bsi

Webinar

ISO/IEC 42001:2023
AI Management System
เครื่องมือในการเสริมพลัง
AI ในด้านที่ดี

อาจารย์ กิตติพงษ์ เกียรตินิยมรุ่ง
Product Technical Manager
**BSI Thailand**

Agenda

01   **แนวคิด AI Management System (ISO/IEC 42001:2023)**

02   **ข้อกำหนด AI Management System (ISO/IEC 42001:2023)**

Let's take a moment to think about these two questions:

- Why is Artificial Intelligence Management System (AIMS) important to your organization?

- Why should your organization manage processes around AI lifecycle model?

What are the benefits of implementing
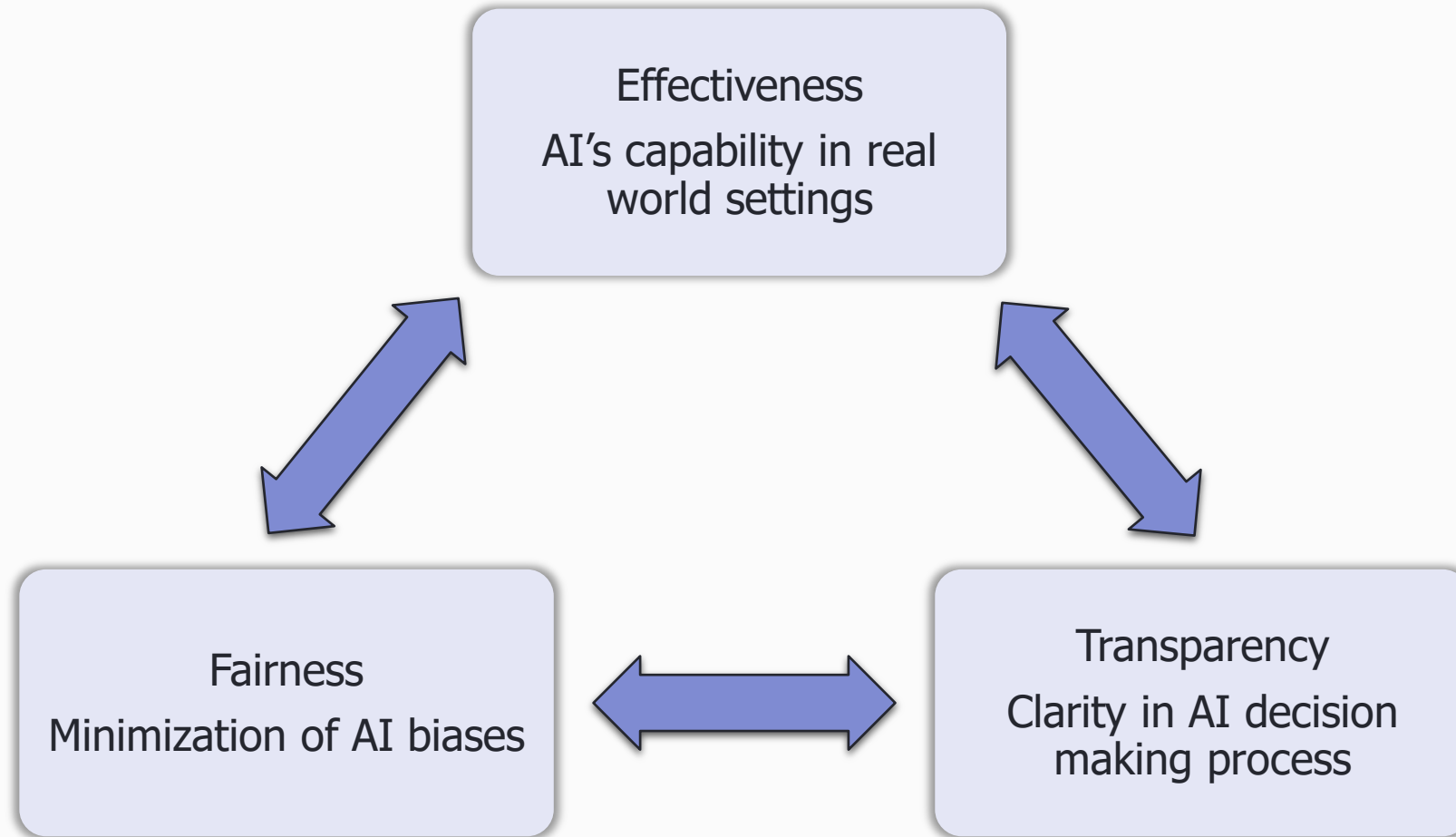
What do we mean by key benefits of an AIMS?

Effectiveness

Fairness

Transparency

The benefits of effective, transparent and fair AIMS

Brand strength

Cost efficiency

Customer loyalty

Revenue and profit growth

Attracting new customers

Employee morale

"
Module 1:
Key concepts and processes

Who was involved in its development?

European Union Agency for
Cybersecurity

International Organization
for Standardization

European Committee
for Standardization

Who was involved in its development?

International
Electrotechnical
Commission

European
Telecommunications
Standards Institute

Joint technical committee
ISO/IEC JTC 21

9

Key concepts (1): Risk-based approach
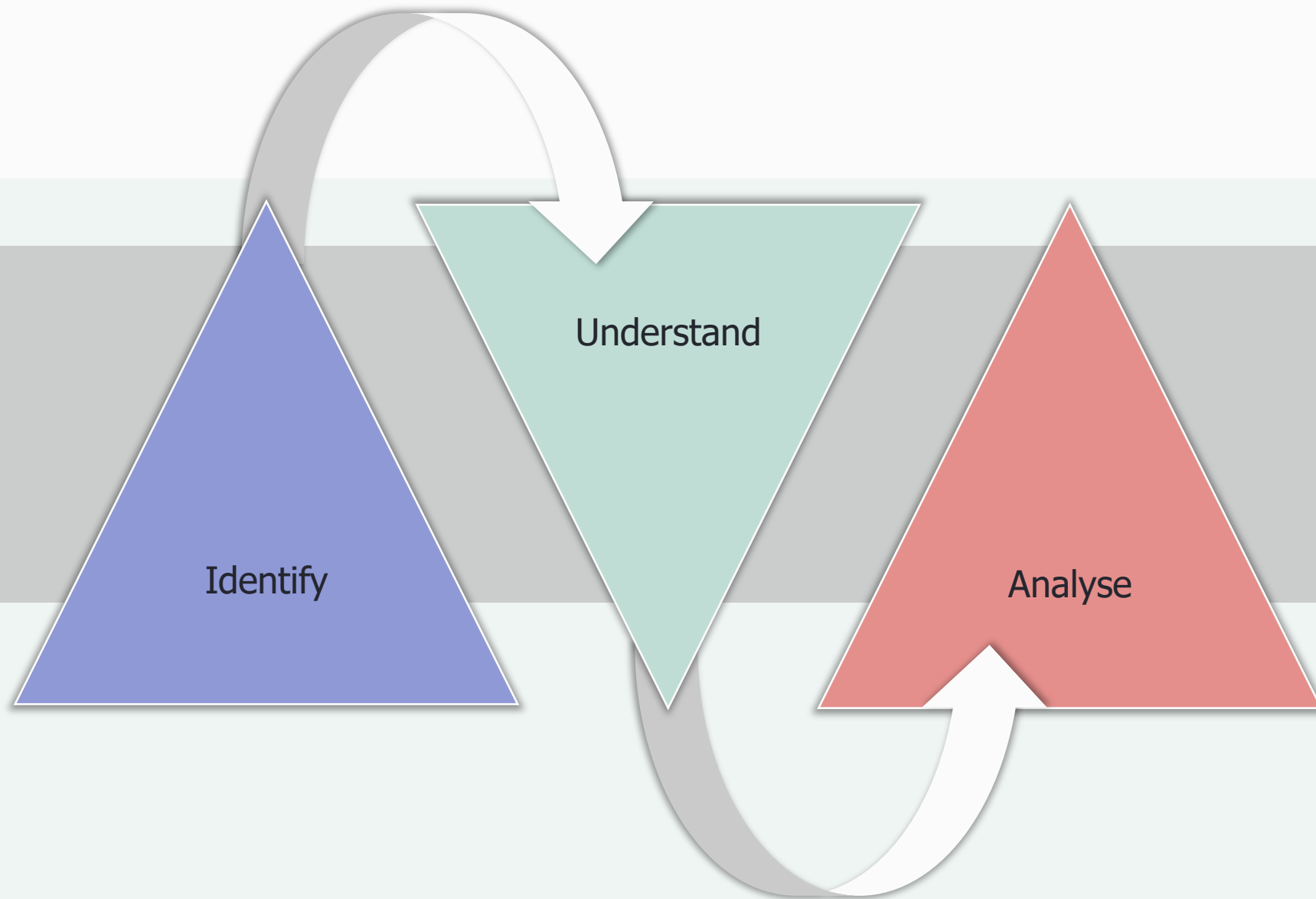
'effect of uncertainty'

<u>Effect</u>

A deviation from the expected – positive or negative

<u>Uncertainty</u>

Information related to knowledge of an event

Key concepts : Process

Identify

Understand

Analyse
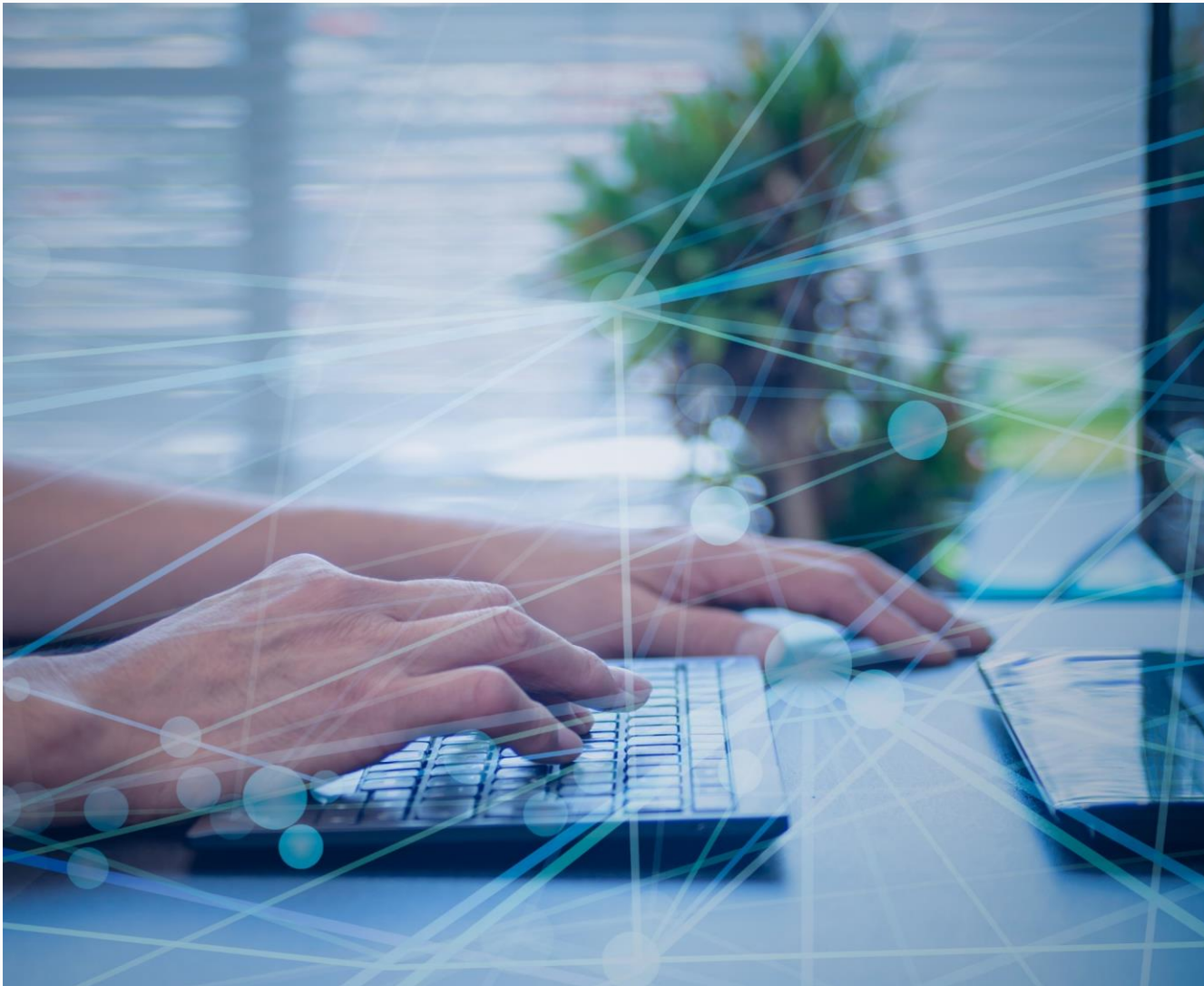
PDCA and AIMS

Establish
(PLAN)

Implement and
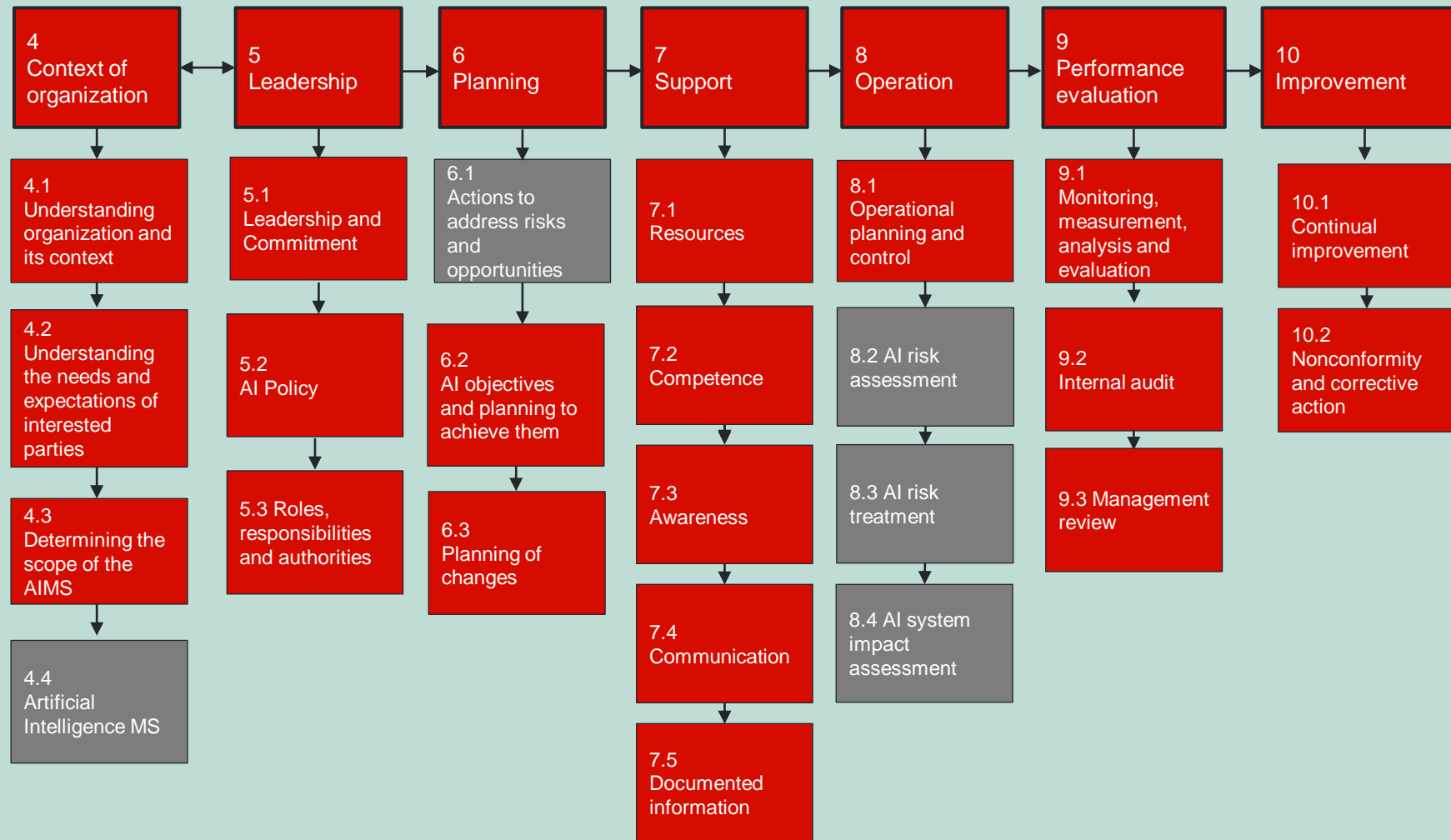operate
(DO)

Monitor and
review
(CHECK)

Maintain and
improve
(ACT)

12

Key concepts : Harmonized approach

The harmonized approach forms the core of ISO management system standards, including ISO/IEC 42001

The harmonized approach with AIMS additions

4 Context of organization	5 Leadership	6 Planning	7 Support	8 Operation	9 Performance evaluation	10 Improvement
4.1 Understanding organization and its context	5.1 Leadership and Commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Continual improvement
4.2 Understanding the needs and expectations of interested parties	5.2 AI Policy	6.2 AI objectives and planning to achieve them	7.2 Competence	8.2 AI risk assessment	9.2 Internal audit	10.2 Nonconformity and corrective action
4.3 Determining the scope of the AIMS	5.3 Roles, responsibilities and authorities	6.3 Planning of changes	7.3 Awareness	8.3 AI risk treatment	9.3 Management review	
4.4 Artificial Intelligence MS			7.4 Communication	8.4 AI system impact assessment		
			7.5 Documented information			

Introduction to ISO/IEC 42001

Clause 1-3

1. Scope

Establish, implement, maintain and continually improve an AIMS, Intended to help the organization develop, provide or use AI systems responsibly in pursuing its objectives and meet applicable requirements, obligations related to interested parties and expectations from them.

2. Normative references

Normative references cites ISO/IEC 22989 as indispensable for its application

3 Terms and definitions

Terms, definitions and concepts from ISO/IEC 22989 are used in ISO/IEC 42001

"
Module 3:
Clauses 4 and 5

Clause 4:
Context of the organization

Both the external and the internal issues will change over time, the issues and their influence on the scope, constraints and requirements of the AIMS should be reviewed regularly

4.1 Understanding the organization and its context

'Combination of internal and external issues that can have an effect on an organization's approach to developing and achieving its objectives'

Understand the context

Analyse the context

Ensure the AIMS is adapted

4.1 Understanding the organization and its context

External issues
Legal, natural, technological, social, cultural or financial aspects

External context
Legal obligations, AI prohibitions, regulatory guidelines, AI use incentives, cultural and ethical norms, AI competition and market trends

4.2 Understanding the needs and expectations of interested parties

Citizens

Customers

Distributors

Shareholders

Investors

Owners

Insurers

Government

Regulators

Recovery service suppliers

The organization

Management

- Top management
- Those accountable for artificial intelligence policy and implementation

Those who implement and maintain the AIMS

- Those who maintain AIMS and risk procedures
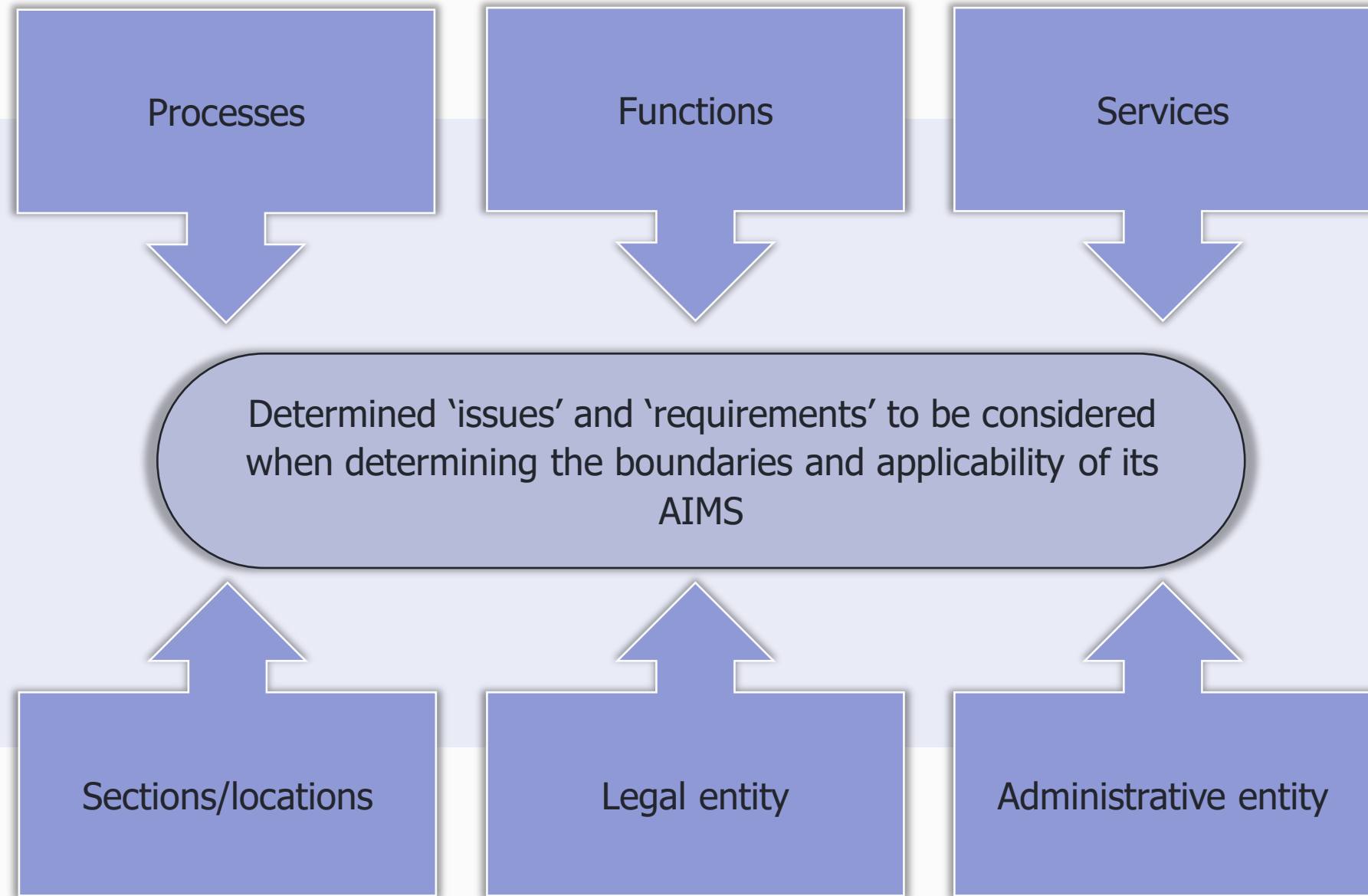
Other staff

Contractors

Competitors

Media

Commentators

Trade groups

Neighbors

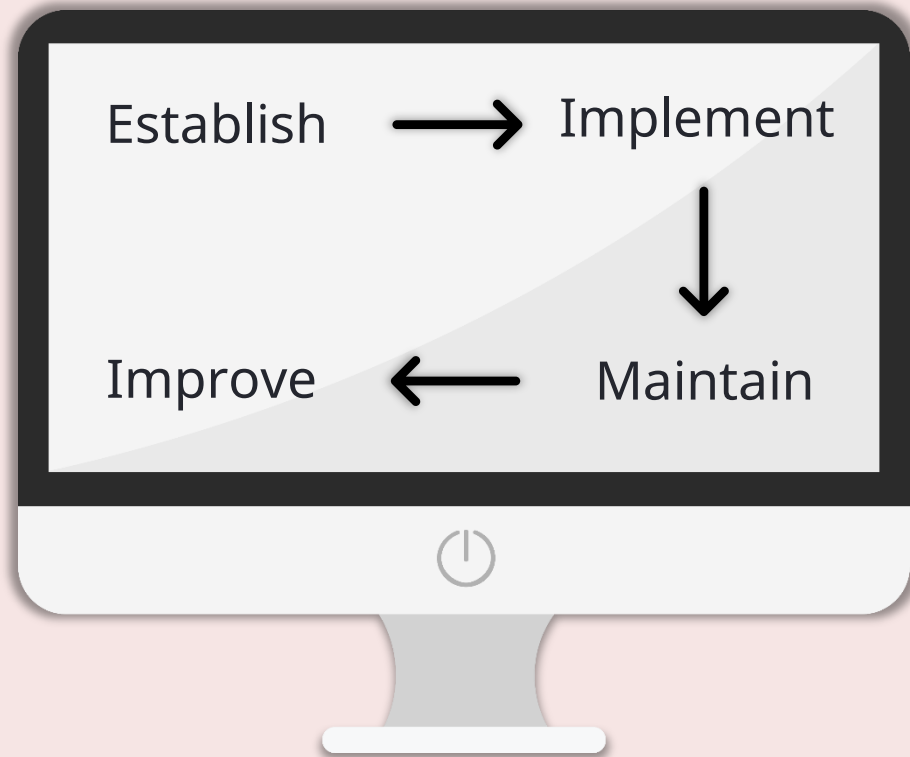Pressure groups

Emergency services

Other response agencies

Transport services

Staff dependents

4.3 Determining the scope of the AI management system

Processes

Functions

Services

Determined 'issues' and 'requirements' to be considered when determining the boundaries and applicability of its AIMS

Sections/locations

Legal entity

Administrative entity

4.4 AI management system

Establish → Implement

Implement ↓ Maintain

Improve ← Maintain

Clause 5: Leadership

Policy and objectives are compatible with the strategic direction and context of the organization

Demonstrate commitment

Integrate requirements of the MS into the organization's business processes

Clause 5: Leadership

Top management should:

Promote improvement and support management roles to demonstrate their leadership

Take accountability of the integrate the AIMS into the organization's processes

"
Module 4:
Clauses 6 and 7

Clause 6: Planning

Clause 6 mandates that in planning for the AI management system, organizations must give due consideration to the issues outlined in 4.1 and the requirements from 4.2

Help ascertain the risks and opportunities that must be addressed

Manage AI risk effectively

Determine the quantum and nature of risks

Guarantee the AIMS meets its intended objectives

Mitigate or curb undesired impacts

Foster ongoing improvement

Distinguish between risks

Conduct comprehensive AI risk assessments

Undertake AI risk treatment measures

Evaluate the ramifications

Domain and context of the application

Specific business requirements

Internal and external contexts

Clause 6: Planning

Likelihood		Minor (1)	Moderate (2)	Major (3)	Extreme (4)
	Almost certain (4)	M	H	H	H
	Likely (3)	M	M	H	H
	Possible (2)	L	M	M	H
	Rare (1)	L	L	M	H
		Minor (1)	**Moderate (2)**	**Major (3)**	**Extreme (4)**
		Consequence			

Clause 6: Planning

Artificial intelligence risk treatment options:

Risk acceptance

Risk avoidance

Risk reduction or mitigation

Risk transfer

Risk increase or risk taking

Clause 6: Planning

ISO/IEC 42001:2023 Controls			Current Controls	Remarks (Justification for exclusion)	Selected controls and reasons for selection						
					DIE	TAA	HIP	RMA	PDD	ETE	CRM
Controls	Sec	Control									
Policies related to AI	B.2.2	AI policy	Y		X	X	X			X	
	B.2.3	Alignment with other organizational policies	Y		X		X				
	B.2.4	Review of the AI policy	Y		X		X				
Internal organization	B.3.2	AI roles and responsibilities	Y		X	X	X				X
	B.3.3	Reporting of concerns	Y			X	X				X
Resources for AI systems	B.4.2	Resource documentation	Y		X			X			X
	B.4.3	Data resources	Y		X	X			X		X
	B.4.4	Tooling resources	Y					X			X
	B.4.5	System and computing resources	Y		X			X			X
	B.4.6	Human resources	Y					X		X	X

Clause 6: Planning

1. Quantitative metrics and boundaries

2. Performance metrics for AI

3. Effectiveness metrics for AIMS

Clause 6: Planning

7. Risk criteria alignment

4. ISO/IEC 42001 compliance

5. AIMS procedure adherence

6. Completion of action plans

Clause 6.3: Planning of change

Useful guidance on risk

BS ISO 31000:2018

BSI Standards Publication

Risk management — Guidelines
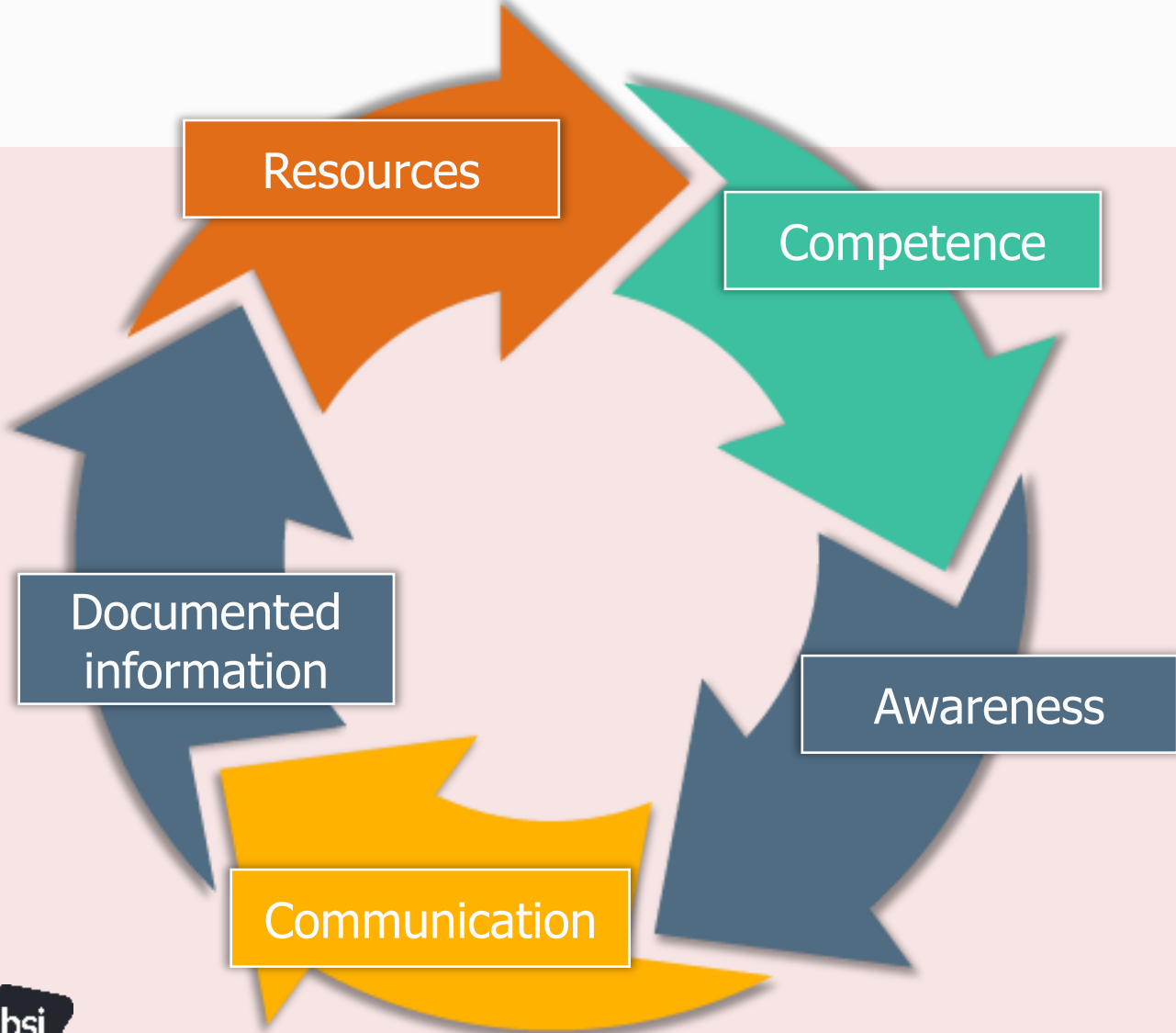
bsi.

BS ISO/IEC 23894:2023

BSI Standards Publication

Information technology — Artificial
intelligence — Guidance on risk management

bsi.

Clause 7: Support

- Resources
- Competence
- Awareness
- Communication
- Documented information

Clause 7.5: Documented information

The requirements for documented information are spread throughout the standard

4.3
Scope of the AIMS

5.2
AI policy

6.1.1
General

6.2
AI objectives

7.2
Evidence of competence

8.2
Results of AI risk assessment

9.1
Evidence of results

10.2
Nonconformities

"
Module 5: Clause 8

Clause 8: Operation

Clause 8.1
- Implementation of the actions determined in Clause 6
- Planning, implementation and control of the processes needed to meet AI requirements and achieve AI objectives

AIMS processes

Determine outsourced processes

Processes for implementation of the AI risk treatment plan

Control outsourced processes

Annex A – Control objectives and controls (38 Controls)

The standard has four different AI control clauses, namely:

- Clause B.2 Policies related to AI (3)

- Clause B.3 Internal organization (2)

- Clause B.4 Resources for AI systems (5)

- Clause B.5 Assessing impacts of AI systems (4)

- Clause B.6 AI system life cycle (9)

- Clause B.7 Data for AI systems (5)

- Clause B.8 Information for interested parties of AI systems (4)

- Clause B.9 Use of AI systems (3)

- Clause B.10 Third party relationships (3)

A.2 Policies related to AI

AI policy	Alignment with other organizational policies	Review of the AI policy

A.3 Internal organization

AI roles and responsibilities

Reporting of concerns

A.4 Resources for AI systems

Resource documentation

Data resources

Tooling resources

System and computing resources

Human resources
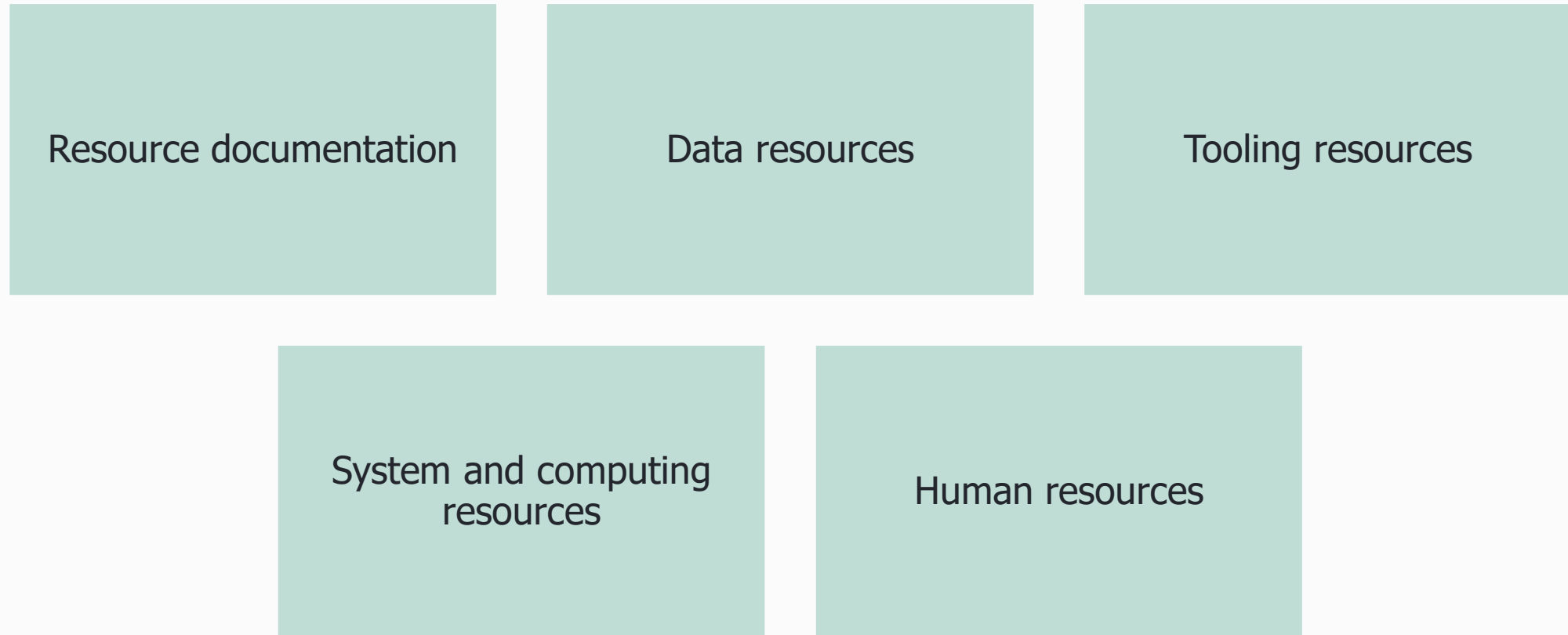
A.5 Assessing impacts of AI systems

AI system impact assessment process

Documentation of AI system impact assessments

Assessing AI system impact on individuals or groups of individuals

Assessing societal impacts of AI systems

A.6 AI system life cycle

A.6.1 Management guidance for AI system development

- Objectives for responsible development of AI system
- Processes for responsible AI system design and development

A.6.2 AI system life cycle

- AI system requirements and specification
- Documentation of AI system design and development
- AI system verification and validation
- AI system deployment
- AI system operation and monitoring
- AI system technical documentation
- AI system recording of event logs

A.7 Data for AI systems

Data for development and enhancement of AI system

Acquisition of data

Quality of data for AI systems

Data provenance

Data preparation

A.8 Information for interested parties of AI systems

System documentation and information for users

External reporting

Communication of incidents

Information for interested parties

A.9 Use of AI systems

Processes for responsible use of AI systems	Objectives for responsible use of AI system	Intended use of the AI system

A.10 Third-party and customer relationships

Allocating responsibilities	Suppliers	Customers

Relationship for Annex A and Annex B

Table A.1 — Control objectives and controls

A.2 Policies related to AI		
Objective: To provide management direction and support for AI systems according to business requirements.		
	Topic	Control
A.2.2	AI policy	The organization shall document a policy for the development or use of AI systems.

B.2   Policies related to AI

B.2.1   Objective

To provide management direction and support for AI systems according to business requirements.

B.2.2   AI policy

Control

The organization should document a policy for the development or use of AI systems.

Implementation guidance

The AI policy should be informed by:

— business strategy;

— organizational values and culture and the amount of risk the organization is willing to pursue or retain;

— the level of risk posed by the AI systems;

— legal requirements, including contracts;

bsi

"

Module 6:
Clauses 9 and 10

Clause 9: Performance evaluation

Clause 9.1 Monitoring, measurement, analysis and evaluation

Specific AI components and processes that need to be monitored and measured

Standardized methodologies that ensure the produced results are both comparable and reproducible across cycles

Clause 9.2
Internal audit

Required at planned intervals

Provides conformance information

Assess the effective implementation and maintenance of the AIMS
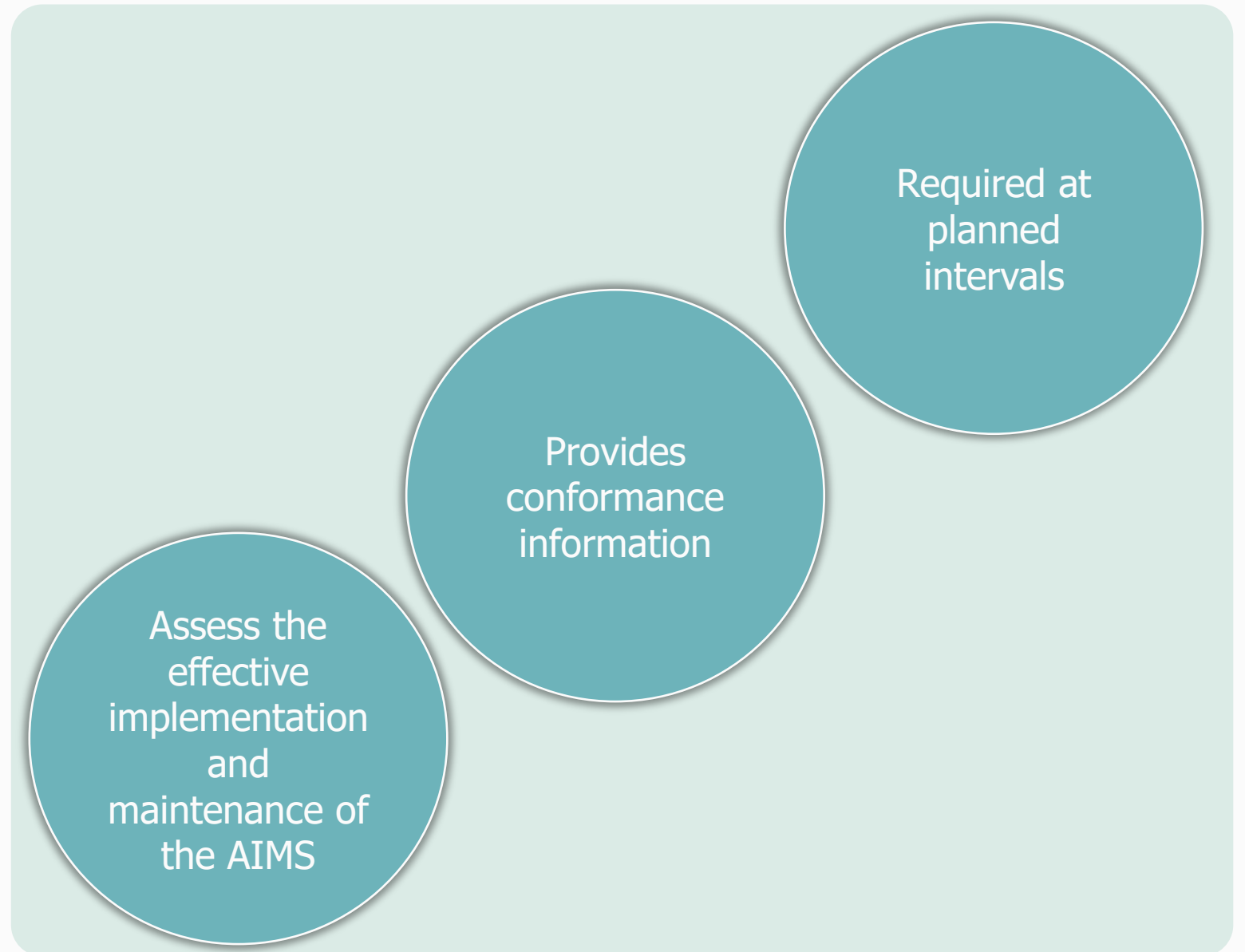
Clause 9.2.2 - Internal audit programme

An audit programme is required, scheduled based on:

Importance of the processes

Changes affecting the organization

Results of previous audits

Clause 9.3 Management review

Continuing suitability

Adequacy

Effectiveness

Alignment with the strategic direction of the organization

Clause 10: Improvement

Improvement

Continual improvement

Corrective action

Preventative action

"
Certification Process

Certification process

BSI - Certification process

1. Ensure ISO/IEC 42001:2023 implemented completely

2. Stage 1 Audit – Document review, confirm scope, objective and criteria

3. Stage 2 Audit – Implementation

4. Submit corrective action plan (If required)

5. Get the certificate

6. Audit as Surveillance Audit Yearly

7. 3 years – Recertification Audit

bsi

Approval Process

- Manual and Procedures
- Policy and objective
- Legislation, regulatory and compliance
- Competence, training and awareness
- Complaints and interested party concerns
- Product realisation and operational control
- Calibration and maintenance activities
- Internal audits
- Corrective and preventive action
- Management review

Implementation

Pre-audit

Stage I

NCs

Stage II

Follow up

Certificate issued

SV

Re-certificate

Certificate of Registration

Review and final questions
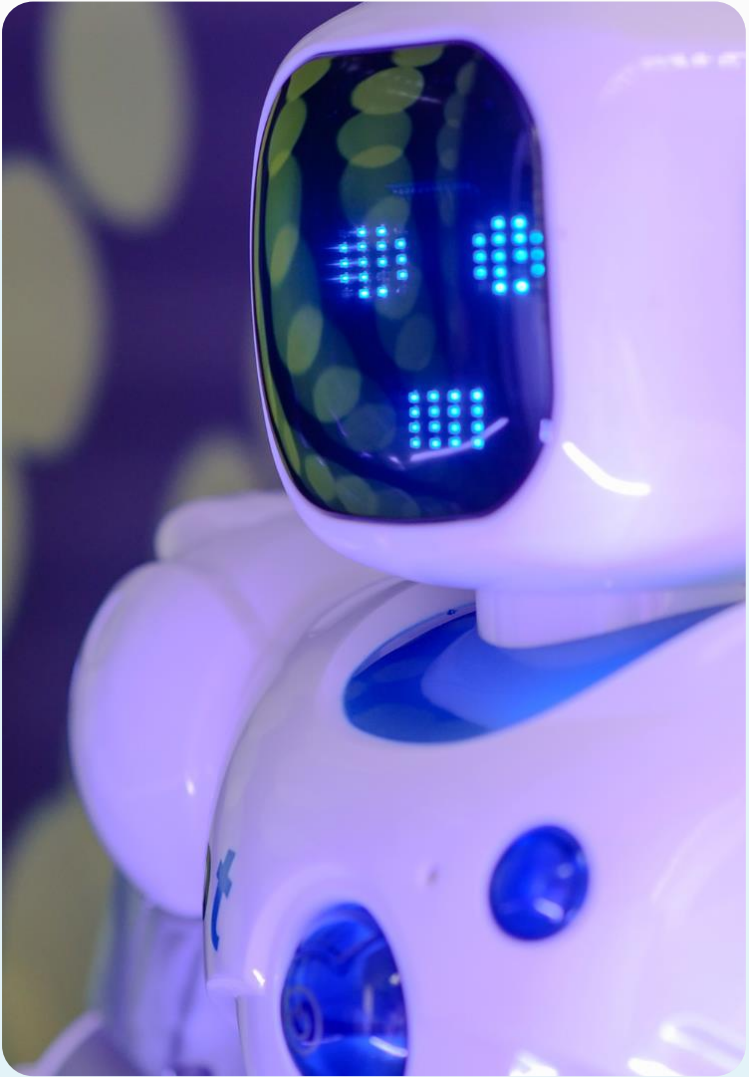
Contact us

www.bsigroup.com/th-TH/

@bsithailand

BSI Thailand

Tel: 02 294 4889-92   Email: infothai@bsigroup.com