WEBINAR RECORDED

PECB

Managing AI Risks and Cyber Resilience: A Joint Approach with ISO 22301 & ISO/IEC 42001

APRIL 30 | 3:00 - 4:00 PM CEST

Rinske Geerlings
Business Continuity, Risk Management, and Information Security Expert

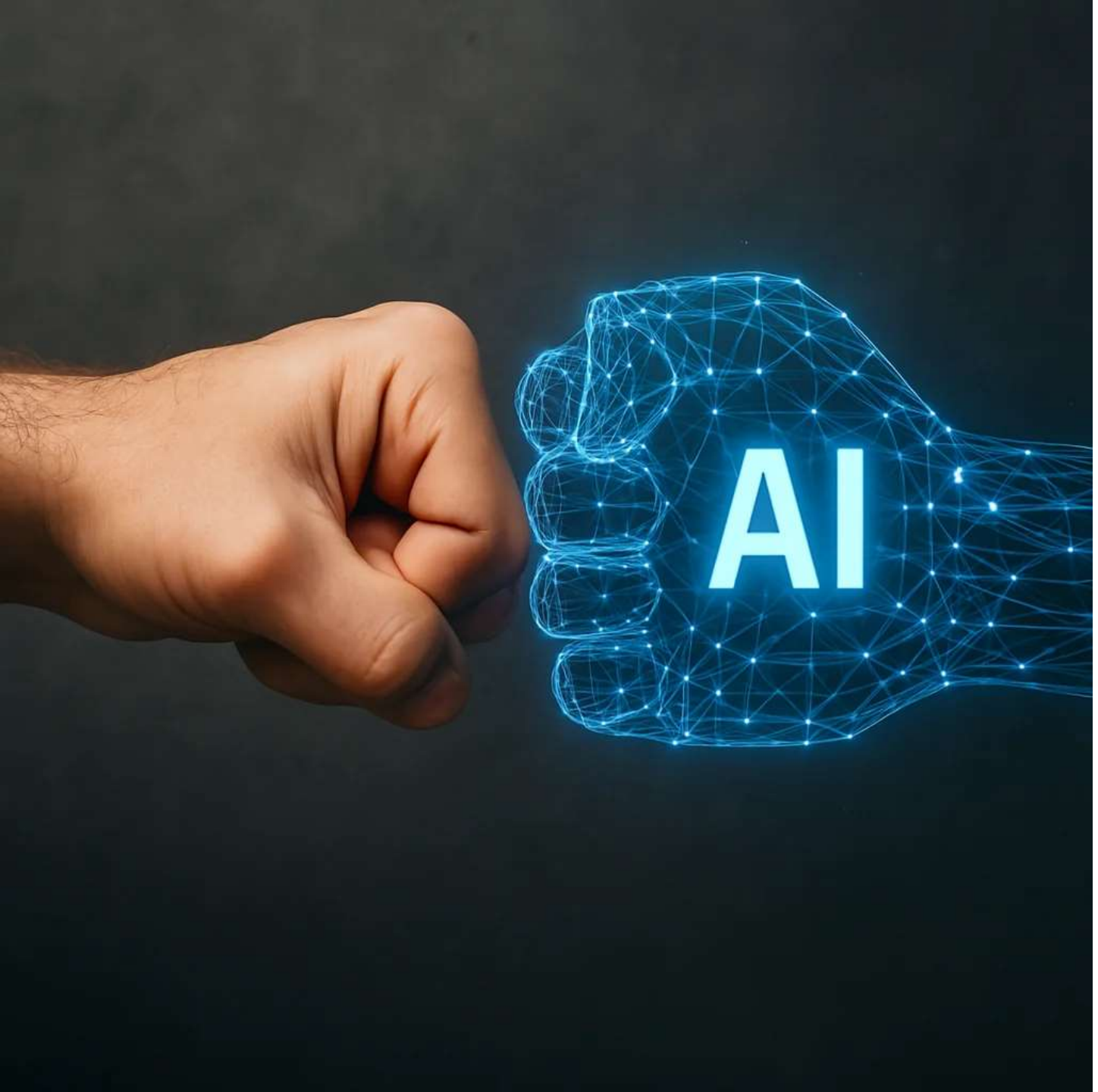
Nathalie Claes
Security Governance Expert, Management Consultant and Auditor

#GlobalLeadingVoices

Agenda

- Organizational Resilience
- What is ISO/IEC 42001?
- AI Risk Management
- What is ISO/IEC 22301?
- Business Continuity and Operational Resilience
- Questions and answers

PECB



AI

An opportunity or not?

PECB

Organizational Resilience

What is Organizational Resilience?

- Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context. Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk.
- An organization’s resilience is influenced by a unique interaction and combination of strategic and operational factors. Organizations can only be more or less resilient; there is no absolute measure or definitive goal.

ISO/IEC 22316:2017

ISO/IEC 42001

ISO/IEC 42001 specifies the requirements for establishing, implementing, maintaining, and continually improving an AIMS within an organization.

It follows the harmonized structure so it aligns with other ISO management system standards.

Its requirements are expressed with the verb “shall.”

Organizations can obtain certification against this standard.

PECB

ISO/IEC 42005

ISO/IEC 42005 guides organizations in assessing the impact of AI systems to determine the potential effects of AI on individuals and societies that are affected by it.
It also provides guidance on documenting AI system impact assessments.
It is applicable for all organizations involved in developing, providing, or using AI systems.
Organizations cannot obtain certification against this standard.

ISO/IEC 23894

ISO/IEC 23894 provides guidance for managing AI risks by integrating risk management principles into their AI-related activities and functions.

It is relevant to all types of organizations regardless of their size or industry.

Organizations cannot obtain certification against this standard.

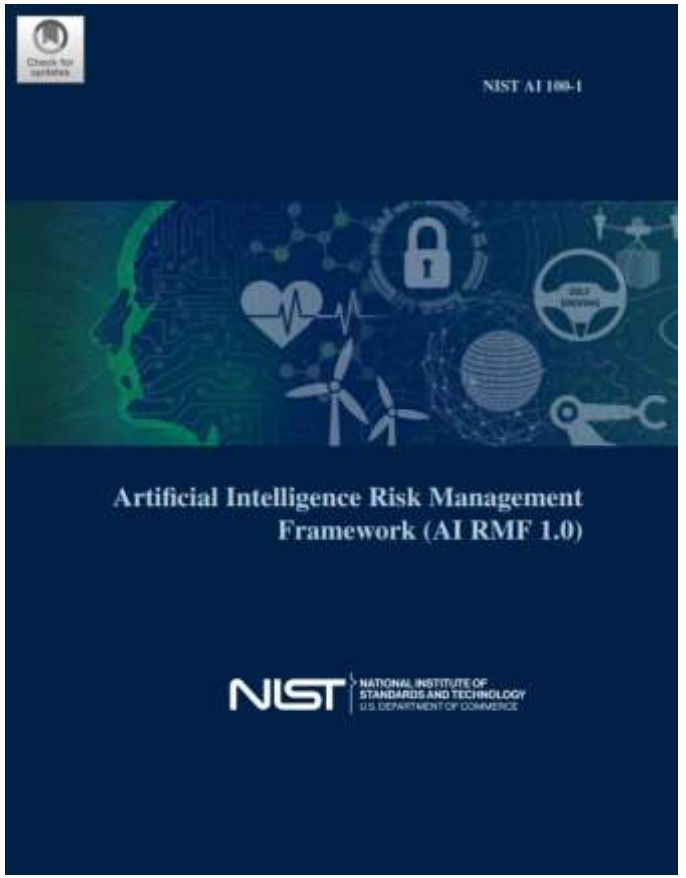
PECB

NIST Artificial Intelligence Risk Management Framework (AI RMF)

The AI RMF is divided into two parts:

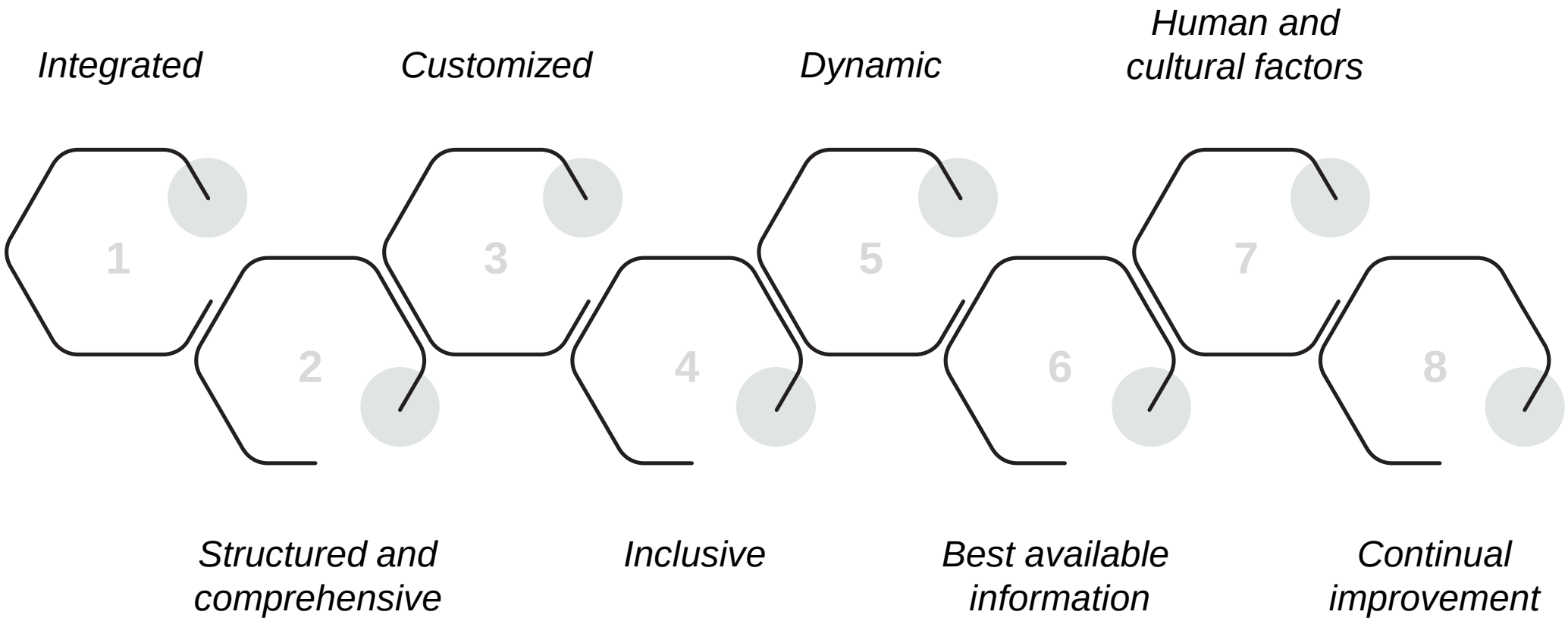
- Part 1 focuses on framing AI risks and introducing the intended audience;
- Part 2, the “core” framework, defines four key functions (govern, map, measure, and manage) with categories and subcategories to help organizations address AI risks in practice.

The AI RMF is developed collaboratively by NIST in coordination with the private and public sectors.



Principles of AI Risk Management

ISO/IEC 23894, Table 1



PECB

AI Risk Management Framework

ISO/IEC 23894, clause 5.1

The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions.
Risk management involves assembling relevant information for an organization to make decisions and address risk. While the governing body defines the overall risk appetite and organizational objectives, it delegates the decision-making process of identifying, assessing and treating risk to management within the organization.

Risk Sources

ISO/IEC 23894, clause 6.4.2.3 and ISO/IEC 42001, Annex C.3.1 to C.3.4

The organization should identify a list of risk sources related to the development or use of AI, or both, within the defined scope.

Complexity of environment	**Lack of transparency and explainability**	**Level of automation**	**Risk sources related to machine learning**
When AI systems operate in complex environments, where the range of situation is broad, there can be uncertainty on the performance and therefore a source of risk (e.g. complex environment of autonomous driving).	*The inability to provide appropriate information to interested parties can be a source of risk (i.e. in terms of trustworthiness and accountability of the organization).*	*The level of automation can have an impact on various areas of concerns, such as safety, fairness or security.*	*The quality of data used for ML and the process used to collect data can be sources of risk, as they can impact objectives such as safety and robustness (e.g. due to issues in data quality or data poisoning).*

PECB

Risk Sources

ISO/IEC 42001, Annex C.3.5 to C.3.7

System hardware issues

Risk sources related to hardware include hardware errors based on defective components or transferring trained ML models between different systems.

System life cycle issues

Sources of risk can appear over the entire AI system life cycle (e.g. flaws in design, inadequate deployment, lack of maintenance, issues with decommissioning).

Technology readiness

Risk sources can be related to less mature technology due to unknown factors (e.g. system limitations and boundary conditions, performance drift), but also due to the more mature technology due to technology complacency.

Identification of Assets

ISO/IEC 23894, clause 6.4.2.2

The organization should identify assets related to the design and use of AI that fall within the scope of the risk management process. Understanding what assets are within the scope and the relative criticality or value of those assets is integral to assessing the impact. Both the value of the asset and the nature of the asset (tangible or intangible) should be considered.

Inventory of Assets – Some examples

Data Assets

- Training, validation, and testing datasets
- Data labeling outputs
- Data lakes and warehouses
- Synthetic datasets
- Metadata (sources, rights, structure)

AI Models and Algorithms

- Trained models (production, prototypes)
- Model weights and parameters
- Model versioning systems
- Proprietary algorithms
- Explainability artifacts (e.g., SHAP, LIME)

Software and Tools

- AI development platforms (TensorFlow, PyTorch)
- Machine learning pipelines and workflows
- AutoML tools
- Custom-built APIs and applications
- Customized open-source libraries

Infrastructure

- Specialized AI hardware (GPUs, TPUs)
- Cloud AI services (AWS, Azure, Google)
- On-premises AI servers
- Edge devices running AI models

Knowledge and Documentation

- Model and data documentation
- Ethical AI assessments
- AI governance frameworks
- Internal development guidelines

Human Resources

- AI developers and data scientists
- Ethics and compliance officers
- AI project managers
- Trainers for AI models

Third-Party Dependencies

- Vendor AI APIs and services
- SaaS tools with embedded AI
- External consulting partners
- Licensing agreements

Intellectual Property

- AI-related patents
- AI trade secrets
- Copyrighted AI-generated content
- Proprietary datasets and models

Security and Compliance Assets

- AI audit trails and logs
- Bias and fairness monitoring tools
- AI cybersecurity models
- Regulatory compliance reports

PECB

Identification of Potential Events and Outcomes

ISO/IEC 23894, clause 6.4.2.4

The organization should identify potential events that are related to the development or use of AI and can result in a variety of tangible or intangible consequences. Events can be identified through one or more of the following methods and sources:

- *published standards;*
- *published technical specifications;*
- *published technical reports;*
- *published scientific papers;*
- *market data on similar systems or application already in use;*
- *reports of incidents on similar systems or application already in use;*
- *field trials;*
- *usability studies;*
- *the results of appropriate investigations;*
- *stakeholder reports;*
- *interviews with, and reports from, internal or external experts;*
- *simulations.*

Sample events and outcomes

Development-Phase Events

- Data quality issues → Biased models, reputational harm
- Model design flaws → Ineffective outputs, product failure
- Inadequate testing → Unexpected behavior in production
- IP breaches during training → Legal disputes, penalties
- Unauthorized datasets → Regulatory fines, trust issues
- Lack of explainability → Trust erosion, compliance challenges

Deployment-Phase Events

- Ethical norm violations → Public backlash, customer loss
- System integration failures → Business disruption
- Model drift → Reduced accuracy, operational errors
- Unintended model behavior → Misinformation, legal risks
- Misinterpretation of inputs → Safety incidents

Use-Phase Events

- Unauthorized AI use → Data breaches, data misuse
- Privacy violations → GDPR fines, lawsuits
- Abuse of AI outputs (deepfakes) → Reputational damage
- Over-reliance on AI → Operational errors, loss of oversight

Maintenance and Monitoring Events

- Failure to update models → Security vulnerabilities
- Ignored bias monitoring → Discrimination claims
- Poor incident response → Extended downtime, penalties
- Non-transparent model updates → Accountability loss

External Factors Events

- Changes in legislation (e.g., EU AI Act) → Compliance pressure, costs
- Adversarial attacks (e.g., model hacking) → Security breaches
- Supplier AI failures → Service disruptions, third-party liabilities

Identification of Consequences

ISO/IEC 23894, clause 6.4.2.6

As part of AI risk assessment, the organization should identify risk sources, events or outcomes that can lead to risks. It should also identify any consequences to the organization itself, to individuals, communities, groups and societies. Organizations should take particular care to identify any differences between the groups who experience the benefits of the technology and the groups who experience negative consequences.

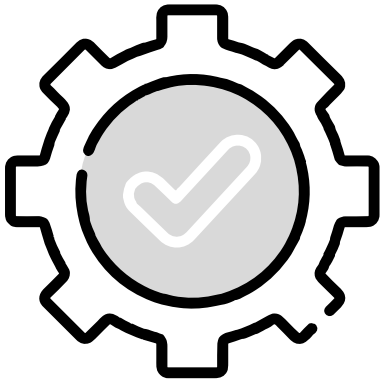
Consequences to the organization necessarily differ from those to individuals and to societies. Consequences to organizations can include but are not limited to:

- *investigation and repair time;*
- *(work) time gained and lost;*
- *opportunities gained or lost;*
- *threats to health or safety of individuals;*
- *financial costs of specific skills to repair the damage;*

Identification of Controls

ISO/IEC 23894, clause 6.4.2.5

The organization should identify controls relevant to either the development or use of AI, or both. Controls should be identified during the risk management activities and documented (in internal systems, procedures, audit reports, etc.).
Controls can be utilized to positively affect the overall risk by mitigating risk sources and events and outcomes.
The operating effectiveness of the identified controls should also be taken into account, particularly control failures.

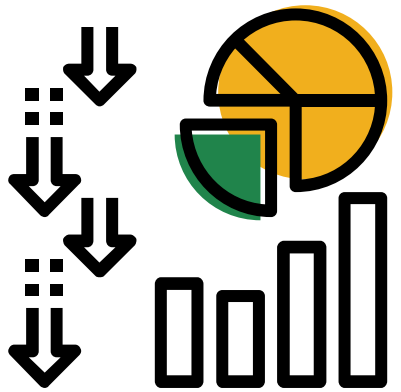


Risk Analysis

ISO/IEC 23894, clause 6.4.3.1 and ISO 31000, clause 6.4.3

The analysis approach should be consistent with the risk criteria developed as part of establishing the context.

Risk analysis should consider factors such as:
—the likelihood of events and consequences;
—the nature and magnitude of consequences;
—complexity and connectivity;
—time-related factors and volatility;
—the effectiveness of existing controls;
—sensitivity and confidence levels.

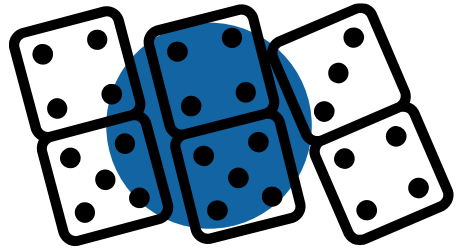


Assessment of Consequences

ISO/IEC 23894, clause 6.4.3.2

When assessing the consequences identified in the risk assessment, the organization should distinguish between a business impact assessment, an impact assessment for individuals and a societal impact assessment.
Business impact analyses should determine the degree to which the organization is affected, and consider elements including but not limited to the following:

- *criticality of the impact;*
- *tangible and intangible impacts;*
- *criteria used to establish the overall impact.*

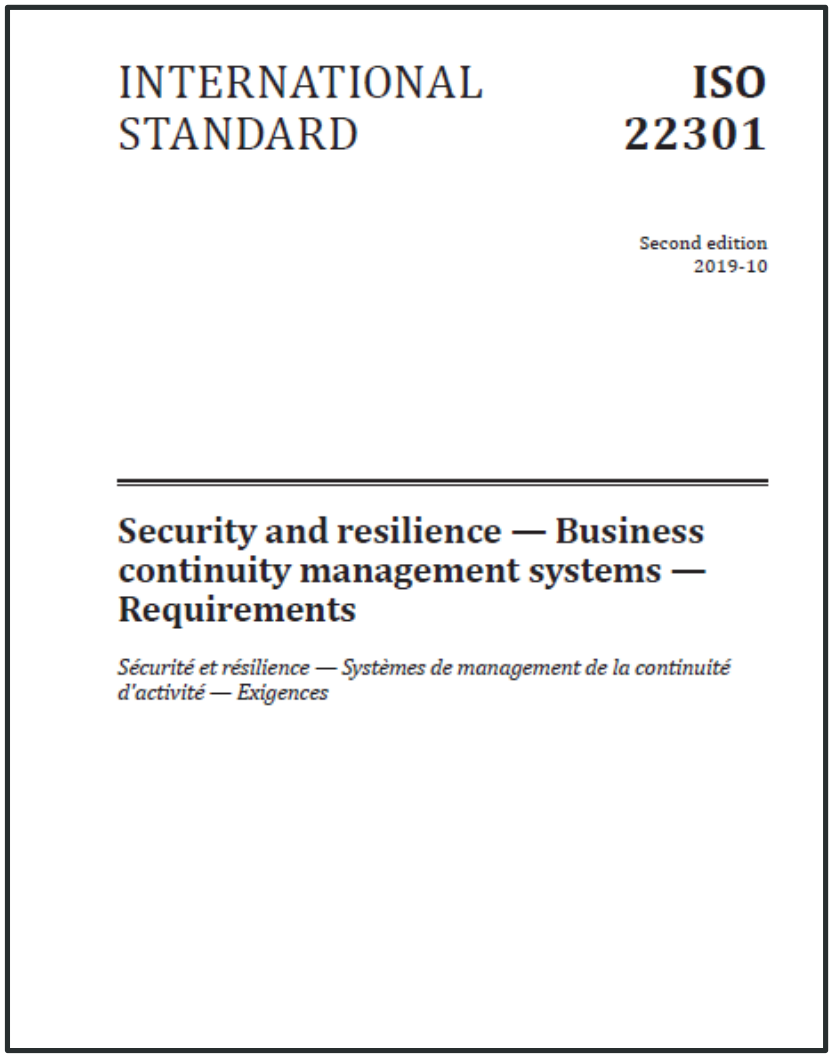


Let’s talk about ISO/IEC 22301, Business Continuity and Operational Resilience

PECB

ISO/IEC 22301

Business Continuity is the capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption



PECB

Operational Resilience

Operational resilience refers to an entity's capacity to endure and rebound from various disruptive events. These events cover a broad spectrum ranging from man-made occurrences like cyber-attacks and system failures to natural disasters such as pandemics and severe weather.

Additionally, they include strategic challenges like regulatory changes and emerging competitive landscapes.

Latest developments – Emerging Risks

Managing AI, ESG, Cyber and other emerging risks

But HOW?

- Multi-disciplinary **Think-Tanks** (IT, OT, Physical Security etc)
- Focus on reducing **impact/consequence** (rather than likelihood)
- **Partner-up** with other organisations where possible

PECB

Latest Standards & Regulations

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

PECB

DORA covers…

ICT risk management

Principles and requirements on ICT risk management framework

ICT third-party risk management

Monitoring third-party risk providers

Key contractual provisions

Digital operational resilience testing

Basic and advanced testing

ICT-related incidents

General requirements

Reporting of major ICT-related incidents to competent authorities

Information sharing

Exchange of information and intelligence on cyber threats

Oversight of critical third-party providers

Oversight framework for critical ICT third-party providers

Third Party Risk Management - TPRM

TPRM & Supply Chain Continuity Planning

- The Cloud is just someone else's computer
- ICT Continuity/Resilience – The 'A' in the CIA triad
- Importance of business continuity options – including for notification and collaboration
- Maintaining ongoing stakeholder confidence, managing reputation
- Who bears the cost of disasters like Crowdstrike?
  Is that really 'force majeure'? Where does actually insurance fit in & help?
- Lessons learned in terms of crisis response – 'them & us' approach, does that still work?
- Physical vs Digital Supply Chain

Typical risks in the **Physical** Supply Chain

How does AI offer opportunities to optimize the supply chain?

Optimization of supply chain processes is critical to the successful running of businesses to achieve competitiveness. Many big corporations including the likes of Amazon, Microsoft, Meta, are investing heavily in Artificial Intelligence (AI) and Machine Learning to address the multifaceted aspects of supply chain in their businesses, ranging from demand forecasting, inventory management, logistics, and warehouse efficiency. The need to manage big data has generated interest in supply chain analytics, especially with the dynamic nature of the marketplace and the need to respond timely to market changes and customer demands. Predictive analytics can play a key role in helping decision makers to leverage artificial intelligence algorithms and machine learning to respond proactively to market demands. There are claims that AI-enabled supply chain management may help to cut logistics cost by 15%, reduce inventory levels by 35%, and improve service levels through increases in throughputs and reduction in error rates.

With the capacity of AI to process large amounts of data in real time and evaluate future marketing trends, operational efficiency can be significantly enhanced. Many aspects of operational management that are intertwined with supply chain management are equally affected as AI and machine learning are applied to streamline operations, reduce disruptions, and improve transparency. The predictive power of AI algorithm is enormous and cannot be understated in optimizing supply chain processes.

How does AI offer opportunities to identify and manage risk in the supply chain?

Identifying Potential Supply Chain Risks

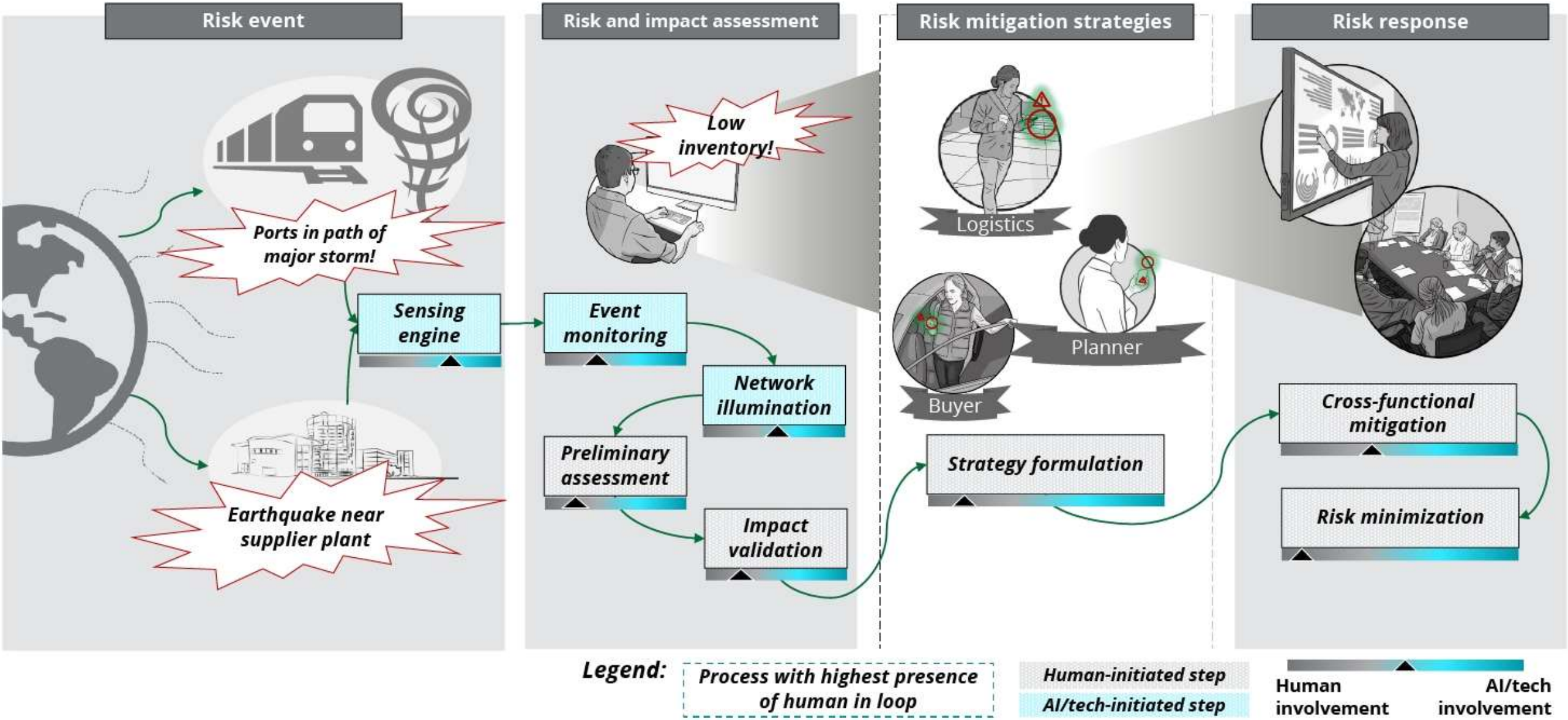
One of the primary applications of generative AI in supply chain risk management could be its ability to continuously monitor and analyze data from multiple sources to identify potential risks. These could include geopolitical risks, natural disasters, economic shifts or even supplier performance issues. Generative AI systems can process data from news outlets, social media and financial reports, flagging any information that might indicate a risk to the supply chain. By identifying risks early, businesses can take preventive actions, such as altering supplier relationships or adjusting inventory levels.

Predicting Supply Chain Disruptions

Generative AI is particularly effective at predicting potential disruptions. By analyzing historical data and external factors such as weather patterns, economic indicators and political events, AI systems could generate forecasts of potential supply chain disruptions at a fraction of the time it might take for a human analyst. This predictive capability would allow businesses to more thoroughly model different scenarios, anticipate challenges and develop contingency plans that reduce the impact of disruptions.

Human vs AI/tech involvement

Source: Deloitte US

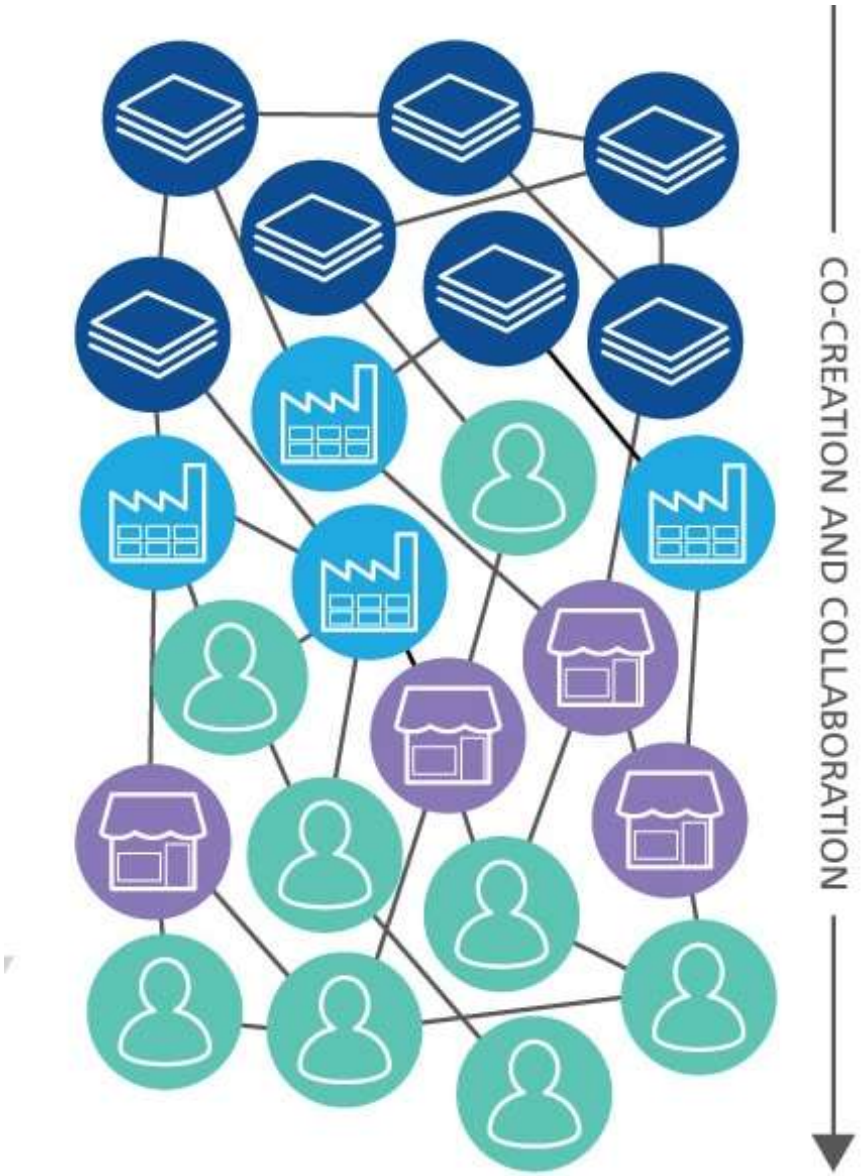


Typical risks in the **Digital** Supply Chain

PECB

The ‘**People Factor**’ remains...
Also in context of the Digital Supply Chain

From Supply Chain to ‘**Value Web**’ or **‘Resilient Hub’**

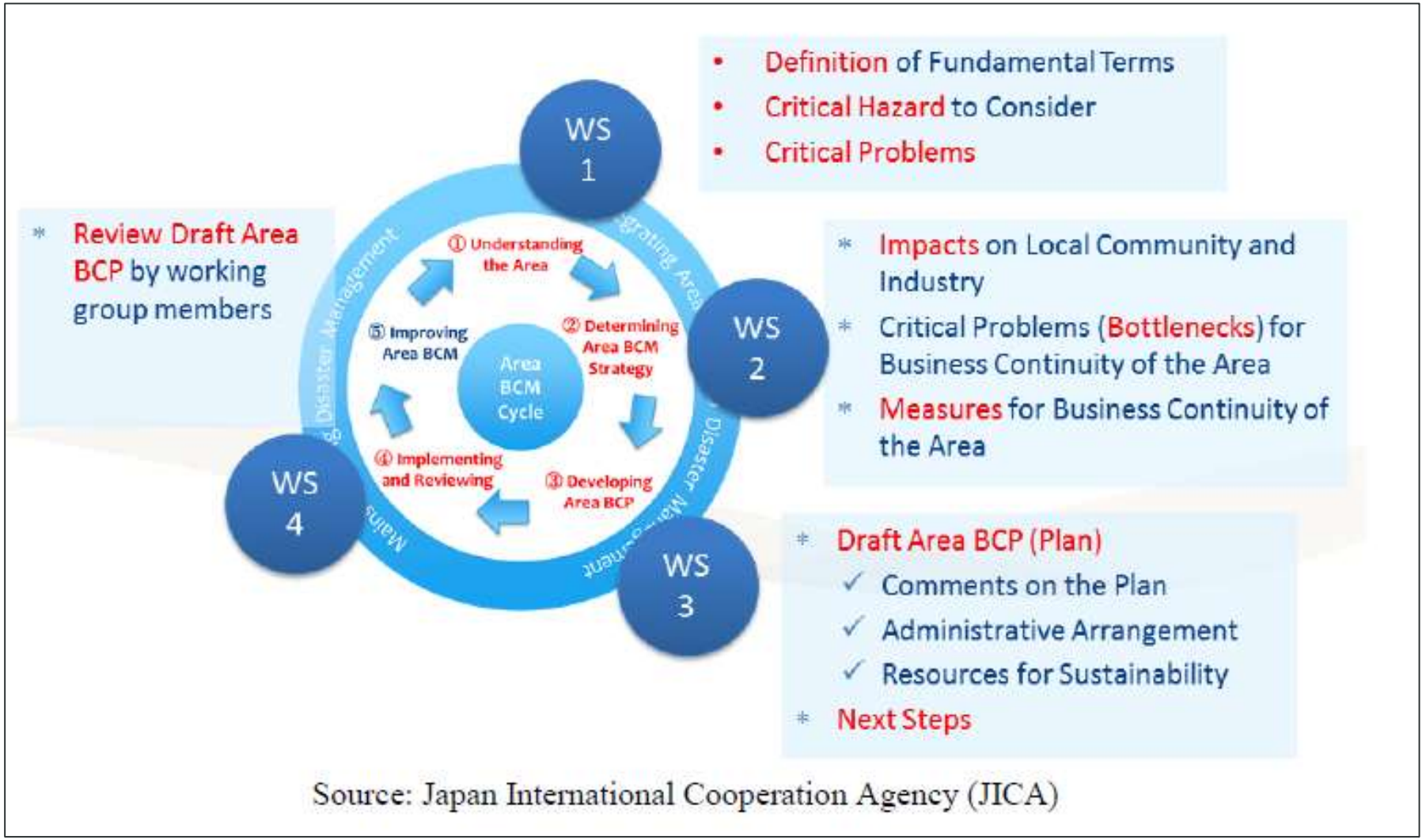


Value is based on knowledge exchange that drives proactive production of goods and services

Graphic: Deloitte University Press | DUPress.com

PECB

Area BCPs



Source: Japan International Cooperation Agency (JICA)

THANK YOU

rinskeg@businessasusual.com.au
https://www.linkedin.com/in/businessasusual/
n.claes@myrnacoachingconsulting.be
https://www.linkedin.com/in/nathalieclaes/