

IBAN verification: securing supplier data and minimising payment risks

IBAN verification is the systematic check of international bank account numbers for formal correctness and plausibility before a payment is executed. In B2B procurement it serves as a key measure against invoice and fraud risks, particularly in so-called fake supplier fraud. Together with supplier bank data verification and other master data checks, it forms an essential basis for secure payment processes across the entire procurement organisation.

Key facts

- IBAN verification validates the length, structure and check digits of an international bank account number in accordance with ISO 13616.
- Formal correctness does not mean that the account exists or belongs to the supplier – additional steps are required for that.
- In practice, IBAN verification typically prevents a large proportion of input errors, but not targeted fraud using stolen account details.
- Amount-optimised changes to supplier bank details are a common fraud pattern and require a four-eyes process.
- IBAN verification is an integral part of supplier bank data verification during the onboarding of new suppliers.
- Automated check rules in the ERP system significantly reduce the manual verification effort as part of procure-to-pay process optimisation.

Definition: IBAN verification

IBAN verification refers to the automated or manual checking of an International Bank Account Number for formal validity. It is a standard component of master data maintenance in procurement and financial accounting.

Structure and composition of the IBAN

Under ISO 13616, an IBAN consists of a two-letter country code, usually a two-digit check number and the national account identifier, which in Germany typically combines the bank sort code and the account number. The maximum length in practice is 34 characters, with the actual length varying by country. Each country defines a fixed format against which a valid IBAN can be checked. Even a single incorrect digit usually results in an invalid check-digit result, which makes the integrity check reliable.

- Country code (2 letters)
- Check number (usually 2 digits)
- National bank and account identifier

Distinction from supplier bank data verification

IBAN verification is a subset of the more comprehensive supplier bank data verification. While IBAN

verification addresses only the formal validity of the account number format, supplier bank data verification also covers BIC matching, account holder verification, the plausibility of the bank country and currency, and consistency with commercial register or tax data. In procurement risk management, both levels are combined because fraudsters often provide formally valid but third-party accounts.

Significance in the procurement process

Bank details are supplier master data with a direct money flow. An error or manipulation leads to mispayments which, in practice, are often difficult to recover. IBAN verification therefore acts at a critical point of the procure-to-pay process and complements organisational controls such as the MRO vs. capex procurement policy or defined approval levels in the procurement organisation.

Methods and procedures for IBAN verification

In practice, a tiered approach has become established, ranging from simple format checks to comprehensive fraud prevention. The depth of the verification typically depends on the payment volume and the supplier's risk profile.

Stage 1: Formal and algorithmic validation

In the first step, the length, character set and country format are checked. A check-digit algorithm then verifies the integrity of the number. Some countries use extended national check procedures that additionally protect the bank sort code or account number. These checks typically run automatically in the ERP or payment system, often already when the bank details are entered. Together with catalogue management and other master data processes, the verification can be seamlessly integrated into procure-to-pay process optimisation.

Stage 2: Plausibility and context checks

A formally correct IBAN can still be suspicious. Common plausibility rules concern the relationship between the bank country and the company's registered office, the currency of the account, whether the BIC belongs to the same bank, and sudden changes to existing bank details. In practice: the higher the payment volume or the more critical the supplier as a key supplier, the stricter the plausibility check. Suspicious findings are incorporated into the supplier risk analysis.

Stage 3: Account holder verification and callback verification

Account holder verification compares the account holder with the official company name from the commercial register, business registration or invoice. Many banks offer matching services for this purpose. In practice, callback verification via already known contact channels from the supplier master data has also proven effective – never via telephone numbers or email addresses given in the suspicious message. Changes to bank details should in principle be approved by a second person.

Key KPIs and process metrics for IBAN verification

The effectiveness of IBAN verification can be steered with a few clearly measurable KPIs. At many companies, these metrics are part of supply risk management reporting in payment transactions.

Quality and error rates

The key metric is the proportion of formal errors intercepted before payment execution. In practice, error rates for manually entered bank details are often in the low single-digit percentage range – every

intercepted error avoids costly returns and research effort. In addition, it is measured how many checks are automated at all and how often manual follow-up work is required.

Fraud prevention metrics

For fraud prevention, the number of identified suspicious changes to bank details, the rate of four-eyes approvals and the time to verification of a new bank account matter. The effects on the supplier financial health check are also recorded: payment blocks due to outstanding checks must not unduly delay critical suppliers, but in the event of irregularities they are a legitimate protective measure, up to and including supplier escalation.

Process efficiency

In addition, the process lead time from creation to payment release is of interest. This shows the effect on procure-to-pay process optimisation: in practice, automated check rules significantly shorten lead times and relieve the administrative staff. These metrics should be evaluated periodically and included in management's internal control report.

Risks and controls around IBAN verification

IBAN verification is an effective but not a complete protective instrument. Those who know its limits can complement it purposefully with organisational and technical controls.

What the check can do – and what it cannot

The algorithmic check reliably detects typos and transposed digits. However, it does not detect whether an account belongs to a fraudster who provides a genuinely existing third-party IBAN. This is precisely the pattern prevalent in fake supplier fraud: attackers pose as the supplier, often with manipulated email threads, and change the bank details. Country risk in procurement – for example accounts in high-risk jurisdictions – is also not detectable on a formal level and requires its own assessment rules.

Organisational controls

The most important controls are the four-eyes principle for changes to bank details, callback verification via known contact channels, and defined approval thresholds depending on the payment amount. These rules should be enshrined in the procurement policy and trained. Violations can, in extreme cases, lead to termination for cause if a supplier was involved in a fraudulent diversion or acted negligently.

Integration into supplier risk management

Bank details belong in holistic supplier risk management. It is worthwhile to incorporate irregularities in bank details into the supplier audit score and to define recurring verification intervals for critical suppliers. Compliance topics such as AEO certification and sanctions list screening of bank details complete the picture. Legal obligations, for example under anti-money-laundering law or sanctions law, must always be examined on a case-by-case basis.

Current developments and digitalisation

Digitalisation and standardised interfaces are fundamentally changing IBAN verification. Automation not only reduces errors but also noticeably accelerates supplier onboarding.

Automated validation in ERP and e-procurement systems

Modern ERP and e-procurement systems verify IBAN, BIC and account holder directly at entry and block invalid records. Linked to a central golden record structure for supplier master data, it can be ensured that there is only a single, verified bank account per supplier. This prevents outdated or manipulated data from local lists from entering the payment run.

Standardised data exchange with suppliers

More and more companies are requesting bank details via structured onboarding portals or standardised formats instead of transcribing them from PDF invoices. This reduces transcription errors and creates a complete audit trail. In catalogue management and onboarding workflows, IBAN verification can be built in as a mandatory step before a supplier is activated.

Payment concepts and fraud patterns in transition

Business email compromise remains the most common form of attack: fraudsters manipulate email threads relating to invoices and deliberately insert new IBANs. As countermeasures, amount-optimised approaches such as cryptographically signed supplier data, continuous change monitoring and AI-supported anomaly detection are spreading. Payment holds on changed bank details until successful callback verification are regarded in practice as an established standard.

IBAN verification in supplier onboarding and day-to-day operations

IBAN verification is not a one-off act but a process spanning the entire lifecycle of a supplier relationship – from initial contact to ongoing monitoring.

Onboarding new suppliers

During onboarding, IBAN verification should be carried out together with supplier bank data verification, commercial register checks and the review of quality agreements and warranty agreements. Only when all master data – including bank details – has been verified is the supplier activated for the procurement process. For international suppliers, it must additionally be assessed whether the bank country indicates country risk in procurement or sanctions risks.

Change management for existing accounts

Changes to existing bank details are the most critical scenario. In practice, the following has proven effective: every change requires documented callback verification via a known contact person, approval by a second person and a waiting period before the first payment. High first payments to a new account should in principle be blocked or at least checked separately.

Typical metrics

Proportion of IBAN errors intercepted before payment: > 99 %

Formally invalid numbers should be blocked fully automatically

Proportion of automated checks: > 95 %

Manual format checks are considered avoidable in practice

Four-eyes approval rate for bank detail changes: 100 %

No exceptions, regardless of the payment amount

Duration of account holder verification: 1–3 working days

Typical benchmark including callback verification with the supplier

First-payment hold on new accounts: > 5,000 EUR

Common threshold for separate approval

Practical example

A medium-sized mechanical engineering company with around 800 active suppliers received an email shortly before the year-end close from a long-standing sheet metal supplier announcing a new bank account. The IBAN was formally correct and would have passed any algorithmic check. Only the mandatory account holder verification and a callback to the known telephone number stored in the supplier master data revealed that the email had come from a spoofed sender domain. The company subsequently tightened its process.

- Mandatory callback verification of every change to bank details via known contact channels
- Payment hold for first payments to new accounts above a defined threshold
- Inclusion in the supplier audit score in the event of repeated irregularities
- Automated IBAN and BIC checks directly during master data entry in the ERP system

Conclusion

IBAN verification is a simple but effective building block for secure payment processes in industrial procurement. It reliably intercepts input errors and forms the formal basis of supplier bank data verification. Its limits become apparent, however, with targeted fraud using third-party, formally valid accounts – which is why it needs complementary controls such as account holder verification, four-eyes approval and callback verification. Those who integrate the verification automatically into ERP and onboarding reduce effort and risk at the same time and strengthen the data basis for supplier financial health and supply risk management. As a result, a consistently implemented IBAN verification pays off directly in fewer mispayments, shorter lead times and lower fraud risk.

Frequently asked questions

What exactly does IBAN verification check?

IBAN verification checks the country code, length, format and check digits of an international bank account number in accordance with ISO 13616. It determines whether the number is formally valid. Whether the account exists and belongs to the stated account holder is clarified by additional steps such as account holder verification (Confirmation of Payee).

Does a valid IBAN protect against fraud?

No. Fraudsters frequently use genuinely existing, formally correct IBANs, for example in fake supplier fraud. IBAN verification only detects errors in the number format. Protection against fraud only comes from combining it with account holder verification, callback verification via known contact channels and a four-eyes approval for changes.

How do I securely verify a new supplier bank account?

A proven approach is tiered: first formal IBAN verification, then a plausibility check of the BIC, bank country and currency, then account holder verification. Changes to existing bank details should always be verified back via an already known telephone number or a known contact person – never via contact

details given in the request itself.

Is IBAN verification mandatory?

As a rule, there is no general statutory obligation to verify IBANs, but internal control systems, compliance requirements and, where applicable, anti-money-laundering obligations can create a duty to verify in individual cases. The specific requirements depend on the industry, company size and legal situation and should be reviewed legally.

Can IBAN verification be automated?

Yes, the formal verification can be fully automated and is typically integrated directly into ERP, e-procurement or payment systems. Many banks also offer account holder verification as a service. Automation significantly reduces input errors and speeds up supplier onboarding.

What is the difference between IBAN and BIC?

The IBAN identifies the specific bank account internationally, while the BIC (Bank Identifier Code) identifies the bank itself. Both belong together and should be checked for consistency during verification, for example whether the BIC country code matches the IBAN country code.