# EFFECTIVE SAFEGUARDING OF SUPPLY CHAINS FROM GLOBAL RISKS

## DEKRA Expert Solution: AI-Based Supply Chain Risk Management Services

**Companies are facing an entirely new magnitude of difficulties in their supply chains. The simultaneous occurrence of geopolitical conflicts, cyber attacks and raw material shortages together with increasing environmental and social sustainability requirements pose considerable challenges. Reversing globalization is not the solution. Instead, it is important to adopt a more resilient risk management system based on forward-looking approaches for the process and supply sectors. DEKRAs Supply Chain Risk Management (SCRM) services integrate an AI-based early warning system that screens weaknesses in different supply stages and facilitates the assessment of risky suppliers. The combined AI and auditor expertise-based solution is founded on globally proven standards and management systems.**

For a long time, just-in-time production, 24/7 availability and the avoidance of stock surpluses and defects have been familiar mantras in purchasing and production management. Largely risk-free global outsourcing of value-adding stages have allowed warehouses and raw material costs to be optimised and regional production disadvantages to be compensated. Large manufacturers and original equipment manufacturers (OEMs) are directly or indirectly inked to thousands of suppliers in many different countries – from supplier level 1 (modules, systems) and 2 (main components) through to levels 3 and 4 for subcomponents and raw materials. Each delivery stage is, in turn, the node of a further delivery network. Even if manufacturers pursue a single sourcing or dual sourcing strategy - with one or two main suppliers – there may be a complex non-transparent global supply structure (inbound) behind the main suppliers. On top of this come the logistics (outbound) in the form of distribution centres, middlemen, distributors and forwarding agents. These structures are particularly susceptible to interference when the nodes and their links are not transparent. A critical event in an unknown location can suddenly spread unchecked and possibly infiltrate the entire supply chain, even to the point of bringing it to a standstill.

## Framework Conditions
## More Critical Now than in a Long Time

### Geopolitics

Established supply relationships are collapsing overnight due to boycotts or armed conflicts. Over 1,000 companies have left Russia, the 11th largest economy in the world, as a result of the Ukraine war. The consequences of the China-Taiwan tension are not foreseeable yet.

### Sustainability

More restrictive global regulations for environmental protection, human rights and corporate governance (ESG) are demanding greater transparency.

### Climate

Local heat waves, floods, storms, earthquakes or forest fires resulting in large-scale air pollution are becoming permanent risks for supply networks.

### Digital transformation

Big data analytics, artificial intelligence and remote solutions are transforming processes and business models at all levels of the value chain. Data transfer stop due to cyber attacks.

A key concern for many CEOs is how to strengthen the resilience of value and supply chains and thereby reduce supply risks. The years following the outbreak of the pandemic have shown that fundamental risks can arise simultaneously and without any significant notice. It is therefore no longer sufficient to simply conduct a risk analysis of the internal network alone. The consequences of geopolitical conflicts, potential natural disasters or new regulations are becoming more serious at each node of the supply network. The *Supply Chain Act* in Germany (*Lieferkettensorgfaltspflichtengesetz, LkSG*) and the forthcoming *Directive on Corporate Sustainability Due Diligence (CSDDD)* at the EU level in 2024 signal the direction in which risk management is moving. German law currently requires companies with at least 3,000 employees to operate a risk management system for the protection of human rights and the environment. Although the German requirement is set to fall to companies with 1,000 employees in 2024, the threshold in other countries is already significantly lower. These higher standards will have an impact at all supply stages because due diligence covers everything from raw material sourcing to the finished product. In addition, there are new regulations in international procurement markets outside the EU. Singapore, for example, is introducing a traffic light system to channel energy, transport and property investments into sustainable activities. This puts great pressure on companies and organizations, especially in regards to their risk management systems. But these due diligences only cover ESG topics from raw material sourcing to the finished product. So far there is no law which drives the real risk management. Purchasing and logistics teams are only able to reduce supplier risks if all specific risk factors and requirements in all supply stages (inbound/outbound) can be identified.

### Supply Chain Management Requirements

- The regulations are increasingly diverging. Opaque, complex supply chains
- Supply vulnerabilities caused by in transparency, cyberattacks, data theft, fraud, counterfeiting
- Consumer awareness of the sustainability, origin, health and ethical aspects of products
- Quality assurance methods are becoming more agile
- Stakeholders and the capital market are demanding greater transparency. Increased reporting obligations

## Resilience through Foreseeable and Identifiable Risks

In highly dynamic risk situations, companies must improve their ability to adapt and react if they are to remain capable of responding to critical external events at short notice. Such acquired resilience allows operations to be resumed within the defined time window.

In the current environment of growing uncertainty, it is becoming increasingly difficult to make predictions and engage in forward planning, calling for a risk culture that allows the unthinkable to be imagined. A distinction needs to be made between **foreseeable and identifiable** risks. Examples: A supplier's financial difficulties are **foreseeable** on the basis of publicly available indicators such as "layoffs, rating downgrades, unpaid wages". The same applies in cases of "labor unrest, protests, strikes or employee suicides" or in cases of "official closures, corruption, theft". Directly **identifiable risks**, on the other hand, are the consequences of "industrial accidents, cyber attacks, ESG risks such as polluted rivers, child labor" or even concretely identifiable operational risks such as "interruptions, undercapacity and delivery problems".

| Risk Categories | Indicators |
|---|---|
| **ESG**<br>Environment, Social, Governance (also combined) Due Diligence Act<br>$CO_2$ Emissions | Pollution (intentional or accidental),<br>Impact on climate,<br>Human and labor rights violation, Child labor,<br>Modern slavery, Ethical scandals,<br>Health and safety hazard... |
| **Cyber**<br>Cyber security<br>Information security<br>Data privacy | Cyber-attack,<br>Phishing,<br>Security breach (intentional or accidental),<br>GDPR non-compliance,<br>Malvertising... |
| **Operations**<br>Business continuity<br>Process safety and performance<br>Health/Safety<br>Demand volatility<br>Delivery shortages | Safety incidents,<br>Equipment or process failure,<br>Natural disasters, disruptions, forecast fluctuations,<br>Unreliable/non-transparent deliveries, missing/incomplete forecast and order processes<br>Labor strikes... |
| **Legal, Compliance, Governance**<br>Human rights<br>Competition rules (fraud control...)<br>International restrictions<br>Finance | Corruption,<br>Fraud, Theft,<br>Lawsuits or public investigations,<br>Sanctions rules busting...<br>Insolvencies |

Each risk category requires specific expert knowledge if risks are to be successfully managed in practice. Identifying administrative risks requires different skill sets to those needed for identifying IT and information security risks. Auditors with years of experience in the application of standards and management systems play an important role when it comes to identifying which indicators and risk characteristics can potentially compromise the ability to deliver. Once the main risks of the respective delivery stage have been defined and the risk indicators have been selected, they can then be weighted based on specific requirements and criticality.

## Foreseeable Risk Management

Not every change in framework conditions will threaten the entire supply chain. But in multipolar, global risk situations, typical supply chain management categories such as goods transport, logistics and supply bottlenecks are inadequate. For this reason, it is important to establish an early warning system which can identify multiple threats on the basis of expert assessments. Ideally, this system will be able to monitor the new risks (ESG, cyber, operations, legal/compliance) to the supply chain simultaneously and real time to detect suppliers‘ specific risks and critical events. This can be provided by AI-supported DEKRA Supply Chain Risk Management services.

The first prerequisite for SCRM is to determine the maturity level of risk management in the company. The internal structures, organisational processes and the interfaces to the main suppliers are analysed. Has the company formulated a risk policy? Have specific preparations already been made and documented for the main risk groups (geopolitics, cyber security, ESG, etc.) and current crisis scenarios? If management systems are already established, e.g. for information security (ISO 27001) or to enhance the environmental performance (ISO 14001), the risk assessments for SCRM are taken into account to avoid duplication of work. Companies with the lowest maturity level have not prepared any risk management and have only reacted to critical events in the supply chain in the past. In contrast, companies with the highest maturity level continuously manage the currently identified risk categories (PDCA cycle) with a tailor-made risk matrix, employee trainings, documentation, software tools, etc.

## Auditor Expertise Combined with AI Screening

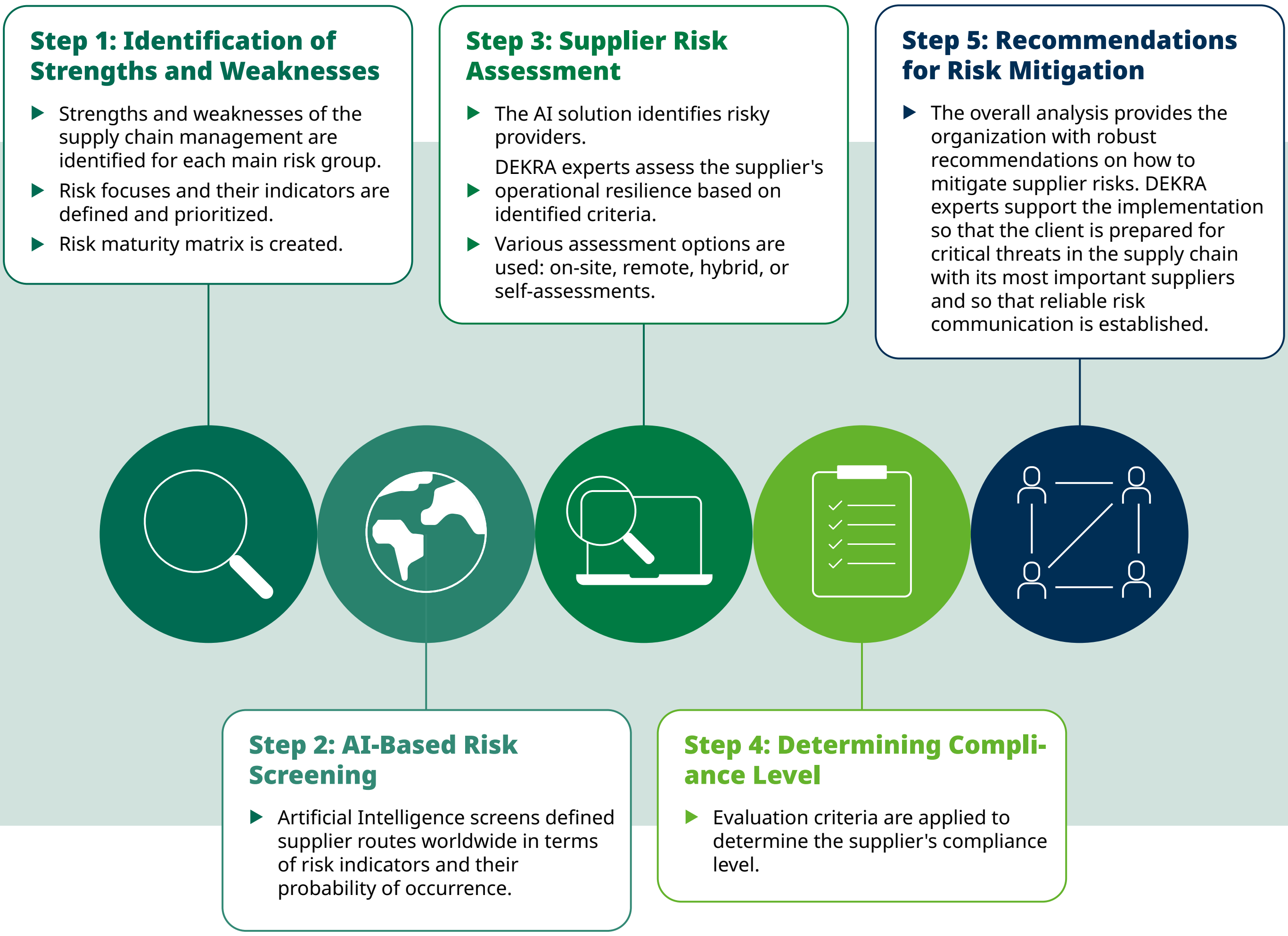
According to estimates by the OECD and the US Department of Commerce, about 80 per cent of world trade is subject to quality standards and conformity assessments. Quality management systems (QMS) and certification have helped bring about a constantly evolving infrastructure based on proven standards, material specifications and customer audits. These requirements are essential for maintaining the stability of global supply chains.  For example, the experience gained during customer audits and certification processes at all supplier levels provides important data for the AI-supported DEKRA SCRM solution. The basis is provided by key risk aspects from standards such as ISO 22301 (Business Continuity Management), ISO 3100 (Risk Management, Finance, Supply Chain), ISO 27001 (Information Security) and ISO 45001 (Occupational Health and Safety). Added to these are quality management aspects relating to corporate governance.

Based on the risk analysis and the defined risk indicators, the AI platform screens the available information for each relevant supply level. Sources include publicly available information in 50 languages, e.g., from social media, reporting, trade portals, databases, and local press. The upstream, software-based assistance system makes previously invisible suppliers visible and damage events – even those in remote regions. This in turn increases the organisation‘s overall understanding of potential risks and significantly improves its response options, both in terms of time and quality. Such acquired resilience allows operations to be resumed within the defined time window.

If the AI platform issues a risk warning on the basis of its continuous monitoring, the company concerned can be requested to assess its current and future ability to deliver. Experience has shown that such early and direct communication alone can significantly increase the resilience of the supply chain. Based on the information obtained, decisions can be made on the necessity of further customer audits, on-site assessments, remote assessments or self-assessments.

The combined DEKRA Supply Chain Risk Management solution, consisting of an AI-based early warning system and auditor audits, sets in motion a cycle of continuous improvement that is central to quality and risk management: The assessments provide additional indicators and input data for the AI system which further refine the discriminatory power of the screening and thereby further improve the resilience of the supply chain.

## DEKRA SCRM Services at a Glance:



### Step 1: Identification of Strengths and Weaknesses

- Strengths and weaknesses of the supply chain management are identified for each main risk group.
- Risk focuses and their indicators are defined and prioritized.
- Risk maturity matrix is created.

### Step 2: AI-Based Risk Screening

- Artificial Intelligence screens defined supplier routes worldwide in terms of risk indicators and their probability of occurrence.

### Step 3: Supplier Risk Assessment

- The AI solution identifies risky providers.
- DEKRA experts assess the supplier's operational resilience based on identified criteria.
- Various assessment options are used: on-site, remote, hybrid, or self-assessments.

### Step 4: Determining Compliance Level

- Evaluation criteria are applied to determine the supplier's compliance level.

### Step 5: Recommendations for Risk Mitigation

- The overall analysis provides the organization with robust recommendations on how to mitigate supplier risks. DEKRA experts support the implementation so that the client is prepared for critical threats in the supply chain with its most important suppliers and so that reliable risk communication is established.

**Schedule SCRM services to support a strong and compliant supply chain operating at peak performance to ensure maximum results for your business goals today!**

CONTACT US

Status 07/2023