

Sanctions list screening: compliance obligation for every supplier and business transaction

Sanctions list screening is the systematic comparison of business partners, contact persons and transactions against national and international sanctions lists. In industrial procurement it is a mandatory compliance task, because violations of foreign trade and sanctions law can lead to heavy fines, supply interruptions and criminal consequences. For buyers, it is therefore as much part of the mandatory programme as credit checks or supplier qualification.

Key facts

- Sanctions list screening is legally required for almost every cross-border business transaction and is also carried out in practice for domestic business.
- Typically screened are EU, UN, US (OFAC) and UK sanctions lists as well as the German 'Eliten und Protagonisten' directory.
- The screening covers suppliers, customers, ownership structures, bank details, end use and end recipients (end-use check).
- Hits are initially initial hits and require manual review before a match is established.
- Screening must be repeated with every business contact and whenever lists change – not just once.
- Gaps in sanctions list screening can lead to fines, reputational damage and the loss of customs or export privileges.

Definition: sanctions list screening

Sanctions list screening (also called sanctions screening) refers to the documented comparison of contracting parties and involved persons against official sanctions and terror lists. It is part of export control and anti-money-laundering prevention and directly affects procurement, because every new supplier relationship and every purchase order must be assessed under sanctions law.

Legal background

In practice, the foundation consists primarily of EU regulations, UN Security Council resolutions, US sanctions (OFAC, including the SDN list) as well as the German Foreign Trade Act (AWG) and the Foreign Trade Ordinance (AWV). The legal situation is dynamic: lists and embargoes change continuously, so statements about the current version must always be verified on a case-by-case basis. For companies the rule is: anyone who comes into business contact with a listed person or organisation must refrain from the transaction or obtain official authorisation. The burden of proof for proper screening effectively lies with the company, which is why documentation is central.

Distinction from export control

Sanctions list screening checks the 'who' – i.e. the person or organisation behind a transaction. Export

control additionally checks the 'what' and 'where to': goods lists, dual-use regulations, end use and destination. Both checks interlock in procurement, especially for components used in sensitive industries or countries. A clean process nevertheless separates the tasks clearly: screening runs automatically and continuously, while export control case-by-case assessment requires specialist knowledge and typically takes place at defined checkpoints in the ordering process, for example anchored in the PO policy.

Scope of screening: what must be screened in procurement?

The screening is not limited to the supplier as a company. Sanctions lists name natural persons, companies, ships and organisations; moreover, ownership and control rules apply that indirectly capture listed shareholders.

Suppliers, owners and contact persons

Screened are the supplier itself, its shareholders to the relevant extent, managing directors and authorised signatories, and in cross-border business frequently also bank details, delivery addresses and intermediaries. Important is the view of concepts colloquially referred to as the '50 per cent rule': companies that are majority-owned or controlled by listed persons are also considered sanctioned in many regimes without being on the list themselves. For procurement this means: the company name alone is not enough; the ownership structure must be documented for high-risk partners.

Transactions, goods and end use

In addition to party screening, transaction screening is part of the process: product, technical data, destination and intended use are assessed for embargo and end-use risks. Red flags include unclear supply chains, resale enquiries from third countries, cash payments or requests to issue invoices to third parties. Freight forwarders, banks and customs agents may also come into focus. In parts shortage management and when expediting under time pressure, the following applies in particular: time pressure does not justify skipping screening steps – short-term alternative sourcing from new, unknown suppliers is a classic risk window.

When must screening take place?

Once is not enough. Screening is customary upon creation of a new supplier or customer, with every transaction or at least risk-based for ongoing business relationships, and with every list update. Since lists are updated frequently, screening in practice runs daily or weekly as a batch across the entire portfolio. Additional triggers are events such as address changes, changes of ownership, site relocations or new business areas of a partner.

Methods and procedure of sanctions list screening

In smaller companies, screening is carried out manually via public government portals; in larger organisations via dedicated screening software that automatically matches company master data and transactions. The process typically follows three steps.

Data preparation and matching

The foundation is clean master data: full name, address, country, where applicable register or tax identification, dates of birth of natural persons. The comparison is fuzzy-based, i.e. tolerant of spellings, transliterations and name components, because sanctioned persons are often listed in several spellings.

Related concepts such as risk classes also play a role here: suppliers are often assigned to risk classes by country, industry, product area and business model, which govern screening depth and frequency.

Initial hit review and release

Every automatic hit is initially an initial hit and not proof: 'Müller GmbH' in Hamburg is not automatically identical to a listed 'Muller Trading FZE'. Clarification is carried out manually by comparing location, legal form, register numbers and persons. The result is documented: either 'no match' with justification, 'match – stop the business' or 'official clarification required'. Release authority in practice usually lies with a compliance officer or executive management, not with the operational buyer.

Integration into procurement processes

Screening is only effective if it is embedded in the process: in supplier onboarding, in the purchase order workflow (PO policy), in the invoice run and when master data changes. It is sensible to have a rule that purchase orders to non-released suppliers are blocked by the system. Also with renaming or address changes following restructurings – for example in low-volume series production or in modular sourcing with many sub-suppliers – master data quality is decisive: incomplete data leads to blind flying in screening.

Key KPIs and control variables

The quality of sanctions list screening can be measured and evidenced in audit and management systems. Typical metrics are oriented towards completeness, speed and error rates.

Completeness and data quality

The central metric is coverage: the share of suppliers and customers subject to a valid screening process should in practice be close to 100%. In addition, master data quality (completeness of country, address, ownership details) and the time to initial screening upon record creation are measured. High initial hit rates are initially not an error but an indication of sensitive fuzzy logic; what matters is the false negative rate – i.e. partners who should have been flagged but were not screened.

Processing and conformity

Further common metrics are the turnaround time for initial hit clarifications, the share of portfolio data re-screened on time, and the number of blocked or aborted transactions. As with delivery performance or the supplier rating model, metrics only work when they are embedded in clear responsibilities and escalation paths. In audits – for example from the perspective of audit rights in customer or certification audits – evidence documentation, the four-eyes principle and the currency of screenings are typically the first things checked.

Risks and controls in procurement

The main risk is not deliberate circumvention but ignorance: outdated master data, untrained staff and emergency procurement without screening. The control architecture should therefore be designed preventively, detectively and reactively.

Typical risk situations

Classic weak points are transshipment or intermediary trade transactions, goods flows via third countries, new online suppliers without verifiable identity, high involvement of commission agents as well as

leasing, service and repair transactions, which are often not perceived as 'exports' at all. Subsequent invoicing parties or changed bank details can also indicate sanctions risks. The freight cost breakdown and preferred carrier specifications provide a side benefit here: anyone who transparently discloses carriers and routes can include them more easily in screening.

Controls and documentation

Proven controls: automated screening with blocking logic, four-eyes review of hits, annual risk assessment of the supplier portfolio, training for procurement and sales, and documented escalation paths. Contracts should contain sanctions clauses with supplier warranties and information obligations upon listing. Documentation must be maintained such that every screening and decision remains traceable years later – including the list version and software version. In unclear cases only one thing helps: pause the business and obtain expert advice.

Role of supplier evaluation

Sanctions compliance should be an integral part of the supplier rating model, alongside quality and delivery metrics such as inventory metrics or delivery performance. A preferred supplier that demonstrably discloses its ownership structure and compliance organisation significantly reduces screening and procurement effort. Conversely: compliance violations or refusal to disclose structures are a hard de-selection criterion – regardless of price and delivery capability.

Current developments and outlook

Sanctions regimes change in short cycles, and the number of relevant lists as well as official enforcement activities has noticeably increased in practice. At the same time, the volumes of data that must be screened automatically are growing.

Dynamics of lists and regimes

Political crises lead to rapidly issued, frequently amended packages with embargoes, import and export bans and individual listings. For buyers this means: these statements are kept general – which regimes are specifically relevant must always be verified at the time of the transaction. Regular legal status updates, a named compliance officer and a subscription or feed of the relevant lists are recommended, rather than manual portal lookups.

Automation and supply chain transparency

Screening increasingly runs as part of integrated compliance and supply chain systems, sometimes combined with human rights and sustainability checks, for example following the approach of Science Based Targets for climate goals or supply chain due diligence obligations. AI-supported suggestions improve match quality but do not replace manual clarification. Forward-looking statements about technology developments are subject to uncertainty and should be verified case by case – the obligation to documented own screening does not change in principle.

Typical metrics

Screening coverage: > 99%

Share of screened suppliers/customers in the total portfolio

Initial hit turnaround time: < 24–48 hours

typically targeted clarification time until documented decision

Master data quality: > 95%

complete screening fields (name, country, address, owner) – typical benchmark

Practical example

A medium-sized mechanical engineering company urgently needs to procure a control module via a previously unknown trading intermediary in a third country because its regular supplier reports a delivery delay and the parts shortage management wants to increase the expedite rate. Before the purchase order is released, the screening system blocks the transaction: the trader shares address and bank details with an initial hit. Manual clarification finds no match, but reveals an unknown ownership structure with participation from an embargoed country. Procurement stops the deal and sources via a qualified preferred supplier.

- Blocking logic in the purchase order workflow: no PO without completed screening
- Documented clarification of initial hits including ownership structure by the compliance officer
- Escalation rule for emergency procurement that does not put time pressure above compliance
- Inclusion of sanctions clauses and disclosure obligations in new supply contracts

Conclusion

For technical procurement, sanctions list screening is not an academic exercise but a daily mandatory task with direct business consequences. It protects against penalties and supply failures while simultaneously strengthening the position with customers and authorities. What matters are clean master data, risk-based screening depth and seamless embedding in ordering and supplier processes. Those who understand screening as part of supplier management – rather than as an isolated compliance hurdle – gain planning certainty and speed. These statements are of a general nature and do not replace legal advice in individual cases.

Frequently asked questions

Which sanctions lists must be screened?

At a minimum, the EU sanctions lists, UN lists, the US OFAC SDN list, the UK list and the German directory 'Eliten und Protagonisten' are customary. Depending on the business model, further national lists may apply. Which regimes are specifically relevant depends on place of business, markets, currency and supplier relationships and should be assessed legally on a case-by-case basis.

When must a sanctions list check be carried out?

In principle, with every business contact: upon creation of a new record, before every transaction or at least risk-based before major transactions, and again when lists are updated. One-off screening at onboarding is not sufficient because lists change continuously. In practice, automated rescreening is therefore run daily or weekly across the entire portfolio.

What is an initial hit in sanctions list screening?

An initial hit (false-positive candidate) is an automatic match that has not yet been proven to concern the listed person or organisation. It must be clarified manually, for example using address, register data, date of birth and ownership structures. Only after documented clarification is it established whether the business is permissible or must be stopped.

Who is responsible for sanctions list screening within the company?

Organisationally, overall responsibility lies with executive management; in day-to-day operations it is frequently delegated to a compliance officer. Operational buyers provide master data and escalate anomalies, but generally do not decide on contested hits. Documented responsibilities and the four-eyes principle are essential.

What are the consequences of violating sanctions lists?

Depending on the legal system, severe fines, confiscation, criminal consequences for responsible individuals, trade restrictions and reputational damage may result. In addition, there are operational consequences such as blocked payments or disrupted supply chains. The specific penalty amounts and legal consequences differ depending on the regime and the individual case.

Can sanctions list screening be carried out manually?

With few partners and transactions, manual screening via the official government portals is possible and must be documented. As the portfolio and transaction volume grow, this approach reaches its limits, for example with list updates and fuzzy matching. In that case, automated screening with blocking logic is recommended – but responsibility for the decision always remains with the company.