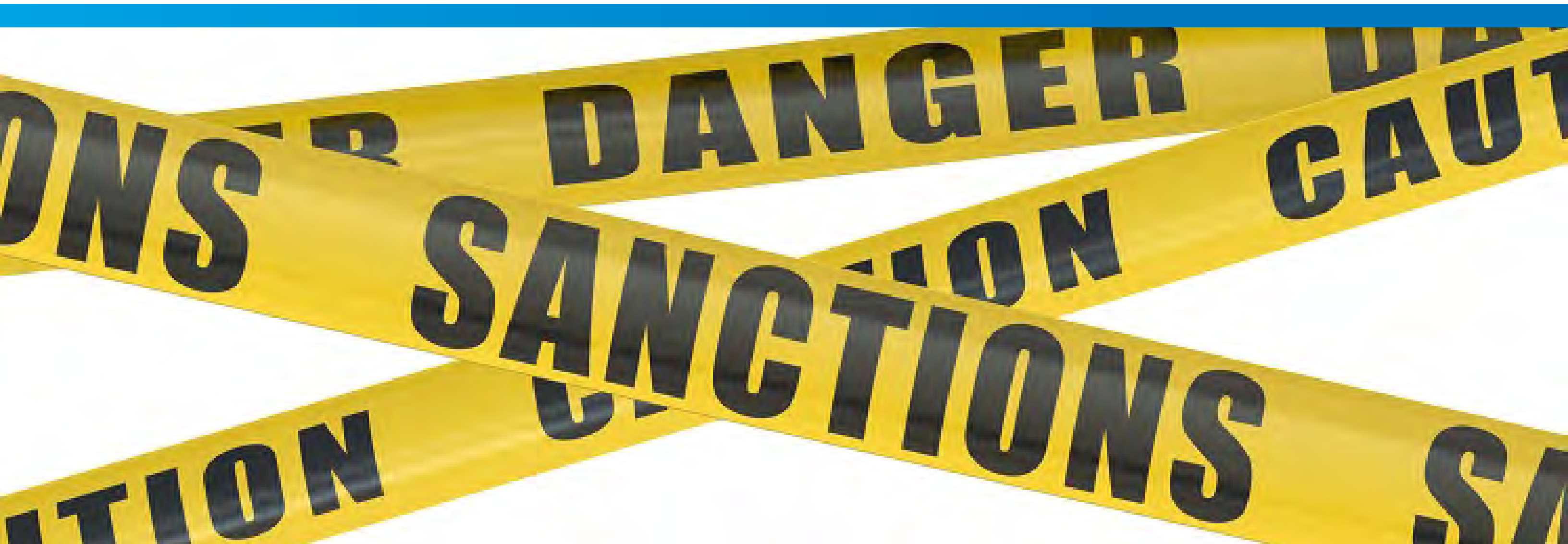
DESCARTES



BUSINESS WHITE PAPER

Sanctions Screening: Practical Solutions to Reduce Risk

Performing Sanctions Screening within Enterprise Resource Planning (ERP) & Customer Relationship Management (CRM) Systems

Sanctions Screening: Practical Solutions to Reduce Risk

Performing Sanctions Screening within Enterprise Resource Planning (ERP) & Customer Relationship Management (CRM) Systems

Sanctions screening is fundamental to ensure that business is not conducted with bad actors worldwide. In an environment of heightened security, ever-changing sanctions regimes, rising fines, and complex sanctions ownership requirements, proper due diligence is a must.

At the core of sanctions screening is a review of information as it flows into and out of a business. Logically following, since most companies operate on centralized platforms such as Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) systems including NetSuite, SAP GTS, Oracle GTM, Salesforce, and others, screening data within these systems is critical to minimize risk.

Key questions and challenges of a sanctions review within internal systems include:

- How can businesses perform screening within ERPs and CRMs **without draining resources**?
- How can companies pinpoint bad actors given the **potentially complex ownership structures** of sanctioned entities?
- How can screening be performed **across global operations**, multiple departments, and various business units?
- How can a sanctions screening **audit trail** be created without adding labor?
- If a sanctioned party "hit" is identified, what are the **best practices to mitigate risk**?

This white paper answers these questions and more to help you reduce risk while keeping productivity at its peak.

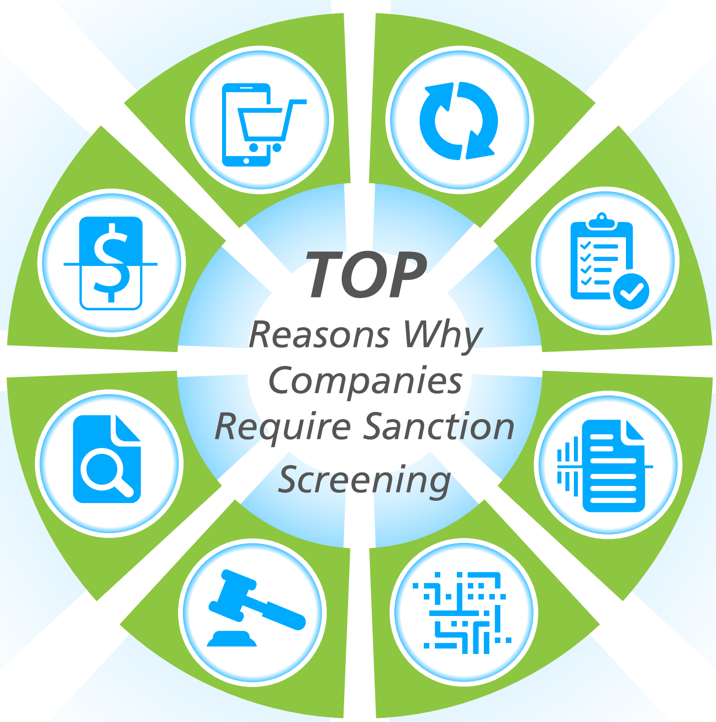
In a Rush? Read This:

At the core of sanctions screening is a review of information as it flows into and out of business systems.

The Basics: What is Sanctions Screening

Sanctions screening is a due diligence review of transactions, employees, partners, contractors, subcontractors, prospects, and more to ensure business is not conducted with entities included on a sanctions list. A sanctioned list is a broad term that can include watch lists, concern lists, restricted party lists, embargoed countries, and more.

A large number of entities maintain sanctions lists, which can include individuals, companies, foreign government agencies, and locations. Companies conducting business with any of the listed persons or entities could be subject to civil and/or criminal prosecution, fines, denial of export and/or import privileges, and closure of financial processing. Beyond this, it is critical to maintain an audit trail and keep records of compliance efforts to hedge against risk.



1. Continuous changes

Denied, restricted and sanctioned lists are in continuous flux. It is essential for businesses to keep pace with constantly shifting DPS updates to minimize risk.

2. Number of lists

With an increasing number of lists that span beyond the scope of traditional sanctions to include cyber security and more, a solution is required that can automatically review a broad range of lists simultaneously.

3. Historical Screening

The need to periodically review previous sanctions compliance is critical for businesses to minimize the potential of fines.

4. Amount of Data

Similar to the number of lists and rate of changing data, the volume of information and records that must be screened calls for an automated solution.

5. Large Penalties

The frequency, number and amount of sanctions fines is increasing. Average penalties are on the rise, and recent fines have been the largest on record.

6. Audit Trail

Companies may be required to demonstrate that they have practiced reasonable care to avoid or reduce penalties. Leading businesses are implementing solutions that include an audit trail.

7. Review of financial transactions

The processing of transactions to or through financial institutions is subject to a sanctions review. Non-compliance has led to penalties into the millions of dollars.

8. Ecommerce

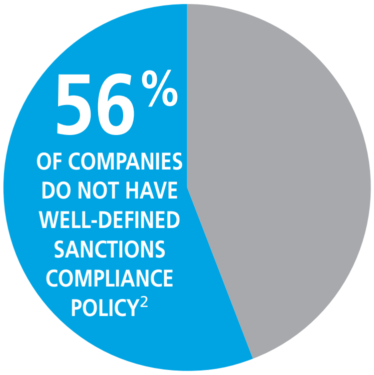
With the continually growing volume of online transactions, it is critical to screen ecommerce transactions and shipments.

Inadequate Screening Is Not an Option

As government enforcement and penalties rise, companies that employ inadequate sanctions screening procedures place themselves at serious risk.

For example, in April 2019, a British company agreed to pay $1.1 billion for sanctions violations[1]. In this case, U.S. and British authorities discovered that the business transacted with sanctioned parties in Cuba, Iran, Sudan, and Syria. The scope of the violations was substantial, with transactions flowing into and out of the company's ERP systems.

In 2018, a French company was fined nearly $1.3 billion for breaching U.S. sanctions[2]. The company engaged in more than 2,500 Cuba-related deals that should have been blocked or stopped by screening within its ERP platform or internal processes. Here too, this penalty illustrates the heavy cost of sanctions violations and the need to monitor ERP systems as part of a robust compliance process.



The largest fine on record remains the $8.9 billion penalty of 2014. In this case, another French business was penalized for violating U.S. sanctions against Sudan and other countries[3].

A German company was fined $258 million in 2017 for helping Russian investors move $10 billion through branches in London, Moscow and New York[4]. Again, sanctioned party data was housed within the company's ERP system, but was not flagged or was overlooked.

Key questions and challenges of a sanctions review within internal systems include:

- Companies outside of a given country or location can face international fines
- Sanctions compliance must be comprehensive and cover global lists
- A review of the information housed within ERP systems is critical to minimize risk since these are the central platforms of information flow

Sanctions Screening & ERPs

For some businesses, solutions such as NetSuite, SAP, or Oracle serve as the central platform to manage finances, operations, the supply chain, sales, human resources, customer relations, and more. These platforms are often used worldwide, across divisions, business units, departments, and by partners.

Since ERPs have multiple touchpoints within a business and connect to a broad range of trading partners, it is critical to ensure that no sanctioned parties are hidden within the data.

One primary challenge of sanctions screening is the large amount of information housed within ERPs. In addition, the set of information within these systems is in endless flux. Beyond this, sanctions lists change and evolve over time. A solution is needed that acts as a funnel to review information before it enters a system and as data changes.

Here is a practical example. Let's say a new vendor is scheduled to be onboarded. Without screening, the vendor would not only enter an ERP, but business would be transacted with this party. Payment information would flow to the vendor and services would be provided. Each one of these touchpoints could be a potential sanctions violation if the vendor was on one of the hundreds of sanctions lists worldwide.

To reduce risk, it is critical to:

1. *Perform screening before a party enters an ERP*
2. *Periodically screen as data is updated and as sanctions lists change*
3. *Historically screen prior data against updated sanctions lists*

The above three items should occur consistently, reliably, and automatically, without adding any extra steps or labor for a business.

Sanctions Screening & CRMs

Customer Relationship Management platforms such as Salesforce often act as the centralized platform for sales, marketing, and other departments. The contact and lead records within CRMs change at a rapid rate since sales and marketing are continuously prospecting and initiating campaigns.

Although, for example, high degrees of due diligence may be performed when a prospect becomes an account, it is often not practical to screen leads before they convert.

This is why sanctions screening in solutions such as Salesforce is critical. Screening of a lead before it becomes a contact can help serve as an added measure of risk management before business is formally transacted.

salesforce

Here is a practical example. Let's say a sales representative is in negotiations with a lead. The representative has allocated bandwidth to interact with the prospect, prepare contracts, and may have even travelled to the lead's location. If such an opportunity is later found to be on a sanctioned party list, the sales representatives will have not only lost valuable bandwidth, but the interactions may have cost the company money.

As in all sanctions reviews, it is essential for CRM screening to have an audit trail. In the unlikely event that business is inadvertently executed with a sanctioned party, the risk may be minimized or the fine may be reduced if a company has clearly demonstrated reasonable care.

In a Rush? Read This:

Screening within CRMs is critical since sales and marketing are often the first point of contact with external entities. A review of a lead before it becomes a contact can help serve as an added measure of risk management before business is formally transacted.

Reasonable Care & Audit Trails

Due to the volume of transactions and the international nature of business, there is a high possibility of eventual contact with a sanctioned entity. In such cases, it is important to have safeguards in place to underscore that a business was not negligent. This is where the concept of "reasonable care" comes into play.

The term reasonable care originally stems from the 1993 U.S. Customs Modernization Act. Reasonable care is simply a demonstration of due diligence. Penalties can potentially be reduced if a company can show that care has been taken to avoid sanctioned parties.

Reasonable care can take the form of technology that screens transactions and that can clearly show that measures were taken to avoid prohibited interactions. The right solution should feature an audit trail that can clearly show:

- When data was screened within an ERP or CRM
- What information was reviewed within the system
- Automated screening within the ERP or CRM
- Historical screening
- If a sanctions "hit" occurred and when

What do to if a sanctions "hit" occurs?

- Have an automated process to place the transaction on hold
- Establish a decision tree to clarify who is responsible for clearing the match
- Review the transaction and document:
  - When it occurred
  - From where the business originated
  - Who interacted with the party
- Communicate inter-departmentally
- Clearly document the resolution in writing

"50 Percent Rules" Add Complexity

U.S. and E.U. regulations state that business should not be transacted with companies with 50 percent ownership by a sanctioned party. However, the process of determining ownership can be challenging. The extensive networks that surround sanctioned actors and jurisdictions can be opaque. Some ownership stakes and business relationships can go undetected by even the most mature, manually-driven risk control frameworks.

Here is a recent example. A global provider of aviation and communication equipment was found to be in violation of the U.S. Office of Foreign Assets Control (OFAC) 50 percent rule. The company, on behalf of its former subsidiary, participated in three shipments of goods through distributors in Canada and Russia. The business shipped to an entity that did not appear on OFAC's Specially Designated Nationals (SDN) list. Although the recipient was not included on a published sanctions list, it was, in fact, blocked under OFAC's 50 percent rule since it had 51 percent ownership by a sanctioned entity.[6] Without screening within the company's ERP system, the business was in violation of sanctions requirements.

In other words, companies must comply both with officially published and unpublished sanctions lists. Companies in violation of the 50 percent rule have noted the challenges of compliance with hidden lists and entities not publicly identified as sanctioned.

If a company can better identify companies with 50 percent or more ownership by a sanctioned party and screen for such parties within ERPs and CRMs, they would be better positioned to reduce risk.

Ownership Structures Can Be Complex & Global

The process of determining business ownership can be challenging. It is critical to use technology that can pinpoint 50 percent ownership by sanctioned parties and unravel complex business relationships.

Conclusion

Globalization and digitization mean that companies regularly interact across borders. While global business can boost profitability and drive growth, there are bad actors hidden across the world and concealed in the data within one's own systems.

The bridge between internal platforms and external parties are often ERPs and CRMs. Such platforms are the critical fulcrum where data must be reviewed to identify potential sanctioned entities.

Technology that can perform such screening in an automated, retroactive, and continuous manner without interfering with workflow can substantially reduce risk. However, not all screening platforms are alike. The right technology must:

- Feature comprehensive global sanctions data
- Include expertly reviewed content to minimize false positives
- Seamlessly integrate with internal systems
- Identify hits by exception
- Contain the most up-to-date sanctions data
- Incorporate options for rapid on-boarding
- Have the ability to be tailored to unique business needs
- And more

With a best-in-class sanctions screening solution in place, businesses are better prepared to hedge against risk and maintain high levels of productivity.

About Descartes' Solutions

In today's changing global regulatory landscape, leveraging accurate sanctions content is more important than ever to help avoid fines, improve processes, and mitigate risk. Descartes' solutions provide companies with the ability to efficiently screen against a comprehensive database of official and unofficial sanctions lists.

Our sanctions content helps reduce risk by streaming data into leading ERPs and CRMs such as NetSuite, Salesforce, SAP GTS, Oracle GTM, and more. In addition, our expert team ensures that information seamlessly powers systems via a number of electronic methods and protocols such as via Application Program Interfaces (APIs)

Beyond this, our comprehensive and continuously updated toolset can help ensure compliance with U.S. and E.U. 50 Percent ownership requirements. The solution helps organizations to conduct critical due diligence by identifying beneficial owners, tracking important changes of ownership over time, storing results, and continuously screening individual names.

Our solution provides organizations of all sizes with easy-to-use options that quickly and efficiently screen sanctioned parties, tailor screening processes to fit unique risk parameters, and flag potential compliance issues for a prompt resolution.

Ask us more.

About Descartes

Descartes (Nasdaq:DSGX) (TSX:DSG) is the global leader in providing on-demand, software-as-a-service solutions focused on improving the productivity, performance and security of logistics-intensive businesses. Customers use our modular, software-as-a-service solutions to route, schedule, track and measure delivery resources; plan, allocate and execute shipments; rate, audit and pay transportation invoices; access global trade data; file customs and security documents for imports and exports; and complete numerous other logistics processes by participating in the world's largest, collaborative multimodal logistics community. Our headquarters are in Waterloo, Ontario, Canada and we have offices and partners around the world. Learn more at www.descartes.com, and connect with us on LinkedIn and Twitter.

The Descartes Systems Group Inc.
120 Randall Drive, Waterloo, Ontario, N2V 1C6, Canada
Toll Free 800.419.8495 | Int'l 519.746.8110
www.descartes.com | info@descartes.com

Network. Applications. Content. Community.

Uniting the People & Technology
That Move the World.