WEBINAR RECORDED

PECB

Does ISO/IEC 42001 Risk Slowing Down AI Innovation, or Is It the Foundation for Responsible Operations?

SEPTEMBER 24 | 03:00 PM CEST

Adrian Resag

OCEG Academic Director, Author and GRC Leader

#GlobalLeadingVoices

Does ISO/IEC 42001 risk slowing down AI innovation, or is it the foundation for responsible operations?

ISO 42001:

Enhances

AI Opportunities

Helps manage

AI Risks

PECB

Agenda

AI Opportunities

AI Adoption
Sample Roadmap

AI Strategic
Adoption

AI Risks

AI Incidents

Security Threats
Specific to AI Systems

ISO 42001

Governance, Risk Management & Compliance

Putting in
Place ISO
42001

PECB

AI Opportunities

How ISO 42001 Enhances AI Opportunities

PECB

AI Adoption Sample Roadmap

Marketing Strategic Roadmap

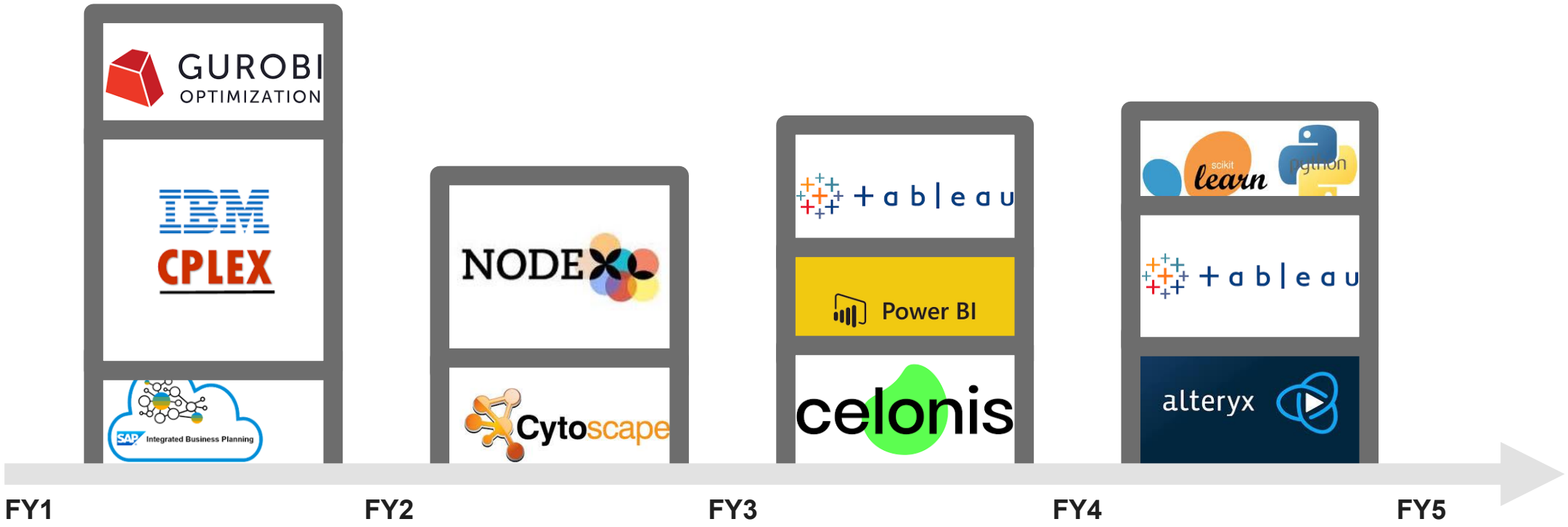
Marketing effort to know customer requirements

Improve customer engagement.

Analyze customer reviews and survey responses.

AI Adoption Sample Roadmap

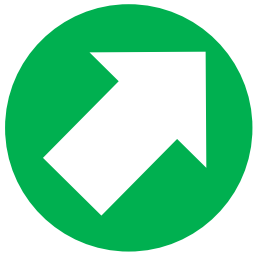
A strategic roadmap could be planned over longer periods, though this is difficult in such a changing environment.



PECB

AI Strategic Adoption

Organizations can chose different strategies when it comes to adopting AI.

Management of external AI risks	Defensive AI adoption	AI advantage seeking
		
Manage AI risks.	**Match competitors in AI use.**	**Develop superior AI capabilities to competitors.**
Adaptation of current operations to AI risks	Use of AI solutions	Development of own AI solutions

Does ISO/IEC 42001 risk slowing down AI innovation, or is it the foundation for responsible operations?

ISO 42001: Enhances  **AI Opportunities**

- Helps **understand the internal and external environment** and from that how to grasp opportunities.
- Puts in place the **strategy, goverance, people, and structures** which help grasp AI opportunities.
- Helps organizations **be ready** for future opportunities.

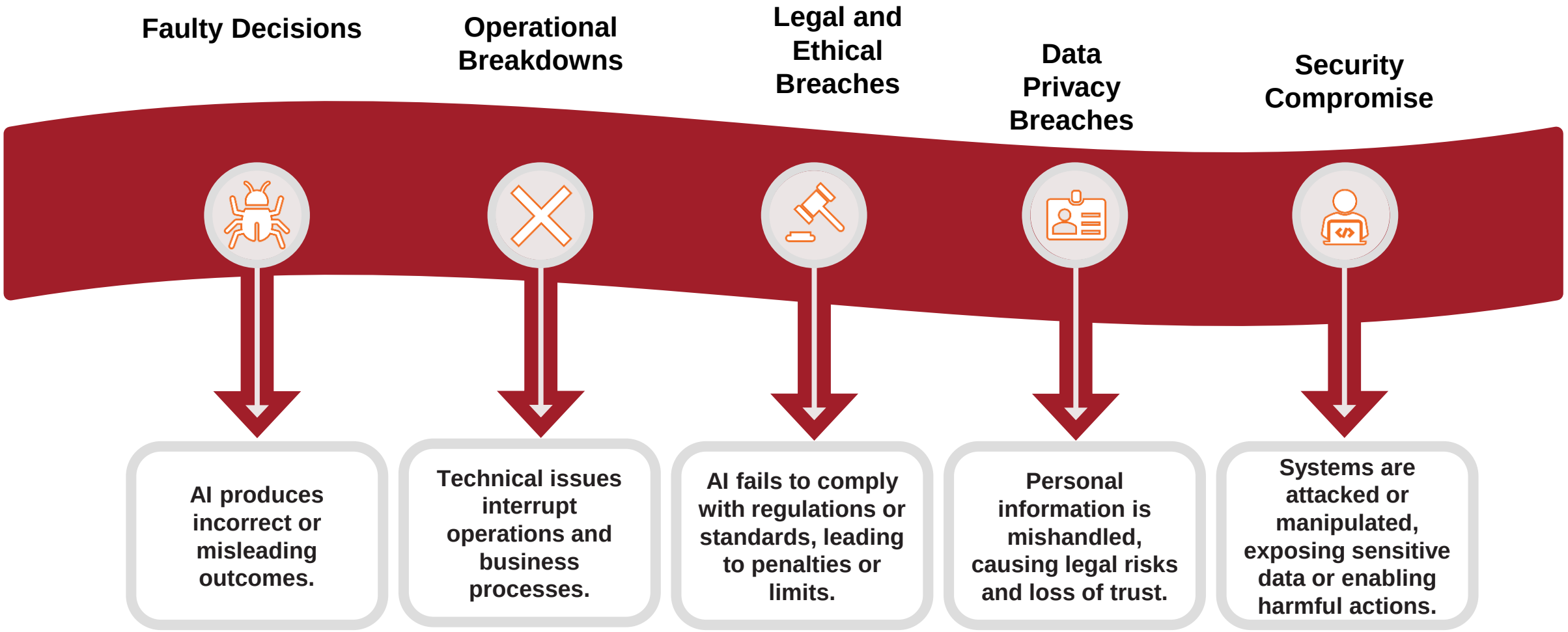
PECB

AI Risks

How ISO 42001 Helps Manage AI Risks

PECB

AI Incidents



PECB

Security Threats Specific to AI Systems

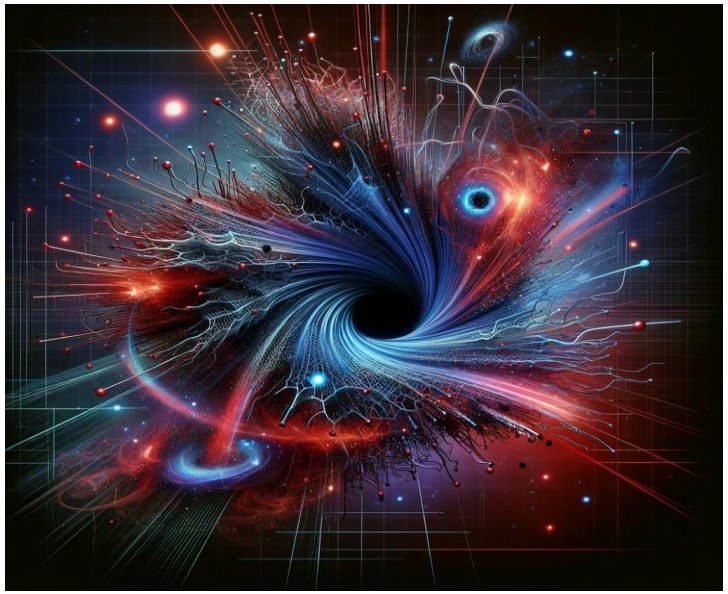
Data Poisoning

AI model data poisoning is the deliberate **injection of malicious or deceptive data into training sets**, aimed at compromising the integrity or performance of machine learning models.

Model Stealing

AI model stealing involves **unauthorized access to or replication of a trained machine learning model**, often for illicit purposes such as intellectual property theft or model replication without proper authorization.

Model Inversion Attacks



AI model inversion attacks involve exploiting a machine learning model's output to **infer sensitive information about the training data** it was trained on, potentially compromising privacy or security.

PECB

Does ISO/IEC 42001 risk slowing down AI innovation, or is it the foundation for responsible operations?

ISO 42001: Helps manage

AI Risks

- Helps increase **resilience**.
- Helps **identify and evaluate AI risks** and their impact.
- Helps **prepare an appropriate response** towards AI risks.

PECB

ISO 42001 GRC

How ISO 42001 Is the Foundation For Responsible AI Operations

PECB

ISO 27001 and ISO 42001

ISO 27001 Information Security Management Systems

ISO 27001 helps organizations ensure information security, cybersecurity and privacy protection.

ISO 42001 Artificial Intelligence Management Systems

ISO 42001 helps organizations responsibly use, develop, monitor or provide products or services that use AI.

ISO 27001 and ISO 42001
Risk Management and Compliance

ISO standards help organizations reach their objectives by ensuring that risks to the achievement of objectives are properly treated.

AI risk management and compliance is not only for organizations putting in place operations dependent on AI, but for any organization with vulnerabilities.

PECB

Putting in place ISO 42001

The ISO 42001 AI management system is designed to be a comprehensive framework that helps an organization to manage its AI operations and risks effectively.

PECB

1 Context of the Organization

2 Leadership

3 Planning

4 Support

5 Operations

6 AI Management System Performance Evaluation

7 Improvement

PECB

1 Context of the Organization

- Internal and external context
- Interested Parties (Stakeholders) Analysis

PECB

2 Leadership

- Leadership and commitment
- Scope of the AI Management System
- AI Policy
- Internal organization

AI Policies and Procedures

Provide management direction and support for AI systems

- AI Policy
- Alignment of Organizational Policies with AI Risks and System Objectives
- Regular Policy Review

Internal Organization

Establish accountability within the organization for AI systems

- AI roles and responsibilities
- Reporting of concerns

PECB

Plan

Planning

Do

Support

Operations

3

Planning

- AI Systems Impact Assessment
- Management Guidance for AI System Development and Maintenance

AI System Risk and Impact Assessment

Assess risks and the impacts to those affected by AI systems

- Assess risks and plan actions to respond to risks and opportunities
- AI system impact on individuals and groups
- AI system societal impact

Management Guidance for AI System Development and Maintenance

Documented Objectives and Processes

Ensure the organization implements processes for the responsible design and development of AI systems

- Documented objectives for responsible development
- Documented processes for responsible design and development

Defined Criteria and Requirements in the AI System Life Cycle

Define the criteria and requirements for each stage of the AI system life cycle

PECB

Management Guidance for AI System Development and Maintenance

Documented Objectives and Processes

Ensure the organization implements processes for the responsible design and development of AI systems

- Documented objectives for responsible development
- Documented processes for responsible design and development

Defined Criteria and Requirements in the AI System Life Cycle

Define the criteria and requirements for each stage of the AI system life cycle

Resources for AI systems

Ensure that the organization accounts for the resources of the AI system

- Data resources
- Tooling resources
- System and computing resources
- Human resources

Information for Interested Parties

Ensure interested parties have the necessary information to understand and assess the AI system's risks and their impact

- System Documentation and User Information
- External reporting
- Incident reporting
- Information for interested parties

4 Support

- Resources for AI systems
- Information for Interested Parties

PECB

Plan

Planning

Do

Support

Operations

Data for AI Systems

Define, document and implement data management processes related to the development of AI systems

- Acquisition
- Quality
- Provenance
- Preparation

Use of AI Systems

Ensure that the organization uses AI systems responsibly and according to organizational policies

- Responsible use of AI systems
- Intended use of the AI system

Third-party and Customer Relationships

Ensure that the organization understands its responsibilities and remains accountable, and 3rd party risks are monitored and treated

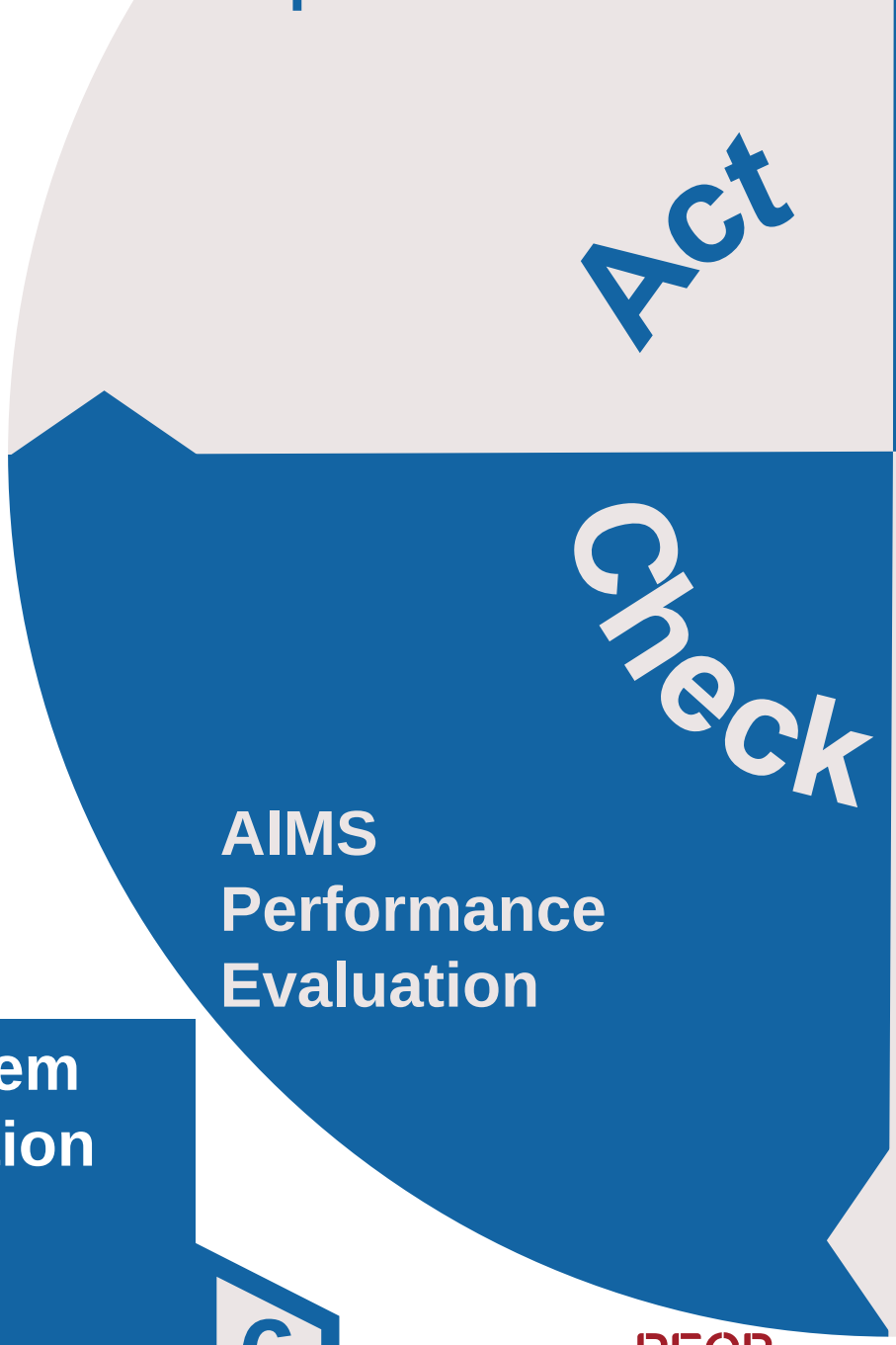
- Allocating responsibilities between supplier and customer

Operations

- Controls and Procedures
- Continuous Risk & Impact Assessment
- Data for AI Systems
- Use of AI Systems
- Third-party and Customer Relationships

5

PECB



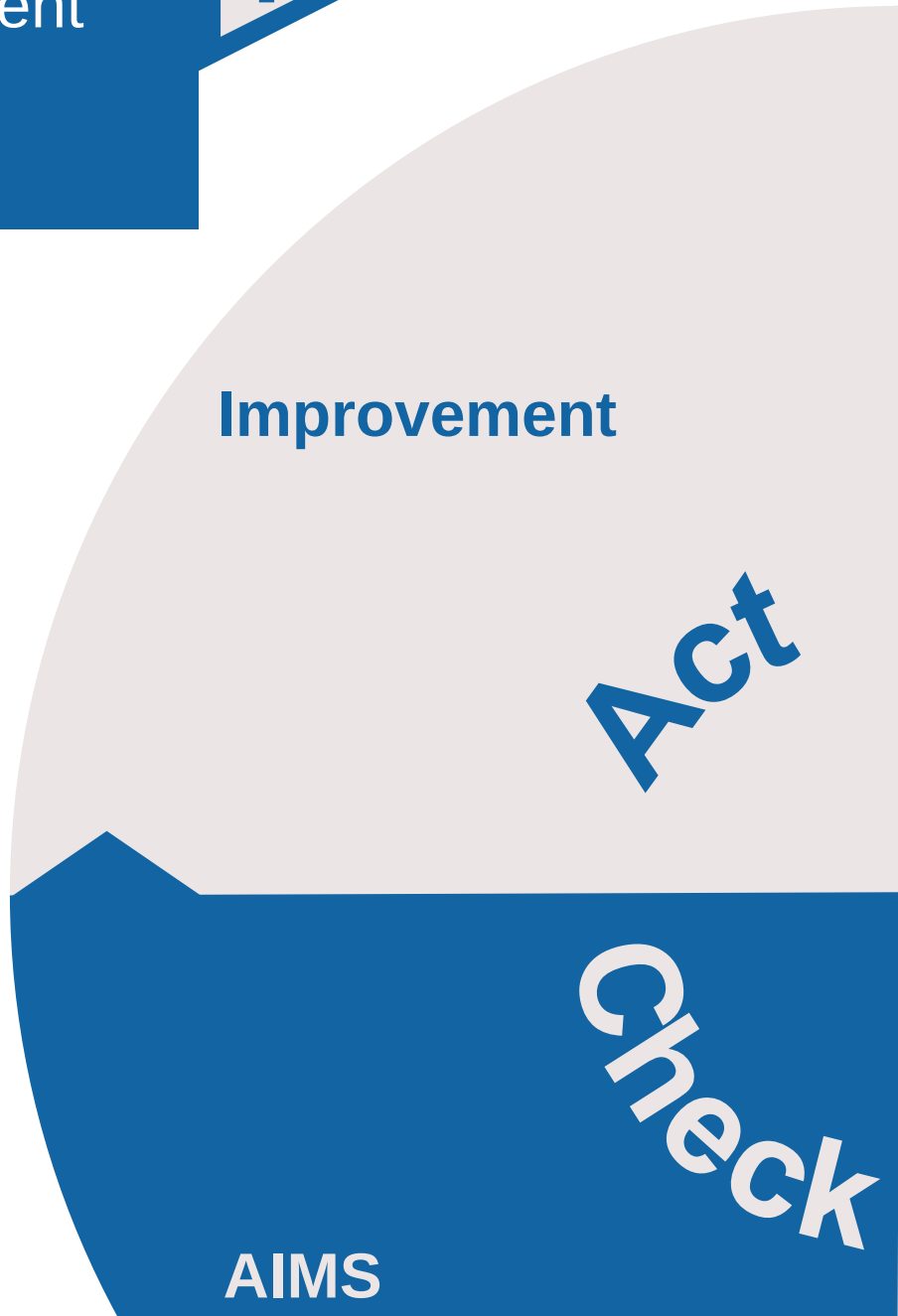
AI Management System Performance Evaluation

- Monitoring
- Internal audit
- Management review

Improvement

- Continual improvement
- Nonconformity and corrective action

7



1 Context of the Organization
- Internal and external context
- Interested Parties (Stakeholders) Analysis

2 Leadership
- Leadership and commitment
- Scope of the AI Management System
- AI Policy
- Internal organization

3 Planning
- AI Systems Impact Assessment
- Management Guidance for AI System Development and Maintenance

4 Support
- Resources for AI systems
- Information for Interested Parties

5 Operations
- Controls and Procedures
- Continuous Risk & Impact Assessment
- Data for AI Systems
- Use of AI Systems
- Third-party and Customer Relationships

6 AI Management System Performance Evaluation
- Monitoring
- Internal audit
- Management review

7 Improvement
- Continual improvement
- Nonconformity and corrective action

PECB


Q&A
THANK YOU
PECB