

Risikoregister: Systematische Erfassung und Steuerung von Beschaffungsrisiken

Ein Risikoregister ist ein strukturiertes Verzeichnis aller identifizierten Risiken eines Unternehmens, in dem Ursachen, Auswirkungen, Wahrscheinlichkeiten und Gegenmaßnahmen dokumentiert werden. Im Einkauf dient es als zentrales Instrument, um Lieferanten-, Beschaffungs- und Compliance-Risiken systematisch zu erfassen, zu bewerten und zu überwachen. Damit wird Risikomanagement von einer Einzelaufgabe zu einem belastbaren, prüfbaren Prozess – eine Grundlage für jede fundierte Beschaffungsstrategie.

Das Wichtigste in Kürze

- Ein Risikoregister dokumentiert Risiken mit Verantwortlichen, Bewertung, Maßnahmen und Status nachverfolgbar und auditfähig.
- Typische Risikokategorien im Einkauf sind Lieferrisiken, Preisrisiken, Compliance-Risiken und Lieferkettensorgfaltspflichten.
- Bewertungen erfolgen häufig als Matrix aus Eintrittswahrscheinlichkeit und Schadensausmaß, ergänzt um einen Residual-Risikowert.
- In der Praxis genügt für den Einstieg oft ein Register mit den 20 bis 50 wichtigsten Risiken, das quartalsweise gepflegt wird.
- Regulatorische Anforderungen wie die CSDDD erhöhen den Dokumentationsdruck entlang der Lieferkette deutlich.
- Das Risikoregister verknüpft sich sinnvoll mit ABC-Analyse, Dual-Source-Management und Auditcheckliste.

Definition: Risikoregister

Das Risikoregister ist das zentrale Dokumentationsinstrument des Risikomanagements: Es listet alle identifizierten Risiken mit einheitlichen Attributen auf und macht sie damit vergleichbar, priorisierbar und steuerbar. Im beschaffungsbezogenen Kontext bündelt es Erkenntnisse aus Lieferantenbewertungen, Marktanalysen und Compliance-Prüfungen an einem Ort.

Aufbau und Standardfelder

Ein praxistaugliches Risikoregister enthält typischerweise mindestens folgende Felder: Risiko-ID und Bezeichnung, Kategorie, Ursache und Auswirkung, betroffene Lieferanten oder Materialgruppen, Eintrittswahrscheinlichkeit, Schadenshöhe, resultierender Risikowert, Risikoeigner, Gegenmaßnahmen, Status und Review-Termin. Ergänzend sinnvoll sind Verweise auf Verträge, Zertifikate und Ergebnisse der Dokumentenprüfung. Je konsistenter die Feldstruktur über Standorte und Abteilungen hinweg, desto eher lassen sich Risiken aggregiert auswerten.

Abgrenzung zu benachbarten Instrumenten

Das Risikoregister ist nicht identisch mit einem Lieferantenbewertungsbogen oder einer Auditcheckliste,

speist sich aber aus beiden. Während die ABC-Analyse Risiken nach Materialwert und Kritikalität klassifiziert, dokumentiert das Risikoregister die konkreten Risikofälle und deren Behandlung. Auch Ergebnisse aus Bow-Tie-Analysen – also Ursachenketten und Barriers – fließen als vertiefte Einzelanalysen in das Register ein.

Methoden und Vorgehen beim Aufbau eines Risikoregisters

Der Aufbau folgt dem klassischen Risikomanagementzyklus: Risiken identifizieren, analysieren, bewerten, Maßnahmen festlegen und regelmäßig überwachen. Entscheidend ist, dass der Prozess klar Verantwortlichkeiten und Update-Rhythmen definiert, damit das Register nicht zur Pflegeleerstelle wird.

Risiken identifizieren

Quellen für die Identifikation sind Lieferantenaudits, Abweichungsworkflow-Menge (Abweichungen bei Liefermengen), Reklamationen, mediale und geopolitische Beobachtungen sowie systematische Analysen wie FMEA oder Bow-Tie-Analyse. Workshops mit Entwicklung, Qualität und Logistik ergänzen den Einkäuferblick, da Risiken wie fehlende Zulassungsfähigkeit von Bauteilen oft außerhalb des Einkaufs entstehen. Eine risikoorientierte Bedarfsplanung zeigt zusätzlich, welche Materialgruppen besonders exponiert sind.

Bewerten und priorisieren

In der Praxis hat sich eine Skalierung von 1 bis 5 für Wahrscheinlichkeit und Schadensausmaß bewährt; das Produkt ergibt einen Risikowert, der Risiken in Stufen von niedrig bis kritisch sortiert. Ergänzend sollte die Wiederherstellungszeit bewertet werden: Wie lange dauert es, einen ausgefallenen Lieferanten zu ersetzen? Bei Single-Source-Positionen ist diese Zeit oft der eigentliche Risikotreiber – hier setzt konsequentes Dual-Source-Management an.

Maßnahmen und Risikoeigner festlegen

Für jedes signifikante Risiko wird eine Maßnahme definiert – vermeiden, reduzieren, übertragen oder akzeptieren – und ein namentlicher Risikoeigner benannt. Typische Maßnahmen im Einkauf sind Zweitquellen-Aufbau, Sicherheitsbestände, vertragliche Absicherungen oder Beschaffungsstrategie-Anpassungen wie Verlagerung in diversifizierte Beschaffungsmärkte. Wichtig: Maßnahmen mit Termin, Verantwortlichem und nachvollziehbarem Abnahmekriterien-Katalog zur Prüfung der Wirksamkeit.

Wichtige KPIs für das Risikoregister

Kennzahlen machen sichtbar, ob das Risikomanagement tatsächlich wirkt. Sie sollten im Controlling-Reporting regelmäßig erscheinen und nicht nur als interne Pflichtübung dienen.

Prozess-KPIs

Relevante Prozesskennzahlen sind der Anteil fristgerecht durchgeführter Risikoreviews, der Anteil geschlossener Maßnahmen überfälliger Termine und die Zeit zwischen Risikoerkennung und Maßnahmebeginn. Diese Kennzahlen zeigen, ob das Register lebendig gepflegt wird oder nur bei Audits herausgekratzt wird.

Wirkungs-KPIs

Wirkungskennzahlen verbinden Risikomanagement mit Liefer- und Qualitätsperformance: Die Delivery

Performance kritischer Lieferanten, die Anzahl supply-bedingter Produktionsstillstände sowie die Summe vermiedener oder eingetretener Schadenskosten. Auch der Anteil kritischer Positionen mit qualifizierter Zweitquelle ist ein guter Belastungstest für die Risikosteuerung.

Risiken und Kontrollen rund um das Risikoregister selbst

Auch das Register selbst kann zur Schwachstelle werden, wenn es falsch geführt wird. Typische Fehler sind überhöhte Detailtiefe, fehlende Verantwortlichkeiten und ein Update-Rhythmus, der an der Realität vorbeiläuft.

Typische Praxisfehler

Häufig entstehen Register mit Hunderten Einträgen ohne Priorisierung – niemand liest sie mehr. Ebenso problematisch: Risiken werden nur einmal erfasst und nie aktualisiert, oder Risikoeigner sind Abteilungen statt Personen. Besser ist eine schlank geführte Kernliste mit regelmäßiger Pflege und eine per Datenkatalog oder Dokumentenablage angebundene Detaildokumentation.

Kontrollen und interne Revision

Das Risikoregister sollte selbst Bestandteil interner Kontrollen sein: Stichprobenhafte Plausibilisierung durch die Revision, Abgleich mit realen Störereignissen und Prüfung, ob identifizierte Risiken tatsächlich überwacht wurden. Bei Zertifizierungen nach ISO 9001 wird der Nachweis systematischen Risikodenkens erwartet; hier unterstützt eine konsistente Dokumentation und die Kopplung an das Control of Nonconforming Product, also die Beherrschung fehlerhafter Produkte und Prozesse.

Integration in Einkaufsprozesse

Damit Risikoinformationen wirken, müssen sie an Entscheidungsstellen anknüpfen: bei der Anfrageerstellung, der Lieferantenauswahl und der Budgetierung. Ein bekanntes Risiko sollte z. B. automatisch bei der Vergabe berücksichtigt werden – etwa vertragliche Lieferzusagen bei risikobehafteten Quellen. Auch Compliance-Themen wie die Datenkontrolle bei Lieferantendaten und die Prüfpflichten aus der CSDDD gehören in den regelmäßigen Register-Zyklus.

Aktuelle Entwicklungen: Lieferkettengesetze und Digitalisierung

Regulatorik und Digitalisierung verändern die Anforderungen an das Risikoregister deutlich. Lieferkettensorgfaltspflichten und Nachweispflichten im Zoll- und Klimabereich machen das Register zum Nachweisinstrument gegenüber Behörden und Kunden.

Compliance- und Nachweispflichten

Die Corporate Sustainability Due Diligence (CSDDD) und das deutsche Lieferkettensorgfaltspflichtengesetz verlangen risikobasierte Analysen entlang der gesamten Lieferkette – inklusive dokumentierter Maßnahmen und Beschwerdeverfahren. Das Risikoregister ist der natürliche Ort, um diese Sorgfallsprozesse nachzuweisen. Auch Zoll- und Klimaregulierungen wie CBAM (CO-Grenzausgleich) erzeugen neue Risikokategorien mit realen Kostenfolgen, die proaktiv im Register bewertet werden sollten.

Digitalisierung und Frühwarnsysteme

In der Praxis ersetzen zunehmend digitale GRC- und SRM-Systeme Excel-Register. Vorteile sind automatisierte Aktualisierungen, Warnungen bei Statusüberschreitungen und die Verknüpfung mit

Lieferantendaten. Externe Datenquellen – Handelsregister, Schifffahrtsdaten, Rohstoffindizes – ermöglichen Frühwarnungen, die Risiken erkennen, bevor sie eintreten. Wichtig bleibt: Die Systemunterstützung ersetzt nicht die fachliche Bewertung durch erfahrene Einkäufer.

Risikoregister als Argument im Einkauf

Ein gepflegtes Risikoregister wird zunehmend auch gegenüber Kunden und Auditoren zum Verkaufsargument: Automobil- und Maschinenbaukunden prüfen die Resilienz ihrer Lieferkette immer kritischer. Wer Lieferantenrisiken systematisch beherrscht, kann bei Lieferzonenzusagen und Preisverhandlungen glaubwürdiger auftreten.

Typische Kennzahlen

Fristgerechte Risikoreviews: > 95 %

Anteil pünktlich durchgeführter Register-Reviews; typischer Zielwert in geordneten Prozessen

Kritische Positionen mit Zweitquelle: > 80 %

Anteil risikobewerteter kritischer Materialien mit qualifizierter Alternativquelle

Überfällige Risikomaßnahmen: < 5 %

Anteil Maßnahmen über Termin; hoher Wert deutet auf Pflegeproblem hin

Delivery Performance kritischer Lieferanten: > 98 %

Liefertreue als Wirkungskennzahl des Risikomanagements

Praxisbeispiel

Ein mittelständischer Maschinenbauer mit rund 250 Mitarbeitern erlitt nach dem Ausfall eines Single-Source-Lieferanten für Gusskomponenten einen vierwöchigen Produktionsstillstand. Im Nachgang führte das Unternehmen ein Risikoregister ein, das zunächst 32 Risiken aus Lieferantenaudits, Abweichungsworkflows und Marktanalysen enthielt. Innerhalb eines Jahres wurden für die sechs kritischsten Positionen Zweitquellen aufgebaut, Sicherheitsbestände definiert und vertragliche Ersatzlieferzusagen vereinbart. Bei einem erneuten Lieferausfall zwei Jahre später betrug die Stillstandsdauer nur noch drei Tage.

- Risikoregister mit einheitlicher 5x5-Bewertungsmatrix und namentlichen Risikoeignern einrichten
- Kritische Materialien per ABC-Analyse identifizieren und für Top-Risiken Zweitquellen aufbauen
- Quartalsweise Risikoreviews mit fester Auditcheckliste und Kopplung an Lieferantenbewertung durchführen
- Maßnahmenwirksamkeit über Delivery Performance und Stillstandstage messen und im Management-Review berichten

Fazit

Ein Risikoregister ist kein bürokratisches Nebenprodukt, sondern das Rückgrat eines funktionierenden Beschaffungsrisikomanagements. Es macht Risiken sichtbar, ordnet Verantwortlichkeiten zu und schafft die Dokumentationsgrundlage für Audits, Kundenanforderungen und regulatorische Pflichten. Entscheidend für den Erfolg sind Kompromisslosigkeit bei der Priorisierung, klar benannte Risikoeigner und ein realistischer Pflege-Rhythmus. Wer das Register konsequent mit ABC-Analyse, Lieferantenbewertung und Beschaffungsstrategie verzahnt, verwandelt es von der Pflichtaufgabe in ein steuerungsfähiges Werkzeug. Der Einstieg gelingt auch ohne Spezialsoftware – entscheidend ist der

Anfang und die regelmäßige Pflege.

Häufige Fragen

Was gehört in ein Risikoregister?

Mindestens Risiko-ID, Bezeichnung, Kategorie, Ursache, Auswirkung, Eintrittswahrscheinlichkeit, Schadenshöhe, Risikowert, Risikoeigner, Gegenmaßnahmen, Status und Review-Termin. Im Einkauf kommen Felder wie betroffene Lieferanten, Materialgruppen und Vertragsreferenzen hinzu. Wichtig ist eine einheitliche Struktur, damit Risiken vergleichbar und aggregierbar bleiben.

Wie erstellt man ein Risikoregister im Einkauf?

Starten Sie mit einem Workshop, in dem die wichtigsten 20 bis 50 Risiken entlang von Lieferanten, Materialgruppen und Prozessen identifiziert werden. Bewerten Sie diese auf einer Wahrscheinlichkeits-Schadens-Matrix, benennen Sie Risikoeigner und definieren Sie Maßnahmen mit Termin. Etablieren Sie anschließend einen festen Review-Zyklus, typischerweise quartalsweise.

Ist ein Risikoregister Pflicht?

Eine generelle gesetzliche Pflicht zu einem Risikoregister als solchem existiert nicht. Jedoch verlangen Lieferkettengesetze wie die CSDDD und das LkSG risikobasierte Sorgfaltsprozesse mit Dokumentation, die ein Register sinnvoll abbildet. Auch Zertifizierungen wie ISO 9001 und Kundenanforderungen setzen nachweisbares Risikomanagement voraus – die konkrete Ausgestaltung sollte rechtlich im Einzelfall geprüft werden.

Wie oft sollte das Risikoregister aktualisiert werden?

In der Praxis hat sich ein quartalsweiser formaler Review-Zyklus bewährt, ergänzt durch ad-hoc-Updates bei kritischen Ereignissen wie Lieferantenausfällen, geopolitischen Entwicklungen oder Insolvenzhinweisen. Wichtiger als die Frequenz ist, dass Reviews tatsächlich stattfinden und der Status dokumentiert wird.

Welche Risiken sind im Einkauf am häufigsten?

Typischerweise dominieren Lieferrisiken (Ausfall, Lieferverzug, Kapazitätsengpässe), Preis- und Währungsrisiken, Qualitätsrisiken sowie Compliance- und Sorgfaltspflichtrisiken in der Lieferkette. Bei kritischen Komponenten ist die Abhängigkeit von Single Sources häufig der größte Einzelfaktor – hier hilft konsequentes Dual-Source-Management.

Excel oder Software für das Risikoregister?

Für den Einstieg genügt häufig eine strukturierte Excel-Tabelle mit einheitlichen Feldern und Berechtigungen. Ab einer bestimmten Komplexität – mehrere Standorte, regulatorische Nachweispflichten, Lieferantendaten-Anbindung – lohnt sich ein digitales GRC- oder SRM-System mit automatisierten Erinnerungen und Auswertungen. Entscheidend ist in beiden Fällen die konsequente Pflege.