

Lieferantenbankdatenprüfung: Schutz vor Zahlungsmissbrauch im Einkauf

Die Lieferantenbankdatenprüfung ist ein Kontrollprozess, bei dem Einkaufs- und Finanzabteilung die Bankverbindungen von Lieferanten vor Zahlungen verifizieren. Ziel ist es, falsche oder manipulierte Bankdaten zu erkennen, bevor Zahlungen ausgelöst werden. Sie ist ein zentraler Baustein gegen Zahlungsstrombetrug, Identitätsdiebstahl und Rechnungsmanipulation und gehört zu den Pflichtdisziplinen eines professionellen Lieferantenstammdatenmanagements.

Stand Oktober 2026 · amplifa-marketplace.ai/lexikon/lieferantenbankdatenpruefung

Das Wichtigste in Kürze

- 01 Die Lieferantenbankdatenprüfung verifiziert Bankverbindungen von Lieferanten, bevor Zahlungen freigegeben werden.
- 02 Typische Prüfschritte sind das Abgleich der IBAN mit Lieferantenstammdaten, Rückruf bei bekannter Kontaktperson und plausibilisierte Vier-Augen-Freigabe.
- 03 Häufige Angriffsmuster sind Fake-Rechnungen, geänderte IBAN auf echten Rechnungen und Social-Engineering-Mails mit dringender Zahlungsänderung.
- 04 In der Praxis bewährt sich ein dokumentierter Freigabeprozess mit hinterlegtem Prüfnachweis je Bankänderung.
- 05 Bankdaten sollten typischerweise bei Neuanlage, bei jeder Änderung und periodisch – etwa jährlich – revalidiert werden.
- 06 Die Prüfung schützt nicht nur vor Betrug, sondern auch vor Fehlbuchungen, Rücklastschriften und verzögerten Zahlungen an echte Lieferanten.

Definition: Lieferantenbankdatenprüfung

Die Lieferantenbankdatenprüfung umfasst alle Maßnahmen zur Verifikation der Bankverbindung eines Lieferanten, bevor Zahlungen auf diese Verbindung erfolgen. Sie ist Teil des

Lieferantenstammdatenmanagements und der internen Kontrollsysteme gegen wirtschaftskriminelle Angriffe.

Abgrenzung zur Bonitätsprüfung

Die Bankdatenprüfung stellt fest, ob die hinterlegte Bankverbindung tatsächlich dem Lieferanten gehört. Die Bonitätsprüfung dagegen bewertet die Zahlungsfähigkeit und Kreditwürdigkeit eines Lieferanten, etwa über Wirtschaftsinformationen, Ratings oder Zahlungsquoten. Beide Prozesse ergänzen sich: Während die Bonitätsprüfung das Ausfallrisiko adressiert, schützt die Bankdatenprüfung vor Zahlungen an Dritte. Beide gehören in den Onboarding-Prozess und sollten mit einer periodischen Revalidierung kombiniert werden.

Rechtliche und organisatorische Einordnung

Bankdaten sind personenbezogene Daten, sobald sie auf eine natürliche Person – etwa einen Inhaber oder Geschäftsführer – bezogen sind. Der Umgang unterliegt daher den Grundsätzen der DSGVO wie Datenminimierung und Zweckbindung. Aus Compliance-Sicht ist die Bankdatenprüfung Bestandteil des angemessenen internen Kontrollsystems; Wirtschaftsprüfer und Haftungsorgane erwarten nachvollziehbare Prozesse. Die konkrete Ausgestaltung sollte rechtlich im Einzelfall – etwa mit Datenschutzbeauftragten und Wirtschaftsprüfern – abgestimmt werden.

| Methoden und Vorgehen bei der Bankdatenprüfung

Bewährte Prozesse kombinieren mehrere Prüfebene, da keine einzelne Methode allein belastbar ist. Je sensibler der Zahlungsprozess, desto stärker sollte die Prüftiefe sein.

Dokumenten- und Datenprüfung

Im ersten Schritt werden die übermittelten Bankdaten auf formale und logische Konsistenz geprüft: Stimmt die IBAN-Prüfziffer? Passt die Bankleitzahl zum Land und zur IBAN-Struktur? Stimmen Empfängername und Rechtsform mit den Stammdaten und der Rechnung überein? Auffälligkeiten sind diskrepante Firmensitzländer, private Kontomuster oder ausländische Konten bei lokal ansässigen Lieferanten. Auch die Datenqualität der Stammdaten insgesamt – von Anschriften bis Steuernummern – ist hier relevant; Schwächen fließen in den Datenqualitätsbericht des Stammdatenmanagements ein.

Rückruf und unabhängiger Kommunikationskanal

Der stärkste Prüfschritt ist die Rückfrage beim Lieferanten über einen bereits bekannten, unabhängigen Kanal – etwa die hinterlegte Festnetznummer einer langjährigen Ansprechperson, nicht die Telefonnummer oder E-Mail-Adresse aus der Änderungsanfrage selbst. Bei der Rückfrage sollten Details abgeklärt werden, die nur der echte Lieferant kennt. Im Umgang mit unbekannten Lieferanten empfiehlt sich zusätzlich ein Identitätsnachweis, etwa ein amtlicher Registerauszug oder eine Bestätigung der Hausbank.

Testzahlung und Freigabeprozess

Vor der ersten Zahlung auf eine neue Bankverbindung hat sich in der Praxis eine Kleinbetrags-Testzahlung bewährt, deren Eingang der Lieferant bestätigen muss. Alternativ bestätigen beide Parteien die Kontodaten schriftlich gegenseitig. Die anschließende Freigabe erfolgt nach dem Vier-Augen-Prinzip: Eine Rolle erfasst, eine zweite – idealerweise aus der Finanzabteilung – prüft und gibt frei. Jede Bankänderung wird mit Prüfnachweis, Prüfdatum und Prüfenden im Stammsatz dokumentiert.

Wichtige KPIs der Lieferantenbankdatenprüfung

Der Prüfabschnitt lässt sich mit wenigen Kennzahlen steuern. Diese eignen sich auch für den Datenqualitätsbericht und das interne Kontrollreporting.

Verifizierungsquote und Prüfquote

Die Verifizierungsquote gibt an, wie viele aktive Lieferanten eine geprüfte und dokumentierte Bankverbindung haben. In reif organisierten Unternehmen liegt dieser Wert typischerweise nahe 100 Prozent für zahlungsaktive Lieferanten; Bestandsaltlasten sind häufig erst nach schrittweiser Revalidierung abgedeckt. Die Prüfquote ergänzt dies: Wie viel Prozent der Bankänderungen durchliefen den vollständigen Prüfablauf?

Durchlaufzeit und Aufdeckungsquote

Die Durchlaufzeit misst, wie lange eine Änderungsanfrage bis zur Freigabe dauert. Kurze Wege sind wichtig, um Lieferanten nicht zu frustrieren – aber nicht auf Kosten der Vier-Augen-Kontrolle. Die Aufdeckungsquote zählt abgelehnte oder verdächtige Anfragen; sie zeigt, ob der Prozess Betrugsversuche tatsächlich filtert. Eine dauerhaft „leere“ Aufdeckungsquote kann auch bedeuten, dass Angriffe unentdeckt durchrutschen.

Kosten der Prüfung versus Schadensvermeidung

Der Aufwand pro Prüfung liegt in der Praxis häufig im niedrigen zweistelligen Eurobereich, wenn Standardroutine und Rückrukskripte genutzt werden. Dem stehen typische Schäden bei Zahlungsstrombetrug gegenüber, die oft im fünf- bis sechsstelligen Bereich pro Fall liegen und rechtlich nicht immer vollständig rückholbar sind. Diese Relation begründet die Prüfung ökonomisch – auch für Lieferanten mit kleinem Volumen, da Betrüger gerade kleine, unauffällige Lieferanten testen.

Risiken, Betrugsmuster und Kontrollen

Die wichtigsten Angriffe auf Zahlungsprozesse nutzen genau die Schnittstelle, die die Bankdatenprüfung absichert. Einkäufer und Finanzteams sollten die Muster kennen.

Typische Betrugsmuster

Beim CEO-Fraud geben sich Täter als Geschäftsführung aus und fordern dringende Zahlungen oder

Kontoänderungen. Beim Fake-Supplier wird ein komplett erfundener Lieferant mit plausiblen Dokumenten angelegt. Beim Invoice-Swapping wird auf einer echten, kopierten Rechnung nur die IBAN geändert – oft kurz vor dem Zahlungsziel, um Zeitdruck zu erzeugen. Social-Engineering per E-Mail von kompromittierten Lieferantenpostfächern ist ebenfalls verbreitet. Besonders gefährdet sind Projekte mit engen Just-in-Time-Beziehungen und hoher Zahlungsfrequenz, da dort kurze Reaktionszeiten erwartet werden.

Organisatorische Kontrollen

Zentrale Kontrollen sind: Trennung von Stammdatenpflege und Zahlungsfreigabe, Vier-Augen-Prinzip bei jeder Bankänderung, keine Änderungen per E-Mail-Weisung allein, Systemberechtigungen nach dem Minimalprinzip sowie Schutz der Lieferantenportale mit Zwei-Faktor-Authentifizierung. Zusätzlich sollten Regelabfragen im ERP prüfen, ob eine neue IBAN bereits bei anderen Lieferanten, Mitarbeitern oder in Betrugsdatenbanken auftaucht. Duplicate Checks und Regeln für Länder- und Währungsmuster ergänzen das Netz.

Kollaborative Vorbeugung mit dem Lieferanten

Prävention gelingt am besten gemeinsam mit dem Lieferanten: Vereinbaren Sie im Vertragsmanagement verbindliche Änderungsprozesse, benannte Kontakte und dokumentierte Kanäle für Bankänderungen. Sensibilisieren Sie die Lieferanten für gefälschte E-Mails „im Namen Ihres Einkäufers“ und legen Sie fest, dass Zahlungsänderungen niemals über normale E-Mail-Threads beauftragt werden. Auch interne Sensibilisierung von Einkauf, Buchhaltung und Controlling gehört dazu – Betrüger wählen gezielt die schwächste Stelle der Kommunikation.

Ablauf im Prozess: vom Onboarding bis zum Payment Run

Die Bankdatenprüfung ist kein isolierter Schritt, sondern ein Segment im Zahlungsprozess vom Lieferantensetup bis zum Payment Run. Wer die Schnittstellen sauber definiert, vermeidet Reibungsverluste.

Onboarding und Stammdatenanlage

Im Onboarding werden Bankdaten zusammen mit Handelsregistrauszug, Steuerdaten und ggf. Zertifikaten erfasst. Die Prüfung sollte in den Standardworkflow der Disposition und Stammdatenpflege eingebunden sein, ähnlich wie die Dispositionparameterpflege definierte Felder und Regeln für den operativen Betrieb setzt. Erst nach abgeschlossener Verifizierung wird der Lieferant für Bestellungen und Zahlungen freigeschaltet. Änderungsanfragen durchlaufen denselben Kanal mit demselben Prüfniveau.

Vor dem Payment Run

Unmittelbar vor dem Payment Run greift eine finale Kontrolle: Bei Änderungen jünger als ein definierter Schwellwert – in der Praxis häufig 30 bis 90 Tage – wird die Zahlung gesperrt oder einer Sonderfreigabe unterworfen. Neue IBAN auf Rechnungen mit hohem Betrag oder kurzem Zahlungsziel

führen zu einer manuellen Rückfrage. Diese Kombination aus Laufzeitkontrolle und Betrags-/Frist-Heuristik fängt die meisten verspätet einlaufenden Manipulationsversuche ab, ohne den Normalbetrieb zu bremsen.

Periodische Revalidierung

Auch unveränderte Bankdaten altern: Konten werden geschlossen, Lieferanten wechseln die Hausbank. Eine periodische Revalidierung – in der Praxis häufig jährlich bzw. zweijährig, lieferantenspezifisch gestaffelt nach Volumen – hält die Stammdaten aktuell. Die Revalidierung lässt sich gut in das routinemäßige Lieferantenreview einbetten, zusammen mit Zertifikatsstatus, Bonitätsprüfung und Konditionsupdate. Wer ohnehin gerade die Skontobedingungen oder Zahlungstage verhandelt, kann die Kontobestätigung mitabfragen und Prozesskosten sparen.

| Aktuelle Entwicklungen und digitale Hilfsmittel

Zahlungsstrombetrug professionalisiert sich, aber auch die Prüfungstechnik entwickelt sich weiter. Einkaufs- und Finanzteams sollten den Stand der Technik kennen, ohne sich von einzelnen Tools abhängig zu machen.

Automatisierte IBAN-Validierung und Datenabgleich

Moderne Systeme prüfen IBAN-Struktur, Prüfziffer, Bankleitzahl-Zuordnung und Registry-Daten automatisiert, sobald Daten erfasst werden. Ergänzend können Datenabgleiche mit Registern, Betrugsdatenbanken und internen Blacklists laufen. Solche Automatisierung reduziert die Routinefehlerquote und entlastet Prüfer, ersetzt aber nicht den Rückruf: Die menschliche Bestätigung über einen unabhängigen Kanal bleibt der Kern der Prüfung. Auch KI-gestützte Anomalieerkennung auf Zahlungsströmen findet zunehmend Verbreitung, sollte aber als Zusatzsignal und nicht als alleinige Entscheidungsbasis verstanden werden.

Standardisierte Lieferantenportale

Immer mehr Unternehmen lassen Bankänderungen nur noch über ein authentifiziertes Lieferantenportal mit Zwei-Faktor-Authentifizierung zu. Das reduziert E-Mail-basierte Angriffe erheblich und erzeugt automatisch einen revisionssicheren Prüfpfad. Für Lieferanten ohne Portalzugang bleibt ein formularbasierter Prozess mit Originaleinsatz und Rückruf. Standardisierung hilft zudem beim Onboarding neuer Lieferanten, etwa im Rahmen eines Category Playbooks oder einer Supplier Shortlist, wo Prozessorientierung von vornherein mitgedacht werden sollte.

Was bleibt manuell und kritisch

Trotz Automatisierung bleiben zwei Punkte manuell: die Prüfung der wirtschaftlichen Berechtigung hinter einer Kontoänderung und die Mensch-zu-Mensch-Rückfrage. Und kritisch bleibt die Schnittstelle zum Verhandlungsmanagement: Änderungen von Kontodaten, Rechnungsanschriften oder Zahlungswegen sollten nie im Rahmen laufender Preis- oder Verhandlungsprozesse „nebenbei“ übermittelt werden. Solche Situationen nutzen Betrüger gezielt aus, weil dort die Wachsamkeit sinkt

und viele Parteien gleichzeitig im Austausch sind.

Typische Kennzahlen

Kennzahl	Typischer Wert
Verifizierungsquote aktiver Lieferanten	typischerweise > 98 % <i>Anteil zahlungsaktiver Lieferanten mit dokumentiert geprüfter Bankverbindung</i>
Prüfquote bei Bankänderungen	100 % <i>Jede Änderung muss den vollständigen Prüfablauf durchlaufen; Ausnahmen sind dokumentiert</i>
Durchlaufzeit Bankänderung	typischerweise < 5 Werktage <i>Zeit von Anfrageeingang bis Freigabe inkl. Rückruf</i>
Aufdeckungsquote	dokumentiert > 0 <i>Anzahl abgelehnter/verdächtiger Anfragen pro Jahr; dauerhaft null kann auf unentdeckte Fälle hinweisen</i>

Praxisbeispiel

Ein mittelständischer Maschinenbauer mit rund 1.200 aktiven Lieferanten erhielt kurz vor Weihnachten eine E-Mail eines langjährigen Blechzulieferers: Neue Bankverbindung, Zahlungsziel laufe in drei Tagen. Der sachbearbeitende Einkäufer folgte der Anfrage fast – der Rückruf über die hinterlegte Festnetznummer ergab jedoch, dass der Lieferant keine Kontoänderung vorgenommen hatte. Der Vorfall führte zu einem überarbeiteten Prozess.

- Bankänderungen nur noch über Lieferantenportal oder schriftliches Originalformular mit Rückruf bei bekannter Kontaktperson
- Systematische Sperrlogik: Zahlungen auf IBANs mit Änderungsalter unter 30 Tagen erfordern zweite Freigabe aus der Finanzabteilung
- Jahresrevalidierung aller zahlungsaktiven Lieferanten, eingebettet in das bestehende Lieferantenreview
- Sensibilisierungsschulungen für Einkauf und Buchhaltung mit Angriffsfallbeispielen, zweimal jährlich

Fazit

Die Lieferantenbankdatenprüfung ist ein vergleichsweise kostengünstiger Kontrollmechanismus mit hoher Schadensvermeidungswirkung. Wirksam wird sie nur als Kombination aus formaler Prüfung, unabhängiger Rückfrage, Vier-Augen-Freigabe und dokumentiertem Nachweis. Wer Änderungskanäle im Vertragsmanagement verbindlich regelt und die Prüfung ins Onboarding sowie in den Payment Run

integriert, entfernt die häufigsten Angriffsflächen. Periodische Revalidierung und wenige klare KPIs halten den Prozess über die Zeit stabil. Für Einkäufer und Supply-Chain-Verantwortliche gehört sie damit zur Grundhygiene des Lieferantenmanagements – nicht zur Kür.

Häufige Fragen

? Wie prüfe ich die Bankdaten eines Lieferanten?

Prüfen Sie zunächst die IBAN auf formale Korrektheit und Übereinstimmung mit den Stammdaten. Verifizieren Sie die Änderung anschließend per Rückruf über einen unabhängig hinterlegten Kontaktweg und fordern Sie bei Bedarf einen Registerauszug oder eine Hausbankbestätigung. Erst nach dokumentierter Freigabe im Vier-Augen-Prinzip sollte die Zahlung erfolgen.

? Woran erkenne ich eine gefälschte Lieferantenrechnung mit geänderter IBAN?

Warnsignale sind kurzfristige Änderungen unmittelbar vor dem Zahlungsziel, neue IBANs mit anderem Ländermuster, abweichende Ansprechpartner und Zeitdruck in der Anfrage. Vergleichen Sie die IBAN immer mit den Stammdaten, nicht nur mit früheren Rechnungen – gefälschte Rechnungen kopieren häufig echte. Im Zweifel gilt: Rückruf statt Zahlung.

? Wer ist für die Lieferantenbankdatenprüfung verantwortlich – Einkauf oder Buchhaltung?

In der Praxis liegt die Stammdatenpflege häufig beim Einkauf oder Shared Service Center, die Zahlungsfreigabe bei der Finanzabteilung. Entscheidend ist die Trennung der Rollen: Wer Bankdaten erfasst, darf sie nicht allein freigeben. Festgelegt werden die Verantwortlichkeiten idealerweise schriftlich im Prozessdokument mit definierten Schwellwerten und Eskalationswegen.

? Wie oft sollten Lieferantenbankdaten revalidiert werden?

Üblich ist eine periodische Revalidierung aller zahlungsaktiven Lieferanten im Abstand von ein bis zwei Jahren, gestaffelt nach Zahlungsvolumen und Risikoprofil. Bei sensiblen Lieferanten oder nach Vorfällen kann ein kürzerer Intervall sinnvoll sein. Wichtig ist, dass die Revalidierung dieselbe Prüftiefe wie das Erst-Onboarding nutzt.

? Was kostet eine Lieferantenbankdatenprüfung?

Der Aufwand liegt bei standardisierten Prozessen typischerweise im niedrigen zweistelligen Eurobereich pro Prüfung, ohne automatisierte Tools gegebenenfalls etwas höher. Dem stehen Schäden durch Zahlungsstrombetrug gegenüber, die häufig im fünf- bis sechsstelligen Bereich pro Fall liegen und nicht immer rückholbar sind. Ökonomisch lohnt sich die Prüfung damit praktisch immer.

? Darf ich bei der Bankdatenprüfung einen Auszug aus dem Handelsregister oder Bankbestätigungen verlangen?

Ja, solche Nachweise sind gängige Mittel der Identitätsprüfung und werden von seriösen Lieferanten üblicherweise akzeptiert. Beachten Sie jedoch Datenschutzgrundsätze: Erheben Sie nur

die Daten, die für den Zahlungszweck erforderlich sind. Für die konkrete Ausgestaltung und etwaige branchenspezifische Vorgaben sollte eine rechtliche Prüfung im Einzelfall erfolgen.

Passende Anbieter auf Amplifa finden

Geprüfte Industrieanbieter aus der DACH-Region. Bedarf beschreiben und vergleichbare Angebote erhalten.

amplifa-marketplace.ai