From Finance to the Defense and Aerospace Industry:

The Sanctions Risk Assessment Model as a Strategic Lever for Risk Management

protiviti®

Global Business Consulting

The defense and aerospace sector is today facing increasing exposure to strategic risks, which heightens its managerial complexity and vulnerability.

By way of example, these risks include involvement in global supply chains — often characterized by complex geographic mapping — the need to automate information analysis, address cyber warfare and rapid technological evolution, as well as the requirement for continuous adaptation to frequent sanction and export control packages affecting the free movement of goods. This results in the need to manage risk through a structured approach that considers not only regulatory compliance, but also big data management, the introduction of artificial intelligence (AI) into decision-making models, and governance capable of supporting informed and timely decisions.

In this context, the implementation of structured models for the assessment and management of such risks — including those related to international sanctions, money laundering, reputational risks and non-compliance with environmental, social and governance (ESG) requirements — has become indispensable to ensure operational continuity, strategic robustness of the defense and aerospace sector, and overall resilience.

Premise

The risks of doing business internationally are not new to companies in the defense and aerospace sector. In the 1970s, a case involving Lockheed Corporation marked the first significant recognition of the need to establish a robust internal control framework and to ensure compliance with applicable regulatory requirements. The case exposed, in a systemic manner, the risks inherent in operating models relying on foreign intermediaries, activities carried out in jurisdictions with heightened geopolitical exposure, and relationships with public-sector counterparties. This case served as a catalyst for the development of regulatory safeguards and control mechanisms that are now regarded as essential, laying the foundation for an integrated approach to corruption, anti-money laundering and sanctions compliance risks.

A further precedent is represented by the Valsella Meccanotecnica case, relating to the export of military materials to Iran in the 1980s. Although situated in a geopolitical and regulatory environment significantly different from today, this case remains a relevant example of the long-term consequences that failure to comply with export restrictions and international embargoes can generate — not only in terms of sanctions, but also with respect to political, reputational and institutional credibility impacts.

Today, in the defense and aerospace sector, the management of risks related to international sanctions and money laundering has become a central element of corporate governance. The growing complexity of the regulatory framework — characterized by multilayered, dynamic sanctions regimes strongly influenced by the geopolitical context — requires the adoption of advanced compliance and risk management frameworks capable of ensuring continuous alignment with legal and regulatory requirements.

International sanctions are no longer limited to traditional trade and financial restrictions, but also include sectoral bans, designated persons lists, and restrictions on dual-use goods, strategic technologies and specialized services. The introduction of secondary sanctions — those targeting persons (individuals or entities) in non-issuer countries who engage in specific prohibited transactions with sanctioned countries, entities, or individuals, even if the transactions have no direct connection to the issuing country — further expands the risk perimeter, extending exposure to indirectly involved third parties and making enhanced controls on counterparties, customers, suppliers and ultimate beneficial owners essential.

The relevance of these risks is further confirmed by recent enforcement activity, which highlights increased scrutiny by authorities over violations related to export controls, dual-use goods and embargoes toward high-risk jurisdictions. Numerous investigations have concerned illicit exports of drone components and armaments, suspicious corporate transfers and corruption schemes involving both Italian and international companies.

More recently, investigations and proceedings initiated by national authorities have shown how, in the defense and dual-use technology sectors, operational vulnerabilities may arise from the management of international supply chains, the use of intermediary companies and the complexity of cross-border commercial flows toward jurisdictions with heightened geopolitical and sanctions sensitivity.

These cases demonstrate that supply chain management, regulatory compliance embedded within business processes, and effective control of counterparties and transactions are critical factors in mitigating risk in the defense and aerospace sector. In this context, the adoption of structured risk assessment models — derived from the experience of global financial intermediaries and adapted to sector-specific features — enables a systematic evaluation of both the likelihood and impact of exposure to sanctions and illicit financial flows, strengthening operational resilience and compliance with increasingly stringent national and international regulations. In summary, such models enable management to make informed decisions based on known and measurable risks.

Regulatory framework

The legal framework governing international sanctions and anti-money laundering strategies in the defense and aerospace sector is characterized by a multilevel structure, involving multilateral sources, as well as recommendations and best practices issued by standard-setting bodies such as the Financial Action Task Force (FATF)/Groupe d’action financière (GAFI).

EU regulatory framework

The European Union has developed a comprehensive regulatory framework integrating sanctions, export controls, foreign investment screening and criminal liability:

- Regulation (EU) 2021/821 (Dual-Use Regulation) requires the adoption of internal compliance programs (ICPs) and enhanced due diligence on end-users and end-use, in line with the standards of the Wassenaar Arrangement.
- Regulation (EU) 269/2014 provides for asset freezes and prohibitions on making funds or economic resources available, extended also to entities that are owned or controlled, directly or indirectly.
- Directive 2009/43/EC governs intra-EU transfers of defense-related products, strengthening supply chain traceability.
- Directive (EU) 2024/1226 harmonizes criminal sanctions for violations of EU restrictive measures.
- Regulation (EU) 2019/452 on FDI Screening and Regulation (EU) 833/2014 reinforce controls on foreign investments and exports to Russia and other sensitive geopolitical contexts.

International and U.S. regulatory framework

The Financial Action Task Force, the preeminent intergovernmental body focused on protecting the global financial system from money laundering, terrorist financing, and proliferation financing, classifies the aerospace and defense sector as high-risk, setting the expectation for enhanced controls, screening and reporting obligations.

U.S. requirements also have a significant impact on non-U.S. operators, due to the extraterritorial reach of sanctions regimes:

- CAATSA (2017) introduces secondary sanctions for entities engaging in significant transactions with the Russian military-industrial complex, requiring enhanced assessments also by European players.
- Sectoral Sanctions (OFAC Directives 3 and 4) restrict access to financing and prohibit exports to entities operating in the Russian defense sector.
- ITAR and EAR regimes regulate, respectively, military items and dual-use goods, requiring structured systems for classification, licensing, monitoring and audit.
- Executive Orders (e.g., E.O. 14024) broaden the scope of restrictions by including entities linked, even indirectly, to strategic industries or foreign armed forces.

Analysis of potential risks

In the defense sector, failure to comply with the above regulatory requirements exposes companies not only to administrative and criminal sanctions (which in the EU can be up to 5% of global turnover and confiscation of assets used or obtained through the violation), but also to the risk of exclusion from international financial systems, debarment from public procurement, loss of credibility with banks and insurers, and severe reputational and operational impacts.

Specifically, violations of sanctions regulations may take multiple forms:

- **Direct violation:** Involvement in operations with parties included in international sanctions lists (e.g., SDN List or EU Reg. 269/2014).
- **Incitement and attempt:** Conduct that is criminally relevant under EU Directive 2024/1226.
- **Failure to notify:** Omission of communication obligations provided for by Decree Law 21/2012.
- **Non-compliance with imposed conditions:** Failure to observe the technical requirements contained in authorization decrees.
- **Indirect violation (including so-called circumvention risk):** Use of triangulation through third countries or special purpose vehicles (SPVs) to bypass restrictions.
- **Reputational and supervisory risk:** Exposure of financial and insurance intermediaries involved in critical operations.

For the purposes of this analysis, the following risk scenarios are explored in detail:

Circumvention risk

The phenomenon of circumvention represents one of the most critical risks in the application of international sanctions today. This term refers to the indirect evasion of restrictions through third countries that act as transit or re-export hubs for prohibited goods and technologies.

In the post-2022 context, following EU, U.S., and G7 restrictive measures against Russia, numerous analyses based on Trade Map-ITC data have highlighted anomalous increases in trade flows from countries such as Turkey, the United Arab Emirates, Armenia, Georgia, Kazakhstan, and Uzbekistan, which significantly increased exports of critical goods precisely while direct exports from Europe to Moscow decreased.

The European Commission, in its September 2023 Guidance for EU Operators on Circumvention Risks, called on EU companies to implement enhanced due diligence procedures toward counterparties located in high-risk jurisdictions, based not only on quantitative indicators of commercial exchange, but also on the nature of the goods involved (e.g., dual-use, avionics, semiconductors, precision optics, etc.). Similar indications come from the United States via the Russia Sanctions Evasion Global Advisory (2023) and the Tri-Seal Compliance Note (2024), which reiterate the responsibility of companies, including non-U.S. ones, in preventing prohibited triangulation or re-export.

From a regulatory perspective, circumvention risk is expressly recognized by Directive (EU) 2024/1226, which classifies as a crime not only the direct violation of restrictive measures, but also the aiding, incitement, and attempt to evade them. This means that a company can incur liability even if the good is not exported directly to a sanctioned country but reaches that destination through an intermediary in a third jurisdiction.

For the defense and aerospace sector, circumvention risk is particularly relevant as it involves goods with high strategic and reputational impact. Avionics components, drones, radar systems, and semiconductors are consistently among the most sought-after items through evasion channels, as confirmed by various enforcement actions and lists of critical goods compiled by the EU, OFAC, and G7. Exposure to such schemes entails not only financial and criminal sanctions, but also long-term reputational consequences, with possible exclusions from NATO tenders, EU calls for proposals, or joint research and development projects.

From this perspective, circumvention risk management is not only a compliance obligation, but an indispensable strategic safeguard for protecting the international position of companies in the defense sector.

Reputational risk

Reputational risk in the defense and aerospace sector represents a critical factor that crosses and amplifies all dimensions of sanctions and anti-money laundering risk. It is not limited to producing direct financial impacts: it affects institutional credibility, access to global markets, and the ability to attract investors, industrial partners, and strategic alliances.

Indeed, companies in the sector operate under a level of public and media scrutiny rarely found in other sectors. The sensitivity of the technologies involved, the proximity to governments, and the geopolitical role of military supplies mean that even a single episode of non-compliance — even if marginal, involuntary, or mediated by third parties (e.g., triangulation with countries subject to restrictions, partnerships with opaque entities, use of non-compliant subcontractors) — can result in deep and lasting reputational damage. The consequences range from the revocation of licenses and the loss of contracts to exclusion from international tenders and joint research and development programs, with repercussions on the company's very ability to operate in strategic markets.

To this is added the impact on the relationship with banks, insurance companies, and supervisory authorities: a reputational deterioration can increase the cost of capital, restrict access to credit lines, and raise the probability of regulatory controls. The relationship with non-financial stakeholders — suppliers, local communities, NGOs, and the media — also becomes vulnerable, as the perception of transparency and integrity is a determining element for the operational sustainability of the sector.

In this scenario, an increasing role is played by the monitoring of negative news: the simple dissemination of unfavorable news in international media or specialized databases can generate significant reputational effects, even in the absence of final judicial findings.

Ultimately, reputational risk management is not an accessory or a merely cosmetic activity: it is a true competitive enabler. Only companies perceived as reliable, transparent, and fully compliant with international standards can build solid and lasting relationships with governments, multilateral institutions, and leading industrial partners.

Transferability of the financial industry's sanctions risk assessment model to the defense and aerospace industry

In the defense and aerospace sector, effective sanctions risk management represents not only a response to regulatory requirements, but also a strategic lever for strengthening the resilience, transparency, and competitiveness of companies.

Companies in the defense and aerospace sector must adopt a proactive and systematic approach, based on:

- Preliminary analysis of counterparties, beneficial owners, and the supply chain.
- Assessment of the level of exposure to sanctions and money laundering risks for each operation.
- Continuous monitoring of suspicious financial flows and periodic review of internal control models.
- Integration between screening tools to timely identify anomalies, circumvention attempts, or interposed parties.
- Specific training of personnel on sanctions and anti-money laundering issues.

In line with the high levels of market sensitivity and stringent international regulatory constraints, a sanctions risk assessment is structured on three levels to ensure a dynamic assessment calibrated to the specificities of the sector:

1. **Inherent risk:** Considers factors such as the presence of dual-use programs, strategic technology transfers, relationships with government entities or partners subject to international restrictions, and geographical location of counterparties, types of distribution channels, and products.

   For risk management in operations involving dual-use products and armaments materials (Regulation EU 2021/821, Directive 2009/43/EC), operators must evaluate not only the end-user but also the end-use and the intermediate parties involved in the distribution chain. Direct operations with defense ministries or government institutions offer traceability and centralized authorizations, while the use of private resellers, subcontractors, or foreign intermediaries entails a higher risk of triangulation, unauthorized re-exports, or diversion to countries subject to embargo.

   Regarding the type of product, the sale of complex systems (e.g., military aircraft, satellites, radar) is subject to rigorous licenses and multilevel controls (ITAR, national authorizations, and EU licenses), acting as a mitigation safeguard. Conversely, small arms, modular components, and ammunition present a higher inherent risk of diversion toward unauthorized parties, as highlighted by FATF Typologies (2021) and UN resolutions on small arms trafficking (UNSCR 2370/2017).

   In summary, an effective RA model must integrate:

   - Mapping of distribution channels and levels of intermediation.

- Product sensitivity, according to applicable regulations (e.g., ITAR, Reg. EU 2021/821).
- Analysis of the end-user certificate and the declared end-use.

The adoption of predictive indicators and what-if scenarios takes on particular importance in contexts of rapid geopolitical change, such as those related to crisis areas or markets under embargo.

2. **Vulnerability:** Considers the assessment of the robustness of corporate safeguards and includes verification of export control systems, end-use/end-user procedures, and the effectiveness of specific training for personnel. In particular, robust tests and violation simulations (e.g., red teaming on procurement processes and supply chain management, etc.) help identify any blind spots and strengthen the risk culture, especially in the presence of international subcontracts and supplies to public entities.
3. **Residual risk:** Highlights the areas of greatest criticality that require immediate escalation to top management or compliance functions.

The risk assessment model

The three-level risk assessment is possible through the use of a specific calculation model fed by elementary data that make up the key risk indicators (KRIs). KRIs can also be extracted and fed through the support of AI tools, which prove particularly effective in analyzing relationship networks, continuous monitoring of information sources (e.g., bad news), analysis of ownership structures and ultimate beneficial owners (UBOs), as well as in managing high volumes of data.

AI can support the user in defining and updating KRIs through the identification of emerging risks. In particular, the use of graph-based approaches, integrated with AI models, allows for supporting the construction of risk scenarios, also through generative AI techniques, as well as developing predictive capabilities through advanced models such as neural networks. These tools also allow for continuously simulating coherent and plausible scenarios (so-called “what-if simulations”), based on the evolution of macroeconomic and geopolitical phenomena.

The model also provides for the attribution of a weight to each result according to simple and intuitive risk scales (e.g., 1–4) calculated based on statistical or mathematical measures, which generate objectivity in the attribution of measures and a correct distribution of weights. The weight attributed to each result contributes to the calculation of the final risk, represented within a matrix, useful for easy reading by the board and control functions. Compared to the financial context, in the defense and aerospace sector, some risk factors must take on a greater weight. These include, for example, the international supply chain, the geographic origin of counterparties, the export of dual-use technologies, the adoption of export control systems, sanctions clauses in contracts, screening of indirect supplies, and procedures for managing secondary sanctions (e.g., OFAC).

Consequently, it is essential to consider these peculiarities in the selection of a dataset of risk indicators, both qualitative and quantitative, aimed at collecting information relating to, by way of example:

- **Presence of relationships with foreign counterparties:** In addition to the geographical identification of counterparties, it is appropriate to evaluate whether they operate in jurisdictions subject to direct or indirect restrictions, also based on secondary sanctions (e.g., CAATSA); risks associated with the use of currencies such as the U.S. dollar, which automatically entail OFAC jurisdiction, must be considered.
- **Operations in countries subject to restrictions:** Mapping of activities must also include distribution and logistics channels, as triangulation with third countries can constitute indirect violations (e.g., use of logistics hubs in off-limits areas); it is useful to verify the existence of exemptions or authorizing derogations connected to dual-use exports.
- **Commodity sector relevant for sanctions purposes:** An updated analysis of customs codes (HS, CN, ECCN) must be conducted to assess whether products are subject to ITAR, EAR, or Regulation EU 2021/821 restrictions. The combination of components must be considered. Even if the final product is not sanctioned, the inclusion of controlled subsystems can expose the entire export to violations.
- **Presence of operations with foreign public entities:** The analysis must consider the degree of state control over the foreign entity (e.g., >50% for the OFAC 50 Percent Rule) and assess whether it is included in lists of designated parties; cross-checking with official databases and the adoption of enhanced due diligence mechanisms in the case of international PEPs is useful.
- **Participation in joint ventures or consortia with foreign partners:** It is useful to map indirect relationships of ownership or influence as well, to avoid violations deriving from parties “hidden” within corporate layers.
- **Transfer of sensitive goods, technologies, or know-how:** The analysis must also include intangible transfers of technology, for example via software licenses, access to databases, or sending technical documentation; the adoption of an internal compliance program (ICP) compliant with Regulation EU 2021/821 and integration into corporate authorization flows is recommended.
- **Presence of customers or suppliers with opaque corporate structures:** It is fundamental to ascertain the identity of the ultimate beneficial owner (UBO) and the presence of any trusts, foundations, or SPVs that may hide ownership structures; OSINT sources and official databases must be used to exclude indirect links to designated parties or sanctioned entities.
- **Use of non-transparent or high-risk financial channels:** It must be verified whether payments transit through banks established in non-cooperative jurisdictions or those not compliant with FATF recommendations, or if fragmented, cash-based, or opaque

payment methods are used, segmentation by critical currencies and values (e.g., OFAC threshold) should be provided.

- **Exposure to reputational or investigative risk:** It is appropriate to actively monitor the presence of the entity or its partners on enforcement databases (e.g., OLAF, SIRENE, Prosecutor's Office, OFAC Enforcement Actions); the adoption of a proactive crisis management strategy (including communication and investigative response) represents a relevant mitigating factor in the model.
- **Presence of contractual exposure to third parties (third-party and contractual risk, AI-enabled):** In addition to the formal identification of suppliers, subcontractors, agents, distributors, joint venture partners, and system integrators, it is appropriate to evaluate to what extent the contracts governing such relationships include effective clauses regarding international sanctions, export controls, end-use, re-export, sub-contracting, audit, and termination; to this end, the use of AI solutions for the analysis, indexing, and continuous monitoring of contractual clauses allows for identifying gaps, inconsistencies, or risk variations deriving from the evolution of sanctions regimes (EU, OFAC, ITAR, EAR, CAATSA) and preventing indirect violations or circumvention phenomena via third parties.

A model designed for collecting this information facilitates the exercise and allows for analyzing in more detail the company's exposure to sanctions risk and adopting the measures necessary to stem it.

The sanctions risk assessment model, structured in this way, goes beyond a simple compliance exercise, configuring itself as a decision support tool for the corporate risk appetite framework (RAF). By systematically measuring inherent risk, vulnerabilities, and residual risk, the risk assessment provides management with an objective representation of the exposure levels associated with specific jurisdictions, commodity sectors, or types of counterparties.

Accordingly, the results of the risk assessment become fundamental inputs for defining risk tolerance thresholds and identifying areas where the company is willing to sustain certain levels of exposure. This allows top management to make informed strategic decisions, such as abandoning markets or geographies deemed too risky in terms of sanctions compliance, circumvention risk, or reputational impacts. This is particularly relevant considering that the use of AI solutions allows for transforming this exercise into a continuous process, strengthening the organization's ability to timely intercept variations in the risk profile.

Sanctions risk assessment models are often integrated with AI — machine learning algorithms can be trained on datasets specific to the defense and aerospace sector, useful for analyzing atypical patterns in the flows of dual-use materials, checking the correspondence of declared end-users, and automating the verification of offset programs.

Conclusion

In light of the specific characteristics of the business and the dynamic environment in which AI and big data play a prominent role, compliance is not merely a regulatory obligation but a key enabler for business protection, market access, financing opportunities, international tenders and cross-border institutional credibility.

How Protiviti can help

Within this evolving context, our support to companies operating in the defense and aerospace sector focuses on the design and implementation of sanctions risk assessment frameworks tailored to business-specific characteristics and the complexities of international supply chains.

The use of advanced data analytics tools, counterparty monitoring and the assessment of indirect relationships enables complex information to be translated into meaningful inputs for decision-making. A sanctions risk assessment, therefore, represents a strategic lever for operational resilience, reputational sustainability and the ability to capture new business opportunities even in highly complex strategic environments.

The paper was written by Francesco Monini (Managing Director), Filippo Andrea Ravizza (Director) and Emanuela Manzo (Manager) from Protiviti's Milan office.