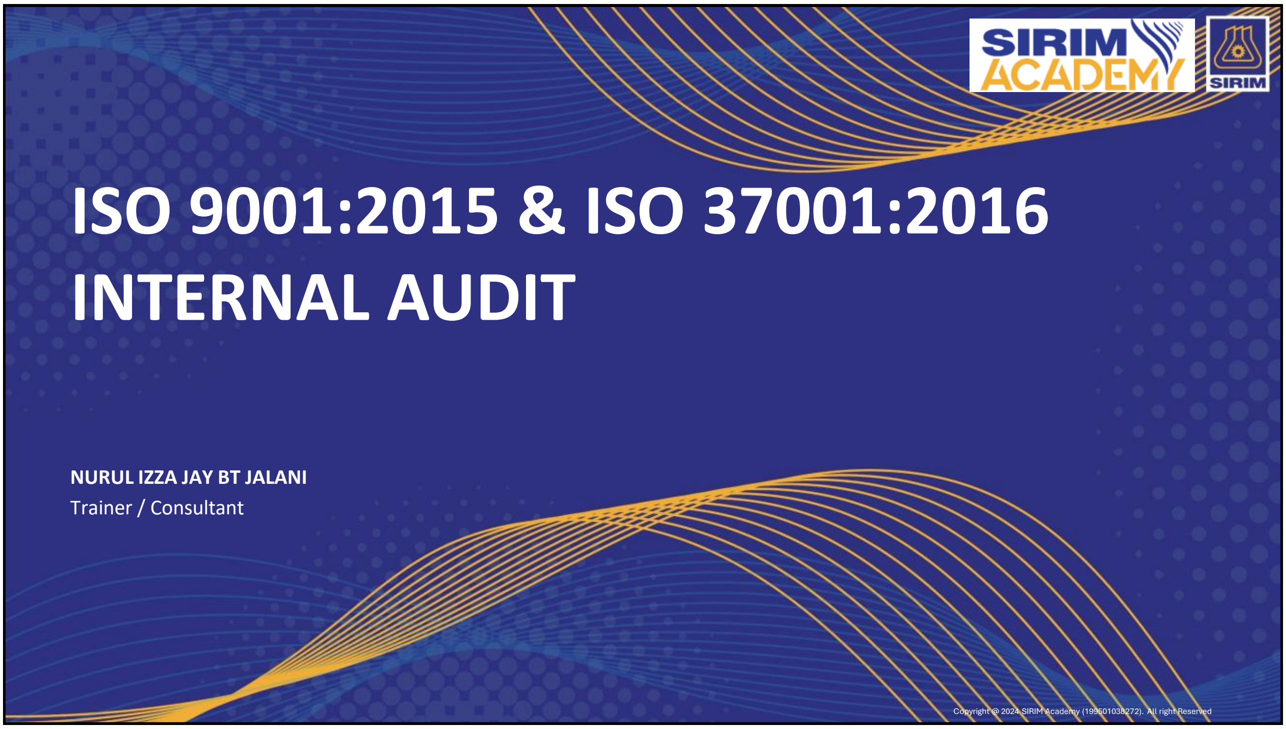
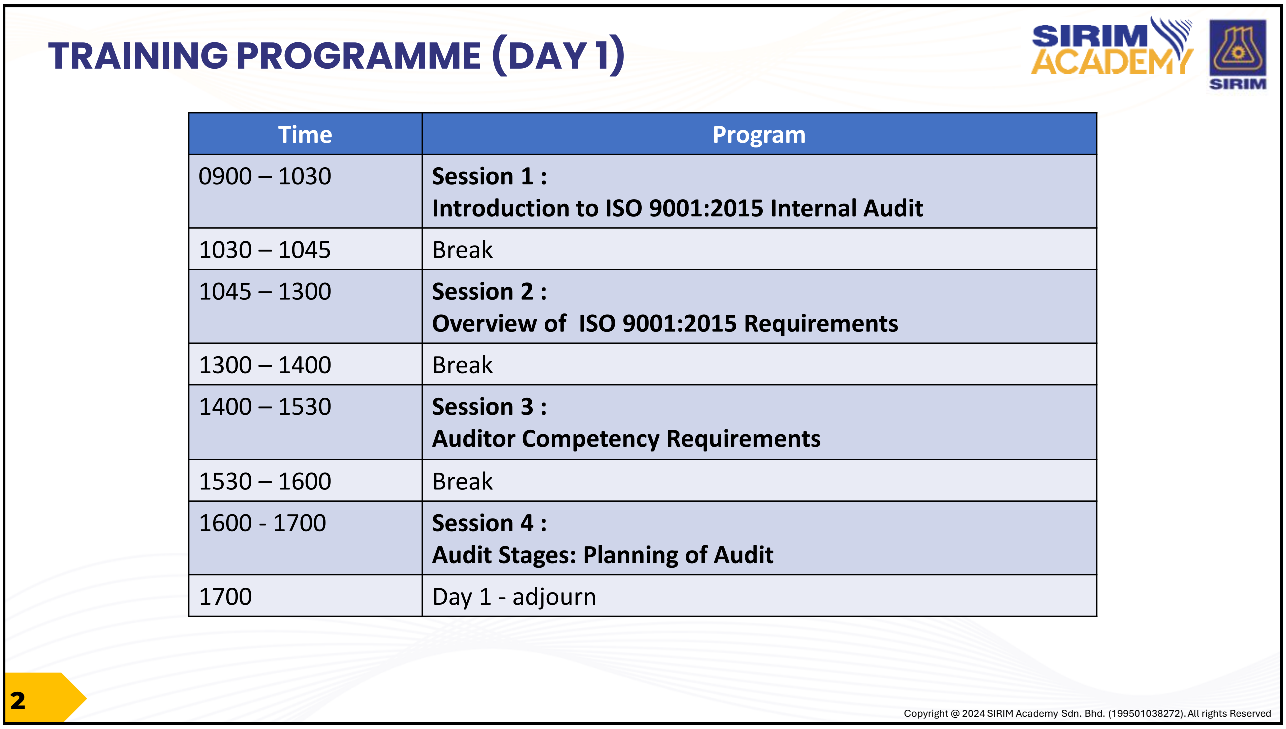


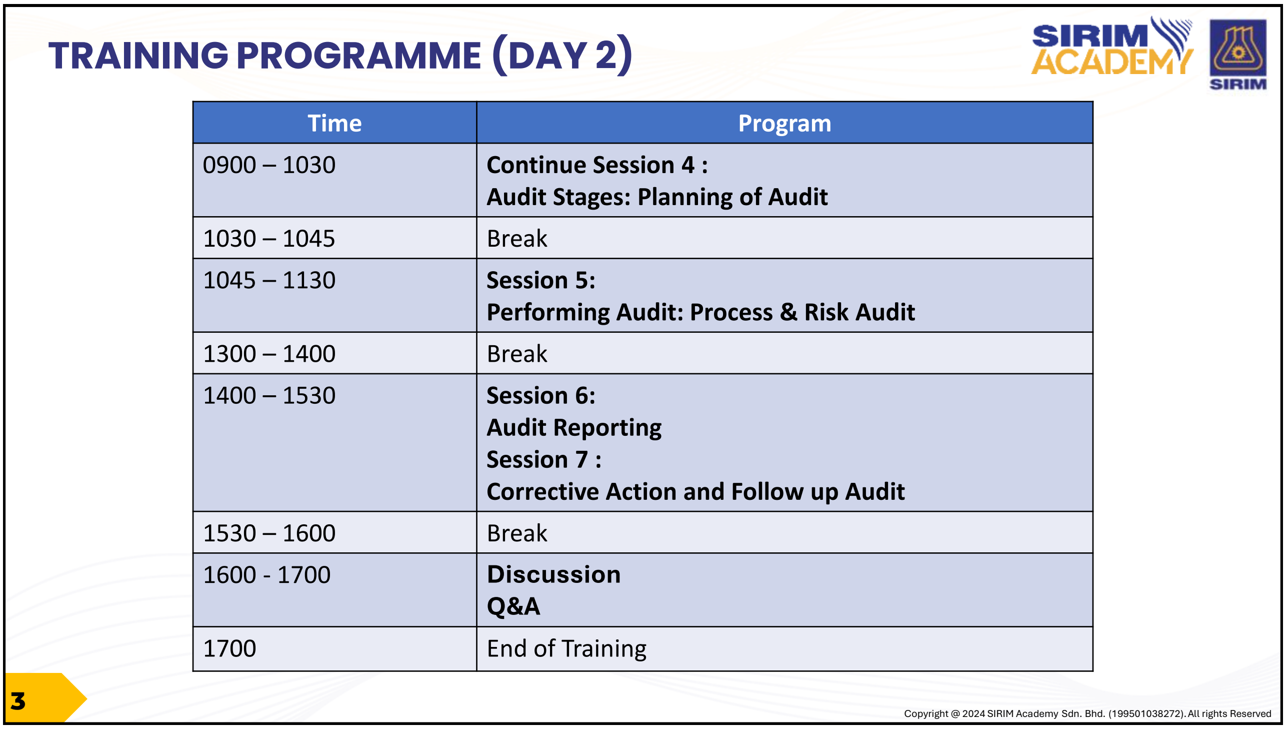
ISO 9001:2015 & ISO 37001:2016 INTERNAL AUDIT

NURUL IZZA JAY BT JALANI
Trainer / Consultant



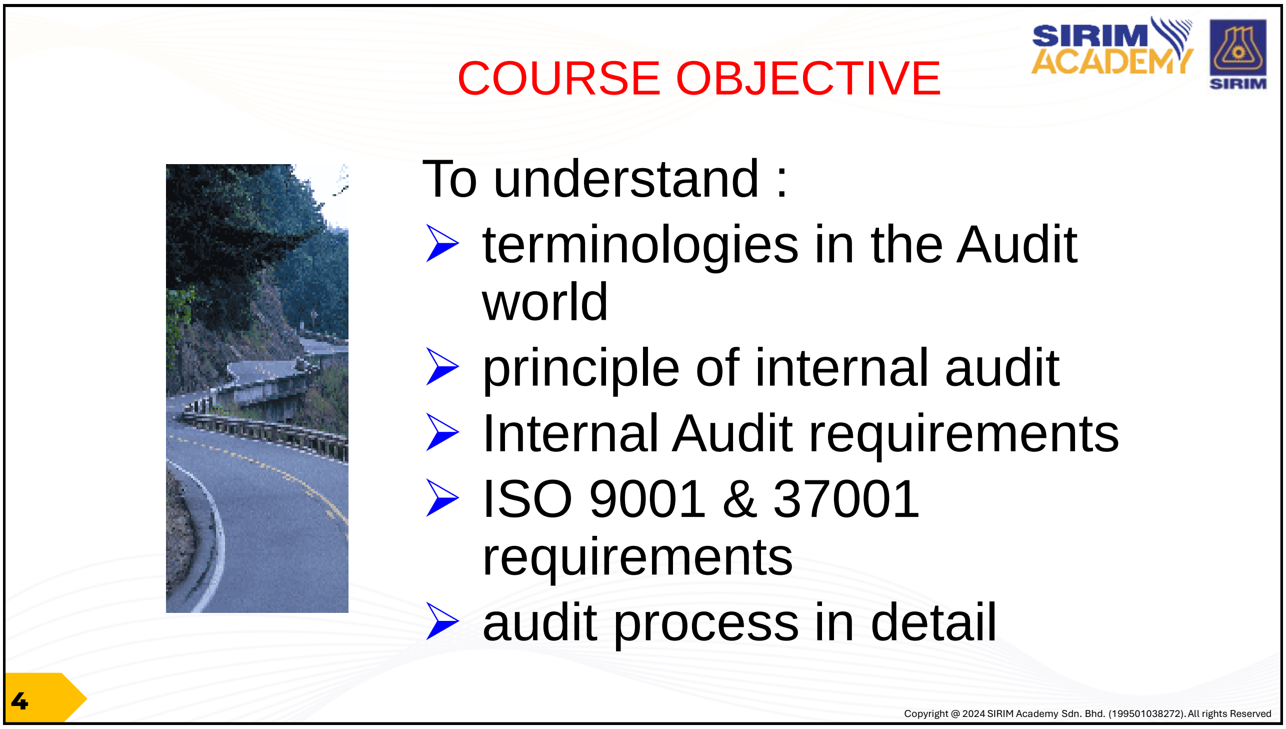
TRAINING PROGRAMME (DAY 1)

Time	Program
0900 – 1030	**Session 1 :** **Introduction to ISO 9001:2015 Internal Audit**
1030 – 1045	Break
1045 – 1300	**Session 2 :** **Overview of ISO 9001:2015 Requirements**
1300 – 1400	Break
1400 – 1530	**Session 3 :** **Auditor Competency Requirements**
1530 – 1600	Break
1600 - 1700	**Session 4 :** **Audit Stages: Planning of Audit**
1700	Day 1 - adjourn



TRAINING PROGRAMME (DAY 2)

Time	Program
0900 – 1030	**Continue Session 4 :** **Audit Stages: Planning of Audit**
1030 – 1045	Break
1045 – 1130	**Session 5:** **Performing Audit: Process & Risk Audit**
1300 – 1400	Break
1400 – 1530	**Session 6:** **Audit Reporting** **Session 7 :** **Corrective Action and Follow up Audit**
1530 – 1600	Break
1600 - 1700	**Discussion** **Q&A**
1700	End of Training



COURSE OBJECTIVE

To understand :

- terminologies in the Audit world
- principle of internal audit
- Internal Audit requirements
- ISO 9001 & 37001 requirements
- audit process in detail

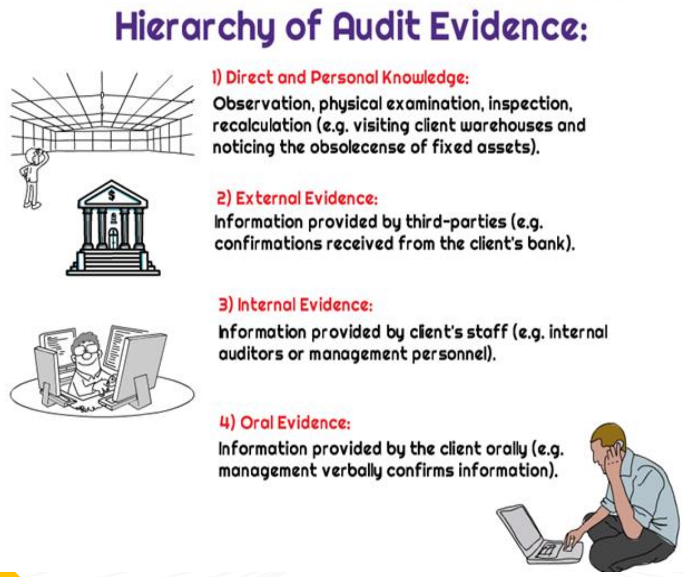
Introduction to Internal Audit

AUDIT

Systematic, independent and documented process for obtaining **audit evidence** and evaluating it objectively to determine the extent to which the **audit criteria** are fulfilled

Source: ISO 19011:2018 Clause 3.1

AUDIT EVIDENCE



Hierarchy of Audit Evidence:

1) Direct and Personal Knowledge:
Observation, physical examination, inspection, recalculation (e.g. visiting client warehouses and noticing the obsolecense of fixed assets).

2) External Evidence:
Information provided by third-parties (e.g. confirmations received from the client's bank).

3) Internal Evidence:
Information provided by client's staff (e.g. internal auditors or management personnel).

4) Oral Evidence:
Information provided by the client orally (e.g. management verbally confirms information).

Records, statements of fact or other information, which are relevant to the **audit criteria** and **verifiable**

Source: ISO 19011:2018, clause 3.9

7

7

OBJECTIVE EVIDENCE

Data supporting the existence or verify of something

Source: ISO 19011:2018, clause 3.8

Objective Evidence
"I have a terrible pain in my back!"
There's no proof
There is proof
Subjective Evidence

8

8

AUDIT CRITERIA

Set of **requirements**, used as a **reference** against which objective evidence is compared

Source: ISO 9000:2015, Clause 3.13.7
ISO 19011:2018, clause 3.7

Eg;

- Policies, practices, procedures
  Gift Policy, Integrity Pacts
- Legal and regulatory requirements
  MACC Act 2009, Whistle Blowing Act 2010
- Standard and guidelines
  Arahan Keselamatan 2017, Official Secrets Act 1972 (Act 88)

AUDIT FINDINGS

Results of the evaluation of the collected **audit evidence** against **audit criteria**

❑ Indicate Conformity & Non Conformity

❑ Lead to Opportunity for improvement

❑ If audit criteria is selected from statutory requirements or regulatory requirements, the audit findings is termed as Compliance or **Non Compliance**

Source: ISO 19011:2018, clause 3.10

AUDIT CONCLUSION

Outcome of an **audit**, after consideration of the audit objectives and all **audit findings**

Note; Strength and weaknesses of overall management system including summary of audit findings

Source: ISO 19011:2018, clause 3.11

AUDIT CLIENT

Organization or person requesting an audit

Source: ISO 19011:2018, clause 3.12

AUDITEE

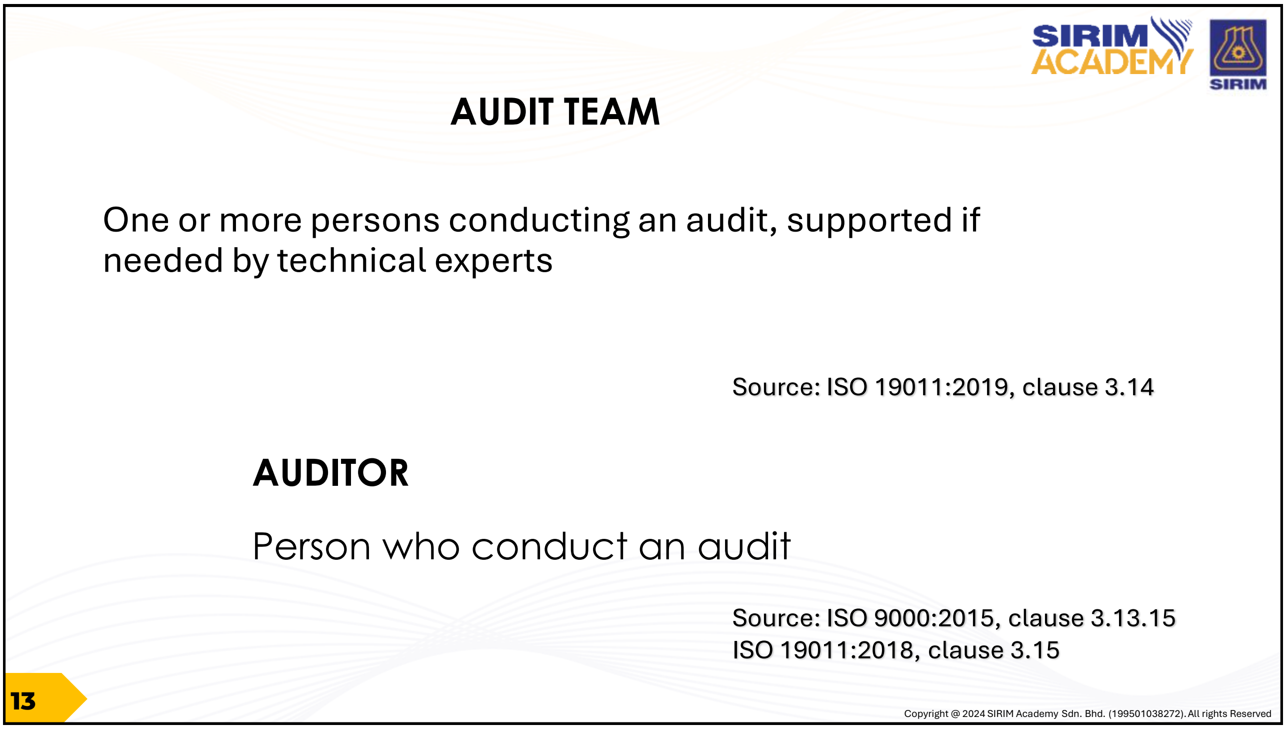
Organization as a whole or parts thereof being audited

Source: ISO 19011:2018, clause 3.13

COMPETENCE

Ability to apply knowledge and skills to achieve intended result

Source: ISO 19011:2018, clause 3.22



AUDIT TEAM

One or more persons conducting an audit, supported if needed by technical experts

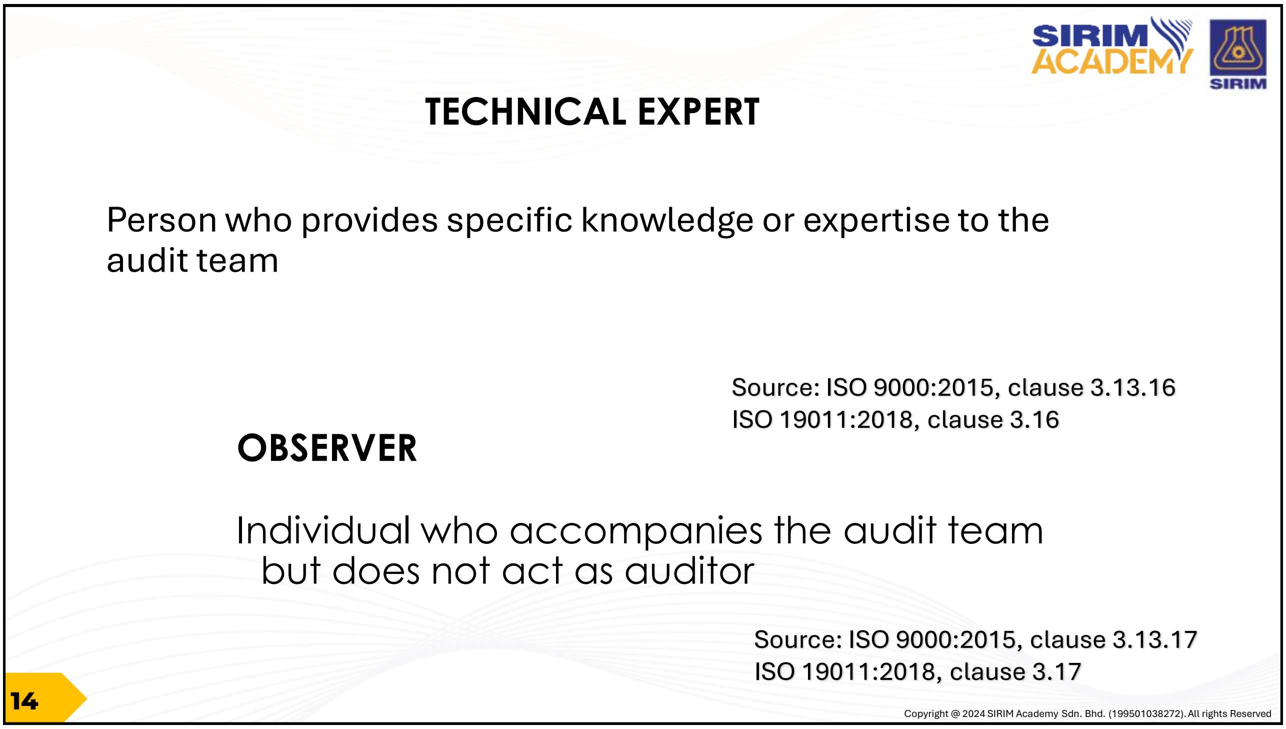
Source: ISO 19011:2019, clause 3.14

AUDITOR

Person who conduct an audit

Source: ISO 9000:2015, clause 3.13.15
ISO 19011:2018, clause 3.15

13



TECHNICAL EXPERT

Person who provides specific knowledge or expertise to the audit team

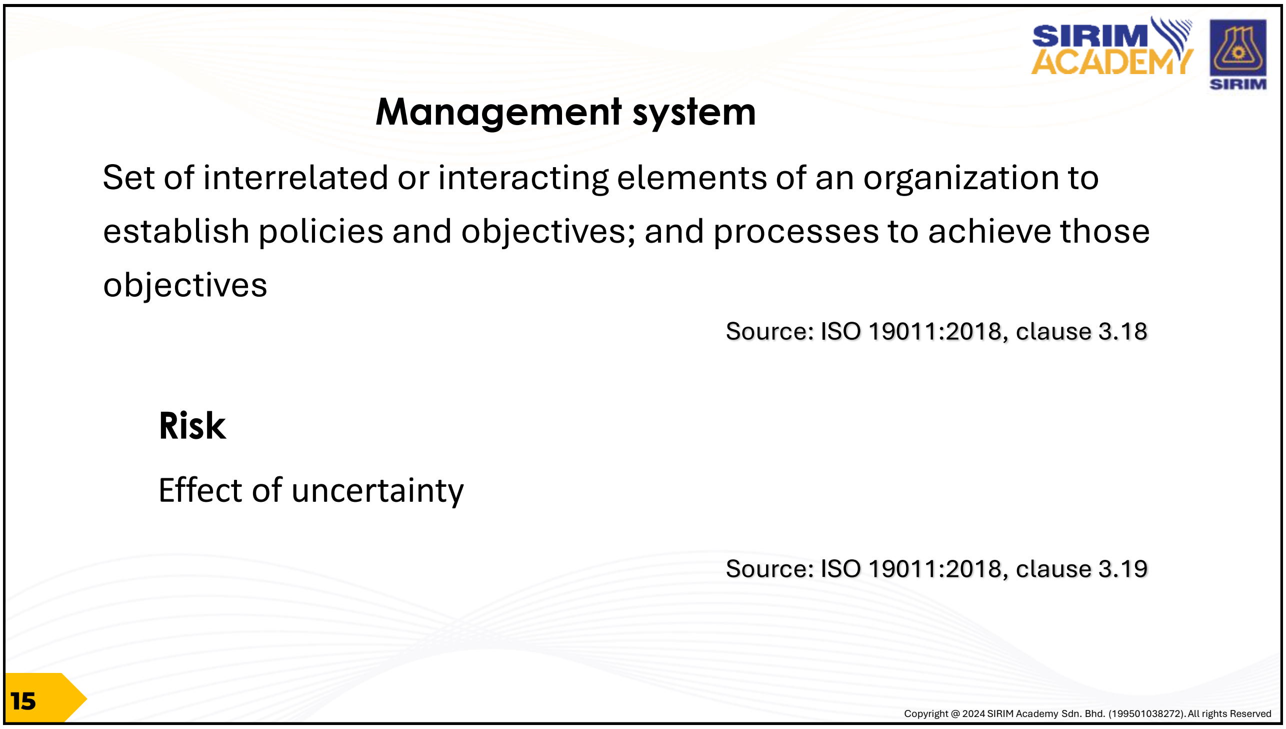
Source: ISO 9000:2015, clause 3.13.16
ISO 19011:2018, clause 3.16

OBSERVER

Individual who accompanies the audit team but does not act as auditor

Source: ISO 9000:2015, clause 3.13.17
ISO 19011:2018, clause 3.17

14



Management system

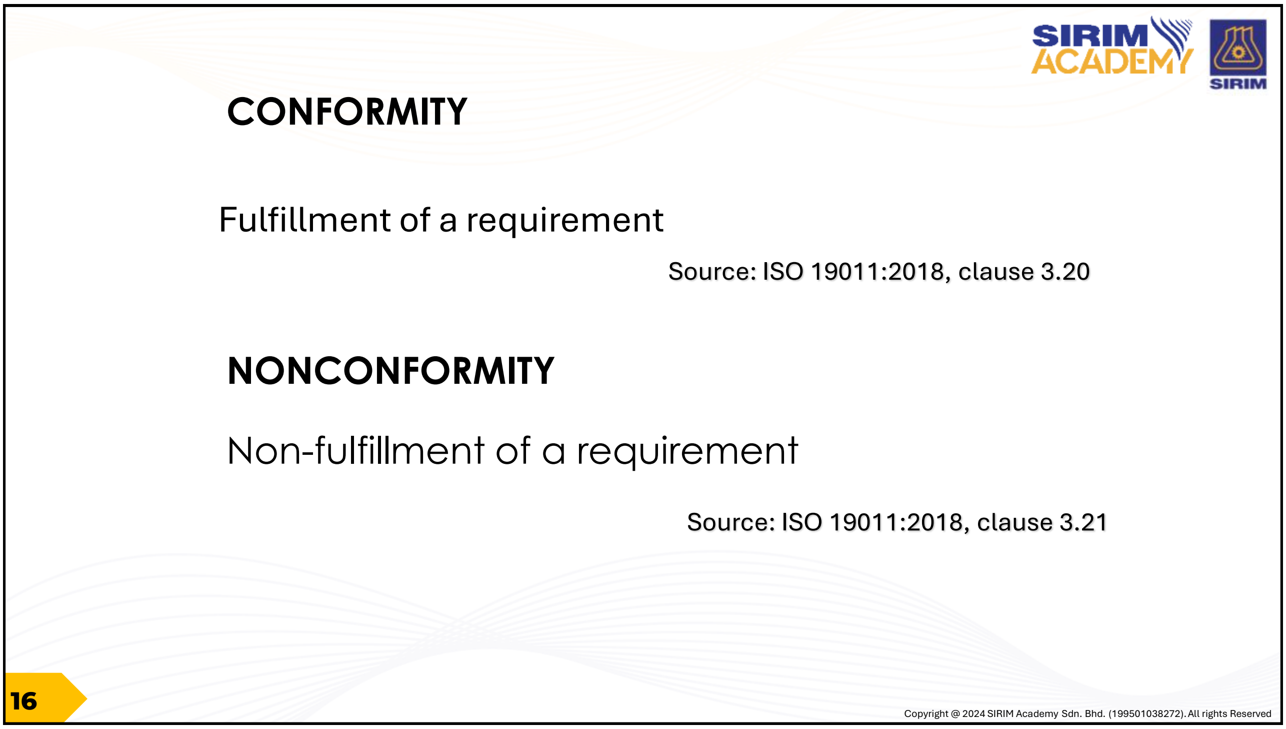
Set of interrelated or interacting elements of an organization to establish policies and objectives; and processes to achieve those objectives

Source: ISO 19011:2018, clause 3.18

Risk

Effect of uncertainty

Source: ISO 19011:2018, clause 3.19



CONFORMITY

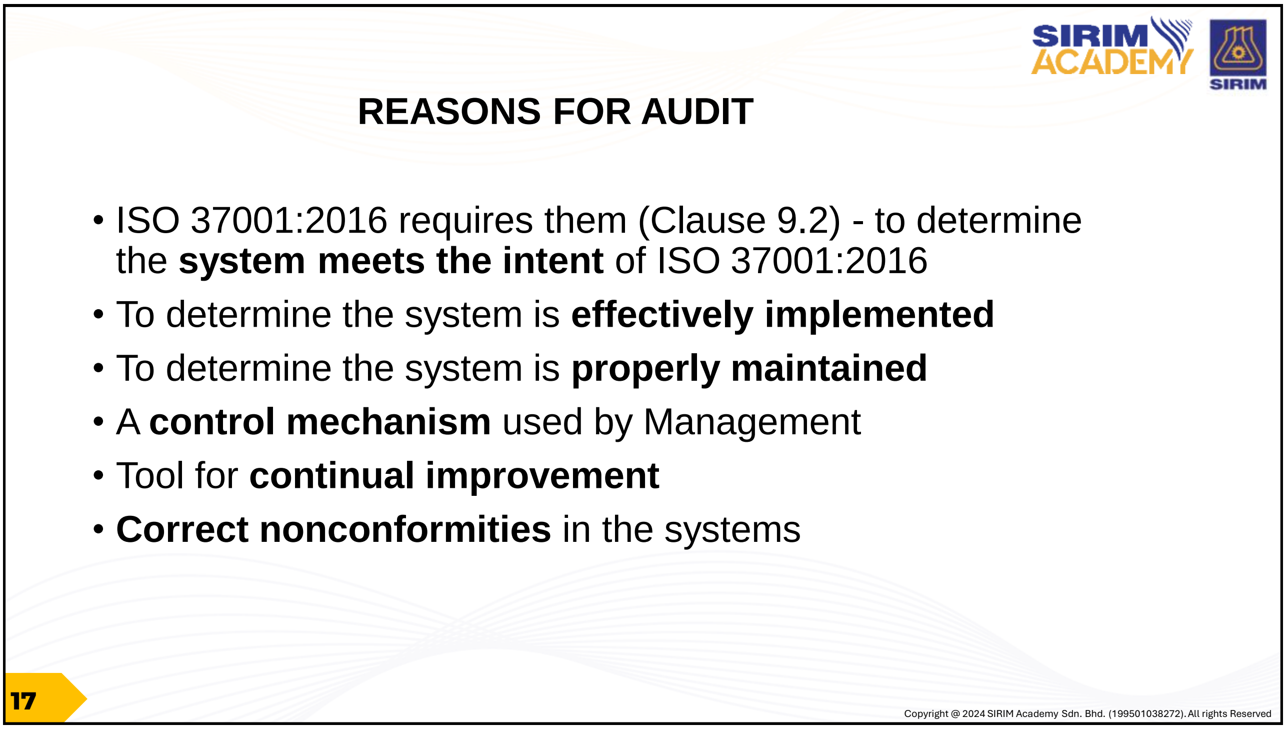
Fulfillment of a requirement

Source: ISO 19011:2018, clause 3.20

NONCONFORMITY

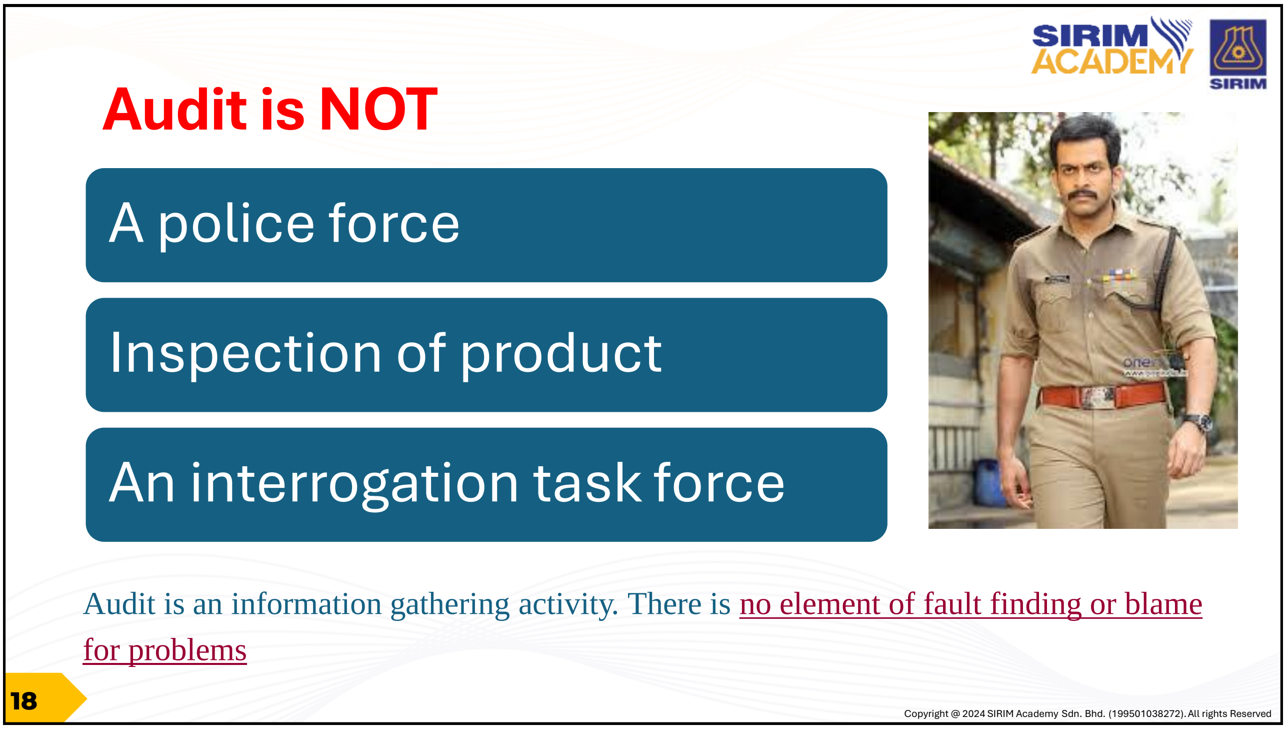
Non-fulfillment of a requirement

Source: ISO 19011:2018, clause 3.21



REASONS FOR AUDIT

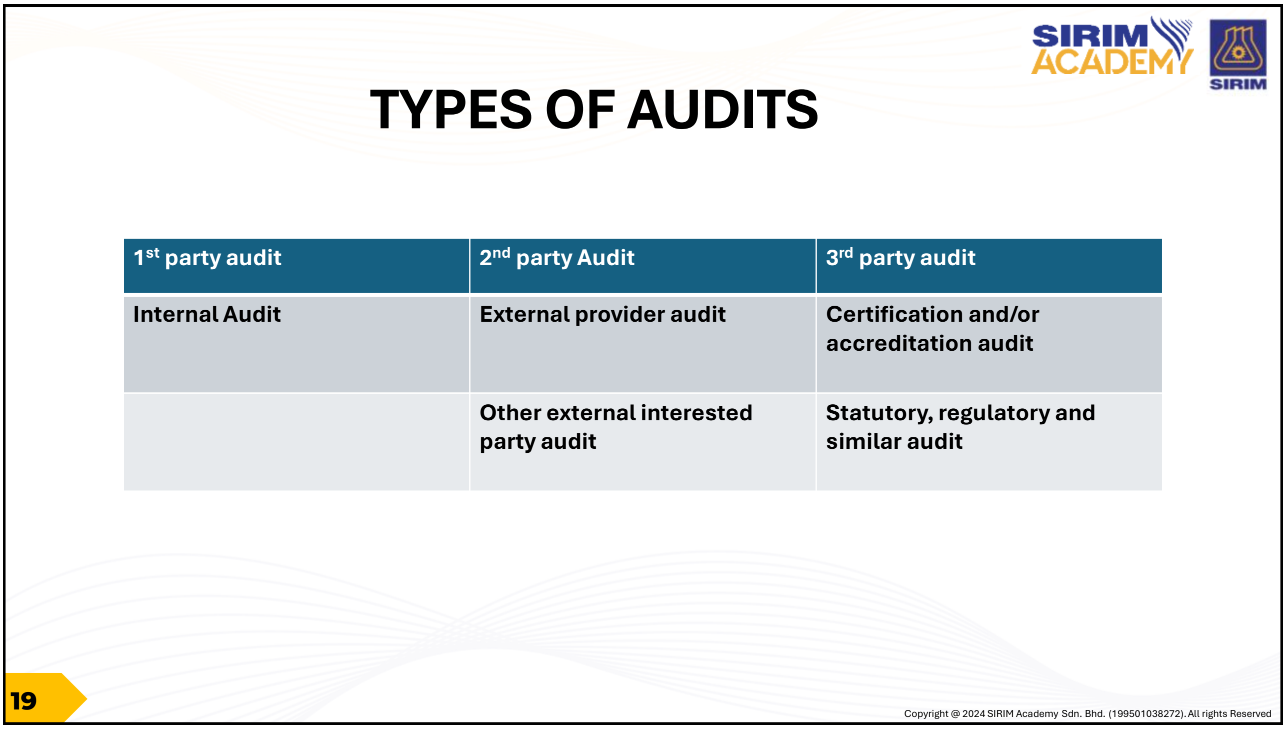
- ISO 37001:2016 requires them (Clause 9.2) - to determine the **system meets the intent** of ISO 37001:2016
- To determine the system is **effectively implemented**
- To determine the system is **properly maintained**
- A **control mechanism** used by Management
- Tool for **continual improvement**
- **Correct nonconformities** in the systems



Audit is NOT

- A police force
- Inspection of product
- An interrogation task force

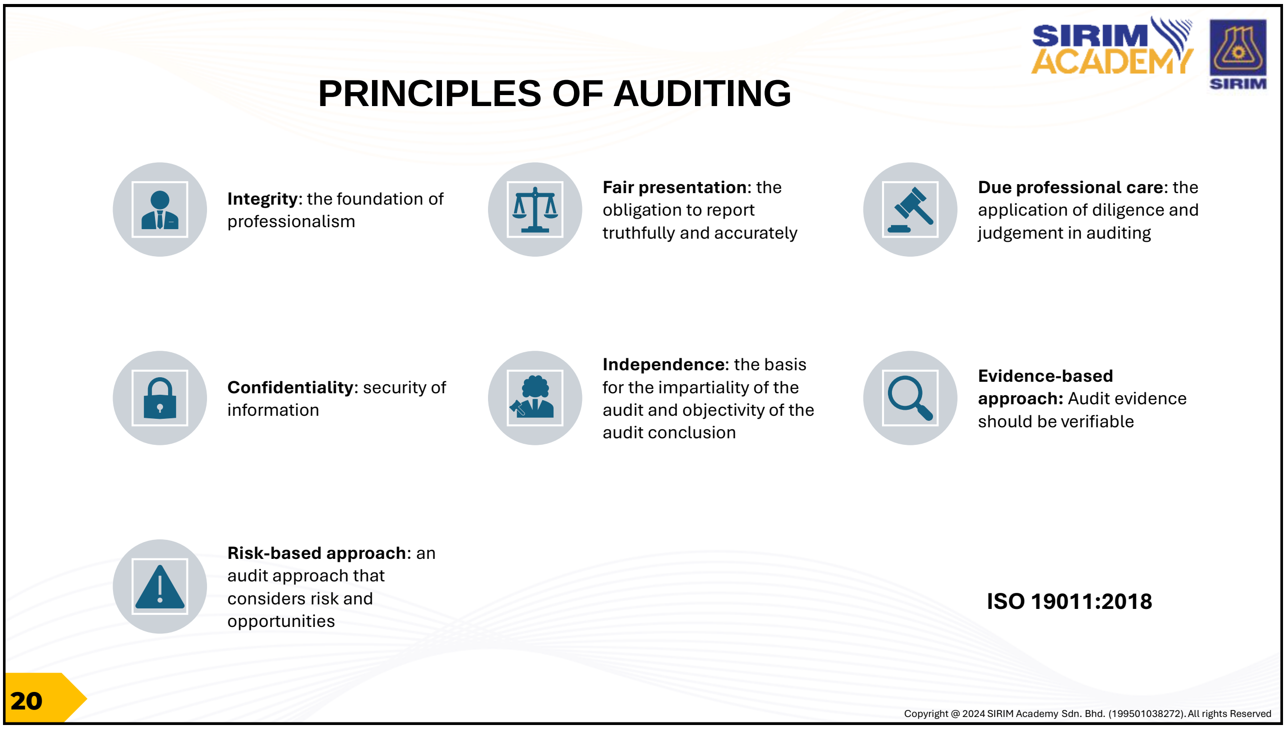
Audit is an information gathering activity. There is no element of fault finding or blame for problems



TYPES OF AUDITS

1st party audit	2nd party Audit	3rd party audit
Internal Audit	External provider audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

19



PRINCIPLES OF AUDITING

Integrity: the foundation of professionalism

Fair presentation: the obligation to report truthfully and accurately

Due professional care: the application of diligence and judgement in auditing

Confidentiality: security of information

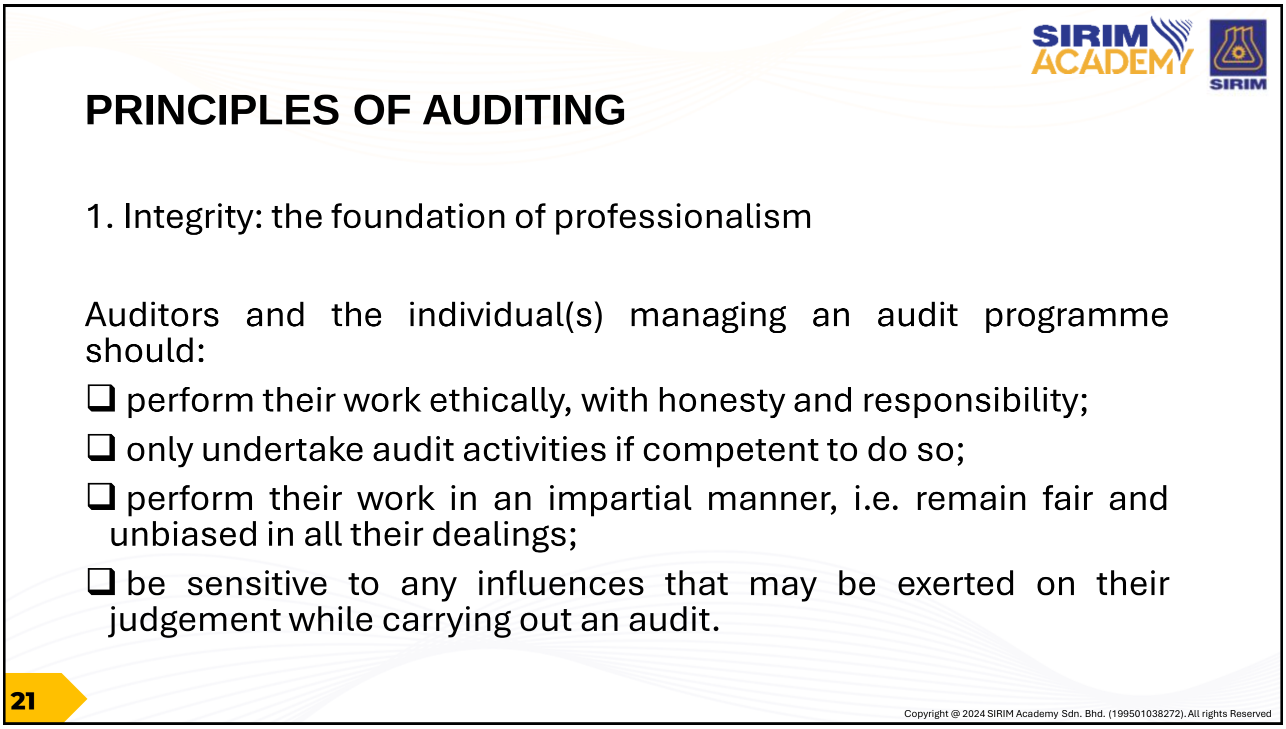
Independence: the basis for the impartiality of the audit and objectivity of the audit conclusion

Evidence-based approach: Audit evidence should be verifiable

Risk-based approach: an audit approach that considers risk and opportunities

ISO 19011:2018

20

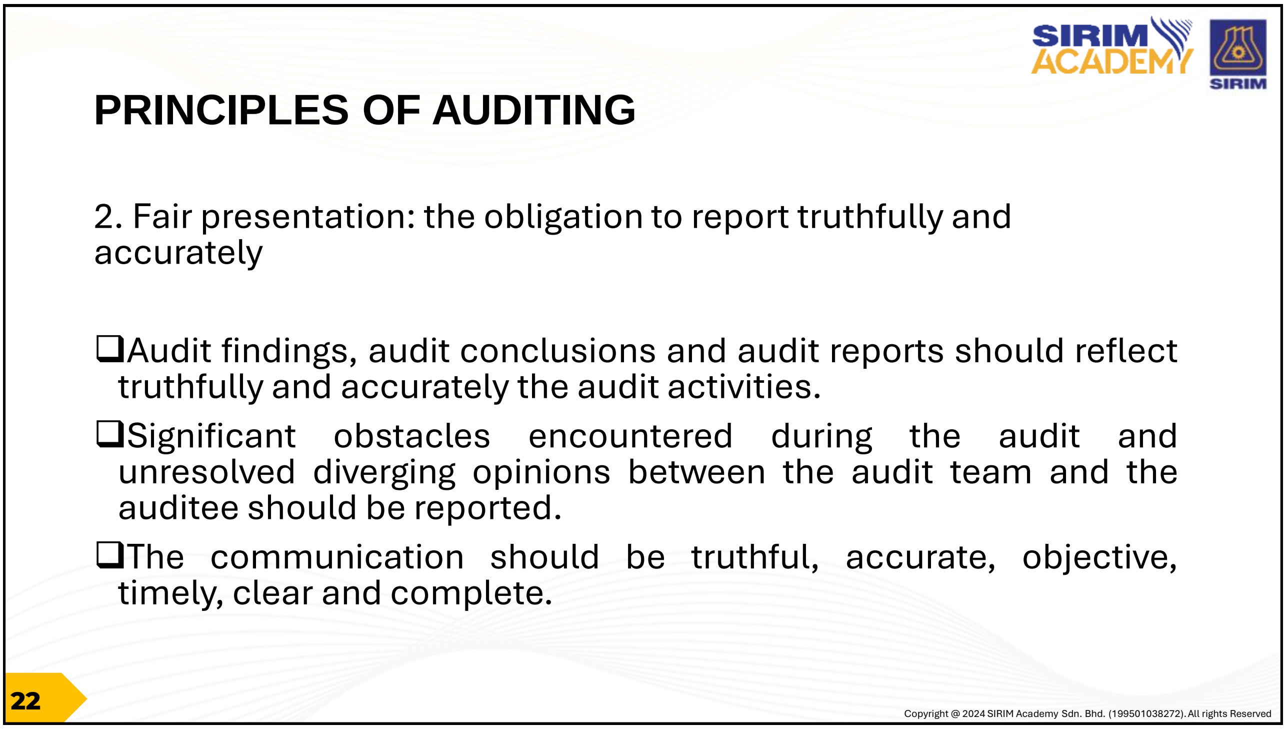


PRINCIPLES OF AUDITING

1. Integrity: the foundation of professionalism

Auditors and the individual(s) managing an audit programme should:

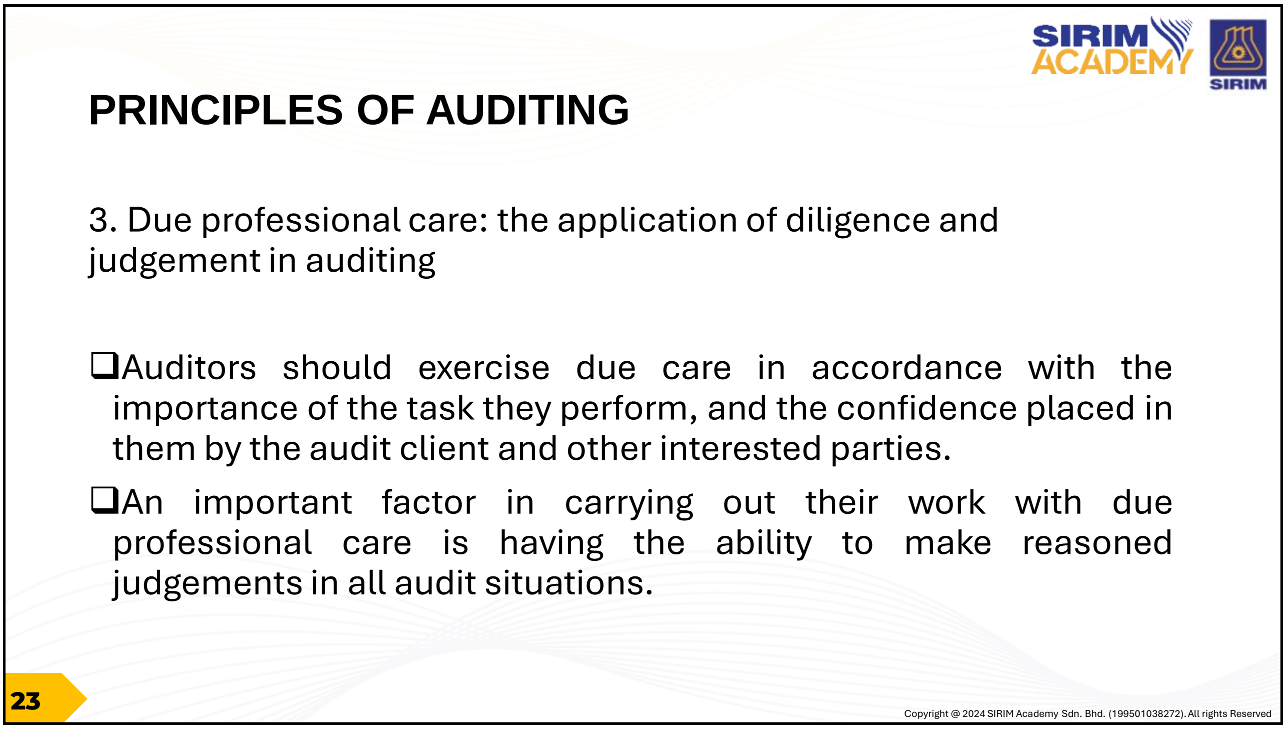
- ❑ perform their work ethically, with honesty and responsibility;
- ❑ only undertake audit activities if competent to do so;
- ❑ perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;
- ❑ be sensitive to any influences that may be exerted on their judgement while carrying out an audit.



PRINCIPLES OF AUDITING

2. Fair presentation: the obligation to report truthfully and accurately

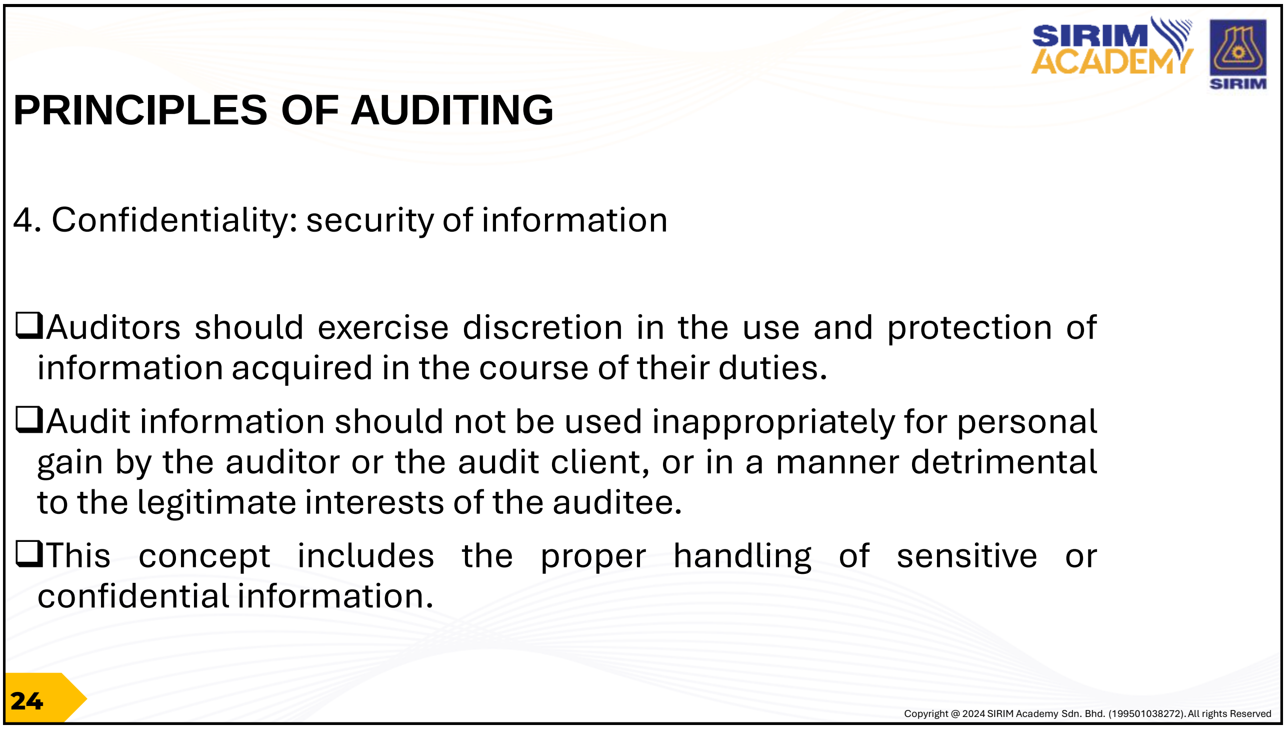
- ❑Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit activities.
- ❑Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported.
- ❑The communication should be truthful, accurate, objective, timely, clear and complete.



PRINCIPLES OF AUDITING

3. Due professional care: the application of diligence and judgement in auditing

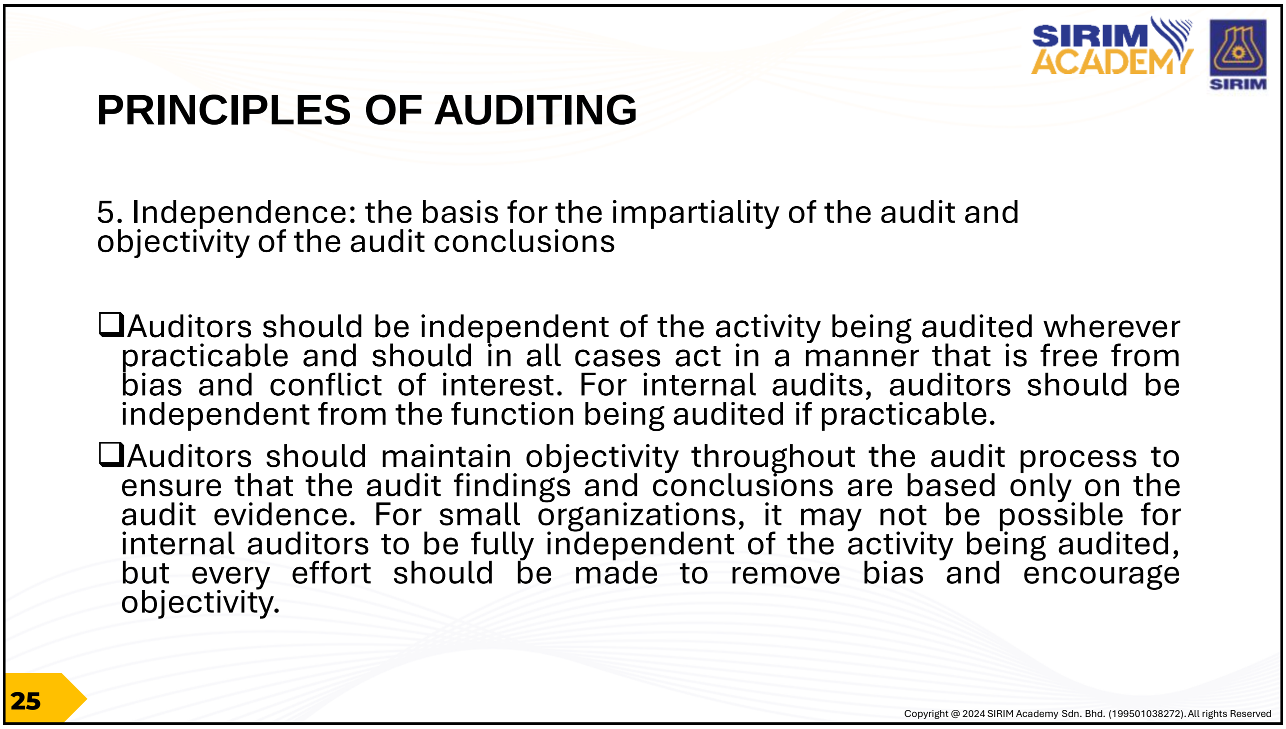
- ❑Auditors should exercise due care in accordance with the importance of the task they perform, and the confidence placed in them by the audit client and other interested parties.
- ❑An important factor in carrying out their work with due professional care is having the ability to make reasoned judgements in all audit situations.



PRINCIPLES OF AUDITING

4. Confidentiality: security of information

- ❑Auditors should exercise discretion in the use and protection of information acquired in the course of their duties.
- ❑Audit information should not be used inappropriately for personal gain by the auditor or the audit client, or in a manner detrimental to the legitimate interests of the auditee.
- ❑This concept includes the proper handling of sensitive or confidential information.

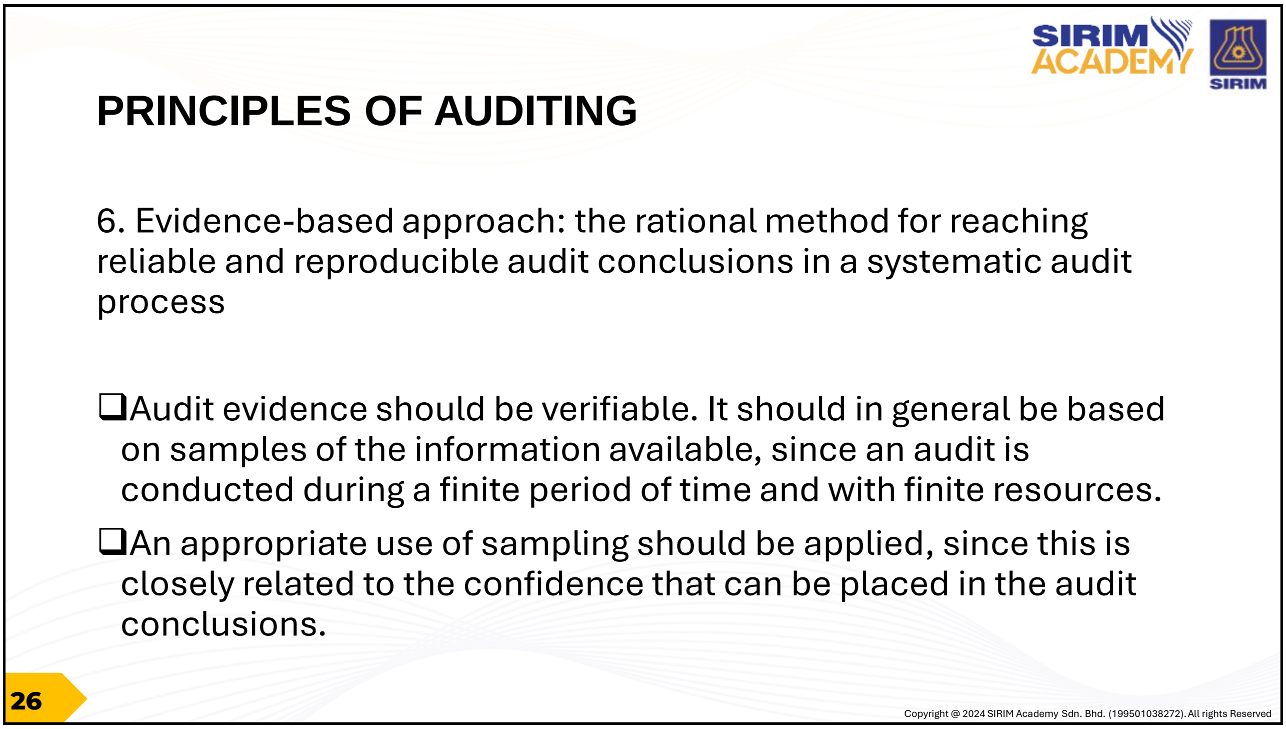


PRINCIPLES OF AUDITING

5. Independence: the basis for the impartiality of the audit and objectivity of the audit conclusions

❑Auditors should be independent of the activity being audited wherever practicable and should in all cases act in a manner that is free from bias and conflict of interest. For internal audits, auditors should be independent from the function being audited if practicable.

❑Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence. For small organizations, it may not be possible for internal auditors to be fully independent of the activity being audited, but every effort should be made to remove bias and encourage objectivity.

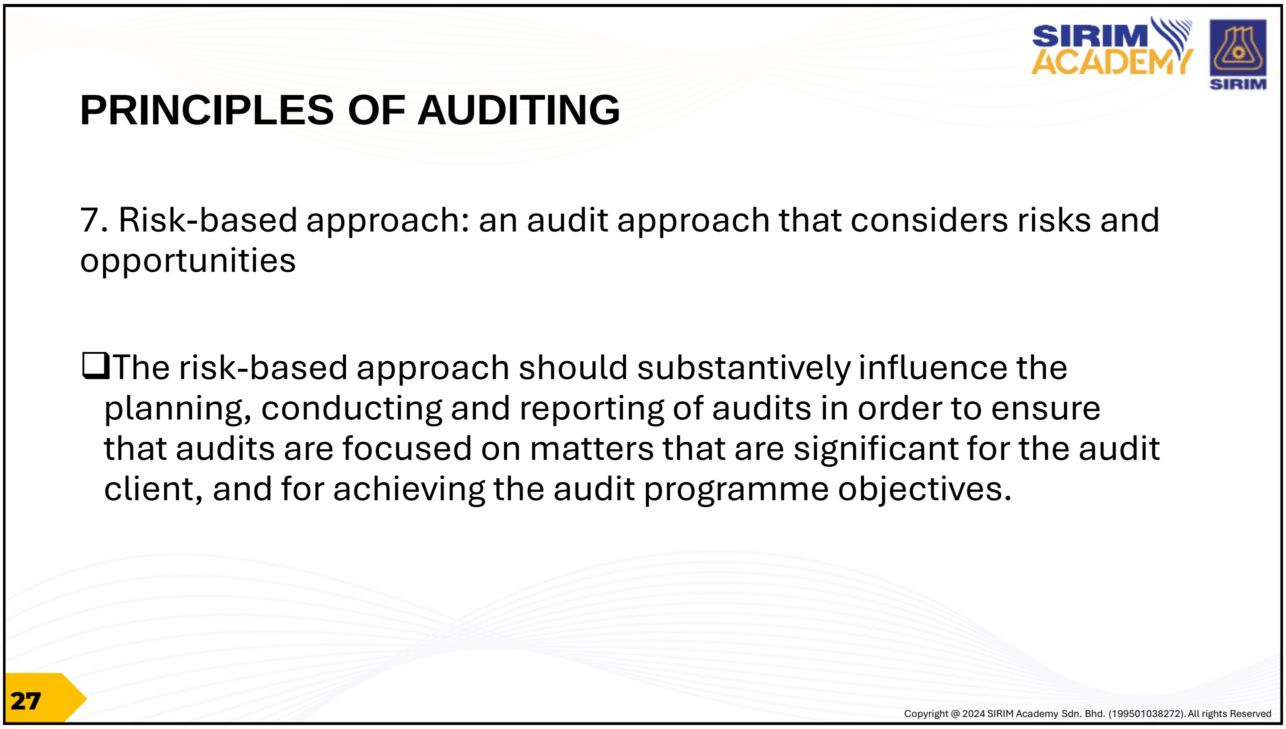


PRINCIPLES OF AUDITING

6. Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

❑Audit evidence should be verifiable. It should in general be based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources.

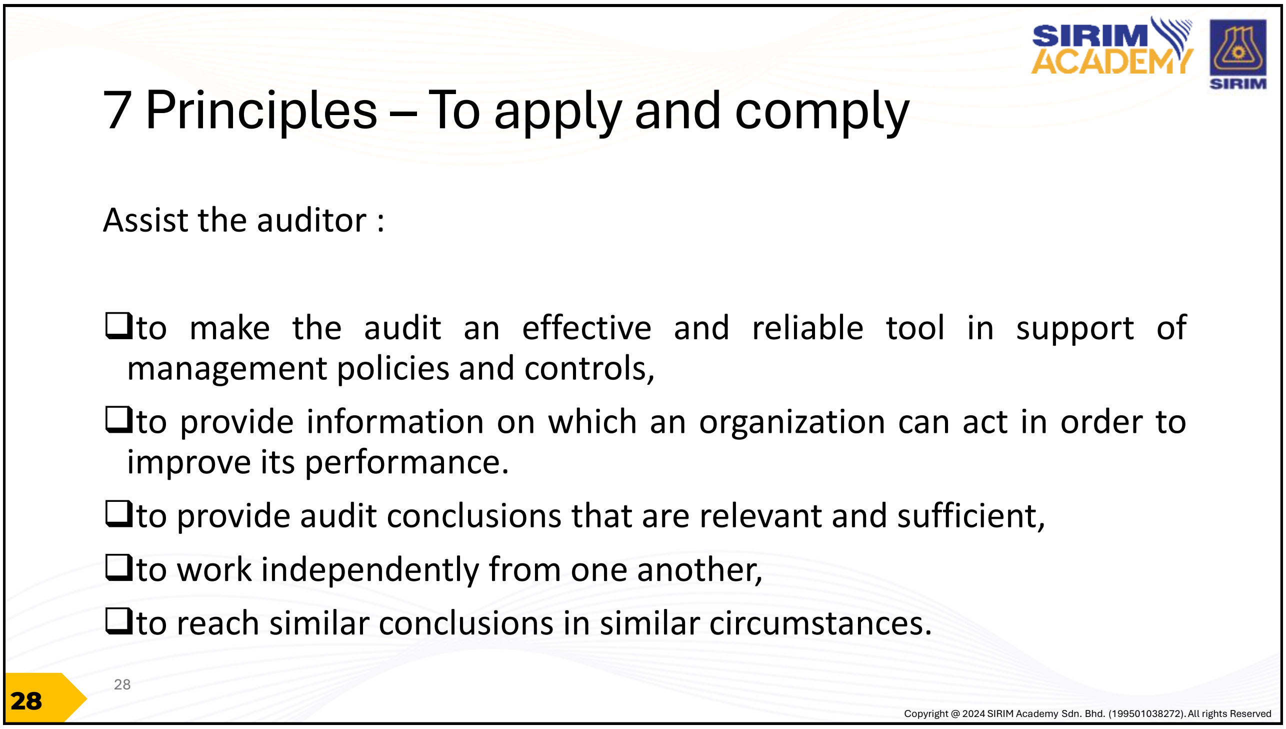
❑An appropriate use of sampling should be applied, since this is closely related to the confidence that can be placed in the audit conclusions.



PRINCIPLES OF AUDITING

7. Risk-based approach: an audit approach that considers risks and opportunities

❑The risk-based approach should substantively influence the planning, conducting and reporting of audits in order to ensure that audits are focused on matters that are significant for the audit client, and for achieving the audit programme objectives.



7 Principles – To apply and comply

Assist the auditor :

❑to make the audit an effective and reliable tool in support of management policies and controls,

❑to provide information on which an organization can act in order to improve its performance.

❑to provide audit conclusions that are relevant and sufficient,

❑to work independently from one another,

❑to reach similar conclusions in similar circumstances.

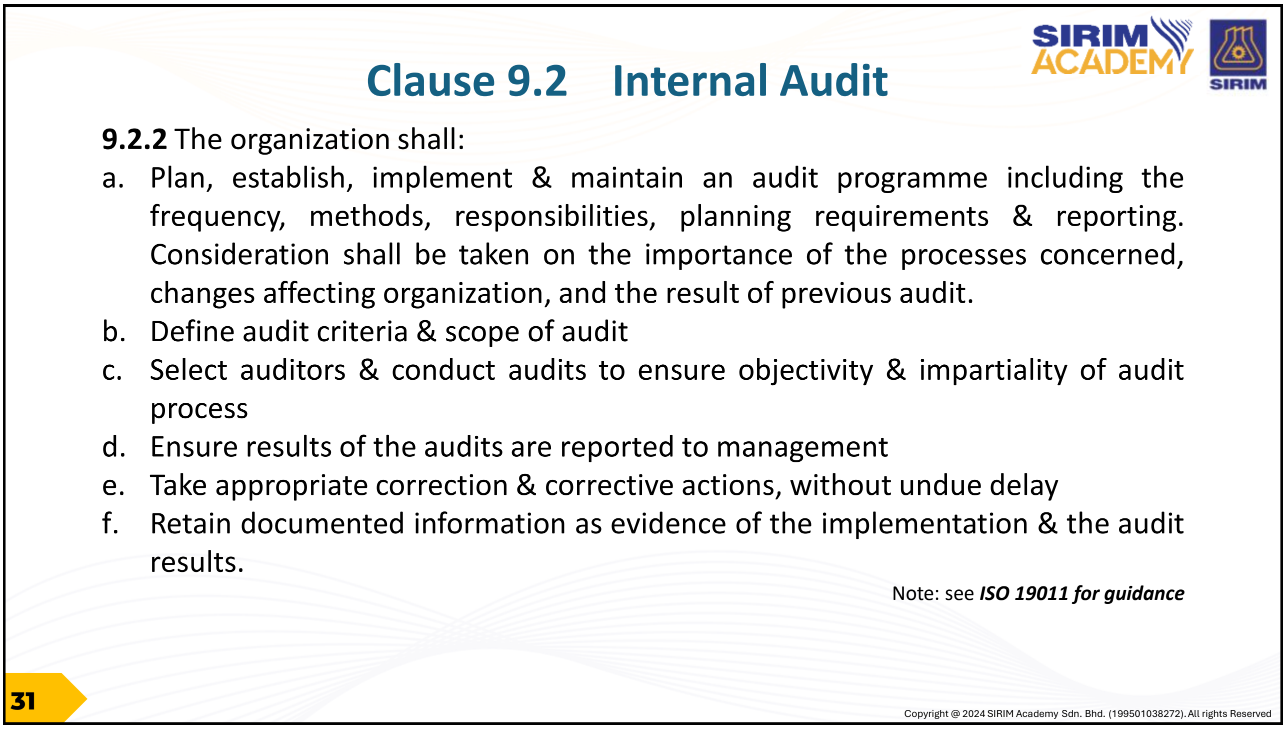
Review of QMS & ABMS Requirements

Clause 9.2 Internal Audit

9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the QMS:

a. Conforms to:
   i. the organization own requirements for its QMS
   ii. The requirements of this International Standards

b. Effectively implemented & maintained



Clause 9.2 Internal Audit

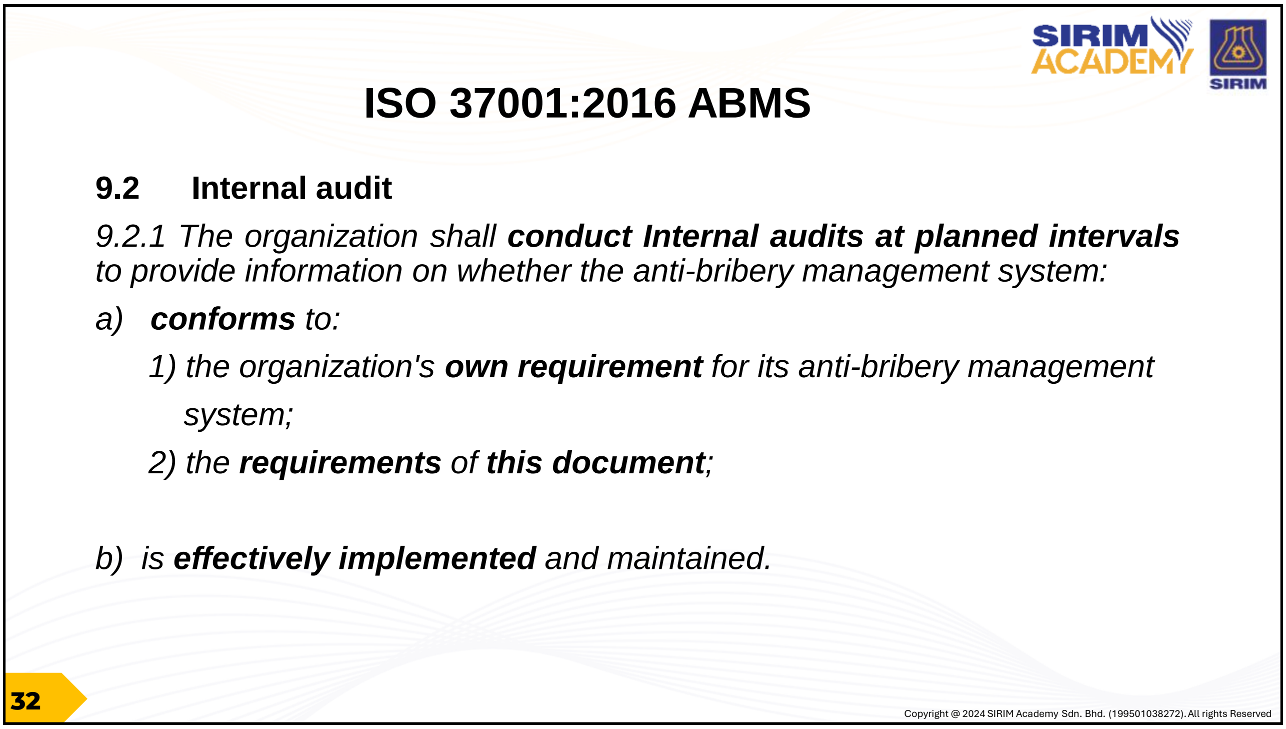
9.2.2 The organization shall:

a. Plan, establish, implement & maintain an audit programme including the frequency, methods, responsibilities, planning requirements & reporting. Consideration shall be taken on the importance of the processes concerned, changes affecting organization, and the result of previous audit.
b. Define audit criteria & scope of audit
c. Select auditors & conduct audits to ensure objectivity & impartiality of audit process
d. Ensure results of the audits are reported to management
e. Take appropriate correction & corrective actions, without undue delay
f. Retain documented information as evidence of the implementation & the audit results.

Note: see ***ISO 19011 for guidance***

31

31



ISO 37001:2016 ABMS

9.2 Internal audit

*9.2.1 The organization shall **conduct Internal audits at planned intervals** to provide information on whether the anti-bribery management system:*

*a) **conforms** to:*

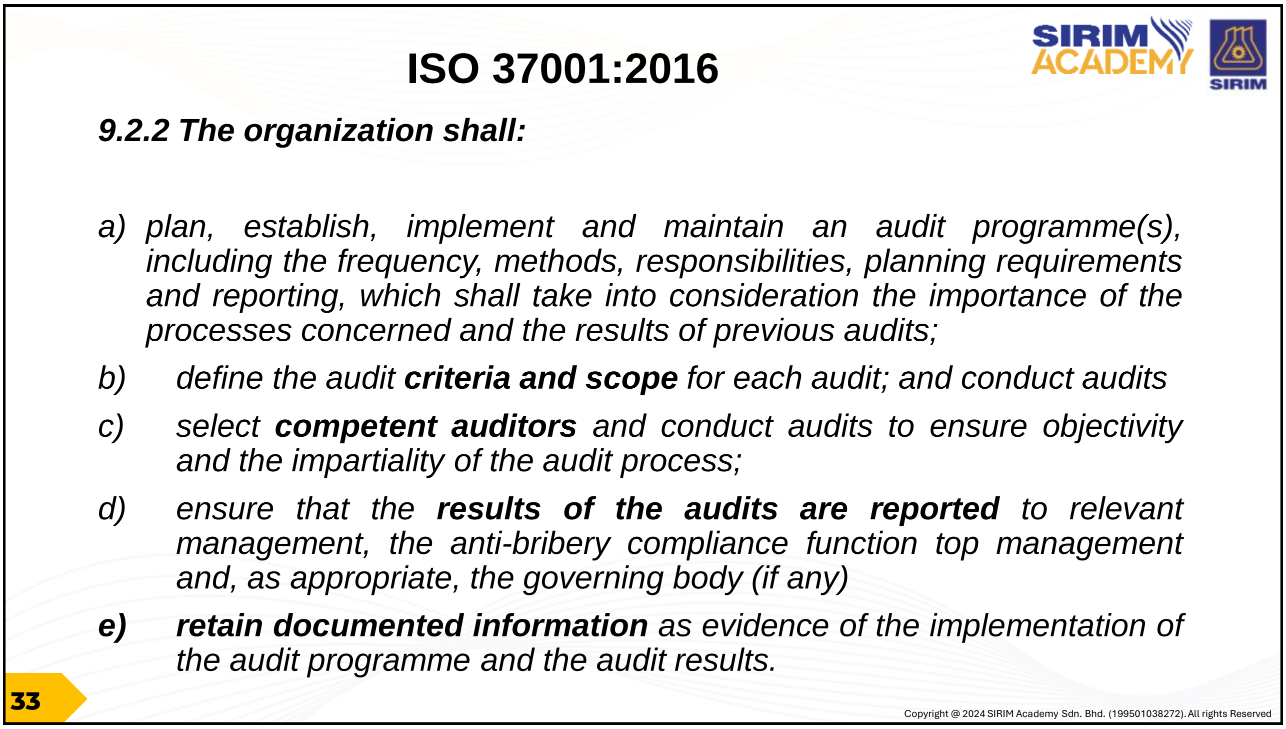
*1) the organization's **own requirement** for its anti-bribery management system;*

*2) the **requirements** of **this document**;*

*b) is **effectively implemented** and maintained.*

32

32



ISO 37001:2016

9.2.2 The organization shall:

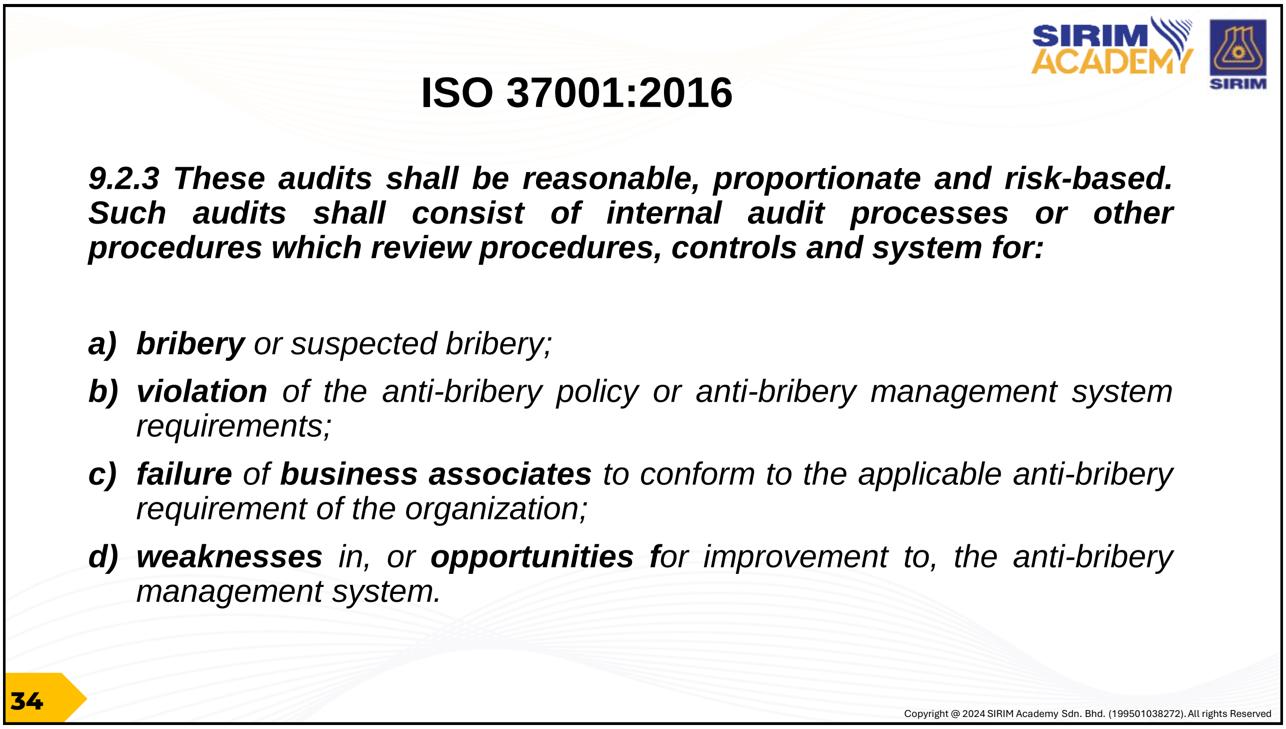
a) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;

*b) define the audit **criteria and scope** for each audit; and conduct audits*

*c) select **competent auditors** and conduct audits to ensure objectivity and the impartiality of the audit process;*

*d) ensure that the **results of the audits are reported** to relevant management, the anti-bribery compliance function top management and, as appropriate, the governing body (if any)*

***e)** **retain documented information** as evidence of the implementation of the audit programme and the audit results.*



ISO 37001:2016

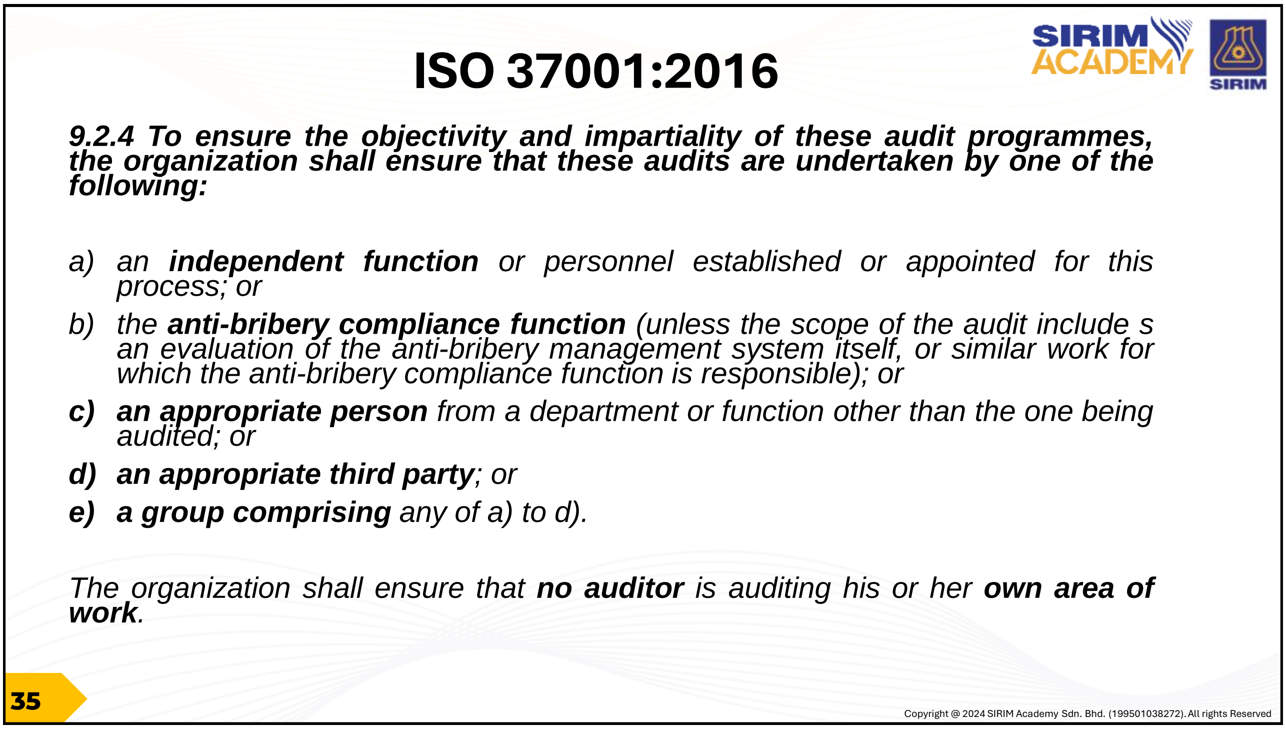
9.2.3 These audits shall be reasonable, proportionate and risk-based. Such audits shall consist of internal audit processes or other procedures which review procedures, controls and system for:

***a) bribery** or suspected bribery;*

***b) violation** of the anti-bribery policy or anti-bribery management system requirements;*

***c) failure** of **business associates** to conform to the applicable anti-bribery requirement of the organization;*

***d) weaknesses** in, or **opportunities f**or improvement to, the anti-bribery management system.*



ISO 37001:2016

9.2.4 To ensure the objectivity and impartiality of these audit programmes, the organization shall ensure that these audits are undertaken by one of the following:

*a) an **independent function** or personnel established or appointed for this process; or*

*b) the **anti-bribery compliance function** (unless the scope of the audit include s an evaluation of the anti-bribery management system itself, or similar work for which the anti-bribery compliance function is responsible); or*

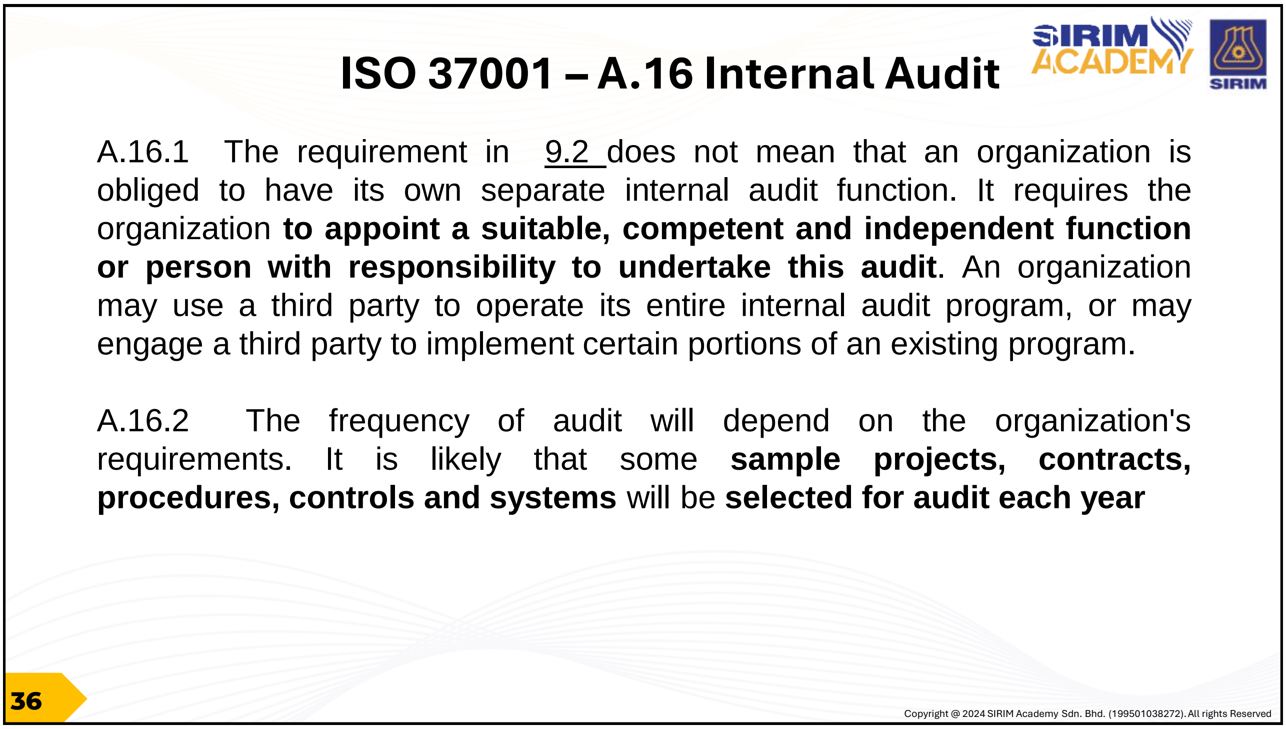
***c) an appropriate person** from a department or function other than the one being audited; or*

***d) an appropriate third party**; or*

***e) a group comprising** any of a) to d).*

*The organization shall ensure that **no auditor** is auditing his or her **own area of work**.*

35

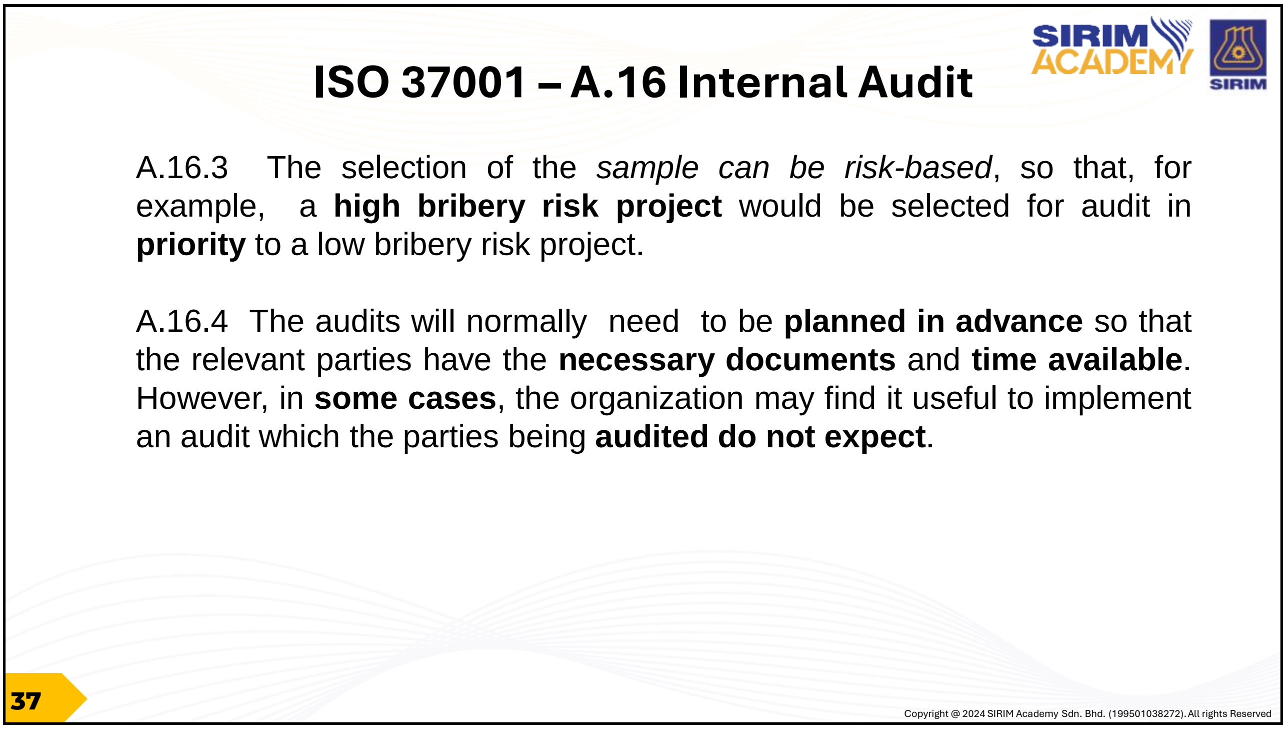


ISO 37001 – A.16 Internal Audit

A.16.1 The requirement in 9.2 does not mean that an organization is obliged to have its own separate internal audit function. It requires the organization **to appoint a suitable, competent and independent function or person with responsibility to undertake this audit**. An organization may use a third party to operate its entire internal audit program, or may engage a third party to implement certain portions of an existing program.

A.16.2 The frequency of audit will depend on the organization's requirements. It is likely that some **sample projects, contracts, procedures, controls and systems** will be **selected for audit each year**

36



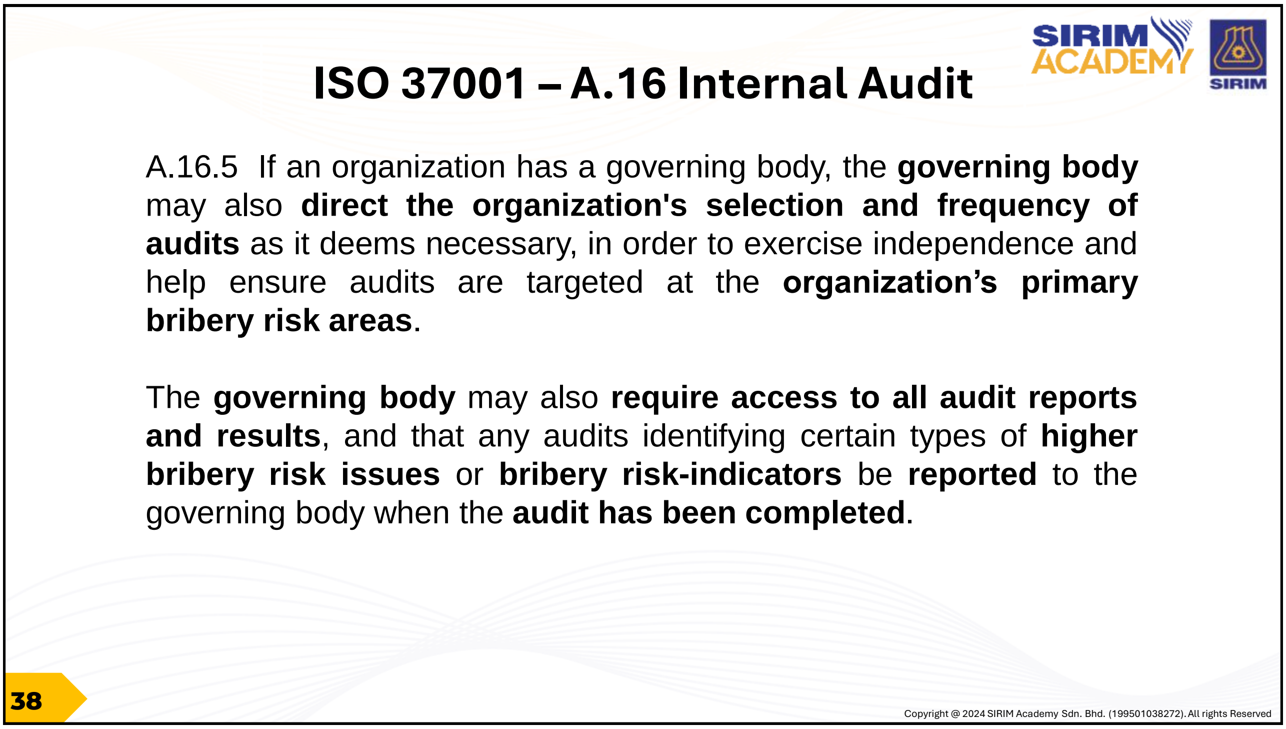
ISO 37001 – A.16 Internal Audit

A.16.3 The selection of the *sample can be risk-based*, so that, for example, a **high bribery risk project** would be selected for audit in **priority** to a low bribery risk project.

A.16.4 The audits will normally need to be **planned in advance** so that the relevant parties have the **necessary documents** and **time available**. However, in **some cases**, the organization may find it useful to implement an audit which the parties being **audited do not expect**.

37

37



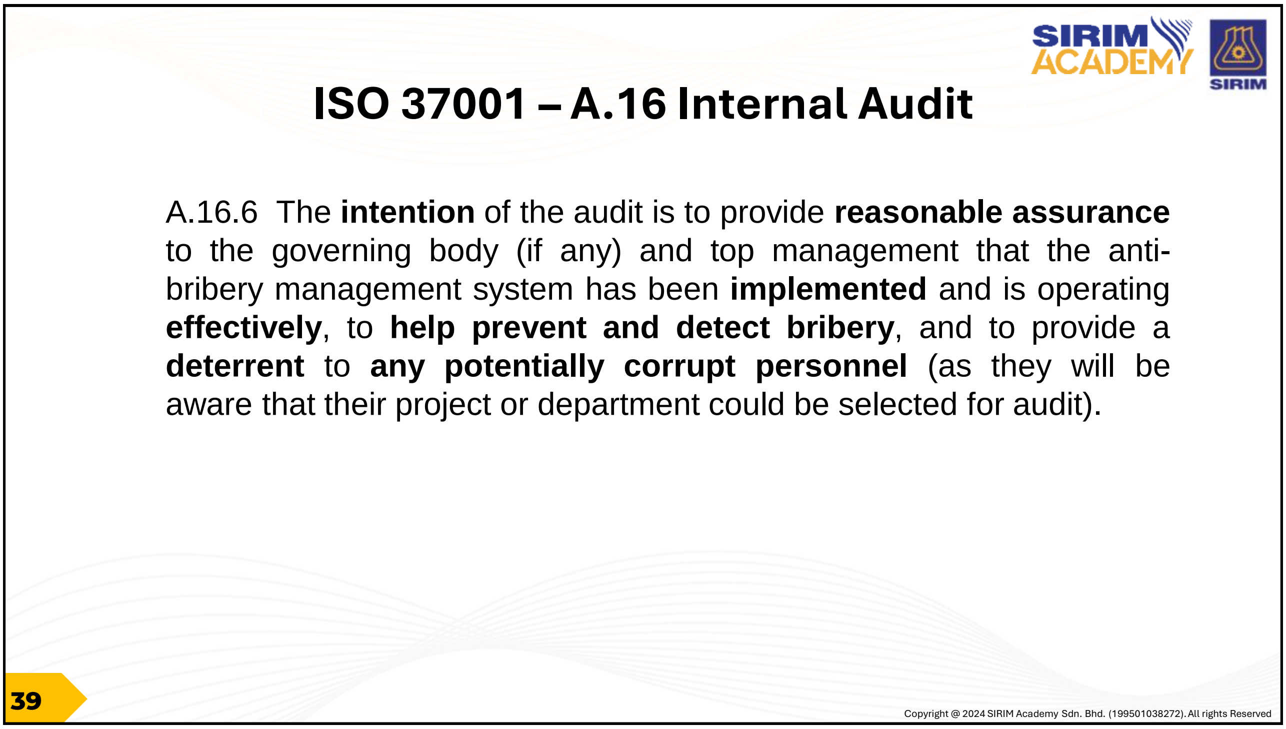
ISO 37001 – A.16 Internal Audit

A.16.5 If an organization has a governing body, the **governing body** may also **direct the organization's selection and frequency of audits** as it deems necessary, in order to exercise independence and help ensure audits are targeted at the **organization's primary bribery risk areas**.

The **governing body** may also **require access to all audit reports and results**, and that any audits identifying certain types of **higher bribery risk issues** or **bribery risk-indicators** be **reported** to the governing body when the **audit has been completed**.

38

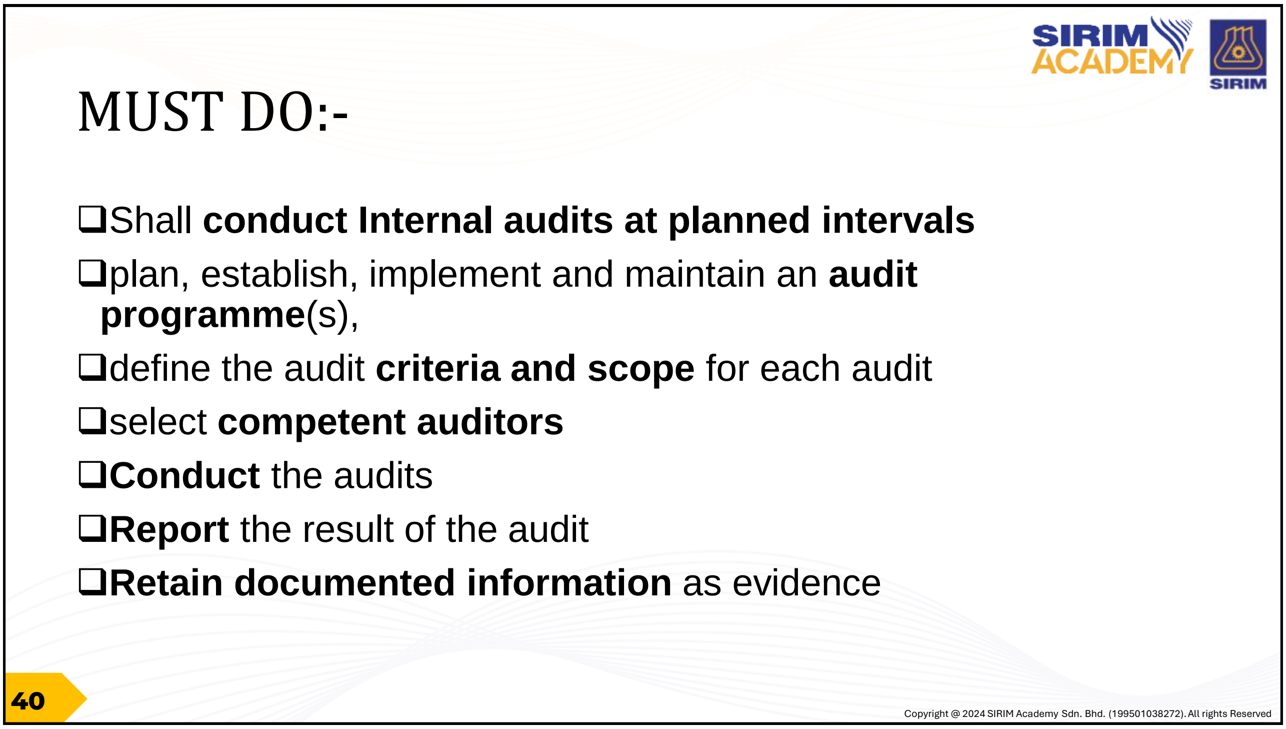
38



ISO 37001 – A.16 Internal Audit

A.16.6 The **intention** of the audit is to provide **reasonable assurance** to the governing body (if any) and top management that the anti-bribery management system has been **implemented** and is operating **effectively**, to **help prevent and detect bribery**, and to provide a **deterrent** to **any potentially corrupt personnel** (as they will be aware that their project or department could be selected for audit).

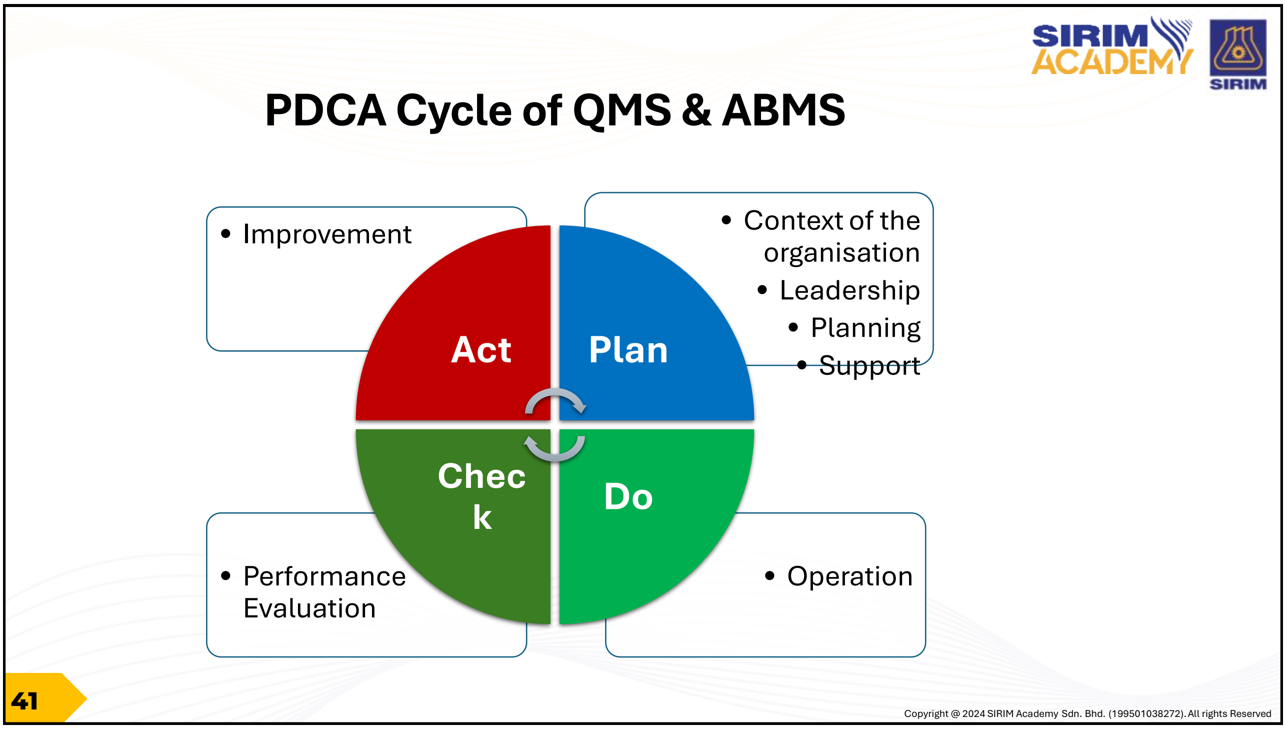
39



MUST DO:-

- ❑Shall **conduct Internal audits at planned intervals**
- ❑plan, establish, implement and maintain an **audit programme**(s),
- ❑define the audit **criteria and scope** for each audit
- ❑select **competent auditors**
- ❑**Conduct** the audits
- ❑**Report** the result of the audit
- ❑**Retain documented information** as evidence

40



PDCA Cycle of QMS & ABMS

Act

- Improvement

Plan

- Context of the organisation
- Leadership
- Planning
- Support

Chec k

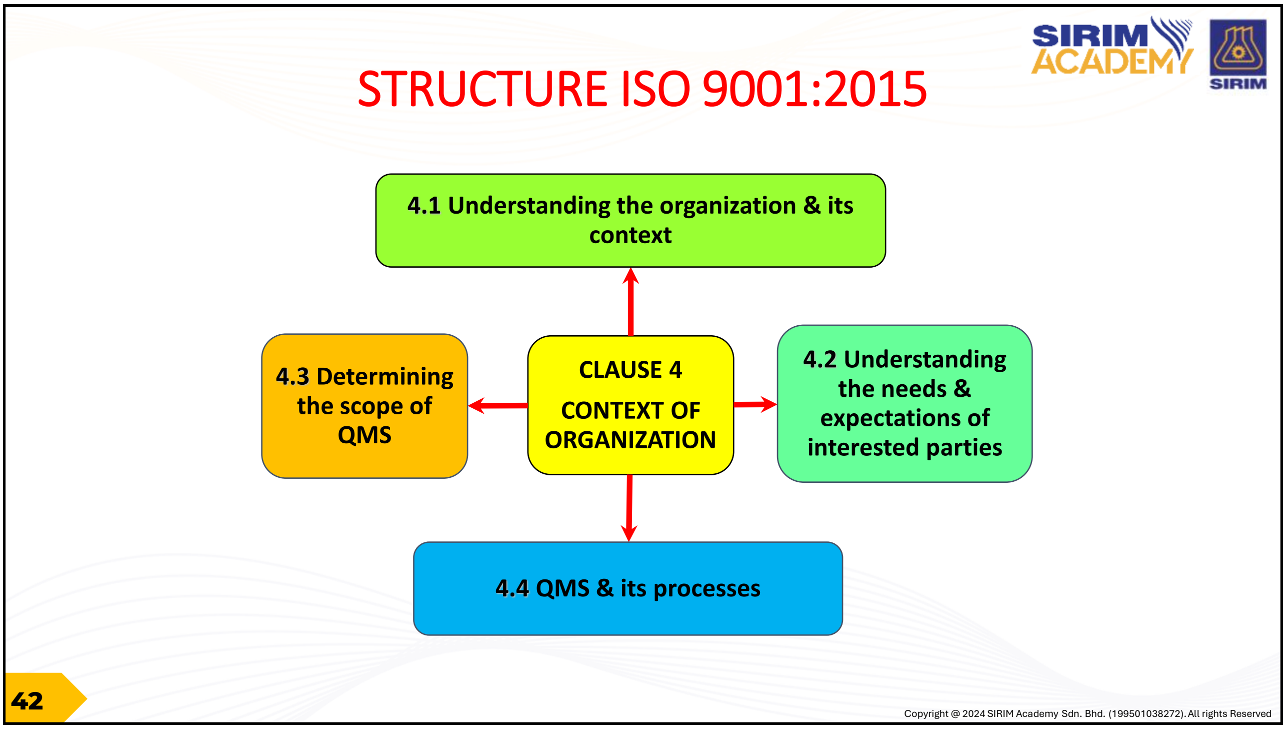
- Performance Evaluation

Do

- Operation

41

41



STRUCTURE ISO 9001:2015

CLAUSE 4

CONTEXT OF ORGANIZATION

4.1 Understanding the organization & its context

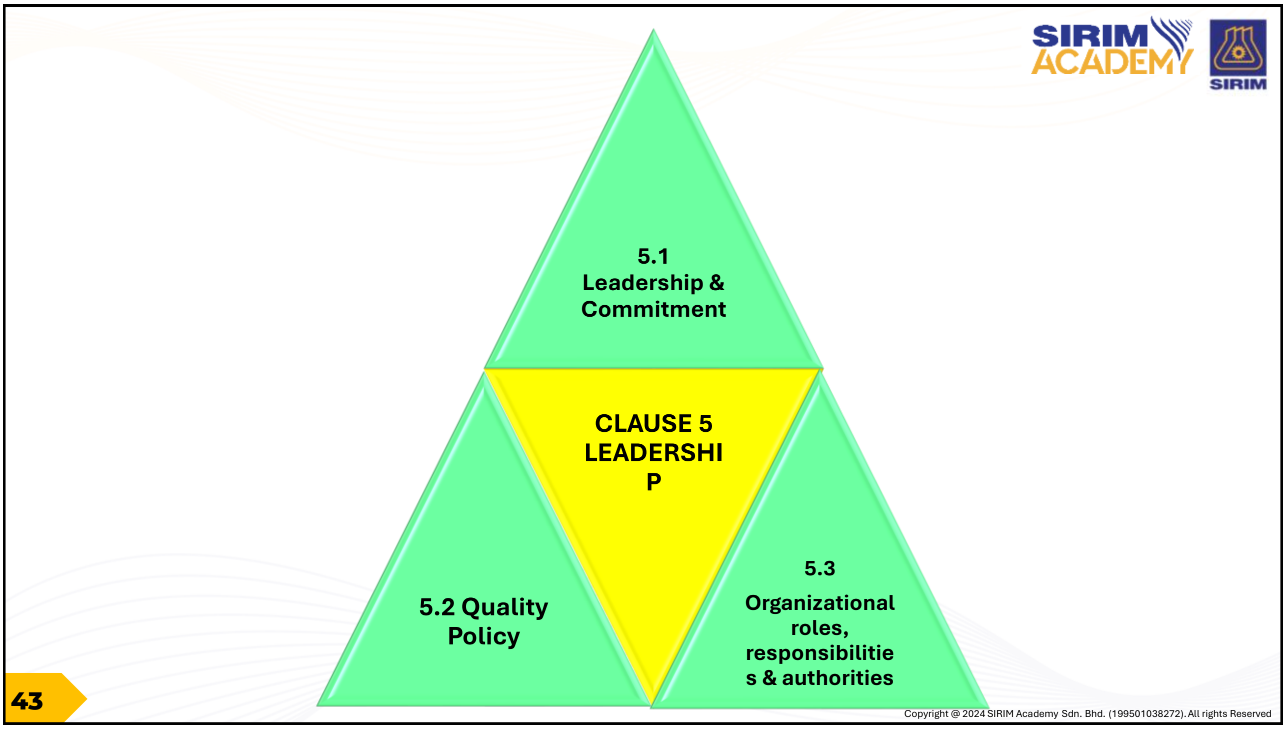
4.2 Understanding the needs & expectations of interested parties

4.3 Determining the scope of QMS

4.4 QMS & its processes

42

42



5.1
Leadership &
Commitment

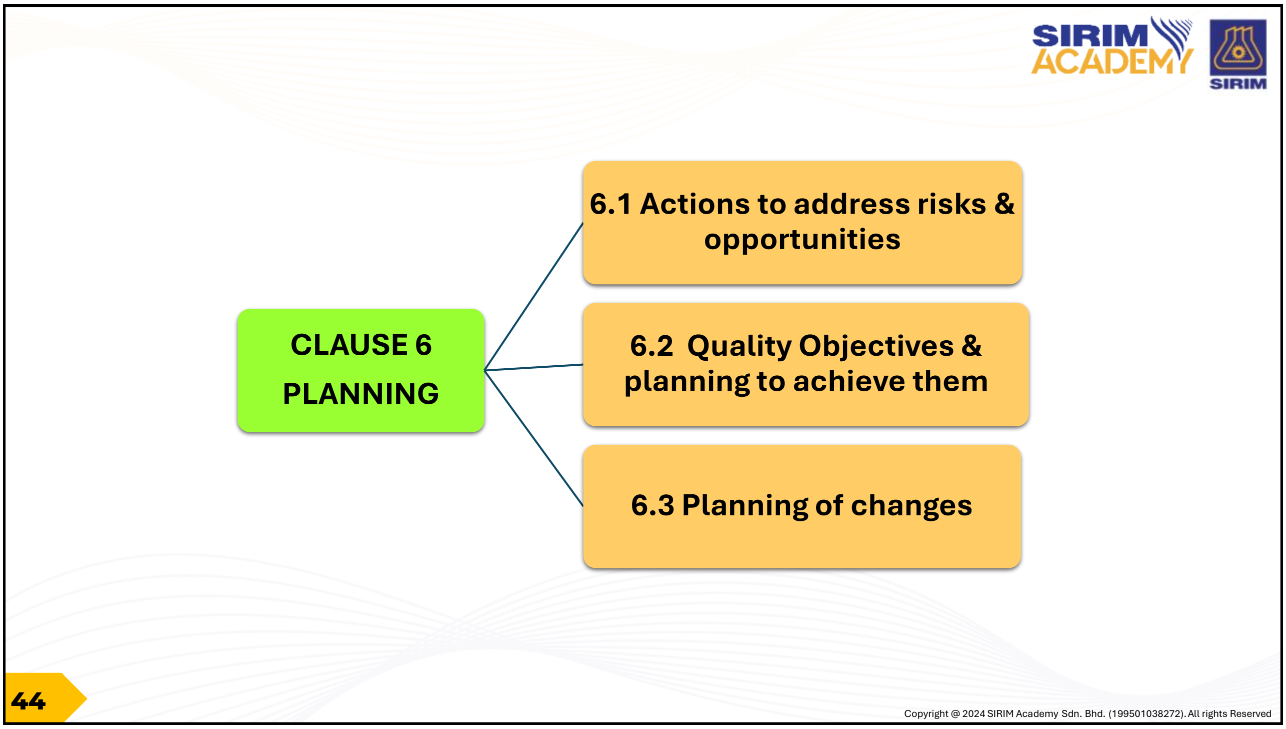
CLAUSE 5
LEADERSHI
P

5.2 Quality
Policy

5.3
Organizational
roles,
responsibilitie
s & authorities

43

43



CLAUSE 6
PLANNING

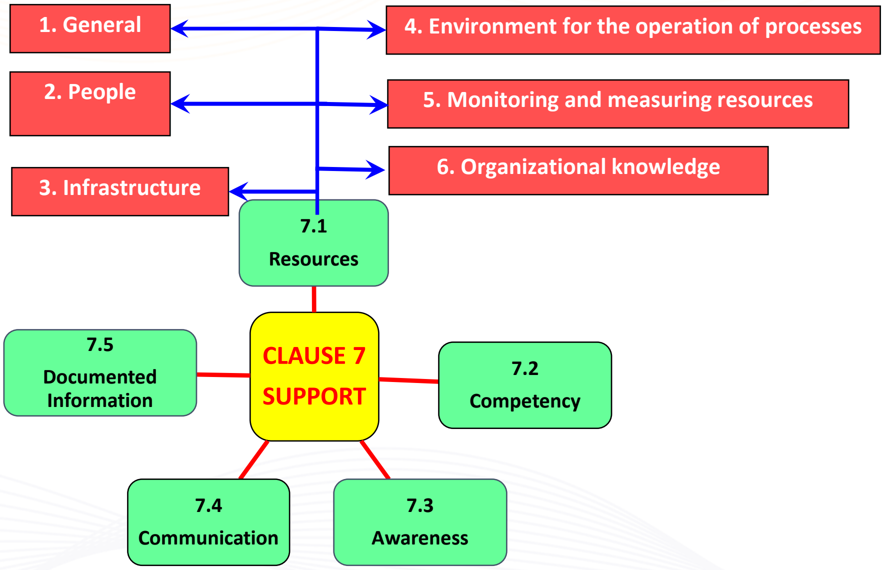
6.1 Actions to address risks & opportunities

6.2 Quality Objectives & planning to achieve them

6.3 Planning of changes

44

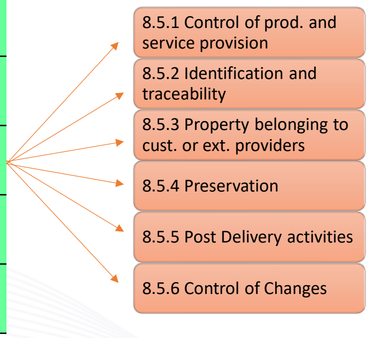
44



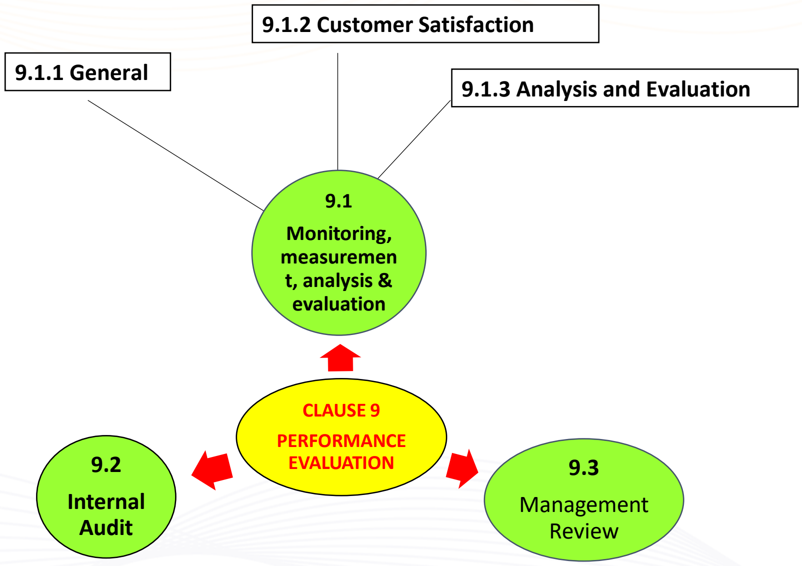
1. General
2. People
3. Infrastructure
4. Environment for the operation of processes
5. Monitoring and measuring resources
6. Organizational knowledge
7.1 Resources
CLAUSE 7 SUPPORT
7.5 Documented Information
7.2 Competency
7.4 Communication
7.3 Awareness

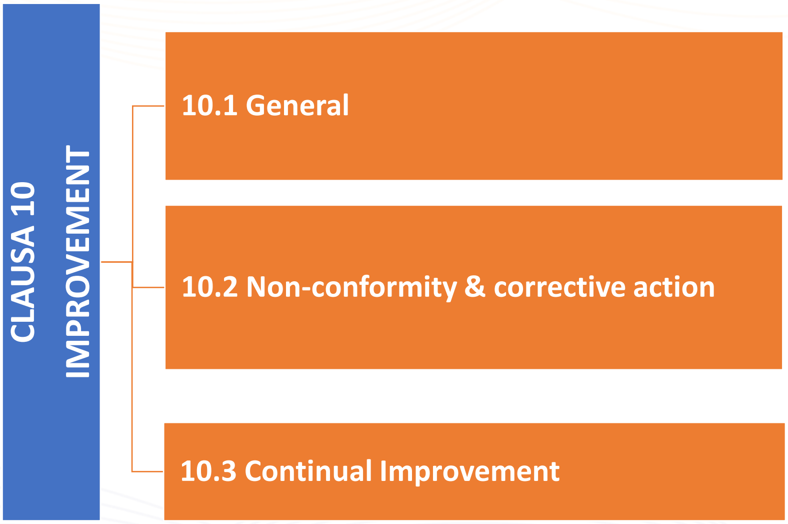
CLAUSE 8 OPERATION

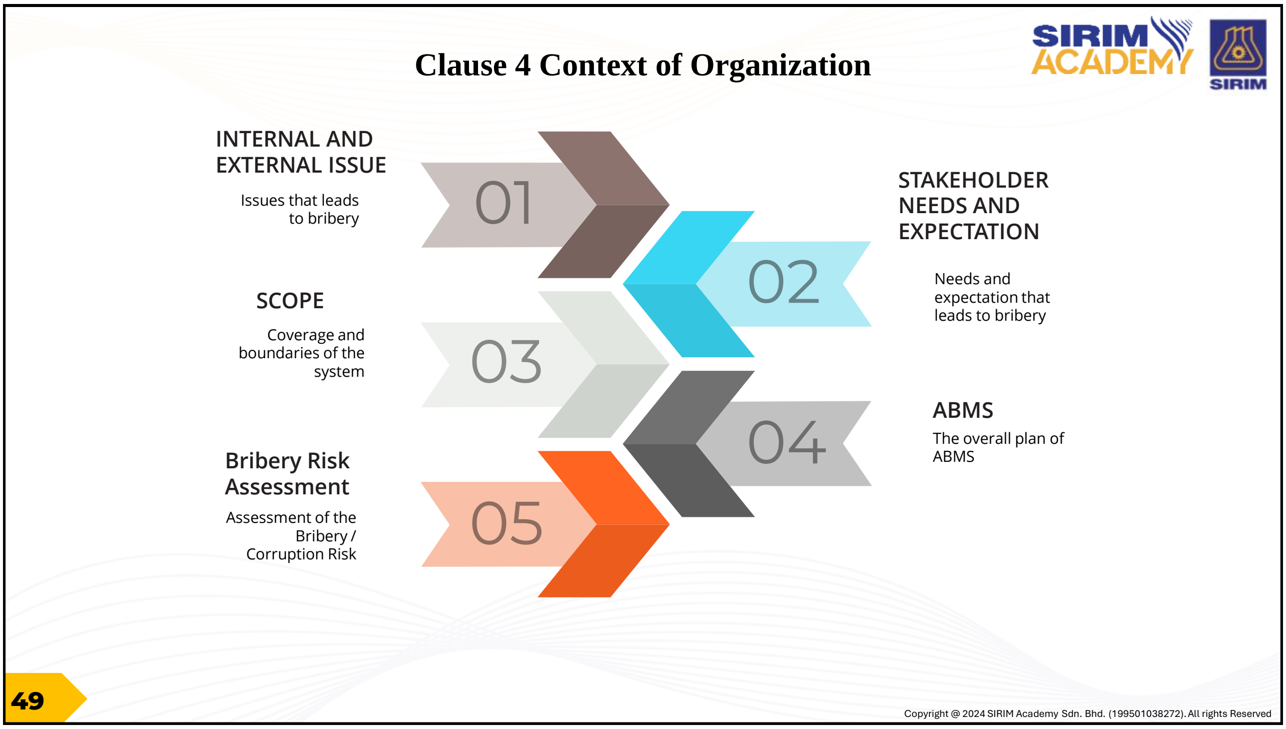
8.1	Operational planning & control
8.2	Determination of requirements for products & services
8.3	Design & development of products & services
8.4	Control of externally provided products & services
8.5	Production & service provision
8.6	Release of products & services
8.7	Control of NC process outputs, products & services



8.5.1 Control of prod. and service provision
8.5.2 Identification and traceability
8.5.3 Property belonging to cust. or ext. providers
8.5.4 Preservation
8.5.5 Post Delivery activities
8.5.6 Control of Changes


9.1.2 Customer Satisfaction
9.1.1 General
9.1.3 Analysis and Evaluation
9.1
Monitoring, measuremen t, analysis & evaluation
CLAUSE 9
PERFORMANCE EVALUATION
9.2
Internal Audit
9.3
Management Review


CLAUSA 10
IMPROVEMENT
10.1 General
10.2 Non-conformity & corrective action
10.3 Continual Improvement



Clause 4 Context of Organization

01

INTERNAL AND EXTERNAL ISSUE

Issues that leads to bribery

02

STAKEHOLDER NEEDS AND EXPECTATION

Needs and expectation that leads to bribery

03

SCOPE

Coverage and boundaries of the system

04

ABMS

The overall plan of ABMS

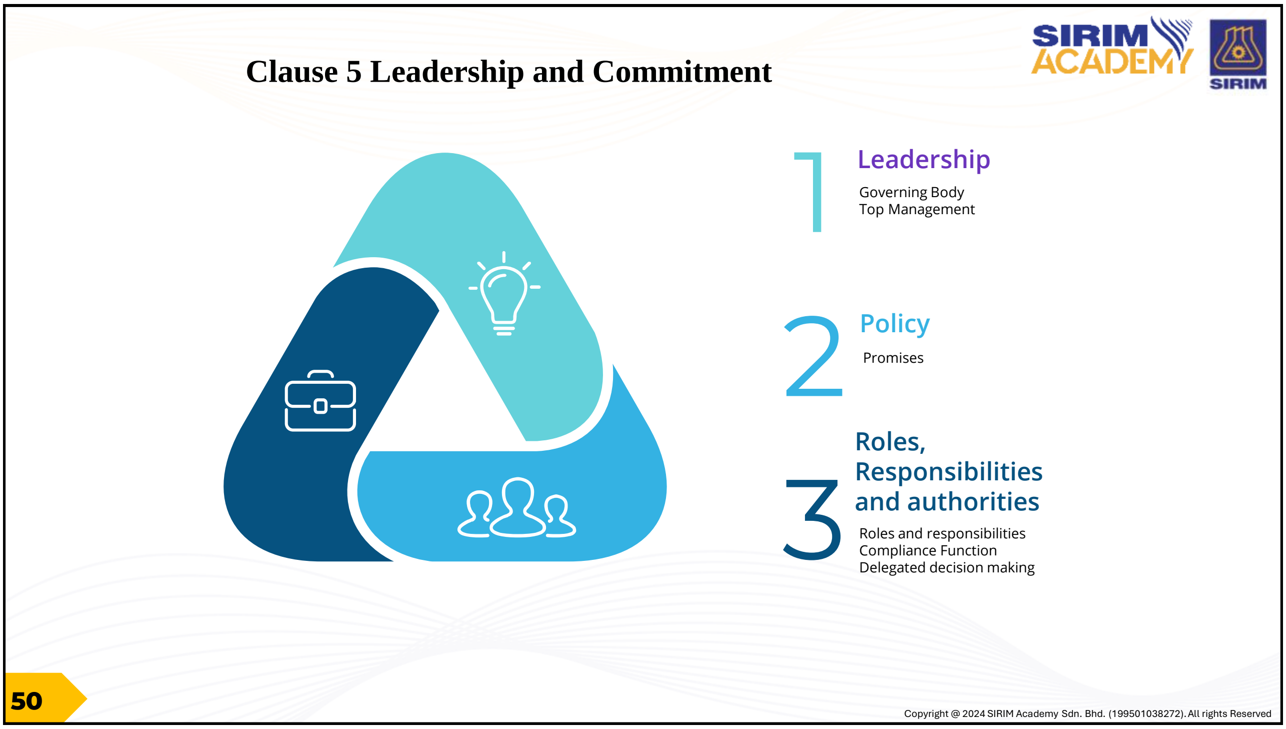
05

Bribery Risk Assessment

Assessment of the Bribery / Corruption Risk

49

49



Clause 5 Leadership and Commitment

1 Leadership

Governing Body
Top Management

2 Policy

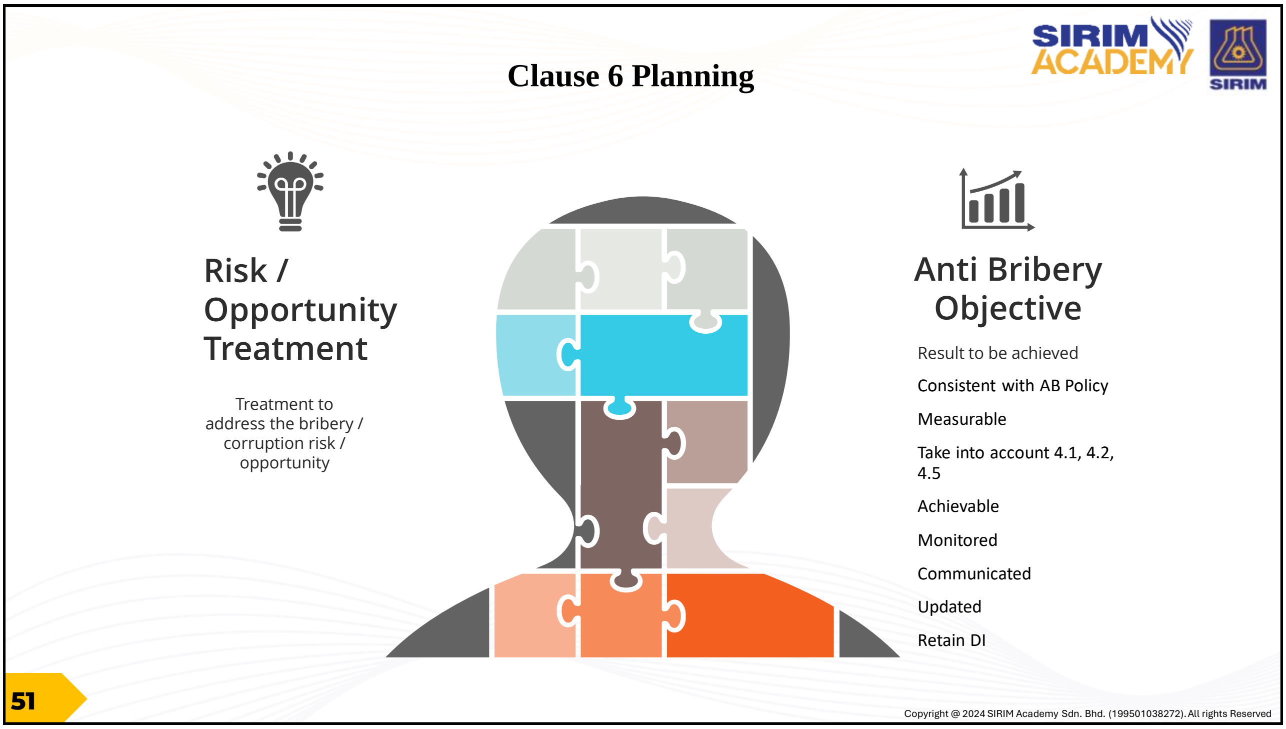
Promises

3 Roles, Responsibilities and authorities

Roles and responsibilities
Compliance Function
Delegated decision making

50

50



Clause 6 Planning

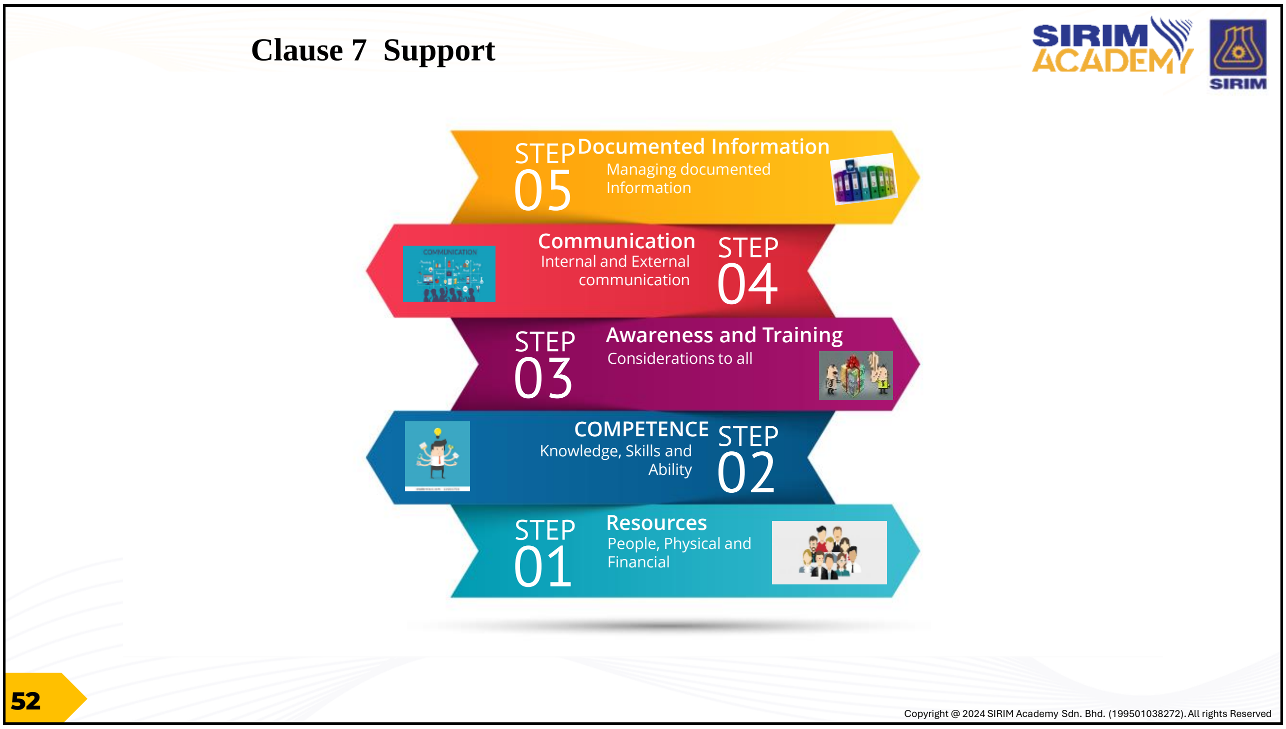
Risk / Opportunity Treatment

Treatment to address the bribery / corruption risk / opportunity

Anti Bribery Objective

- Result to be achieved
- Consistent with AB Policy
- Measurable
- Take into account 4.1, 4.2, 4.5
- Achievable
- Monitored
- Communicated
- Updated
- Retain DI

51



Clause 7 Support

STEP 05 Documented Information
Managing documented Information

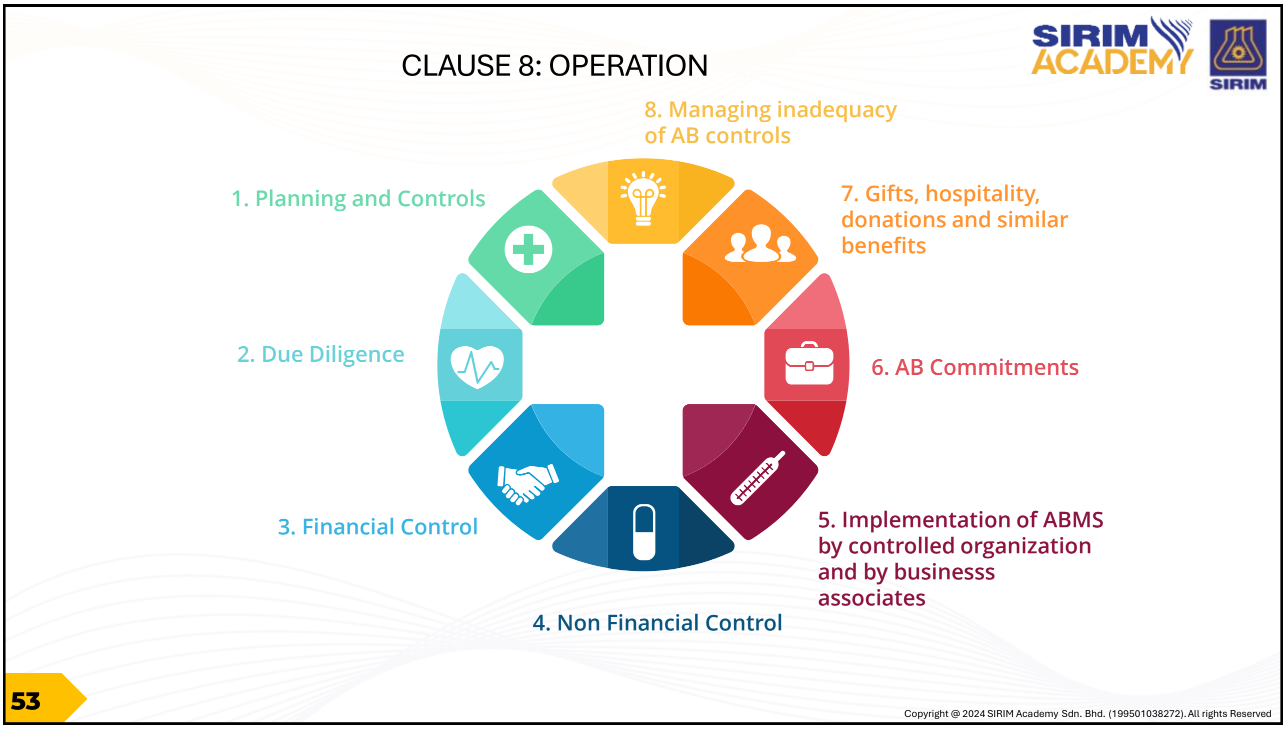
STEP 04 Communication
Internal and External communication

STEP 03 Awareness and Training
Considerations to all

STEP 02 COMPETENCE
Knowledge, Skills and Ability

STEP 01 Resources
People, Physical and Financial

52



CLAUSE 8: OPERATION

1. Planning and Controls

2. Due Diligence

3. Financial Control

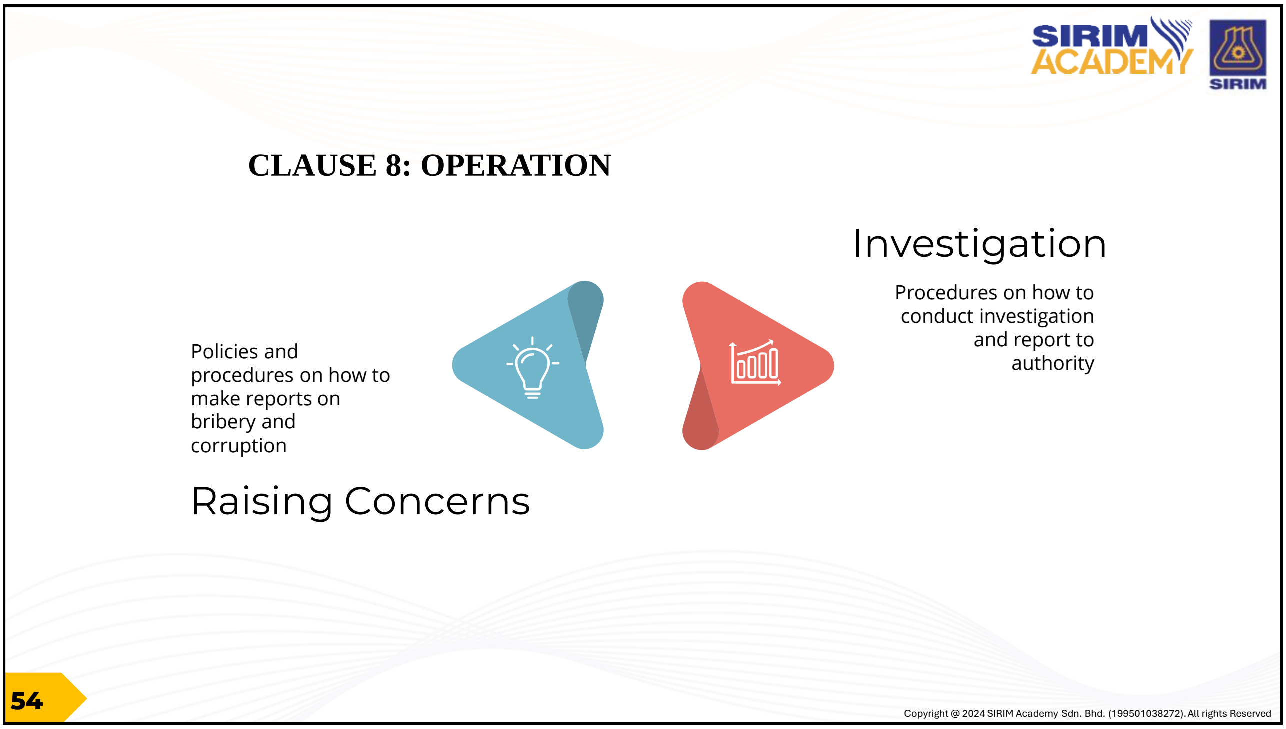
4. Non Financial Control

5. Implementation of ABMS by controlled organization and by businesss associates

6. AB Commitments

7. Gifts, hospitality, donations and similar benefits

8. Managing inadequacy of AB controls



CLAUSE 8: OPERATION

Raising Concerns

Policies and procedures on how to make reports on bribery and corruption

Investigation

Procedures on how to conduct investigation and report to authority

CLAUSE 9 : PERFORMANCE EVALUATION

1 Monitoring Measurement Analysis Evaluation

2 Internal Audit

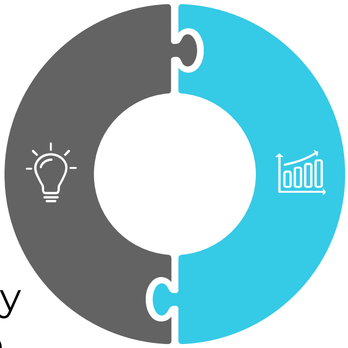
3 Management Review Governing Body Review

4 Compliance Function Review

CLAUSE 10 : IMPROVEMENT

Continual Improvement

Recurring activity to enhance performance



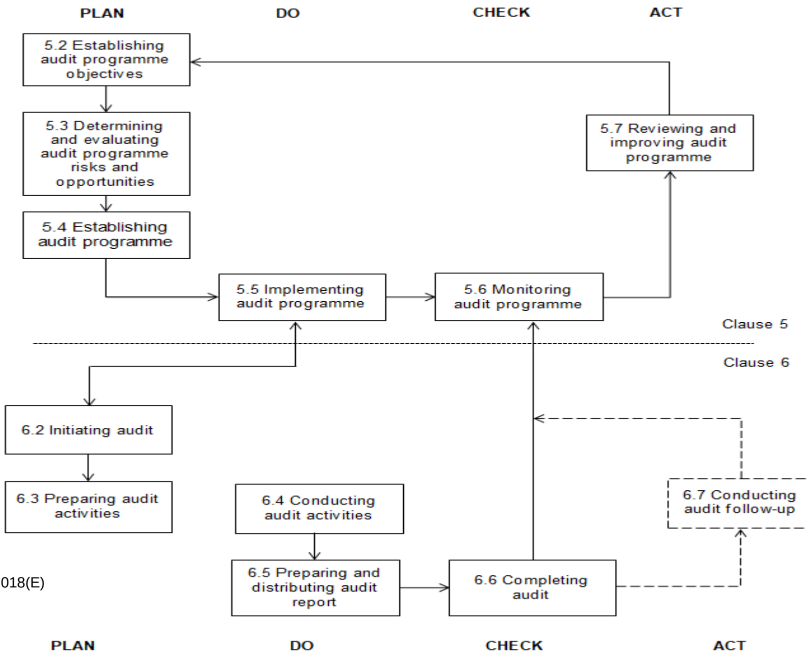
Non fulfilment of a requirement

Action to eliminate the cause of nonconformity and to prevent recurrence

Nonconformity and corrective action

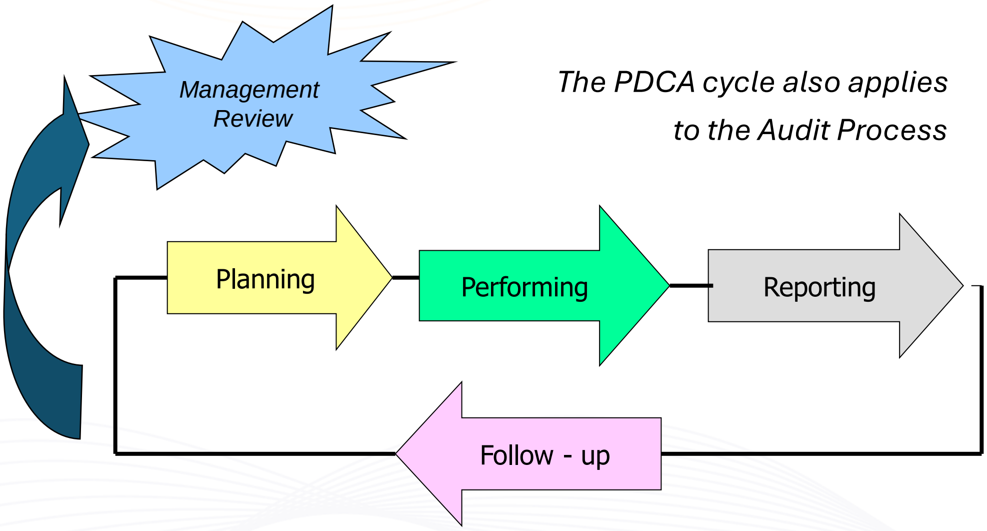
AUDIT PLANNING

Figure 1: Process flow for the management of an audit programme


PLAN
DO
CHECK
ACT
5.2 Establishing audit programme objectives
5.3 Determining and evaluating audit programme risks and opportunities
5.4 Establishing audit programme
5.5 Implementing audit programme
5.6 Monitoring audit programme
5.7 Reviewing and improving audit programme
Clause 5
Clause 6
6.2 Initiating audit
6.3 Preparing audit activities
6.4 Conducting audit activities
6.5 Preparing and distributing audit report
6.6 Completing audit
6.7 Conducting audit follow-up
PLAN
DO
CHECK
ACT

Source: ISO 19011:2018(E)

Audit Process

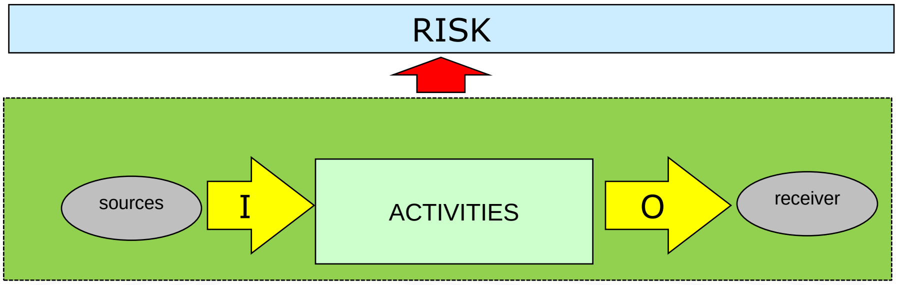


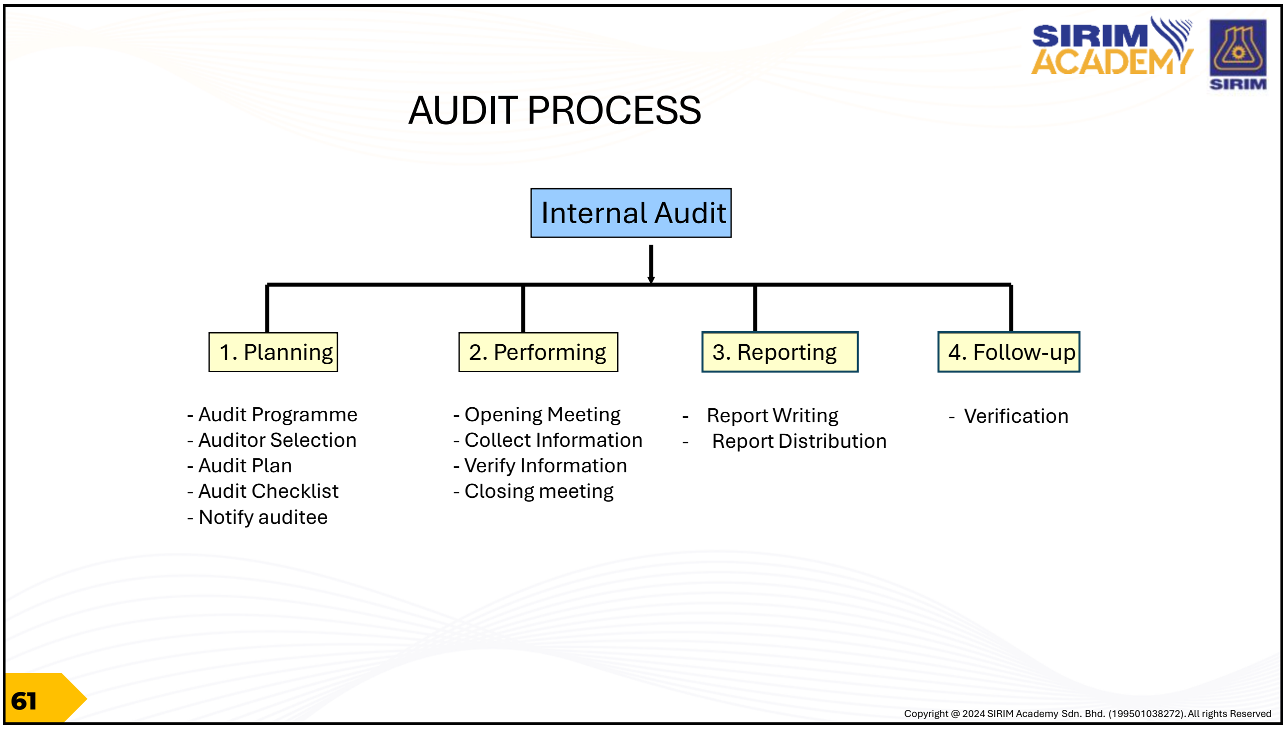
The PDCA cycle also applies to the Audit Process

WHAT IS RISK BASED AUDITING?

Examination to an organization's overall risk management framework. It is primarily focused on the inherent risk involved in the activities or system and provide assurance that risk is being managed by the management within the defined risk appetite levels.

By doing this, it provides assurance to the organization that risk management processes are managing risks effectively, in relation to the risk appetite.





AUDIT PROCESS

Internal Audit

1. Planning

- Audit Programme
- Auditor Selection
- Audit Plan
- Audit Checklist
- Notify auditee

2. Performing

- Opening Meeting
- Collect Information
- Verify Information
- Closing meeting

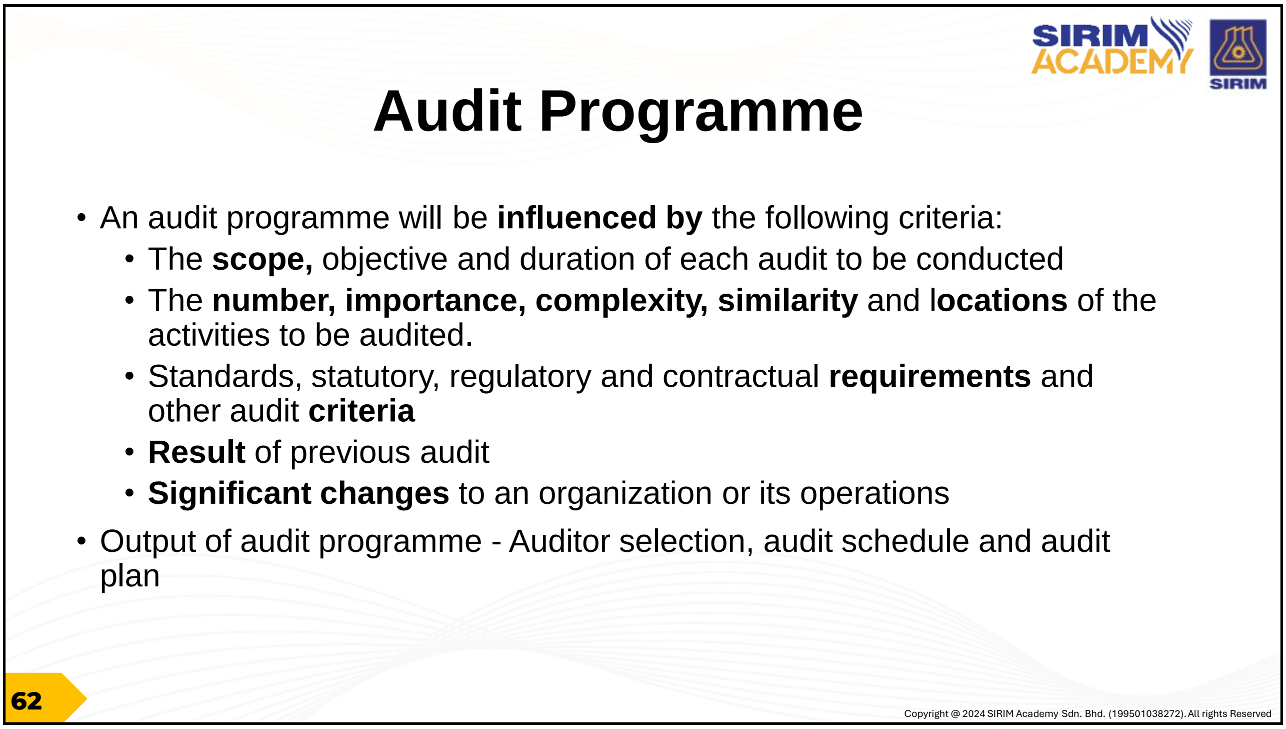
3. Reporting

- Report Writing
- Report Distribution

4. Follow-up

- Verification

61



Audit Programme

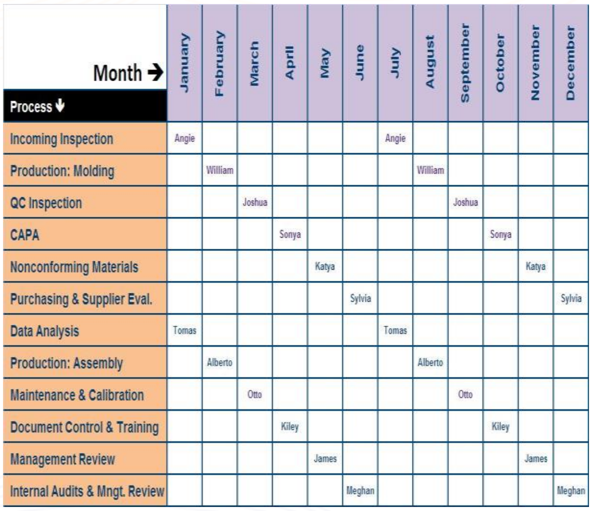
- An audit programme will be **influenced by** the following criteria:
  - The **scope,** objective and duration of each audit to be conducted
  - The **number, importance, complexity, similarity** and l**ocations** of the activities to be audited.
  - Standards, statutory, regulatory and contractual **requirements** and other audit **criteria**
  - **Result** of previous audit
  - **Significant changes** to an organization or its operations
- Output of audit programme - Auditor selection, audit schedule and audit plan

62

AUDIT PROGRAMME

Set of one or more audits planned for specific time frame and directed towards a specific purpose

Source: ISO 19011:2018, clause 3.4



Month ➔ Process ↓	January	February	March	April	May	June	July	August	September	October	November	December
Incoming Inspection	Angie						Angie					
Production: Molding		William						William				
QC Inspection			Joshua						Joshua			
CAPA				Sonya						Sonya		
Nonconforming Materials					Katya						Katya	
Purchasing & Supplier Eval.						Sylvia						Sylvia
Data Analysis	Tomas						Tomas					
Production: Assembly		Alberto						Alberto				
Maintenance & Calibration			Otto						Otto			
Document Control & Training				Kiley						Kiley		
Management Review					James						James	
Internal Audits & Mngt. Review						Meghan						Meghan

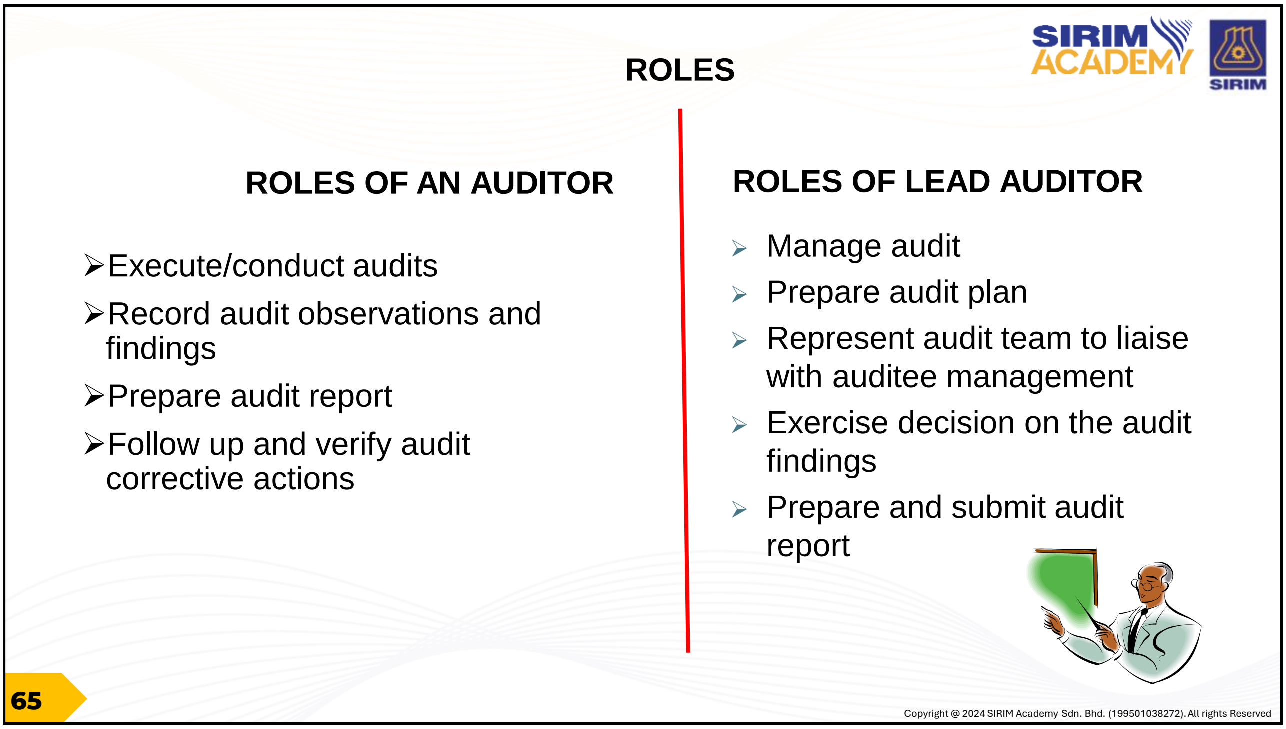
AUDITOR SELECTION

<u>Auditor</u>

A person with the competence to conduct an audit

<u>Lead Auditor / Team Leader</u>

An Auditor qualified and appointed to lead and manage the audit team.



ROLES

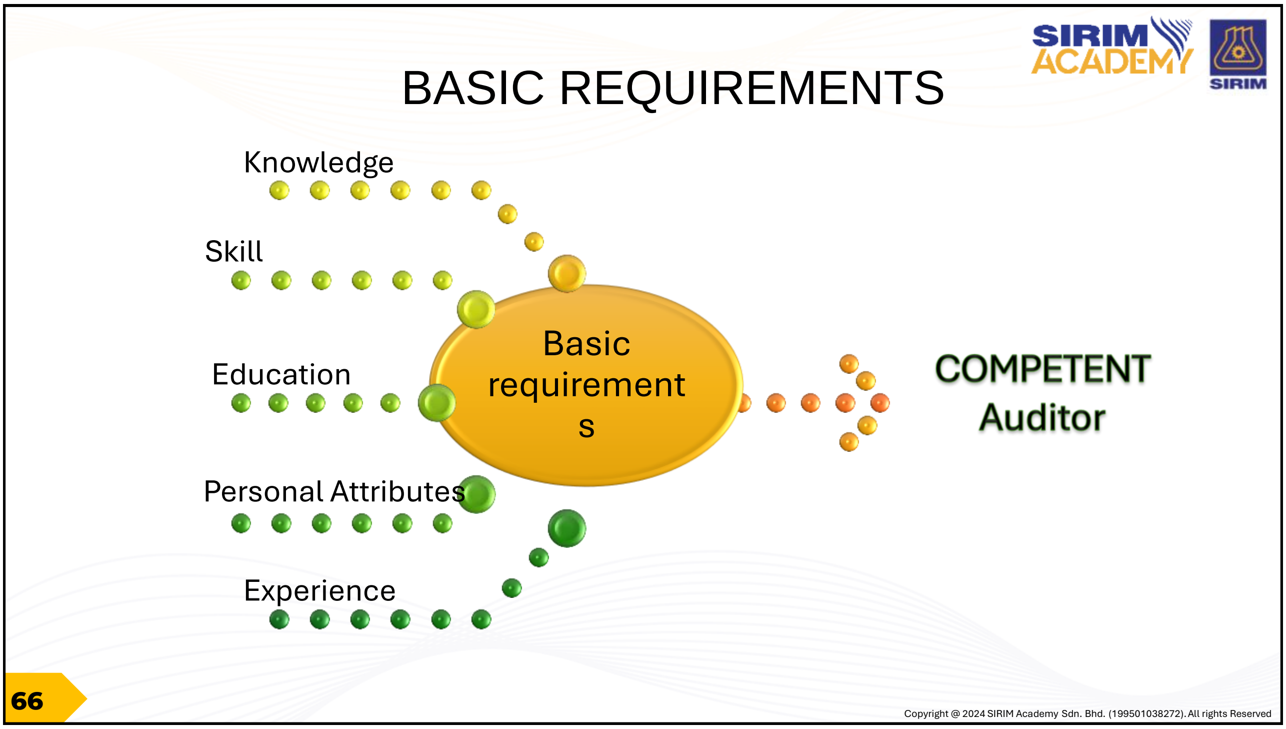
ROLES OF AN AUDITOR

- ➢Execute/conduct audits
- ➢Record audit observations and findings
- ➢Prepare audit report
- ➢Follow up and verify audit corrective actions

ROLES OF LEAD AUDITOR

- ➢ Manage audit
- ➢ Prepare audit plan
- ➢ Represent audit team to liaise with auditee management
- ➢ Exercise decision on the audit findings
- ➢ Prepare and submit audit report

65



BASIC REQUIREMENTS

66

Knowledge and Skills

Knowledge and Skills

- KNOWLEDGE

Understands the requirements of ISO 37001, Company practices, legal requirements

- SKILLS

Good audit techniques, good communication skills in writing and conversation and able to make fair judgements

Education and Experience

Education

Education level and background

Experience in related industry

Related training such as Understanding ISO ISO 37001, Internal Auditors Training

Audit Plan

Description of the activities and arrangement of an audit

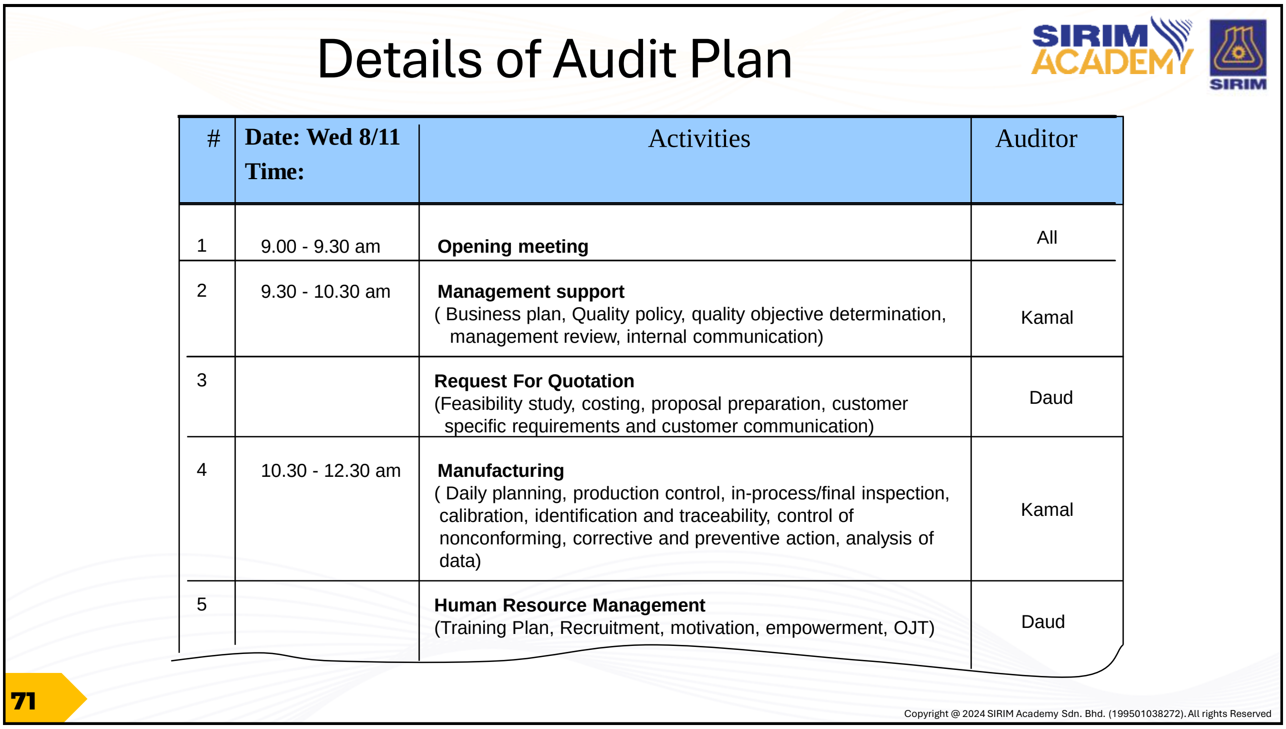
Source:
ISO 19011:2018, clause 3.6

Audit Plan should include:

- Identification of auditee's organization and functional units to be audited
- Audit objectives and scope
- Audit criteria
- Procedure/methodology for auditing
- Identification of reference documents
- Identification of audit team members
- Expected time and duration for major audit activities
- Schedule of meetings with auditee's management
- Confidentiality requirement (if necessary)

Sample of Audit Plan

Objective:	To verify the compliance of the organization's documented quality management system and its effective implementation in relation with the requirements of ISO 37001:2016
Audit team:	Azhar Dollah (Audit team leader) Abraham Lincon (Auditor) Donald Trump (Auditor) Mariah Carey (Auditor)
Audit criteria:	ISO 37001:2016 standard Organization's documentation Customer specific requirements Regulatory requirements.
Audit Method:	Verification and evaluation of documents, data, records, and forms, witnessing the on-going activities, interviewing the company personnel, reporting of non-conformances, presenting audit finding summary and recommendations..
Facilities:	Meeting/discussion rooms, 4 sets of documented quality system, access to photocopy machine, guides to accompany auditors during the audit and personal protective equipment.

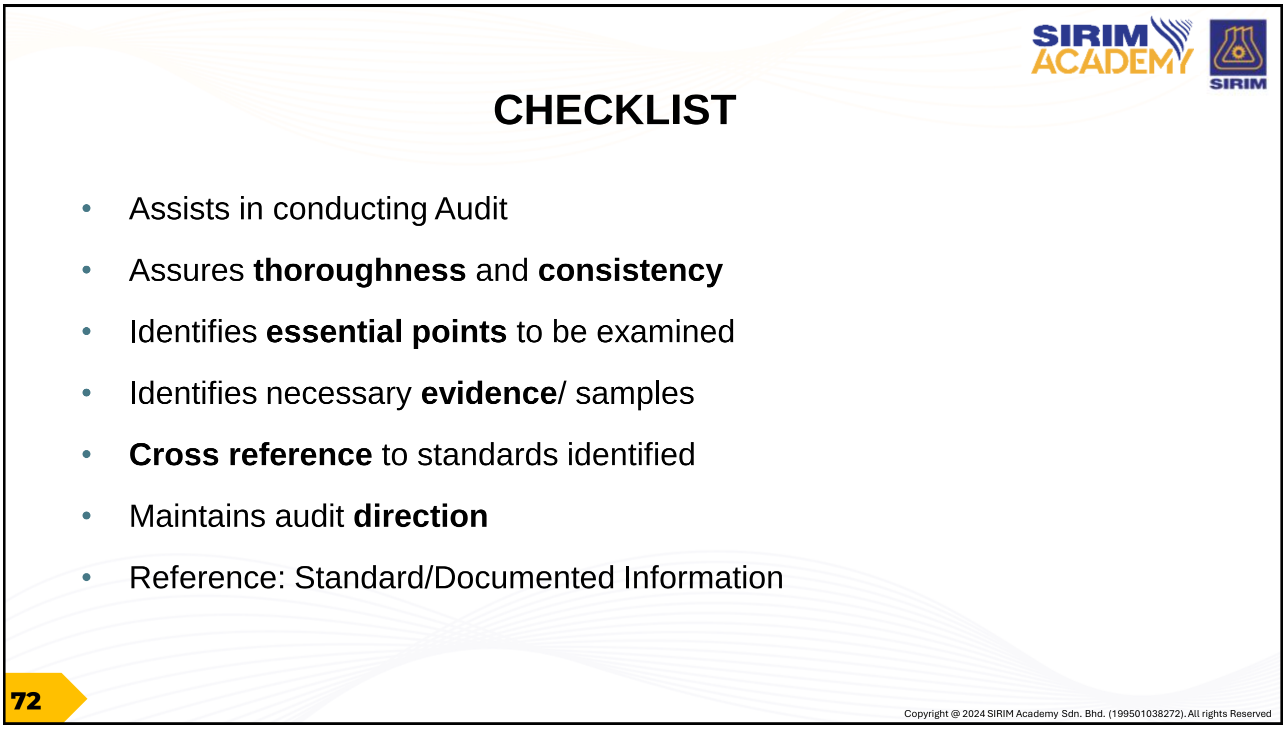


Details of Audit Plan

#	Date: Wed 8/11 Time:	Activities	Auditor
1	9.00 - 9.30 am	**Opening meeting**	All
2	9.30 - 10.30 am	**Management support** (Business plan, Quality policy, quality objective determination, management review, internal communication)	Kamal
3		**Request For Quotation** (Feasibility study, costing, proposal preparation, customer specific requirements and customer communication)	Daud
4	10.30 - 12.30 am	**Manufacturing** (Daily planning, production control, in-process/final inspection, calibration, identification and traceability, control of nonconforming, corrective and preventive action, analysis of data)	Kamal
5		**Human Resource Management** (Training Plan, Recruitment, motivation, empowerment, OJT)	Daud

71

71

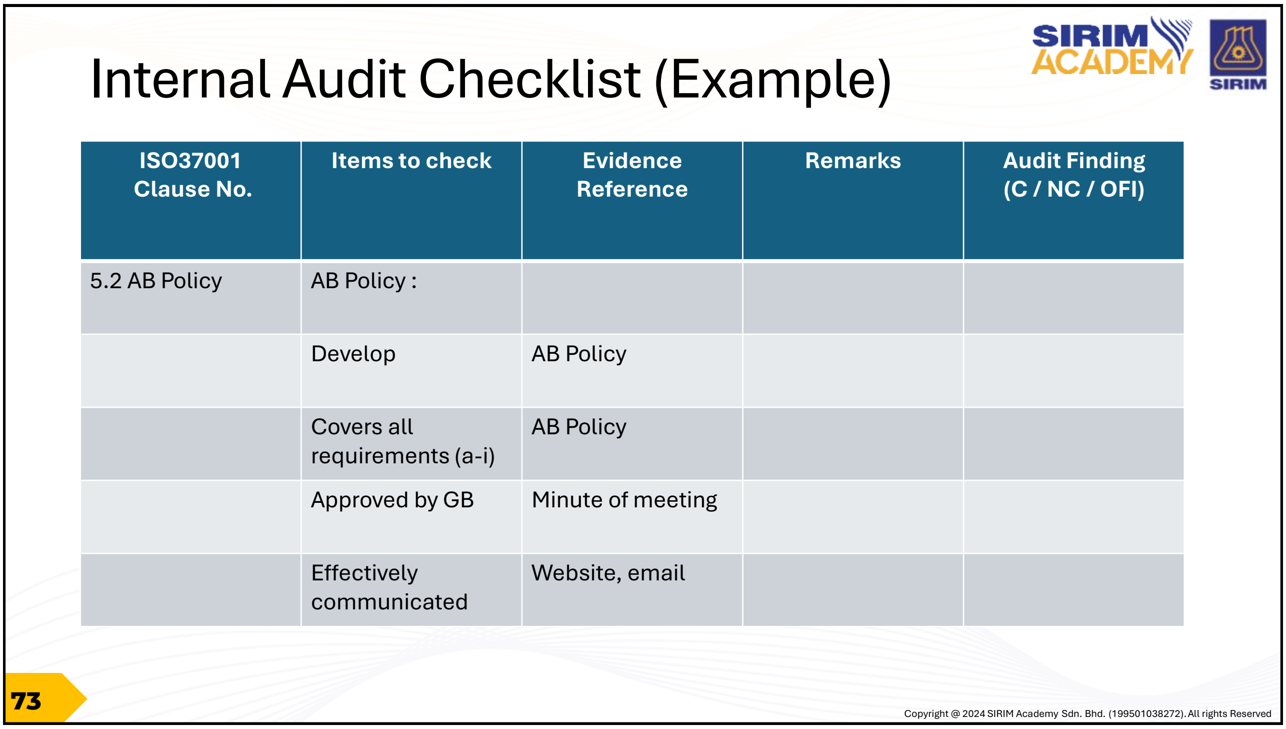


CHECKLIST

- Assists in conducting Audit
- Assures **thoroughness** and **consistency**
- Identifies **essential points** to be examined
- Identifies necessary **evidence**/ samples
- **Cross reference** to standards identified
- Maintains audit **direction**
- Reference: Standard/Documented Information

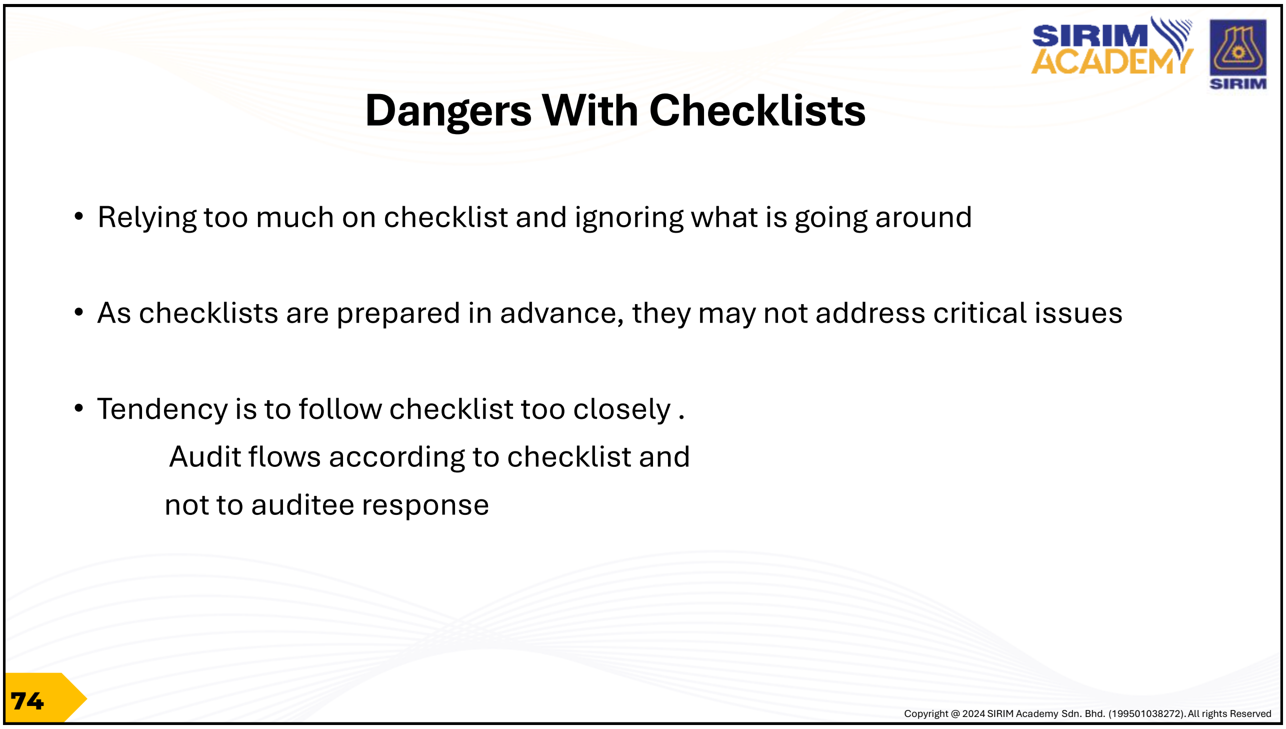
72

72



Internal Audit Checklist (Example)

ISO37001 Clause No.	Items to check	Evidence Reference	Remarks	Audit Finding (C / NC / OFI)
5.2 AB Policy	AB Policy :			
	Develop	AB Policy		
	Covers all requirements (a-i)	AB Policy		
	Approved by GB	Minute of meeting		
	Effectively communicated	Website, email		



Dangers With Checklists

- Relying too much on checklist and ignoring what is going around
- As checklists are prepared in advance, they may not address critical issues
- Tendency is to follow checklist too closely .
  Audit flows according to checklist and
  not to auditee response

Notify Auditee

(1) Confirm the authority to conduct the audit

(2) Provide information on proposed audit timing and audit team composition

(3) Request access to relevant information including records

(4) Determine applicable site safety rules if applicable

(5) Make arrangements for the audits

75

75

PERFORMING AUDIT

76
76

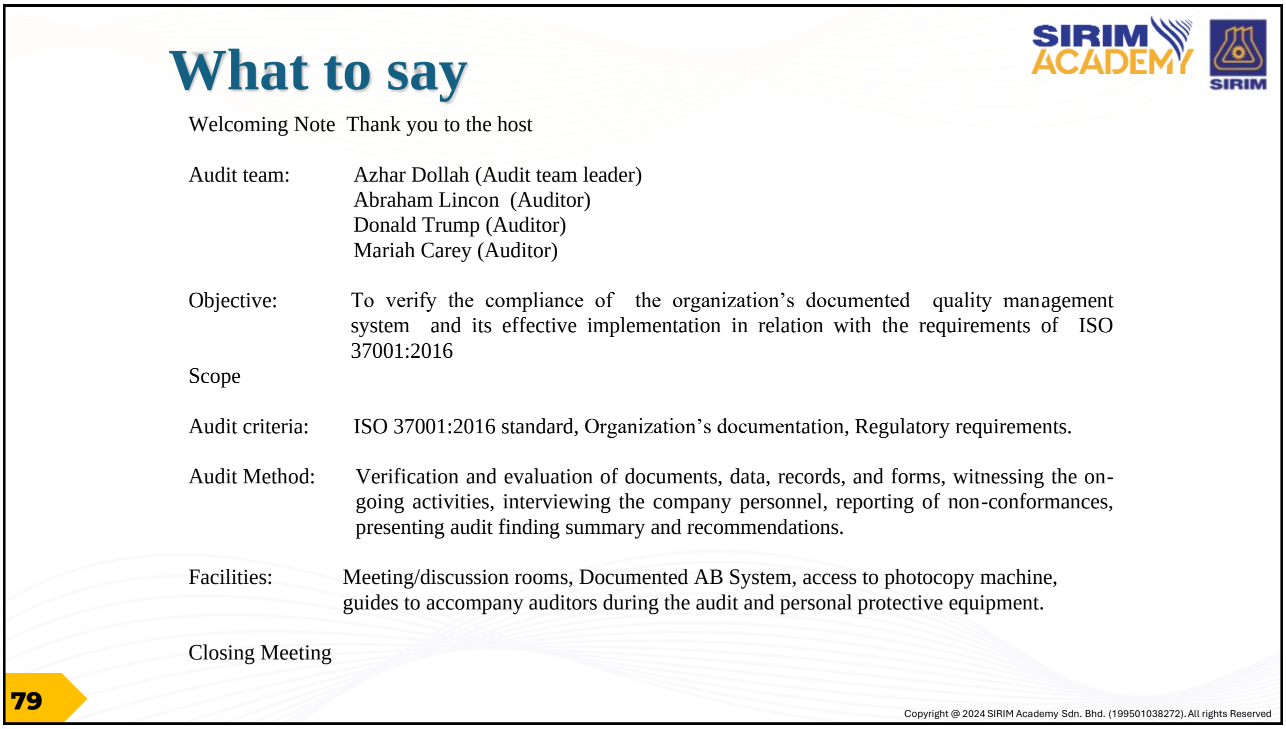
76

PERFORMING AUDIT

- Opening Meeting
- Collecting Information
- Verifying Information

Opening Meeting-Guideline

- Thank you and Introduction of **team**, if deem necessary
- Confirm **Objective** and **Scope**
- Confirm **Audit program**
- Explaining the **audit method**
- **Resources** and **Facilities**
- Matters relating to confidentiality
- Availability of any **guides**
- The audit is taken on a **sample basis**
- Confirm **time** of **closing meeting**
- Questions



What to say

Welcoming Note Thank you to the host

Audit team: Azhar Dollah (Audit team leader)
Abraham Lincon (Auditor)
Donald Trump (Auditor)
Mariah Carey (Auditor)

Objective: To verify the compliance of the organization’s documented quality management system and its effective implementation in relation with the requirements of ISO 37001:2016

Scope

Audit criteria: ISO 37001:2016 standard, Organization’s documentation, Regulatory requirements.

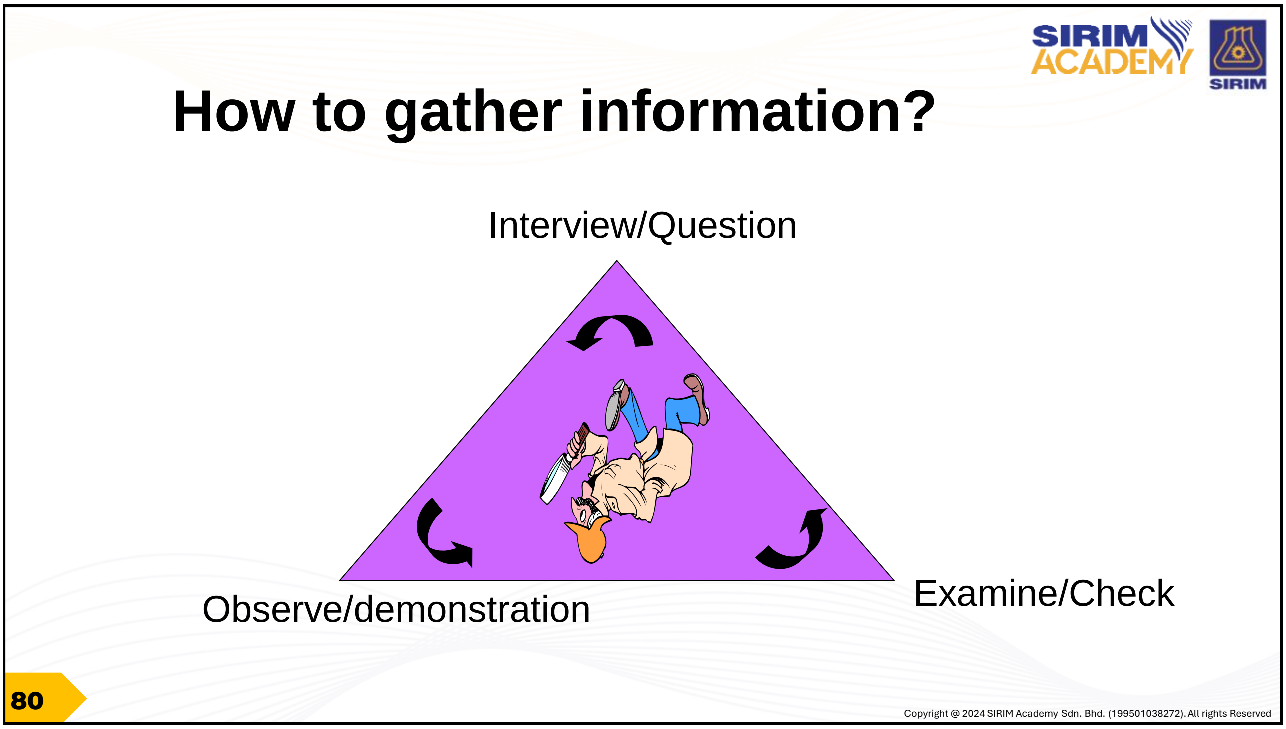
Audit Method: Verification and evaluation of documents, data, records, and forms, witnessing the on-going activities, interviewing the company personnel, reporting of non-conformances, presenting audit finding summary and recommendations.

Facilities: Meeting/discussion rooms, Documented AB System, access to photocopy machine, guides to accompany auditors during the audit and personal protective equipment.

Closing Meeting

79

79



How to gather information?

80

80

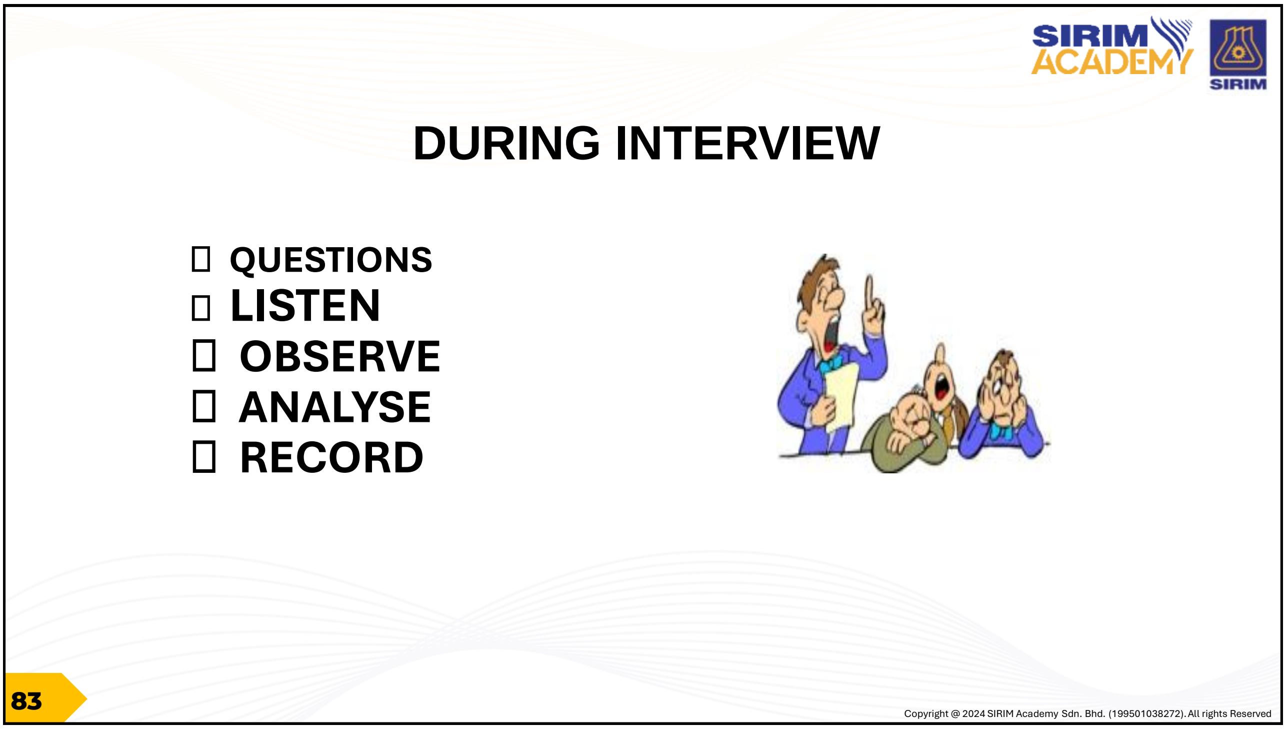
Interview

- Main source of information gathered during the audit is by interviewing people

- Interviewing people is a critical skill that all auditors must strive to master

How to start interviews:

- Start with some ‘small-talk’
- Interviews can be initiated by asking the persons to describe their job scope, work process
- Explain clearly the purpose of the audit
- Express your interest in his/her work
- Interviews the “right’ persons
- Be polite and sincere, and have empathy, i.e. to put one in another person’s place, to understand the problems and pressure



DURING INTERVIEW

□ QUESTIONS
□ LISTEN
□ OBSERVE
□ ANALYSE
□ RECORD

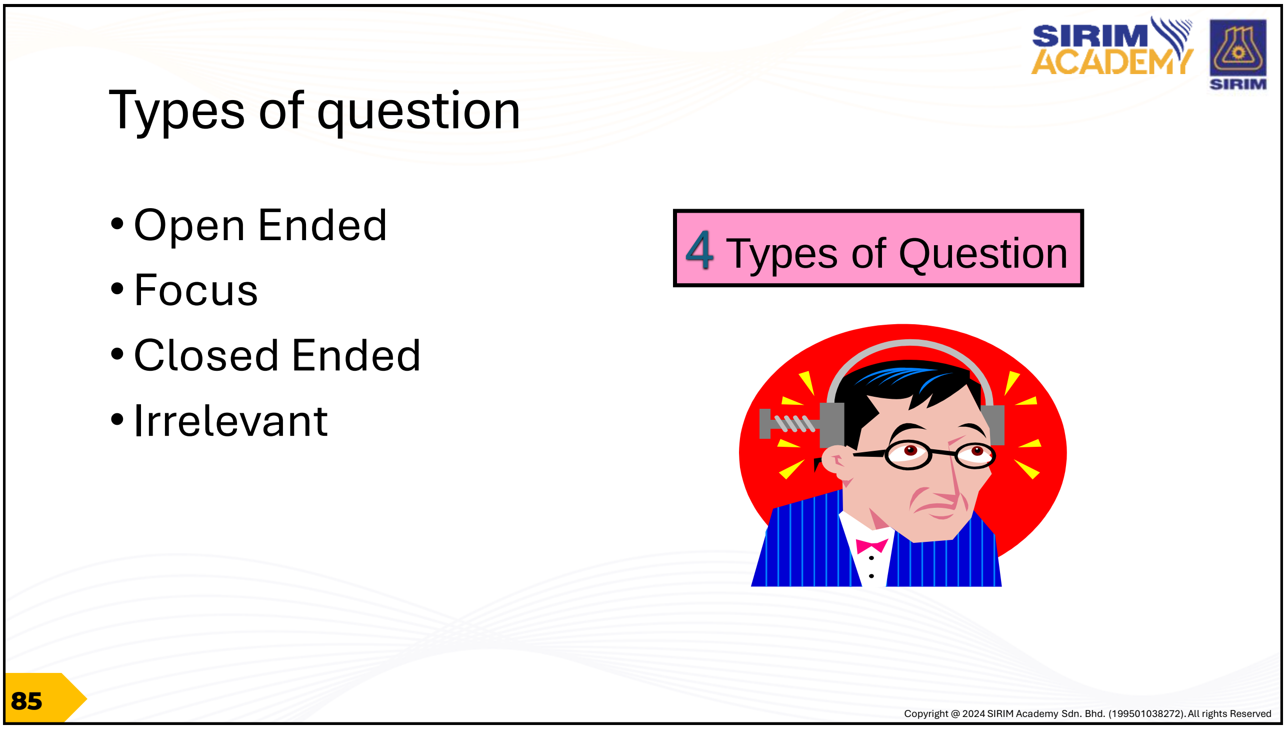
83

AUDITOR'S BEST FRIEND

Please Show Me!

Don't forget !

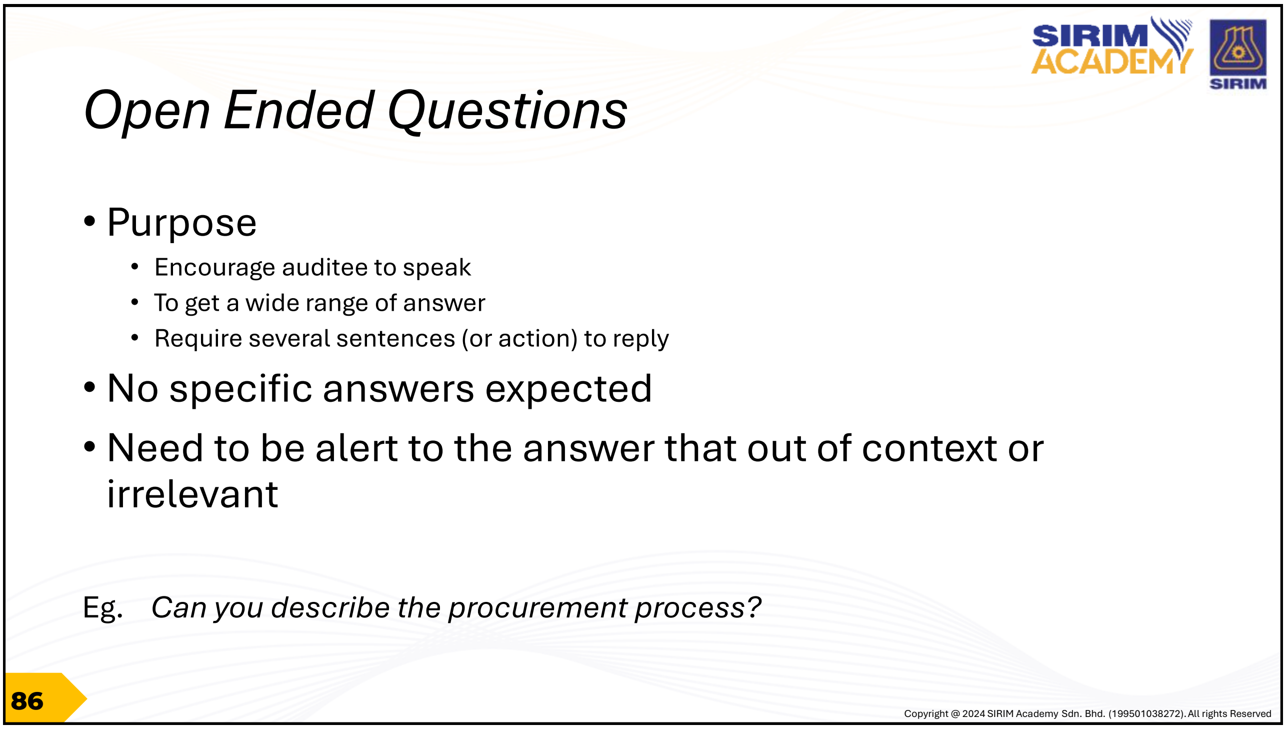
84



Types of question

- Open Ended
- Focus
- Closed Ended
- Irrelevant

4 Types of Question



Open Ended Questions

- Purpose
  - Encourage auditee to speak
  - To get a wide range of answer
  - Require several sentences (or action) to reply
- No specific answers expected
- Need to be alert to the answer that out of context or irrelevant

Eg. *Can you describe the procurement process?*

What ?

Please explain... ?

When ?

How... ?

Who ?

Can you describe how..?

Where ?

Tell me ...

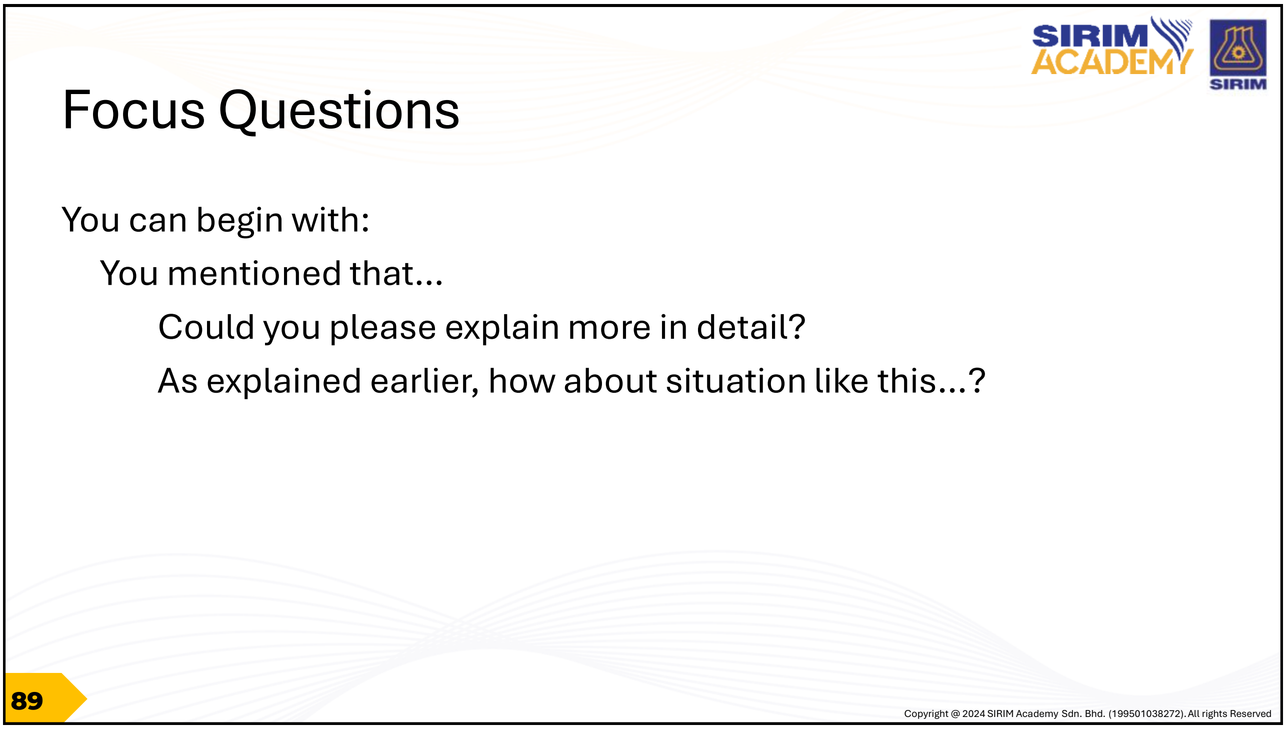
Why ?

87

Focus Questions

- Purpose
  - Follow up on activities highlighted during open questioning
  - Go deeper into the understanding
- May use auditee words as lead to focus questions

88



Focus Questions

You can begin with:

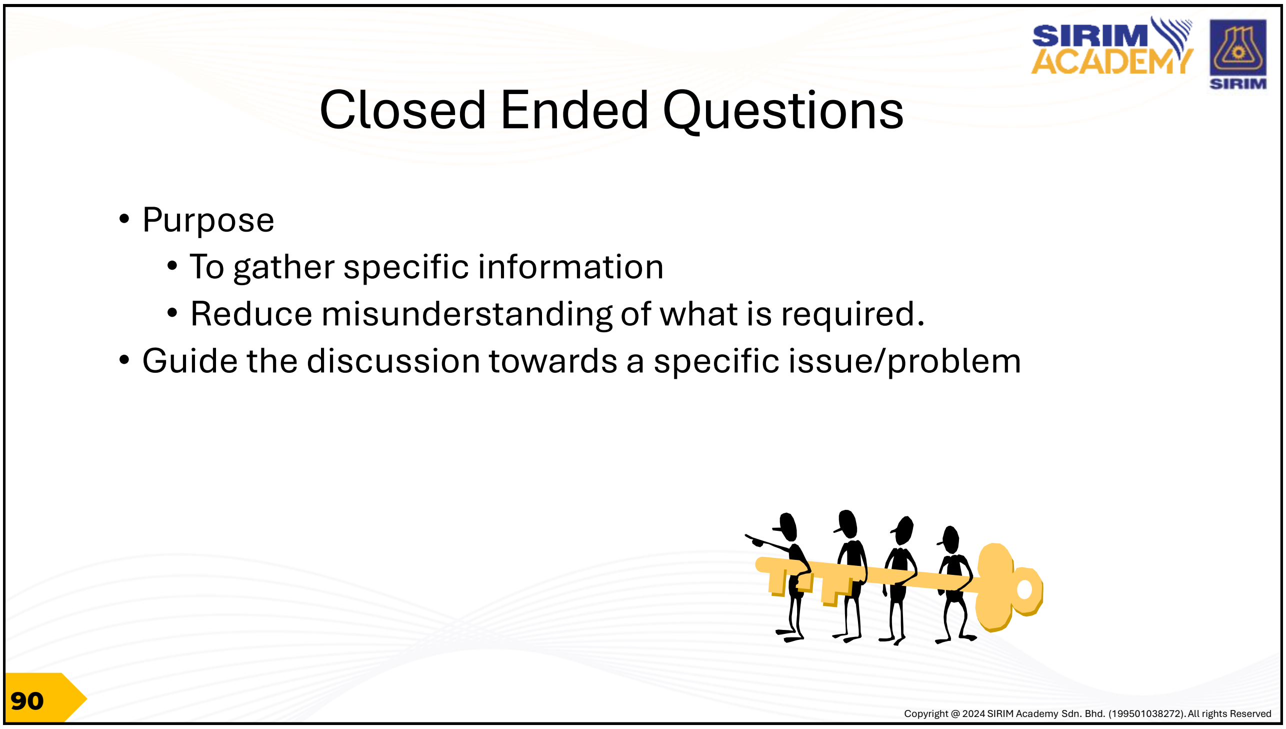
You mentioned that…

Could you please explain more in detail?

As explained earlier, how about situation like this…?

89

89



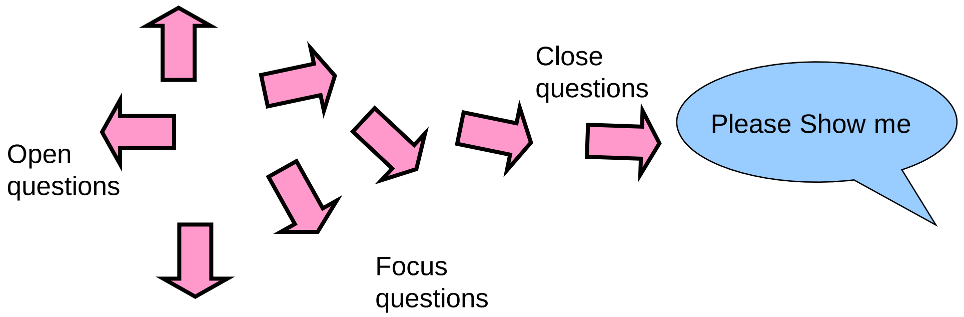
Closed Ended Questions

- Purpose
  - To gather specific information
  - Reduce misunderstanding of what is required.
- Guide the discussion towards a specific issue/problem

90

90

Skills of Questioning



An Effective Audit

The **“stair-step’ approach** when conducting interview is an effective audit method. This begins broad, and **narrows through the discussion**:

- *Can you explain the procurement process?*

How do you select your suppliers?

Can you show me the evaluation records?

Active Listening

Active listening encourages auditee go deeper for further communication.
Some of “door openers”:

- Interesting!
- Tell me about it
- Tell me more
- Would you like to talk about it
- Let’s discuss it
- You have something on your mind
- Your thoughts are important to me

93

LISTENING SKILLS

- When listening, try to *avoid* the following behaviors…

- Making judgments
- Mentally rehearsing what you are going to say in response
- Interrupting or completing sentences
- Assuming you already know what the speaker is going to say
- Offering advice or solutions

94

Think about this

- Use correct Tone
- Beware of nonverbal body language
  - Facial expressions
  - Body positions and movement
- Beware of communication barriers
  - work environment
  - perceptions
  - mind set
  - culture

95

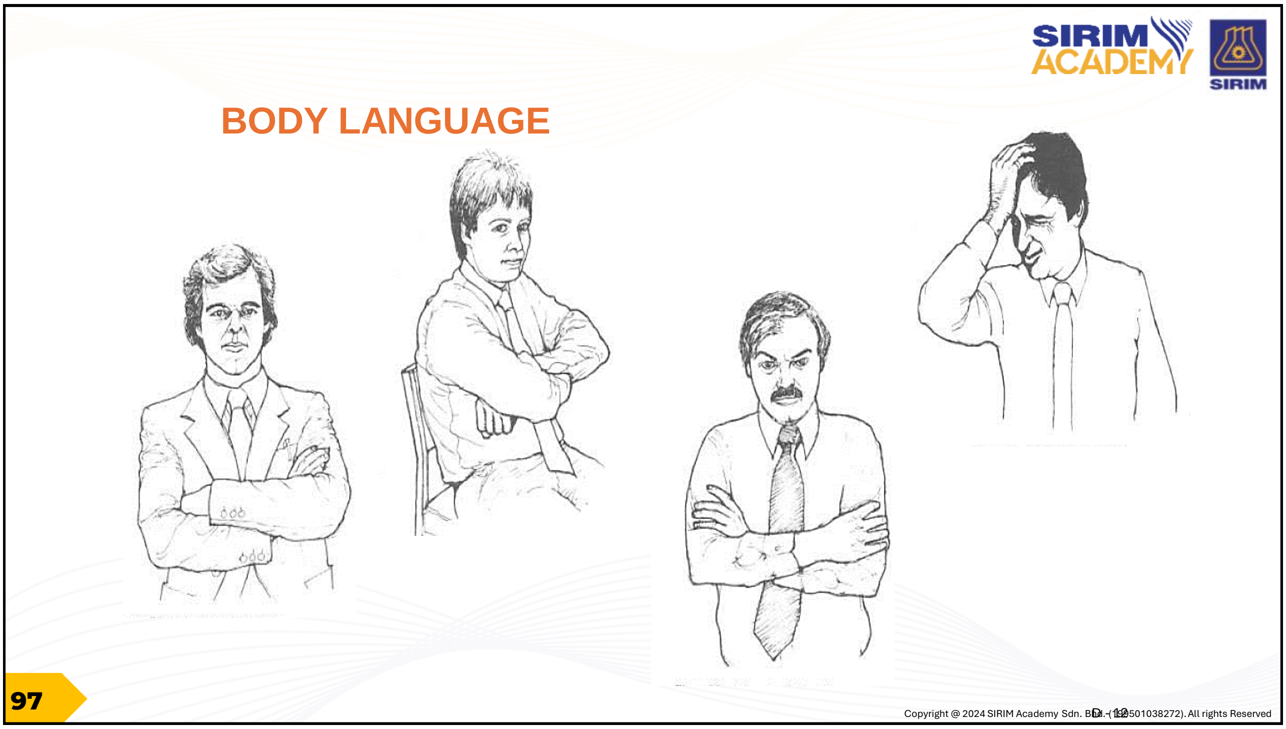
95

BODY LANGUAGE

96

D - 12

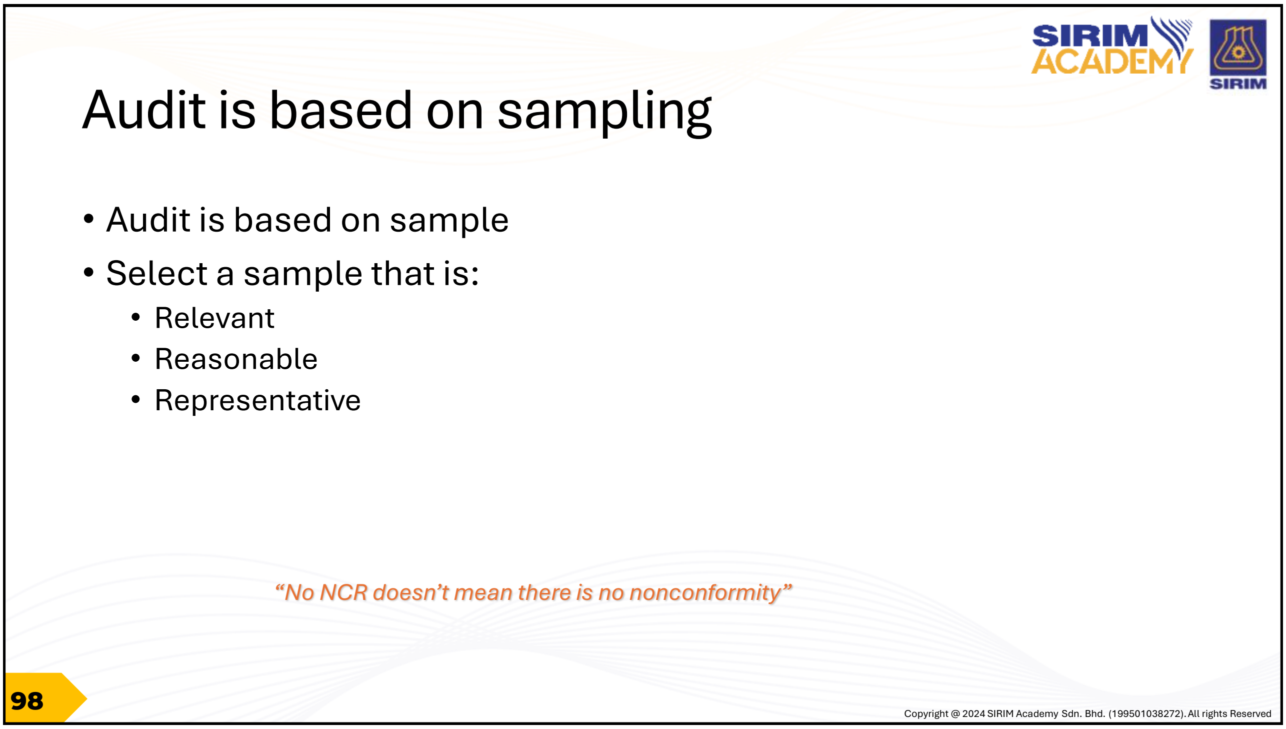
96



BODY LANGUAGE

D - 12

97



Audit is based on sampling

- Audit is based on sample
- Select a sample that is:
  - Relevant
  - Reasonable
  - Representative

“No NCR doesn’t mean there is no nonconformity”

SIRIM ACADEMY
SIRIM
98

98

Taking Notes As Reference

Please, Please Take Notes !!!

[For Investigation Now

[For Investigation Later

[For Use During Report Writing

[For Use By Other Auditor

99

99

Auditor Toolkit

- **No Paper , No Pen = No Audit**
  - **Clipboard**
  - **Audit plan**
  - **Audit checklists**
  - **Note pad**
  - **Audit report forms**
  - **Pen**
  - **ISO 37001:2016 Standard**

100

100

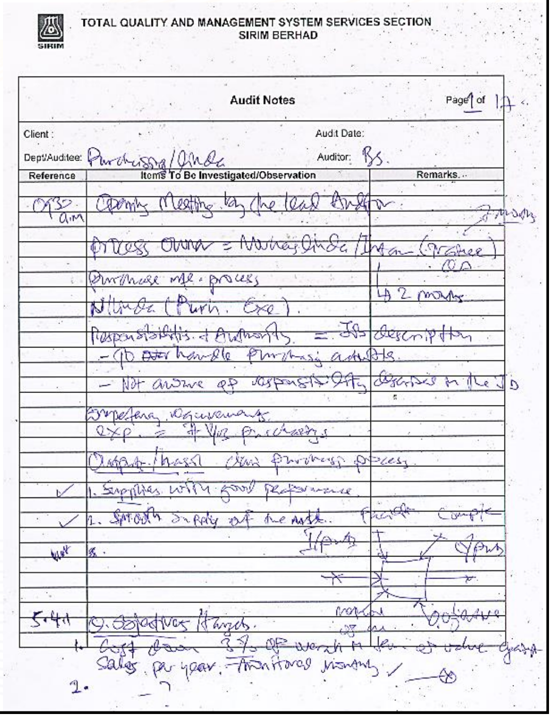
Audit Note

Before start to take note, pls record the following :

- Auditee’s name
- Date
- Process/ department
- Other necessary information

While auditing, please record

- Auditee’s statements
- Audit evidence/Reference
- Verification Result



TOTAL QUALITY AND MANAGEMENT SYSTEM SERVICES SECTION
SIRIM BERHAD

Audit Notes Page 1 of 17

Client :
Audit Date:
Dept/Auditee: Purchasing/Linda
Auditor: Bs.

Reference	Items To Be Investigated/Observation	Remarks
0930 am	Opening Meeting by the lead Auditor	2 mins
	Process owner = Norhayati/Intan (Trainee)	QA
	Purchase mtl. process	↳ 2 months
	N. Linda (Purch. Exe).	
	Responsibilities & Authority = Job description	
	- To ~~oter~~ handle purchasing activities.	
	- Not aware of responsibility described in the JD	
	Competency requirements	
	exp. = 4 yrs purchasing	
	Output/target [illegible] purchasing process	
✓	1. Supplies with good performance.	
✓	2. Smooth supply of the mtl.	Process Complete
	Inputs	Outputs
5.4.1	Q. objectives/targets.	Method of m. Objective

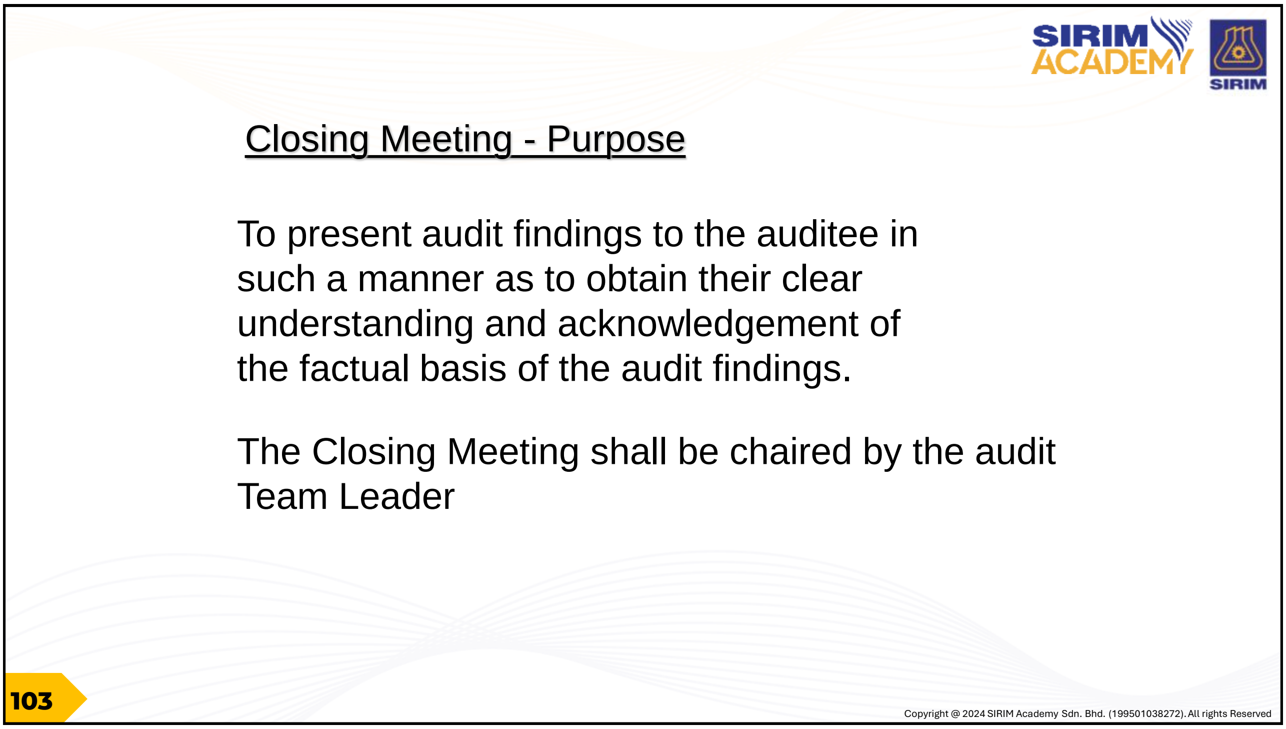
1. Cost down 3% of [illegible] in term of value against sales per year. Monitored monthly ✓
2.

Audit Note

Audit notes shall include the following item:

- input/output
- method
- machine
- man
- measurement

*Will be an evidence that the audit is performed in a process approach manner



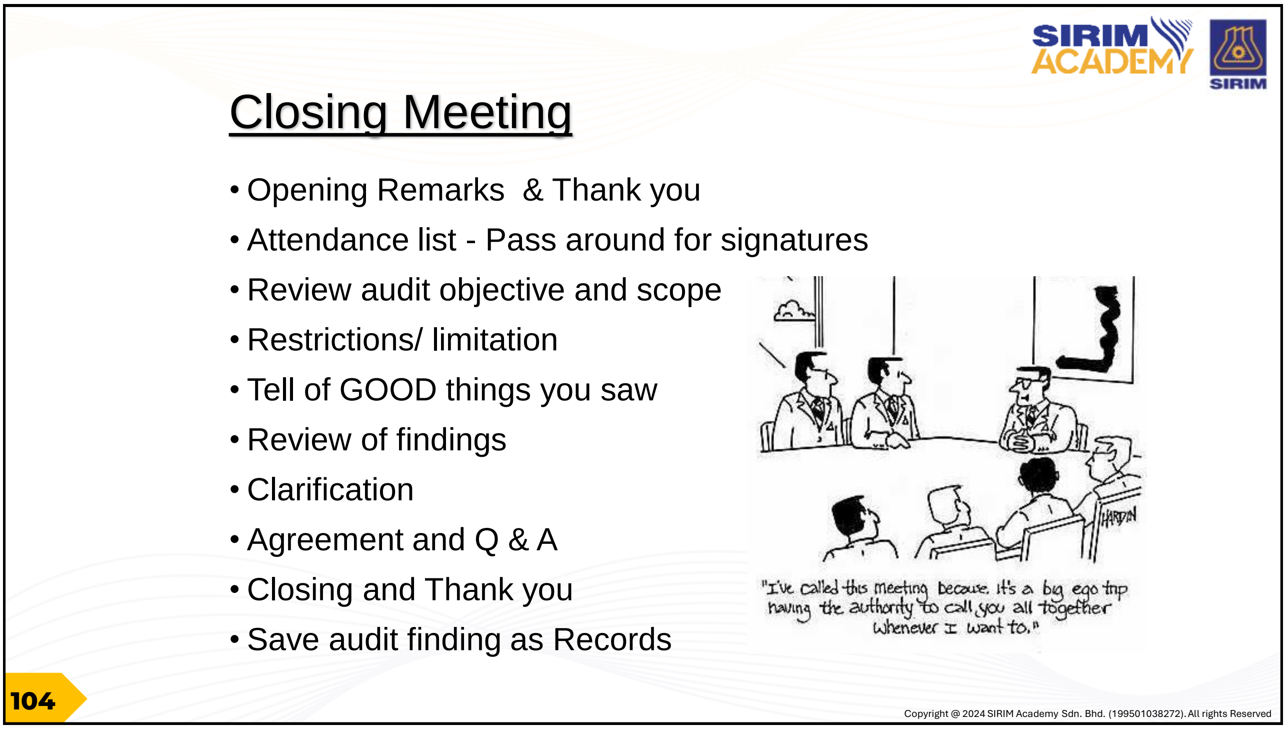
Closing Meeting - Purpose

To present audit findings to the auditee in such a manner as to obtain their clear understanding and acknowledgement of the factual basis of the audit findings.

The Closing Meeting shall be chaired by the audit Team Leader

103

103



Closing Meeting

- Opening Remarks & Thank you
- Attendance list - Pass around for signatures
- Review audit objective and scope
- Restrictions/ limitation
- Tell of GOOD things you saw
- Review of findings
- Clarification
- Agreement and Q & A
- Closing and Thank you
- Save audit finding as Records

"I've called this meeting because it's a big ego trip having the authority to call you all together whenever I want to."

104

104

SIRIM ACADEMY SIRIM

Good Ethic of Auditor

- Punctual
- Objective
- Opened minded
- Analytical
- Good judgement
- Good listener
- Polite
- Honest
- Hardworking
- Patient

105

105

SIRIM ACADEMY SIRIM

AUDIT REPORTING

106
106

106

What is Audit Report

- Audit report is the **final product**
- The **evidence** of the **audit** was **conducted**
- Must be completely **factual**
- Tone must be be **courteous** and **professional**
- Should be **verifiable** (track down the evidence)

Audit Findings

Audit evidence shall be evaluated against audit criteria to generate audit findings. Audit findings indicate :

Conformity

Non Conformity

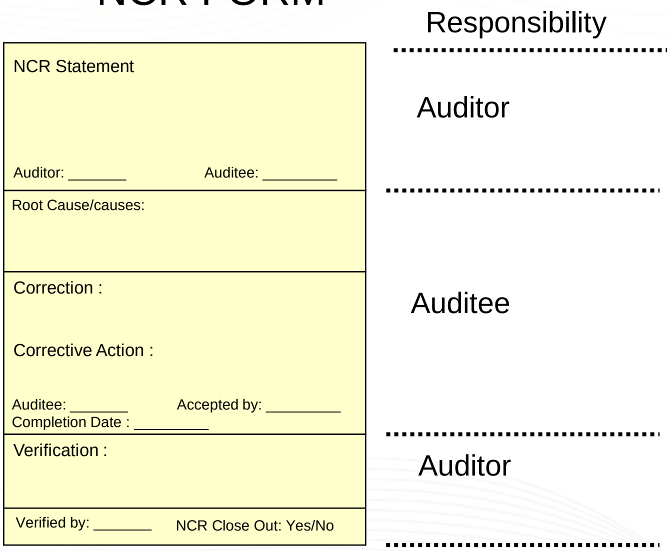
Observation

*Opportunity for further improvement

Nonconformance Exists Because

- The system **does not comply** with the standard, procedure or other requirements
- Performance **does not comply** with the system
- Performance is **not effective**

NCR FORM



NCR Statement Auditor: _______ Auditee: _________	Responsibility Auditor
Root Cause/causes:	Auditee
Correction : Corrective Action : Auditee: _______ Accepted by: _________ Completion Date : _________	
Verification : Verified by: _______ NCR Close Out: Yes/No	Auditor

NCR Statement

- **Audit Criteria / Requirements – cite specific requirements**
  - Reference Standard, ABMS
  - Regulatory, Statutory and other relevant requirement
- **Audit Findings / Nonconformance - Why a nonconformance?**
  - Deviation against requirements
  - Deviation against system
- **Audit Evidence**
  - Something you found and confirmed by authorized personnel
  - Specific – what, where, what number
  - Make it retrievable
  - Correct – check your fact

How to start writing

- It was found that...
- It was noted that...
- It was observed that ...
- There is no evidence that...
- During the audit ...

Examples :

Audit Criteria :

Clause 9.3.1 Top Management review shall be conducted on interval basis

Audit Findings :

It was noted that Top Management Review 2022 has yet to be conducted during our audit in March 1, 2023.

Audit Evidence :

- Minutes of Top Management Review Meeting 2021,
- Meeting Planner 2022
- Based on interview session (Monday 3pm @Bilik Kenangan Level 50 SIRIM Building) with Mr X, who has confirmed that Top Management Review has yet to be conducted

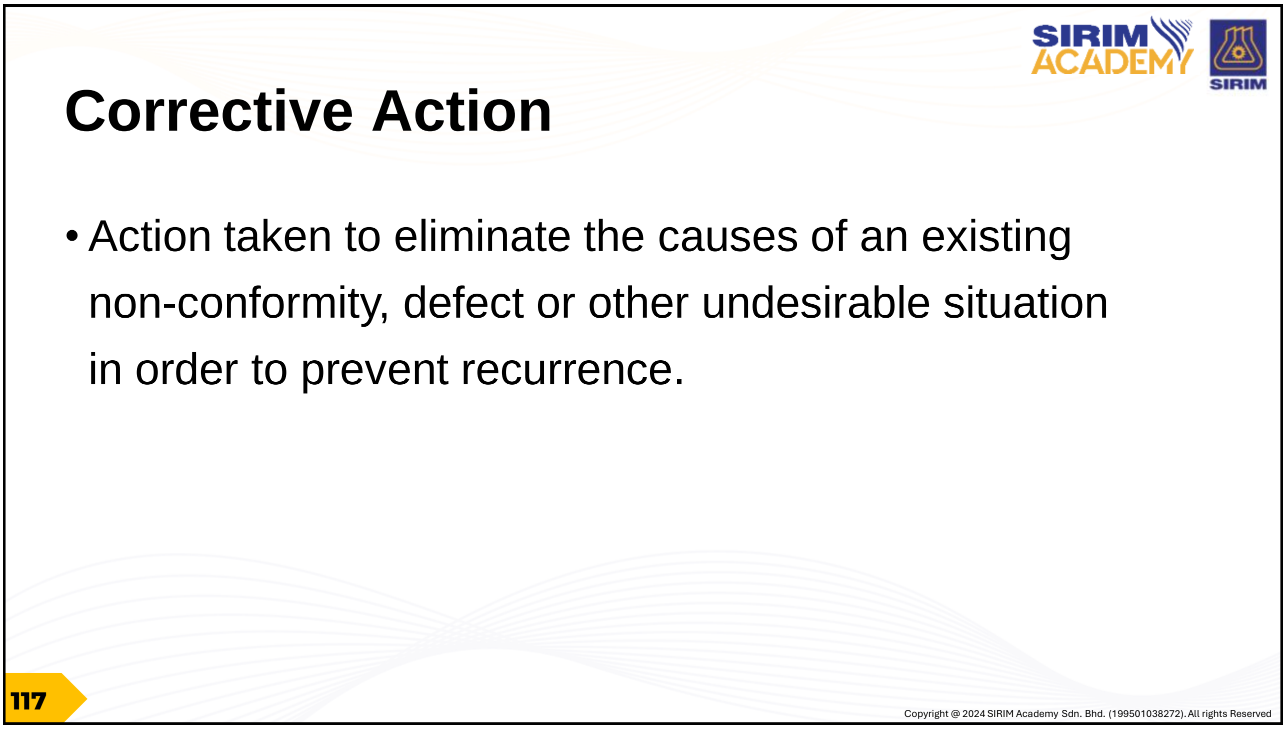
FOLLOW UP

Follow up

- ❑Issue corrective Action – Auditor
- ❑Correction - Auditee
- ❑Identify root cause - Auditee
- ❑Corrective action - Auditee
- ❑Verify corrective action - Auditor

NCR FORM

	Responsibility
NCR Statement Auditor: _______ Auditee: _________	Auditor
Root Cause/causes:	Auditee
Correction : Corrective Action : Auditee: _______ Accepted by: _________ Completion Date : _________	
Verification : Verified by: _______ NCR Close Out: Yes/No	Auditor

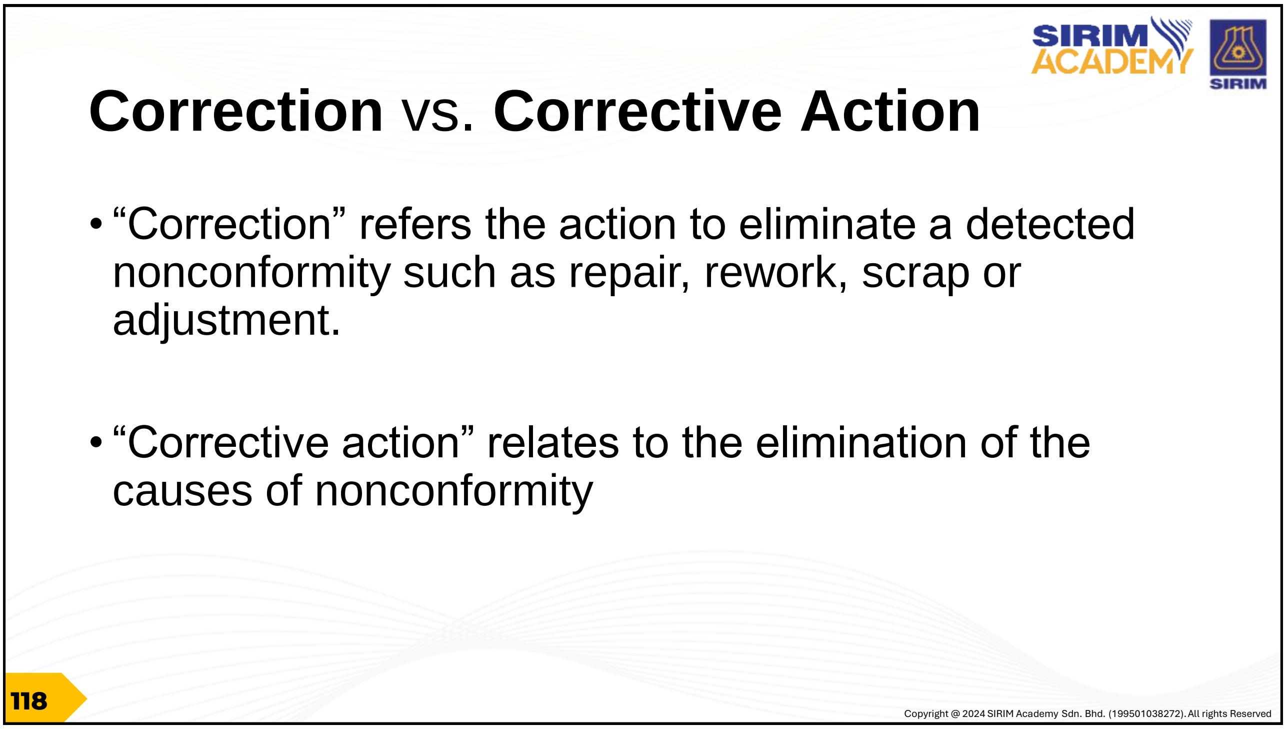


Corrective Action

- Action taken to eliminate the causes of an existing non-conformity, defect or other undesirable situation in order to prevent recurrence.

117

117



Correction vs. Corrective Action

- “Correction” refers the action to eliminate a detected nonconformity such as repair, rework, scrap or adjustment.
- “Corrective action” relates to the elimination of the causes of nonconformity

118

118

Response to the Audit Report

- An action plan of things to come
- Response time shall be timely without undue delay
  - Third Party – 30 - 90 days
  - Second party - typically 30 days
  - First party - typically 14 - 30 days
- Team leader to keep track of the response
- To remind the auditee where necessary

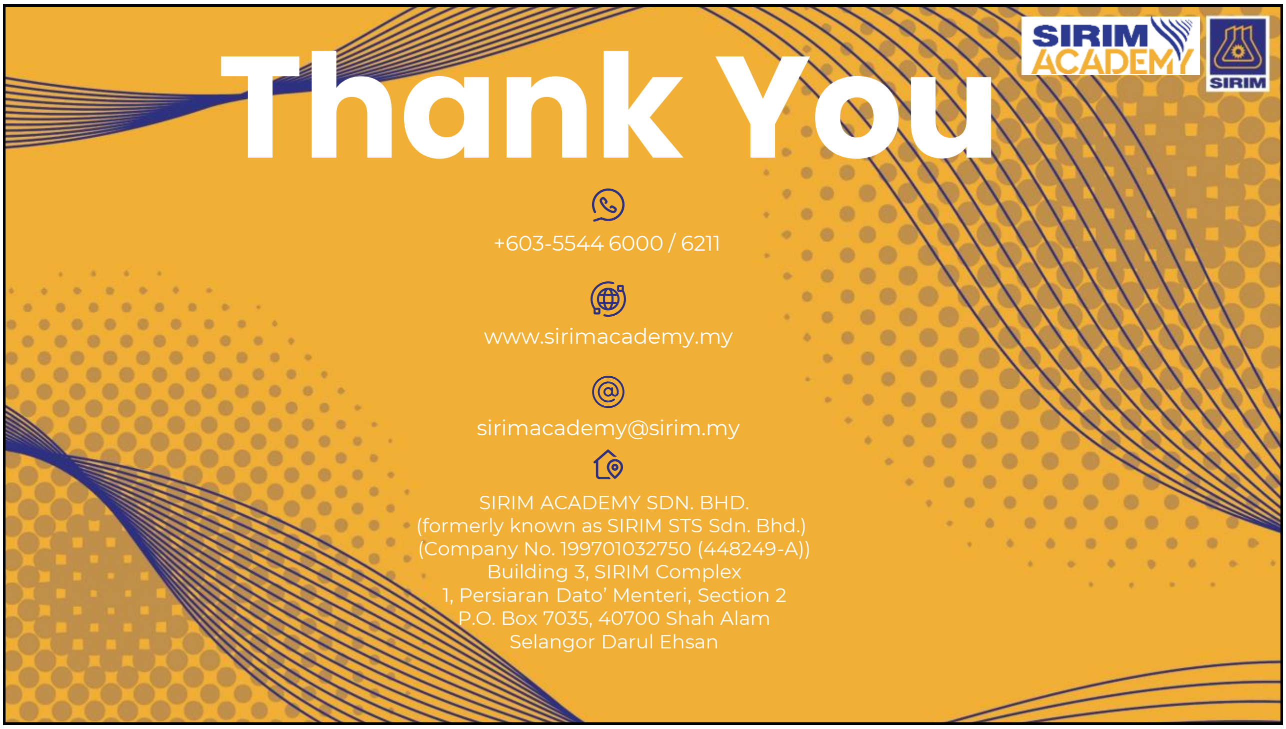
119

119

- Accept the response if there is a reasonable chance of success
- Request the changed or revised documents where promised document change involve.
- Perform brief follow-up visit to personally verify the implementation of the promised corrective action

120

120



Thank You

SIRIM ACADEMY

SIRIM

+603-5544 6000 / 6211

www.sirimacademy.my

sirimacademy@sirim.my

SIRIM ACADEMY SDN. BHD.
(formerly known as SIRIM STS Sdn. Bhd.)
(Company No. 199701032750 (448249-A))
Building 3, SIRIM Complex
1, Persiaran Dato' Menteri, Section 2
P.O. Box 7035, 40700 Shah Alam
Selangor Darul Ehsan

121