

Risk Matrix: systematically assessing supply and procurement risks

The risk matrix is a risk management tool used to assess and visualise procurement risks by likelihood of occurrence and potential impact. In procurement, it serves to systematically capture supplier, material and process risks and to derive prioritised measures. As a basis for a risk mitigation plan and supplier classification, the risk matrix is part of the standard toolkit of strategic procurement organisations.

Key facts

- A risk matrix assesses risks in two dimensions: likelihood of occurrence and impact (severity of loss or impact on production and delivery capability).
- Typical scales in practice range from 3×3 to 5×5 cells; five levels from 'very unlikely' to 'very likely' are frequently used.
- In procurement, the matrix primarily covers supplier failures, price and currency risks, geopolitical dependencies and supplier cyber risks.
- Highly prioritised risks in the upper right zone of the matrix usually require immediate countermeasures such as safety stock buffers, second sources or contractual safeguards.
- The risk matrix should be updated at least once a year and whenever material changes occur – for example supplier changes or geopolitical developments.
- It forms the bridge between the procurement portfolio analysis and operational measures such as inventory management, supplier rating and a structured risk mitigation plan.

Definition: risk matrix

The risk matrix (also known as a risk matrix diagram or Risk Matrix) is a graphical assessment tool that arranges identified risks along two dimensions: the probability of their occurrence and the severity of their potential impact. In a procurement context, it is used to classify supplier and material risks, set action priorities and deploy risk management resources in a targeted manner.

Structure and zones of the matrix

A typical risk matrix consists of five probability levels and five impact levels; reduced 3×3 variants are also common in practice. Each risk is positioned as a point in one of the cells. The cells can be divided into zones: green cells are considered acceptable, yellow cells as requiring monitoring and red cells as critical. In practice, the zone allocation is guided by the organisation's risk tolerance and should be agreed with management.

Distinction from other tools

The risk matrix is not identical to the procurement portfolio analysis, which arranges suppliers by business importance and supplier risk – however, the two tools complement each other. The portfolio analysis provides an overview of the supplier landscape, while the risk matrix assesses individual risks

in detail and prioritises measures. The spend cube, which analyses procurement volumes by supplier and category, likewise provides valuable input data for a well-founded risk assessment.

Risk classes as an assessment framework

Many organisations combine the risk matrix with predefined risk classes, such as strategic risks, operational risks, financial risks and compliance risks. Assigning risks to classes facilitates the allocation of responsibilities and reporting. It is important that the class and level definitions are documented uniformly across the organisation so that results from different sites or buyers remain comparable.

Methods and approach for creating a risk matrix

Creation follows a structured process: risk identification, risk assessment, positioning in the matrix and derivation of measures. The quality of the result depends less on the graphical presentation than on the rigour of the preceding analyses, such as supplier classification and the examination of dependencies.

Step 1: identify risks and build the data basis

At the outset, all relevant procurement risks are captured: supplier failures, quality problems, delivery delays, price and currency fluctuations, geopolitical risk in sourcing markets and supplier cyber risk. Clean inventory records and an up-to-date spend cube help make critical procurement volumes visible. In addition, the Approved Vendor List (AVL), the supplier rating and external data sources such as the D-U-N-S Number (DUNS) provide indications of suppliers' financial stability.

Step 2: assess likelihood and impact

Each risk is assessed using uniform definitions. The likelihood of occurrence can be derived partly from historical data – for example documented delivery delays, cancelled orders or revoked take-or-pay obligations – and partly from expert judgement. The impact should be measured not only in monetary terms but also in production-related categories, such as downtime duration or replenishment lead time for critical components. To enhance the validity of the assessment, involving specialist departments such as manufacturing, quality and controlling is recommended.

Step 3: derive and prioritise measures

For all risks outside the green area, measures are defined and documented in the risk mitigation plan. Typical measures include building second sources, increasing safety stock buffers, adjusting contract clauses (for example obtaining a binding offer instead of a non-binding commitment), agreeing expedite rate arrangements with critical suppliers or entering into purchasing alliances with other companies to improve negotiating power and protection. Each measure should specify an owner, a deadline and a review criterion; a subsequent cost-benefit analysis helps assess the balance between protection and effort.

Key KPIs and assessment fields in the procurement matrix

The risk matrix itself is qualitative, but its soundness depends on measurable metrics. These make assessment scales more objective and allow continuous monitoring of the risk position.

Supplier and procurement metrics

Key metrics are on-time delivery (in practice typically target values above 95 to 98 per cent), the number of critical single sources, the replenishment lead time for key components and the share of spend with

suppliers classified as critical risk. The supplier rating and the average expedite rate also provide indicators of operational resilience. These values are usually collected periodically and linked to the entries in the risk matrix.

Criticality of materials and components

For materials, the quality of alternative suppliers on the Approved Vendor List (AVL), the long-horizon availability of key components and dependence on individual regions are relevant. For components with long replenishment lead times, it is worth defining a safety stock buffer, whose size typically ranges from a few days to several weeks depending on criticality and procurement duration. Take-or-pay obligations under framework agreements should also be assessed, as they can lead to additional costs in the event of disruption.

Compliance and sustainability metrics

Alongside operational metrics, compliance risks are gaining in importance, such as child labour risk assessment in supply chains or audit rights agreed as part of supplier audits. This includes the proportion of audited suppliers, the enforceability of audit rights in contracts and the certification status of critical suppliers. Such criteria should be incorporated into the matrix as a separate risk category.

Risks and controls: limitations and safeguards of the risk matrix

The risk matrix is a helpful but not self-executing tool. Its validity depends on data quality, the systematic nature of the assessments and the consistent implementation of the derived measures.

Typical pitfalls

Common mistakes are subjective or non-standardised assessments, updating only during acute crises and restricting the scope to tier 1 suppliers. Tier 2 and tier 3 risks often remain invisible, although in practice they are frequently the cause of supply failures. Neglecting cumulative risks – for example several suppliers in the same region or with the same upstream product base – also leads to distorted results.

Controls and review mechanisms

Effective controls include standardised assessment forms, reviews within the procurement team, management spot checks and documented traceability of every classification. The supplier classification should be reconciled regularly against the supplier rating and current supplier data. For critical suppliers, supplier audits and the contractual anchoring of audit rights are recommended in practice, so that statements on process efficiency and compliance can actually be verified.

Legal and tax aspects

In cross-border procurement, customs and compliance issues are also relevant, such as correct documentation with an ATA Carnet for temporary exports or electronic integration via cXML in highly automated ordering processes. How such an approach should be designed correctly in tax and customs law terms should be examined on a case-by-case basis with specialists; this article does not constitute legal advice.

Current developments: digitalisation, supply chain legislation and resilience

The risk matrix is evolving from a static Excel tool to a dynamic component of supply chain management. Drivers are regulatory requirements, geopolitical disruption and the increasing digitalisation of procurement.

Regulatory requirements

Legal requirements on corporate due diligence in supply chains require companies in Germany and the EU to carry out a systematic risk analysis across the supply chain, particularly regarding human rights and environmental violations. As a result, child labour risk assessment and the anchoring of audit rights in contracts are gaining practical importance. The risk matrix offers a suitable framework for documenting and reporting on these requirements in a structured manner; however, the specific design should be legally reviewed.

Geopolitical and logistical risk drivers

Trade conflicts, sanctions, raw material dependencies and disruptions to logistics corridors have increased the weight of geopolitical risk in procurement matrices. Issues such as the security of transport routes – for example in connection with documents such as the ATA Carnet – as well as customs changes and export control regulations are increasingly a fixed part of the assessment. Companies are responding with regionalisation, multiple sourcing and adjusted safety stock buffers.

Digital tools and automation

Digital platforms and data providers now enable semi-automated risk assessment: supplier data, ratings, news monitoring and cyber risk screening (for example of supplier cyber risk) can be fed into the matrix continuously. Electronic order processing via cXML and operating an active Approved Vendor List (AVL) with integrated risk alerts also improve timeliness. Nevertheless, human assessment of critical cases remains decisive; tools are no substitute for sound supplier classification and a functioning supplier rating.

Typical metrics

On-time delivery of critical suppliers: > 95%

typical target value; figures below this indicate an elevated supply risk

Number of single sources in critical zones: 0–5 suppliers

typical benchmark for a manageable risk; more single sources require additional safeguards

Replenishment lead time for critical components: < 12 weeks

long-running components require increased safety stock buffers in practice

Proportion of audited suppliers with a critical classification: > 80%

usual benchmark for companies with a well-established audit programme

Update interval of the risk matrix: at least annually, quarterly for critical cases

common practice in industry segments with dynamic supply markets

Practical example

A mid-sized mechanical engineering company with around 400 active suppliers creates a risk matrix to assess its dependence on precision components. The analysis shows: an Asian supplier of a long-running cast part has a long replenishment lead time (over 20 weeks) and is also located in a geopolitically tense region. The risk is classified as 'highly likely / very critical' and assigned to the red

zone. The risk mitigation plan provides for qualifying a European second source and activating it via the Approved Vendor List (AVL), establishing a six-week safety stock buffer, expanding audit rights under the framework agreement and monitoring the supplier's rating monthly. After twelve months, the risk classification drops to yellow, as the second source delivers reliably and on-time delivery has stabilised.

- Qualify a second source and release it on the Approved Vendor List (AVL)
- Define safety stock buffers for critical components and adjust inventory management
- Anchor audit rights in the contract and conduct an annual supplier audit
- Monitor the supplier rating and replenishment lead time monthly and update the matrix quarterly

Conclusion

The risk matrix is a practical tool for making procurement risks transparent and managing them in a targeted manner. Its value arises not from the graphical presentation itself but from a sound data basis, uniform assessment criteria and consistently implemented measures in the risk mitigation plan. Those who link the matrix with the procurement portfolio analysis, the spend cube and an active supplier rating obtain a reliable picture of their own risk position. Regular updates – ideally quarterly for critical suppliers – ensure it remains current. In this way, the risk matrix becomes more than a compliance exercise: it becomes a genuine steering instrument for resilient procurement.

Frequently asked questions

What is a risk matrix in procurement?

A risk matrix is an assessment tool that arranges procurement risks by likelihood of occurrence and impact. In procurement, it is used to prioritise supplier, material and process risks. From it, concrete measures such as second sources, safety stock buffers or contractual safeguards can be derived.

How do I create a risk matrix step by step?

First, all relevant risks are identified, for example supplier failures, geopolitical risk or supplier cyber risk. Next, likelihood and impact are assessed according to uniform definitions and plotted in the matrix. For risks in critical zones, measures are defined in the risk mitigation plan, assigned to owners and reviewed periodically.

Which scales does a risk matrix use?

In practice, 3×3 and 5×5 scales are common, with five levels per dimension frequently used. What matters less than the number of levels is that the levels are defined uniformly across the organisation. The cells are often subsequently divided into green, yellow and red zones.

How often should a risk matrix be updated?

A full update at least annually is common practice; for critical suppliers and geopolitically dynamic markets, quarterly updates are frequent. In addition, an extraordinary update should be carried out in response to major events, such as supplier failures, company acquisitions or new regulatory requirements.

What is the difference between a risk matrix and portfolio analysis in procurement?

The procurement portfolio analysis arranges suppliers by business importance and supplier risk in order to define management models. The risk matrix assesses individual risks in more detail and derives concrete countermeasures. The two tools complement each other and partly draw on the same data

basis, such as the spend cube and the supplier rating.

Which risks belong in a procurement risk matrix?

Typical examples are supplier failures, delivery delays, quality problems, price and currency risks, geopolitical risk, supplier cyber risk and compliance risks such as those addressed in child labour risk assessment. Risks arising from take-or-pay obligations, long replenishment lead times or single-source dependencies should also be captured. The selection depends on the industry and the supply chain structure.