurance (QA) procedures
- Physical access controls
- BCP/DRP
- Networks and communication technology (e.g., local area networks, wide area networks, wireless)
- Database administration

RISK BASED AUDIT PLANNING

- Inherent Risk
- Control Risk
- Detection Risk
- Overall Audit Risk

RISK MANAGEMENT PROCESS



TYPES OF AUDITS

- Information Systems Audit
- Compliance Audit
- Financial Audit
- Integrated Audit
- Administrative Audit
- Third-Party Service Audit
- Fraud and Forensic Audit
- Functional Audit

SELF-ASSESSMENT QUESTIONS

1-1 Which of the following outlines the overall authority to perform an IS audit?

A. The audit scope with goals and objectives
B. A request from management to perform an audit
C. The approved audit charter
D. The approved audit schedule

1-1 A. The audit scope is specific to a single audit and does not grant authority to perform an audit.

B. A request from management to perform an audit is not sufficient because it relates to a specific audit.

C. The approved audit charter outlines the auditor's responsibility, authority and accountability.

D. The approved audit schedule does not grant authority to perform an audit.

1-2 In performing a risk-based audit, which risk assessment is completed **FIRST** by an IS auditor?

A. Detection risk assessment
B. Control risk assessment
C. Inherent risk assessment
D. Fraud risk assessment

1-2 A. Detection risk assessment is performed only after the inherent and control risk assessments have been performed to determine ability to detect errors within a targeted process.

B. Control risk assessment is performed after the inherent risk assessment has been completed and is to determine the level of risk that remains after controls for the targeted process are in place.

C. Inherent risk exists independently of an audit and can occur because of the nature of the business. To successfully conduct an audit, it is important to be aware of the related business processes. To perform the audit, an IS auditor needs to understand the business process; by understanding the business process, an IS auditor better understands the inherent risk.

D. Fraud risk assessments are a subset of a control risk assessment in which an audit and assurance professional determines if the control risk addresses the ability of internal and/or external parties to commit fraudulent transactions within the system.

1-3 Which of the following would an IS auditor **MOST** likely focus on when developing a risk-based audit program?

A. Business processes
B. Administrative controls
C. Environmental controls
D. Business strategies

1-3 **A. A risk-based audit approach focuses on the understanding of the nature of the business and being able to identify and categorize risk. Business risk impacts the long-term viability of a specific business. Thus, an IS auditor using a risk-based audit approach must be able to understand business processes.**

B. Administrative controls, while an important subset of controls, are not the primary focus needed to understand the business processes within scope of the audit.

C. Like administrative controls, environmental controls are an important control subset; however, they do not address high-level overarching business processes under review.

D. Business strategies are the drivers for business processes; however, in this case, an IS auditor is focusing on the business processes that were put in place to enable the organization to meet the strategy.

1-4 Which of the following types of audit risk assumes an absence of compensating controls in the area being reviewed?

A. Control risk
B. Detection risk
C. Inherent risk
D. Sampling risk

1-4 A. Control risk is the risk that a material error exists that will not be prevented or detected in a timely manner by the system of internal controls.

B. Detection risk is the risk that a material misstatement with a management assertion will not be detected by an audit and assurance professional's substantive tests. It consists of two components: sampling risk and nonsampling risk.

C. Inherent risk is the risk level or exposure without considering the actions that management has taken or might take.

D. Sampling risk is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is taken. Nonsampling risk is the detection risk not related to sampling; it can be due to a variety of reasons, including, but not limited to, human error.

1-5 An IS auditor performing a review of an application's controls finds a weakness in system software that could materially impact the application. In this situation, an IS auditor should:

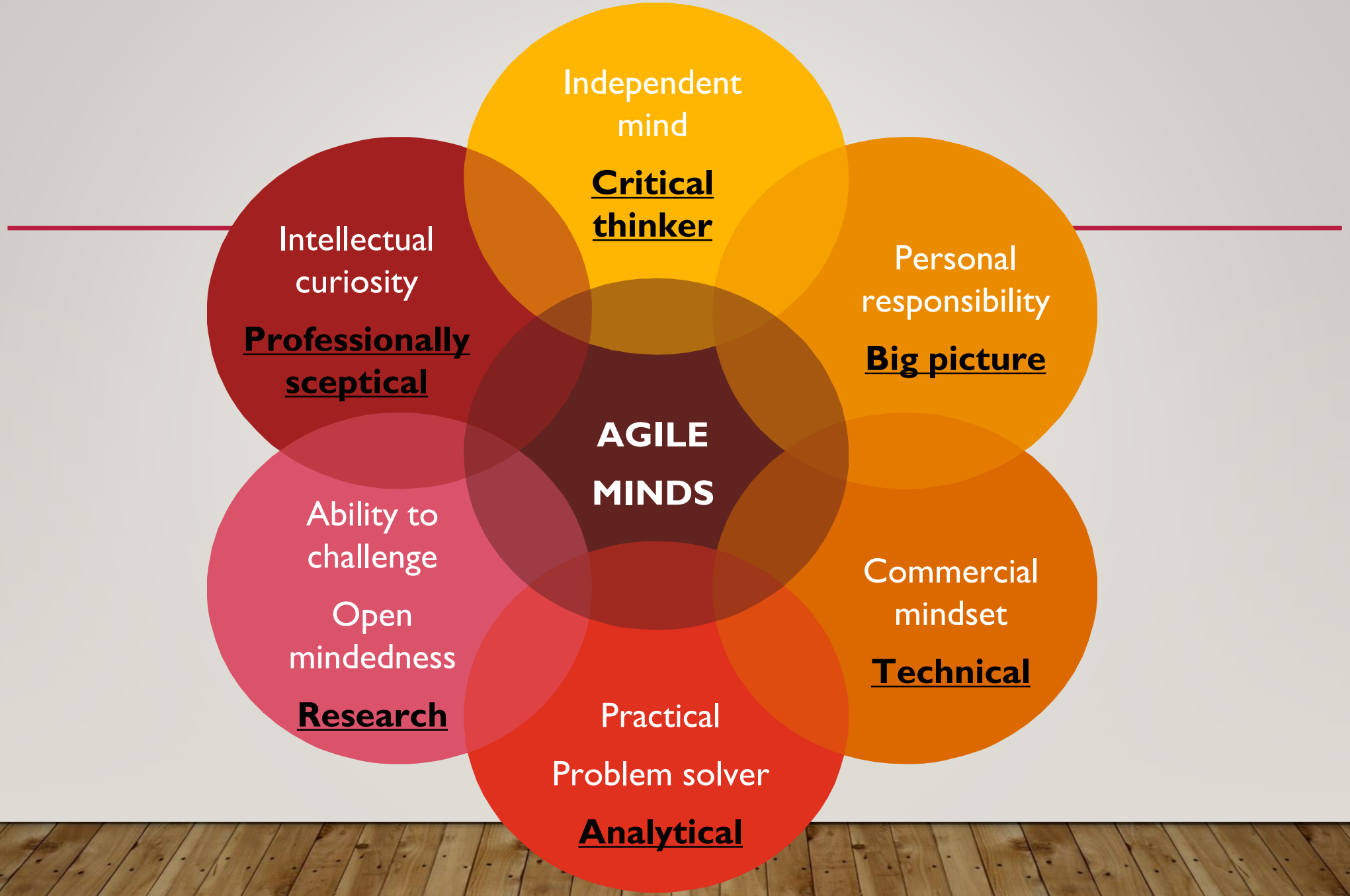
A. Disregard these control weaknesses because a system software review is beyond the scope of this review.
B. Conduct a detailed system software review and report the control weaknesses.
C. Include in the report a statement that the audit was limited to a review of the application's controls.
D. Review the system software controls as relevant and recommend a detailed system software review.

1-5 A. An IS auditor is not expected to ignore control weaknesses just because they are outside the scope of a current review.

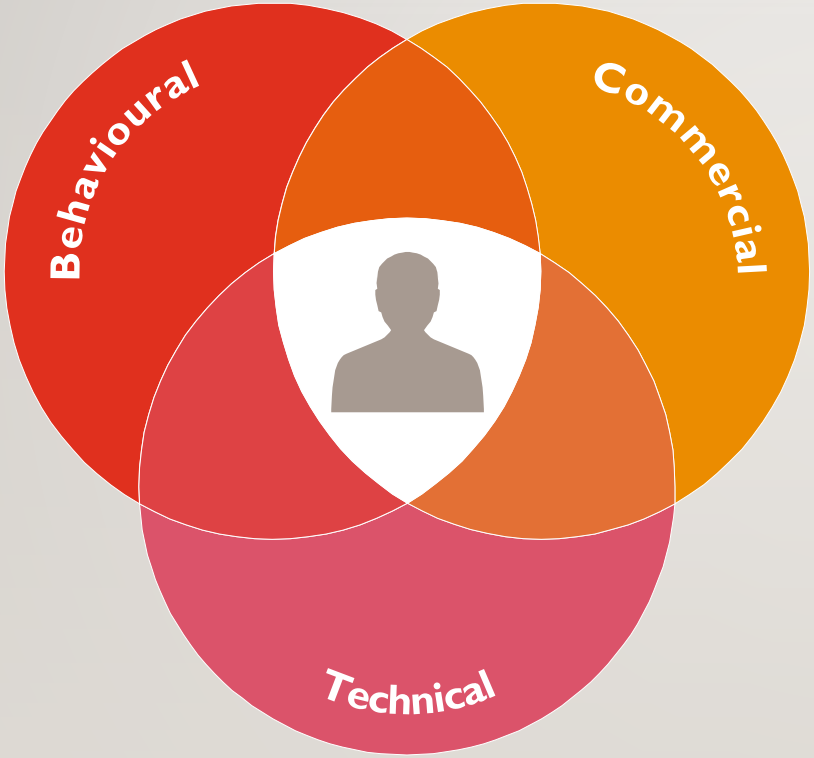
B. The conduct of a detailed systems software review may hamper the audit's schedule, and an IS auditor may not be technically competent to do such a review at this time.

C. If there are control weaknesses that have been discovered by an IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived.

D. The appropriate option would be to review the systems software as relevant to the review and recommend a detailed systems software review for which additional resources may be recommended.


Independent mind
Critical thinker
Intellectual curiosity
Professionally sceptical
Personal responsibility
Big picture
AGILE MINDS
Ability to challenge
Open mindedness
Research
Commercial mindset
Technical
Practical
Problem solver
Analytical

AUDIT AS PROFESSION – ESSENTIAL SKILLS



Demonstrating a business perspective, delivering value and insight and communicating with impact and empathy are important foundations for strong client relationships.

You Define Your Targets…