Cartels as terrorist organizations

The challenges posed to companies by the new U.S. decree

Introduction

On January 20, 2025, the U.S. government issued an executive order declaring a national emergency and initiating a process to designate certain cartels and international drug trafficking organizations as Foreign Terrorist Organizations (FTOs) or Specially Designated Global Terrorists (SDGTs). This measure seeks to intensify efforts against these groups by imposing stricter sanctions and harsher legal measures. Designating cartels as FTO or SDGT would increase the risks for entities both in the U.S. and internationally that interact with them, which could lead to serious legal and financial consequences. The executive order instructs cabinet members to recommend which cartels should receive these designations, marking a significant shift in strategy to combat international drug trafficking.

What changed after the recent signing of the new decree?

The recent decree represents a drastic turnaround, which elevates the status of cartels to terrorist entities. This expands the legal tools for the U.S. government, enabling the following:

Asset freeze:

It affects not only the cartels, but also those who maintain commercial relations with them.

Legal sanctions:

Includes criminal measures against individuals and companies that provide material support.

Military or coercive action:

Justified under the anti-terrorist framework.

Key areas of focus for companies in the short term

Given the designation of Mexican cartels as foreign terrorist organizations, companies operating in Mexico and having commercial ties with the United States must prioritize certain strategic areas to adapt to new challenges. Here are the main areas on which they should focus their efforts:

Strengthen sanctions compliance policies

Ensuring compliance with international regulations will be essential to avoid sanctions and maintain strong business relationships:

- Conduct internal audits focused on key areas such as payments, contracts, and third-party relationships to identify irregularities and regulatory risks.
- Implement solutions based on artificial intelligence and data analytics to track suspicious movements and ensure transparency in operations.
- Invest in training programs to update staff on regulations and their impact on the business.

Improve risk management in supply chains

Companies must protect their supply chains against disruptions and links to illicit activities by:

- Conducting thorough vetting of vendors, assessing their legal, reputational, and financial integrity, and developing risk maps in sensitive areas.
- Implementing traceability systems to trace the origin of products and ensure that they are not linked to illicit activities.
- Analyzing suppliers and logistics routes to identify possible risks in areas controlled by cartels.
- Diversifying routes and suppliers, redesigning logistics strategies and looking for new partners in safer regions.
- Increasing investments in security in the transport and storage of goods to minimize extortion and operational risks.
- Adding or reinforcing clauses that allow for termination of the contract if a supplier is designated as an FTO or SDGT.
- Ensuring that contracts provide legal protection against potential breaches.
- Conducting compliance audits with high-risk third parties.

Corporate reputation protection

Public perception and the trust of international partners are critical to sustaining operations and attracting investment. This can be strengthened by implementing the following:

- Implementing transparency policies to demonstrate regulatory compliance and disengagement from illicit activities.
- Investing in communication strategies to reinforce the confidence of investors, customers and business partners.
- Establishing mechanisms to maintain the trust of foreign partners, especially in key markets such as the United States.

Protection of human capital

The safety and well-being of staff must be a strategic priority. Some key recommendations include the following:

- Identify vulnerable areas and adjust staff deployment and mobility strategies.
- Design customized safety protocols with preventive measures and contingency strategies.
- Implement psychological support programs to address stress in high-risk settings.
- Conduct detailed employment background checks for sensitive roles.
- Train staff on the new regulatory environment and the risks of dealing with FTOs or SDGTs.
- Encourage internal reporting of suspicious activity to avoid unintentional legal exposure.

Adaptation of mergers and acquisitions (M&A) policies

The M&A market requires greater care in assessing risks when contemplating a transaction. The following activities are worth considering:

- Conduct thorough due diligence to ensure regulatory compliance and rule out illicit links.

- Monitor asset valuations in high-risk regions to identify opportunities or avoid losses.
- Take a conservative stance on transactions in sensitive regions or sectors.

Strengthening cybersecurity

The increase in the volume of sensitive data to comply with regulations, as well as the possibility for cartels to diversify their illicit activities into cybercrime, makes it necessary to:

- Strengthen cybersecurity infrastructure.
- Conduct cyberattack drills.
- Train staff in cybersecurity.
- Assess the cybersecurity of vendors that handle sensitive data or have access to key systems.
- Include specific cybersecurity clauses in contracts with strategic partners.
- Perform frequent scans to identify vulnerabilities and fix them before they are exploited.
- Monitor corporate networks in real-time to detect unusual activity.

Forensics-based crisis management

- Establish multidisciplinary crisis teams with skills in communication, data analysis, and operational management.
- Conduct crisis drills to test the ability to respond to critical scenarios.
- Design clear internal and external communication protocols to manage crises with transparency.
- Perform post-crisis analysis to investigate root causes and improve preventive strategies.

Anti-Money Laundering (PLA)

The designation of cartels as FTO places a greater emphasis on the prevention of money laundering:

- Implement robust Know Your Customer (KYC) procedures with background checks and ongoing reviews.
- Use automated systems to monitor financial transactions and detect suspicious patterns.
- Update internal anti-money laundering policies based on regulatory changes and specific risks.
- Regularly audit cash flows to identify potential inconsistencies.
- Design training programs for employees on identifying and reporting red flags related to money laundering.

Conclusion

The designation of Mexican cartels as Foreign Terrorist Organizations by the United States presents challenges and opportunities for businesses in Mexico. Companies must not only comply with current regulations, but also anticipate future sanctions expansions. Being proactive now can prevent financial, legal, and reputational damage in the future.

Likewise, companies that adjust their operations will be able to mitigate risks, protect their assets and maintain sustainable operations. In the medium term, the use of advanced tools and more rigorous management of suppliers and supply chains will strengthen its position. The integration of anti-money laundering, risk management and tax compliance policies will make companies more competitive and ethical.

This challenging environment is also an opportunity to innovate and adapt, ensuring a more sustainable and competitive future.

Contacts

José Claudio Treviño, CFE, CFI
Partner Forensic & Financial Crime
Deloitte Spanish Latin America
jotrevino@deloittemx.com

Fernando Peyretti
Partner Forensic & Financial Crime
Deloitte Spanish Latin America
fpeyretti@deloittemx.com