

Risk Register: Systematic Capture and Control of Procurement Risks

A risk register is a structured directory of all identified risks of a company, in which causes, impacts, probabilities and countermeasures are documented. In procurement, it serves as a central instrument for systematically capturing, assessing and monitoring supplier, sourcing and compliance risks. This turns risk management from an individual task into a robust, auditable process – a foundation for any sound procurement strategy.

Key facts

- A risk register documents risks with owners, assessment, measures and status, making them traceable and audit-ready.
- Typical risk categories in procurement are supply risks, price risks, compliance risks and supply chain due diligence obligations.
- Assessments are often carried out as a matrix of probability of occurrence and potential damage, supplemented by a residual risk value.
- In practice, a register with the 20 to 50 most important risks, maintained quarterly, is often sufficient to get started.
- Regulatory requirements such as the CSDDD significantly increase the documentation burden along the supply chain.
- The risk register links usefully with ABC analysis, dual-source management and audit checklists.

Definition: Risk Register

The risk register is the central documentation instrument of risk management: it lists all identified risks with uniform attributes, making them comparable, prioritisable and controllable. In the procurement context, it consolidates findings from supplier evaluations, market analyses and compliance checks in one place.

Structure and standard fields

A practical risk register typically contains at least the following fields: risk ID and description, category, cause and impact, affected suppliers or material groups, probability of occurrence, financial impact, resulting risk value, risk owner, countermeasures, status and review date. It is also useful to include references to contracts, certificates and results of document verification. The more consistent the field structure across sites and departments, the more easily risks can be evaluated in aggregate.

Distinction from adjacent instruments

The risk register is not identical to a supplier evaluation form or an audit checklist, but draws on both. While ABC analysis classifies risks by material value and criticality, the risk register documents the concrete risk cases and their treatment. Results from bow-tie analyses – i.e. cause chains and barriers – also flow into the register as in-depth individual analyses.

Methods and approach for building a risk register

The structure follows the classic risk management cycle: identify, analyse and assess risks, define measures and monitor regularly. It is crucial that the process clearly defines responsibilities and update rhythms so that the register does not become a maintenance void.

Identify risks

Sources for identification include supplier audits, the volume of deviation workflows (deviations in delivery quantities), complaints, media and geopolitical monitoring, as well as systematic analyses such as FMEA or bow-tie analysis. Workshops with development, quality and logistics complement the buyer's perspective, as risks such as missing component approval eligibility often arise outside procurement. Risk-oriented demand planning additionally reveals which material groups are particularly exposed.

Assess and prioritise

In practice, a scale of 1 to 5 for probability and potential damage has proven effective; the product yields a risk value that ranks risks from low to critical. In addition, the recovery time should be assessed: how long does it take to replace a failed supplier? For single-source items, this time is often the real risk driver – this is where consistent dual-source management comes in.

Define measures and risk owners

For every significant risk, a measure is defined – avoid, reduce, transfer or accept – and a named risk owner assigned. Typical measures in procurement include building second sources, safety stocks, contractual safeguards or adjustments to the sourcing strategy, such as shifting to diversified sourcing markets. Important: measures with a deadline, a responsible person and a comprehensible set of acceptance criteria for verifying effectiveness.

Key KPIs for the risk register

KPIs reveal whether risk management is actually working. They should appear regularly in controlling reports and not merely serve as an internal compliance exercise.

Process KPIs

Relevant process KPIs include the proportion of risk reviews completed on time, the proportion of closed measures with overdue deadlines, and the time between risk identification and the start of measures. These KPIs show whether the register is actively maintained or only dug out at audits.

Impact KPIs

Impact KPIs link risk management with delivery and quality performance: the delivery performance of critical suppliers, the number of supply-related production standstills, and the total of avoided or incurred damage costs. The proportion of critical items with a qualified second source is also a good stress test for risk control.

Risks and controls around the risk register itself

The register itself can also become a weak point if it is managed incorrectly. Typical mistakes are excessive level of detail, missing responsibilities and an update rhythm that is out of touch with reality.

Typical practical mistakes

Registers often emerge with hundreds of entries without prioritisation – nobody reads them any more. Equally problematic: risks are recorded only once and never updated, or risk owners are departments rather than individuals. Better is a leanly maintained core list with regular upkeep, plus detailed documentation attached via a data catalogue or document repository.

Controls and internal audit

The risk register should itself be part of internal controls: spot-check plausibility reviews by internal audit, reconciliation with actual disruption events, and verification of whether identified risks were actually monitored. For ISO 9001 certification, evidence of systematic risk thinking is expected; consistent documentation and linkage to the control of nonconforming product – i.e. the management of defective products and processes – support this.

Integration into procurement processes

For risk information to have an effect, it must connect to decision points: at the creation of enquiries, in supplier selection and in budgeting. A known risk should, for example, automatically be taken into account in the award decision – such as contractual delivery guarantees from risk-prone sources. Compliance topics such as data control for supplier data and the verification obligations arising from the CSDDD also belong in the regular register cycle.

Current developments: supply chain laws and digitalisation

Regulation and digitalisation are significantly changing the requirements for the risk register. Supply chain due diligence obligations and documentation requirements in customs and climate matters turn the register into an evidencing instrument towards authorities and customers.

Compliance and documentation obligations

The Corporate Sustainability Due Diligence Directive (CSDDD) and the German Supply Chain Due Diligence Act require risk-based analyses along the entire supply chain – including documented measures and complaints procedures. The risk register is the natural place to evidence these due diligence processes. Customs and climate regulations such as CBAM (carbon border adjustment) also create new risk categories with real cost consequences, which should be proactively assessed in the register.

Digitalisation and early warning systems

In practice, digital GRC and SRM systems are increasingly replacing Excel registers. Advantages include automated updates, alerts when deadlines are exceeded and integration with supplier data. External data sources – commercial registers, shipping data, commodity indices – enable early warnings that identify risks before they materialise. What remains important: system support does not replace the professional assessment by experienced buyers.

The risk register as an argument in procurement

A well-maintained risk register is increasingly also becoming a selling point towards customers and auditors: automotive and mechanical engineering customers are scrutinising the resilience of their supply chains ever more closely. Those who systematically control supplier risks can negotiate delivery zone guarantees and prices with greater credibility.

Typical metrics

Risk reviews completed on time: > 95 %

Proportion of register reviews carried out punctually; typical target value in well-organised processes

Critical items with second source: > 80 %

Proportion of risk-assessed critical materials with a qualified alternative source

Overdue risk measures: < 5 %

Proportion of measures past their deadline; a high value indicates a maintenance problem

Delivery performance of critical suppliers: > 98 %

On-time delivery as an impact KPI of risk management

Practical example

A medium-sized mechanical engineering company with around 250 employees suffered a four-week production standstill after the failure of a single-source supplier for cast components. In response, the company introduced a risk register that initially contained 32 risks from supplier audits, deviation workflows and market analyses. Within one year, second sources were established for the six most critical items, safety stocks defined and contractual substitute delivery guarantees agreed. When another supply failure occurred two years later, the standstill duration was only three days.

- Set up a risk register with a uniform 5x5 assessment matrix and named risk owners
- Identify critical materials via ABC analysis and build second sources for top risks
- Conduct quarterly risk reviews with a fixed audit checklist, linked to supplier evaluation
- Measure the effectiveness of measures via delivery performance and standstill days, and report in the management review

Conclusion

A risk register is not a bureaucratic by-product, but the backbone of functioning procurement risk management. It makes risks visible, assigns responsibilities and creates the documentation basis for audits, customer requirements and regulatory obligations. Decisive for success are uncompromising prioritisation, clearly named risk owners and a realistic maintenance rhythm. Those who consistently integrate the register with ABC analysis, supplier evaluation and sourcing strategy transform it from a mandatory task into a controllable tool. Getting started is possible even without special software – what matters is making the start and maintaining it regularly.

Frequently asked questions

What belongs in a risk register?

At minimum: risk ID, description, category, cause, impact, probability of occurrence, financial impact, risk value, risk owner, countermeasures, status and review date. In procurement, additional fields such as affected suppliers, material groups and contract references are added. A consistent structure is essential so that risks remain comparable and aggregatable.

How do you create a risk register in procurement?

Start with a workshop in which the 20 to 50 most important risks are identified across suppliers, material groups and processes. Assess them on a probability-impact matrix, assign risk owners and define

measures with deadlines. Then establish a fixed review cycle, typically quarterly.

Is a risk register mandatory?

There is no general legal obligation to maintain a risk register as such. However, supply chain laws such as the CSDDD and the German LkSG require risk-based due diligence processes with documentation, which a register usefully maps. Certifications such as ISO 9001 and customer requirements also presuppose demonstrable risk management – the specific design should be legally examined on a case-by-case basis.

How often should the risk register be updated?

In practice, a quarterly formal review cycle has proven effective, supplemented by ad-hoc updates following critical events such as supplier failures, geopolitical developments or insolvency indications. More important than frequency is that reviews actually take place and the status is documented.

Which risks are most common in procurement?

Typically dominated by supply risks (failure, delivery delays, capacity bottlenecks), price and currency risks, quality risks as well as compliance and supply chain due diligence risks. For critical components, dependence on single sources is often the single largest factor – consistent dual-source management helps here.

Excel or software for the risk register?

To get started, a structured Excel spreadsheet with uniform fields and access permissions is often sufficient. Above a certain level of complexity – multiple sites, regulatory documentation requirements, supplier data integration – a digital GRC or SRM system with automated reminders and reporting is worthwhile. In both cases, consistent maintenance is crucial.