

Risk Policy: Systematic Control of Procurement and Supply Chain Risks

The risk policy comprises the company-wide binding principles according to which an industrial company identifies, assesses, limits and monitors procurement and supply chain risks. It forms the strategic framework for operational instruments such as dual sourcing, safety stocks or contractual safeguards. In the procurement context, it ensures that risk decisions are not made ad hoc but according to uniform criteria with clear accountability. In doing so, it links procurement management with overarching corporate and financial planning.

Key facts

- The risk policy defines risk fields, assessment scales, escalation paths and risk-bearing capacity at company level.
- In procurement, it takes effect through risk analyses of the supply base, multi-sourcing, contract strategies and stock or hedging concepts.
- Typical procurement risks are supply failures, price volatility, quality defects, exchange rate and compliance risks.
- An effective risk policy combines preventive measures (prevention) with responsive plans (crisis response).
- Key metrics are supplier risk classes, safety stock cover, single-sourcing shares and replenishment lead times.
- Policy documents are living documents and in practice are frequently updated annually or after significant events.

Definition: Risk Policy

The risk policy is the written framework that defines which risks a company accepts, to what extent it can bear them, and which measures for limiting them are permissible. It is part of the risk management system and is often adopted by the executive board or managing directors. For procurement, it translates the company's risk tolerance into concrete sourcing rules.

Distinction from risk management

The risk policy sets the objectives and principles, while risk management implements them operationally – for example through risk identification, assessment, action planning and monitoring. Simply put: the policy states what is permitted and desired; management states how it is done in day-to-day business. Both levels interlock, because without workable processes every policy remains paper.

Risk policy in the procurement context

In procurement, the risk policy is operationalised through sourcing guidelines, approval thresholds, permissible contract templates and supplier requirement profiles. It determines, for example, from which share of turnover a supplier is considered critical, when second sources of supply should be

established, and which countries or substances are preferred, conditionally permissible or not permissible. This creates a workable decision-making logic for buyers and functional departments.

Risk fields and methods of risk identification

The first step of any risk policy is a structured stocktake of the relevant risk fields. Usual categories are supply risks, price and currency risks, quality and liability risks, legal and compliance risks, and geopolitical risks. Identification usually follows a fixed annual rhythm and is supplemented on an event-driven basis.

Supplier and commodity group analysis

Methodically, the combination of ABC analysis and supplier evaluation has proven effective: products and suppliers are classified according to business importance and probability of failure. In practice, a two-dimensional matrix of influence on production and degree of market scarcity is typical. Articles in the higher risk classes receive additional measures such as emergency suppliers or increased safety stocks, whose effectiveness can be verified through stock analysis and inventory metrics.

Scenario and failure analysis

In addition, many companies examine failure scenarios: what happens if a critical supplier is unavailable for several weeks, a logistics route is blocked, or a commodity price rises sharply? Such stress tests can also include capital-related effects, for example through a DPO-effect simulation or consideration of days inventory outstanding (DIO), in order to assess liquidity and stock risks together.

Compliance and legal risks

Mandatory components include supply chain due diligence obligations, export control and customs matters, for example when using a carnet (ATA) for temporary goods movements. Legal assessments must always be examined on a case-by-case basis and with legal counsel; the risk policy should define clear responsibilities and review loops here without replacing detailed legal advice.

Instruments and approach for risk mitigation

Concrete mitigation measures follow from the assessment. The distinction between risk-avoiding, risk-reducing, risk-transferring and risk-accepting strategies has proven effective. Procurement selects the appropriate set of instruments per risk class and anchors it in sourcing strategies and category playbooks.

Procurement-strategy measures

The most effective levers include risk diversification and dual sourcing for critical components, demand consolidation and bundling levers to strengthen the negotiating position, as well as a targeted increase in safety stocks. In the request for quotation, alternative offers and a streamlined award opening can be designed so that short-term switchable sources of supply are known. For complex packages, consortia or a best and final offer (BAFO) can accelerate the award when time pressure is the main risk.

Contractual and logistical safeguards

Contracts address risks through warranties, penalties, supply commitments, termination rights and alternative supply obligations. Logistically, incoming quality, a moderate buffer stock and transparent advance notifications via the advance shipping notice (ASN) secure the supply; for in-house

warehousing, available-to-promise (ATP) helps ensure that commitments to customers are made only against stock that is actually available. For external warehousing via 3PL providers, the risk policy should provide for defined service levels and rights of recourse. Incoterms such as DDP shift transport and customs risks – with sometimes considerable cost, liability and tax consequences that must be examined on a case-by-case basis.

Processes, approvals and escalation

The policy sets thresholds: from which volume direct awards are excluded, from when multiple quotes must be obtained, and which approvals are required for critical investments – for example for a plant or services order. An escalation path up to the executive level ensures that serious risks do not 'get stuck' at departmental level. Regular audits and duplicate checks in the master data increase the data quality on which every risk analysis is based.

Key KPIs for steering the risk policy

Measurability is a prerequisite for control. The metrics should be properly stored in the data model of the procurement system and evaluated periodically. In practice, risk metrics that simultaneously capture availability, concentration and capital tie-up have proven effective.

Supply and availability metrics

Core metrics are on-time delivery and incoming quality (on-time delivery typically above 95–98%, quality rate clearly above 98% as usual guideline values), replenishment lead time for critical articles and the single-sourcing share of direct materials. A high single-sourcing share is not inherently bad but must be combined with alternative source planning.

Stock and capital metrics

Safety stocks tie up capital: days inventory outstanding (DIO) and the coverage derived from it show how many days of risk buffer are being financed. A DPO-effect simulation helps assess the balance between payment behaviour and supplier loyalty – excessively aggressive payment terms can increase supply risks. Stock analysis per risk class reveals where buffers make sense and where they are ballast.

Risks and controls: limits and weaknesses of the risk policy

Risk policy itself can fail – through abstract formulations, lack of implementation in day-to-day business, or incentives that gloss over risks. Excessive risk aversion can also impair procurement costs and innovative capacity. Controls and governance are therefore part of the policy itself.

Typical implementation weaknesses

Common mistakes: the policy describes risks but does not name responsible parties; risk assessments run once instead of continuously; supplier risk data lives in Excel rather than in the system; warning signals reach decision-makers too late. Clear responsibilities, automated evaluations and a short, binding risk class logic that every buyer can apply provide the remedy.

Controls, audit and reporting

Effective internal controls include the four-eyes principle for critical awards, periodic supplier audits, documentation of risk assessments in award dossiers and management reporting with defined thresholds. Isolated data silos reduce informative value: a clean duplicate check and a consistent data

model for suppliers and materials are fundamental prerequisites for reliable risk reporting.

Current developments: regulation, resilience and digitalisation

The requirements placed on the risk policy are increasing: supply chain legislation, geopolitical fragmentation, commodity volatility and growing digitalisation are changing the rules of the game. Companies are increasingly aligning their procurement with resilience rather than pure cost efficiency.

Regulatory requirements

Supply chain due diligence and sustainability reporting require structured risk screening of the supply base – from raw material origin to working conditions. The risk policy should address these topics explicitly: which risk groups are screened and how, who documents, which escalation paths apply in the event of indications. Legal details are case-dependent and must be clarified with the involvement of legal and compliance officers.

Digitalisation and transparency

Digital supplier mapping, automated risk alerts and platform data improve responsiveness. AI-supported applications assist, for example, with preparing tenders or monitoring supply chain events; however, the benefit depends largely on data quality and process integration. Market overviews and supplier directories help identify alternative sources systematically instead of searching ad hoc under stress.

Typical metrics

On-time delivery: > 95–98%

typical guideline value; shortfalls below this require escalation

Incoming quality: > 98%

common benchmark for qualified suppliers

Single-sourcing share (critical parts): < 10–20%

a high share is only uncritical with qualified alternative sources

Days Inventory Outstanding (DIO): industry-dependent, often 40–90 days

rising DIO can signal a risk buffer or capital ballast

Supplier risk class review cycle: at least annually

critical classes more frequently, e.g. quarterly

Practical example

A mid-sized mechanical engineering company with an annual procurement spend of around EUR 200 million introduces a formal risk policy following a multi-week supply failure by an electronic components supplier. First, the company classifies all direct materials according to probability of failure and production relevance; around a dozen article groups fall into the highest risk class. For these groups, the team defines concrete measures with responsibilities and deadlines.

- Establishing dual sourcing and qualified alternative sources for critical electronics and casting part groups
- Increasing selective safety stocks, governed by stock analysis and days inventory outstanding (DIO) per risk class
- Mandatory risk query and approval for direct awards above a defined threshold value, as well as

integrated duplicate checks of supplier master data

- Quarterly risk reporting to the executive management with defined escalation thresholds for on-time delivery and incoming quality

Conclusion

The risk policy is the corporate compass for dealing with procurement risks – without it, risk management remains a matter of chance. It translates risk tolerance into concrete rules: which suppliers, concepts and contracts are permissible and who decides in a crisis. It becomes effective through measurable KPIs, clean master data and regular updates. Companies that anchor both prevention and crisis response equally gain a genuine competitive advantage over improvising competitors. In the end, risk policy pays off as a combination of avoided failure costs, stable supply and a better negotiating position.

Frequently asked questions

What belongs in a risk policy?

Core components are risk fields and risk classes, assessment scales (probability of occurrence, amount of damage), the company's risk-bearing capacity, responsibilities and escalation paths, as well as permitted risk treatment measures. In procurement, sourcing policies operationalise these principles, for example through thresholds for multi-sourcing or contract templates. Measurable KPIs and a regular review cycle are essential.

Who is responsible for the risk policy within the company?

The risk policy is usually adopted and endorsed by the managing directors or executive board; controlling or a risk management function coordinates its implementation. In the procurement context, the head of procurement or category management is responsible for operational application and supplier monitoring. A clear allocation per risk class and a documented escalation path up to the executive level are essential.

How often should the risk policy be updated?

In practice, an annual formalised review has become established, supplemented by event-driven updates following significant events such as supply failures, acquisitions, market shortages or regulatory changes. In addition, a rolling risk monitoring with quarterly evaluation of the core KPIs is recommended. The fixed cycle and event logic should be defined in the policy itself.

Which risks particularly affect procurement?

Central risks are supply failures and shortages, price and currency volatility, quality defects, compliance and supply chain obligations, as well as dependencies on single or few sources. Added to this are logistics risks and capital tie-up risks from excessively high safety stocks. A structured commodity group and supplier analysis using ABC analysis and a risk matrix prioritises these risks.

How do risk policy and safety stocks relate?

Safety stocks are a classic instrument of risk policy for hedging against supply and demand uncertainty. The policy defines for which risk classes buffer stocks are permissible and economically viable; stock analysis, days inventory outstanding (DIO) and available-to-promise (ATP) govern implementation and monitoring. The aim is a balance between supply security and capital tie-up.

What is the difference between risk policy and risk management?

The risk policy strategically defines which risks are accepted, limited or avoided and according to which criteria decisions are made. Risk management implements these requirements operationally: through risk identification, assessment, action planning and monitoring. The policy is therefore the framework, and management is the process that goes with it – the two interlock and should be aligned in a documented manner.