# Managing Evolving Third Party Risks: Exploring Best Practices

February 5, 2026

GIBSON DUNN

Control Risks

# MCLE Certificate Information

## MCLE Certificate Information

- Approved for 1.0 hour General PP credit.
- CLE credit form must be submitted by ***Thursday, February 12th.***
- Form Link:

  https://gibsondunn.qualtrics.com/jfe/form/SV_1NVVJbxgjil65AG

  Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.

- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

# PANELISTS

GIBSON DUNN

Control Risks

**Oleh Vretsona**
Partner
Washington, D.C.

**Victor Tong**
Associate Attorney
London

**Michele Wiener**
Partner
Washington, D.C.

**Ulla Pentinpuro**
Principal
Mexico City

# AGENDA

**01** **The Evolving Landscape**

FCPA enforcement trends post-February 2025 pause, global regulatory convergence, resource constraints with expanding vendor portfolios

**02** **New Trends and Developments**

FTO designations, AI governance gaps, shifting focus to supply chain transparency and national security

**03** **Governance Frameworks**

Stakeholder roles, risk acceptance frameworks, operating models, escalation authority, and portfolio optimization

**04** **Insights and Opportunities**

Analytics case studies, monitoring frameworks, recent enforcement lessons, practical implementation roadmaps

# THE EVOLVING LANDSCAPE

01

# FCPA Enforcement: The Third-Party Connection

## Historical Enforcement Pattern

- **90%+** of FCPA enforcement actions involve third-party intermediaries—agents, consultants, distributors, joint venture partners.
- Direct bribery by company employees is now the exception, not the rule.
- Third parties used to create perceived distance from corrupt payments while maintaining deniability.

## Administration Comparison (Total DOJ/SEC FCPA Actions)

- **Obama II (2012-16)**: 126 actions.
- **Trump I (2017-20)**: 164 actions—30% higher than Obama II.
- **Biden (2021-24)**: 96 actions.
- **2024 alone**: 40 enforcement actions.
- **Trump II (2025)**: 6 actions.

## The February 2025 Pause—and What Came Next

- **Executive Order paused** FCPA enforcement for 180 days pending policy review.
- **June 2025 Guidelines** resumed enforcement with new priorities: cartels/TCOs, U.S. economic/national security interests, individual accountability.
- **FCPA remains in DOJ's top 10 white collar priorities** (May 2025 Criminal Division memo).
- **August 2025: First post-pause corporate resolution** (Liberty Mutual/India)—declination under the revised Corporate Enforcement Policy.
- **November 2025: 50% discount in Part III resolution** (Comcel/Guatemala)—voluntary self-disclosure, cooperation, and remediation still decisive factors.

# Global Risk: Trade and Supply Chain Controls

- The Trump Administration has signaled an intention to **increase criminal enforcement of tariffs and customs as it relates to fraud and national security issues**.
- Trade, tariff, and customs fraud can involve:
  - **Making false statements** in connection with an import (e.g., the country of origin in an effort to avoid tariffs).
  - **Failing to pay customs duties**, including antidumping, countervailing, and Section 301 tariffs.
  - **Misclassifying imports** to avoid certain customs duties or tariffs.

This focus on supply chain invites several areas for **vigilant compliance consideration** in fraud, including:

- "Country of origin" determinations, due diligence on suppliers, and the potential for downstream liability if indirect suppliers are in jurisdictions under tariff or sanctions pressure.
- Increased verification and documentation requirements along the supply chain; stronger "know your supplier" and vendor risk controls.
- The administration may also equate a company's trading partners to alignment with U.S. national security or foreign policy goals; companies should review how their global footprint is viewed in that context.

# Regulatory Developments: A Global Convergence

## DOJ Evaluation of Corporate Compliance Programs (ECCP)

- **Published in September 2024**: DOJ's most recent updates to this guidance account for changing circumstances and new risks.
- "**Disruptive technology risks"**: The updates focused on technology/AI deployment and risk mitigation; leveraging company data for compliance purposes; and expanded whistleblower protection and encouragement.
- **Third-party considerations**: Continuous (not point-in-time) monitoring expected; data analytics for red flag detection; AI risk assessment required; lessons learned from peer incidents.
- **Third-party updates**: Prosecutors will consider whether and how Companies use data to assess vendor risk.

## Interagency Guidance on Third-Party Relationships

- **Collaborative effort:** This guidance, first issued in June 2023 and expanded in May 2024, reflects input from the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency.
- **Third-party Relationship Life Cycle**: Continuous monitoring of the life cycle includes (i) planning (whether third party is needed); (ii) due diligence and third-party selection; (iii) contract negotiations; (iv) ongoing monitoring (including subcontractor visibility); and (v) termination.
- **Governance**: Considerations include board-level oversight and accountability; independent reviews; documentation and reporting.

## BIS Affiliates Rule

- **Effective Date:** U.S. Department of Commerce's Bureau of Industry and Security issued an interim final rule effective September 29, 2025.
- **Scope:** The Affiliates Rule extends licensing requirements, exceptions, and review policies applicable to listed parties to any foreign affiliate owned 50 percent or more by one or more listed entities, significantly expanding the number of companies that fall under a license requirement.
- **Due diligence**: Companies would need to consider comprehensive diligence to include beneficial ownership of third-parties.
- **Suspended November 10, 2025**: BIS issued a final rule suspending the Affiliates Rule for one year, so it can evaluate U.S. national security and foreign policy interests.

# Regulatory Developments: A Global Convergence (cont'd)

## UK Failure to Prevent Fraud

- **ECCTA 2023, s.199**: In force from September 1, 2025. Large organizations criminally liable if associated person commits fraud for organization's benefit.
- **"Associated person" includes**: Employees, agents, subsidiaries, and any person performing services for or on behalf of the organization.
- **Threshold for "large organization"**: Meets 2 of 3 criteria: >250 employees, >£36m turnover, >£18m assets.
- **Defense**: "Reasonable procedures" to prevent fraud—mirrors Bribery Act adequate procedures framework.
- **Penalty**: No specific limit on fines; SFO has signaled aggressive early enforcement intent.

## EU Corporate Sustainability Due Diligence Directive

- **Scope (post-Omnibus I, December 2025)**: >5,000 employees AND >€1.5bn net turnover—70% reduction from original directive.
- **Application date**: July 26, 2029; Member State transposition by July 26, 2028.
- **Due diligence obligation**: Identify, prevent, mitigate adverse human rights and environmental impacts across own operations and value chain.
- **Penalties**: Up to 3% of net worldwide turnover. EU-harmonized civil liability regime removed—now governed by national law.

## EU Anti-Corruption Directive

- **Provisional agreement**: December 2, 2025. First EU-wide criminal law harmonizing corruption offences across all Member States.
- **Offences harmonized**: bribery (public and private), misappropriation, trading in influence, obstruction of justice, enrichment from corruption.
- **Corporate penalties**: Fines up to 3-5% of worldwide turnover or €24-40m, depending on offence.
- **Prevention requirements**: Member States must adopt national anti-corruption strategies and establish independent specialized bodies.

# NEW TRENDS AND DEVELOPMENTS

02

# Shifting Focus for Third Party Risk

## Supply Chain Transparency & Resilience

Organizations need visibility into subcontractors and fourth-party relationships to identify concentration risks and ensure business continuity.

## Trade & Tariff Compliance

To ensure compliance with international trade regulations and avoid supply chain disruptions or penalties third party relationships, practices, documentation and behaviors need to be scrutinized.

## Foreign Terrorist Organizations

Third party assessments of links of third-parties to cartels/TCOs, including cartel-controlled businesses should include enhanced evaluation of high-risk third parties.

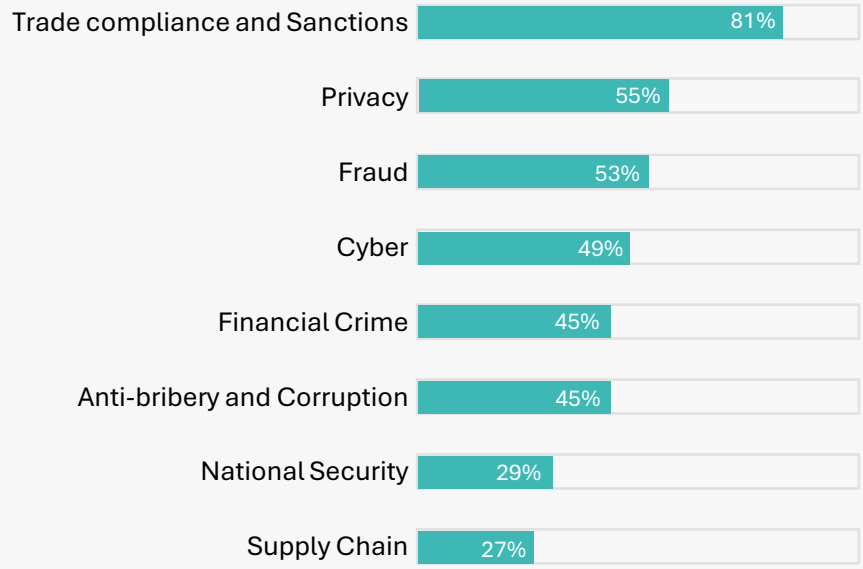
## AI & Algorithmic Risk Assessment

Due diligence must evaluate third parties' use of AI systems for bias, explainability, and compliance with emerging AI regulations.

## Enhanced Cybersecurity Due Diligence

Vendors must demonstrate robust security frameworks, including incident response plans, data encryption standards, and regular security audits to meet regulatory expectations.

**Figure 2 | Areas of responsibility and effectiveness**



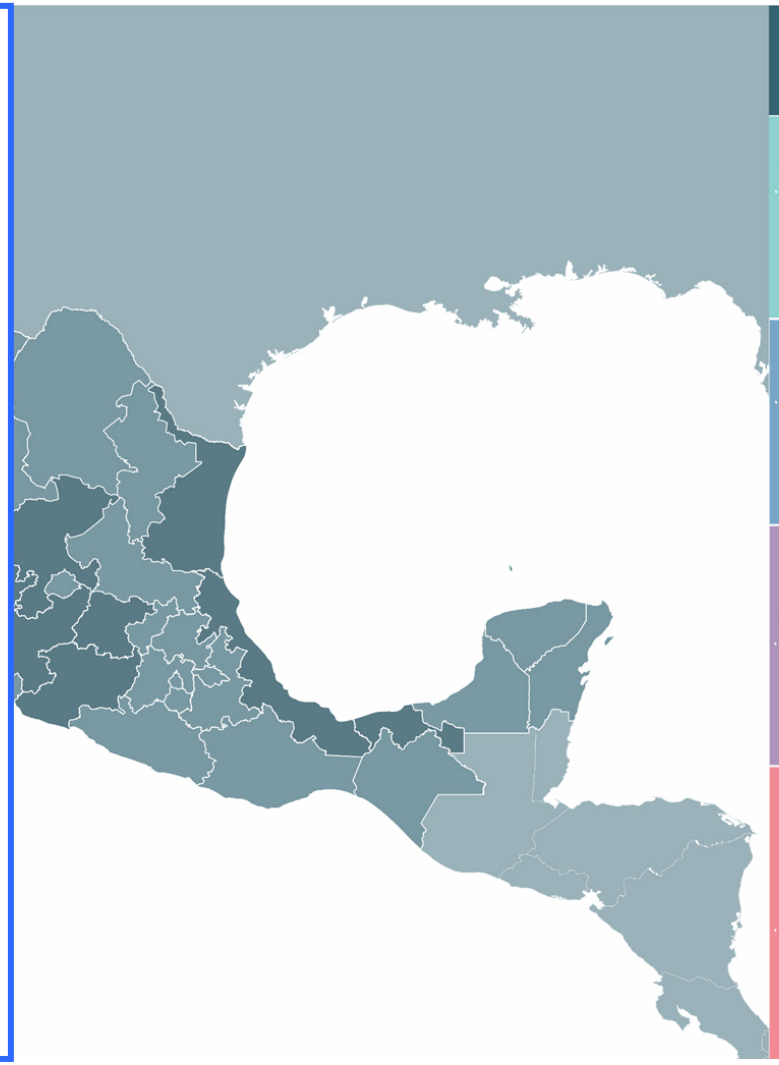

**Q3: For which areas do you have responsibility?**

Corporate Compliance Survey, Control Risks 2025

# US: February 2025 Cartel Designations

## The Designations (as of February 20, 2025)

- Eleven organizations across Mexico and LATAM designated as Foreign Terrorist Organizations.
- Focus on cartels is a high priority for the Trump administration and enforcement has begun.
- The designated cartels are involved in a vast array of illicit activities and “legitimate” businesses.
- The risk exposure can manifest itself in a variety of ways; direct or indirect through third parties. This can vary significantly from location to location and can depend on the sector.



| Location | Dominant group | Key sectors | Main red flag sources |
|---|---|---|---|
| Tamaulipas state  | Gulf Cartel, Northeast Cartel | • Logistics<br>• Construction | • Unions<br>• Intermediaries (”*gestores*”) |
| Michoacán state  | United Cartels, La Familia Michoacana | Agriculture | • Unions<br>• OCG ties with local communities |
| Gulf states (Tamaulipas, Veracruz and Tabasco)  | Gulf Cartel, CJNG | Oil and gas | • Intermediaries<br>• Unions |
| Bajío states (mainly Jalisco, Zacatecas and Guanajuato)  | CJNG | • Real estate<br>• Logistics<br>• Construction<br>• Mining | • Local service providers<br>• Intermediaries<br>• Unions<br>• OCG ties with local communities |

# US: February 2025 Cartel Designations (cont'd)

## Industries with Heightened Exposure

- **Logistics and freight forwarding** (particularly U.S.-Mexico cross-border): customs brokerage; warehousing in border regions; carriers routinely face derecho de paso ("right of way") extortion demands.
- **Agriculture and food processing** (avocados, limes, and produce from cartel-controlled regions such as Michoacán and Jalisco): supply chains are difficult to verify back to farm level.
- **Mining and oil & gas** as their operations are usually visible and immovable, and both industries tend to operate in cartel ridden remote areas.
- **Real estate** (high-value residential and commercial property purchases used as money laundering vehicles): luxury developments particularly vulnerable.
- **Financial services** (correspondent banking, remittances, trade finance, currency exchange): FinCEN has issued geographic targeting orders requiring enhanced reporting for border-area money services businesses.
- **Any business with Mexican or LATAM supply chain exposure**: cartels have infiltrated procurement functions, tourism, hospitality, and manufacturing operations.

## Mitigation measures

- **Screen against FTO and SDGT lists** (not just OFAC SDN); these designations now appear on the Consolidated Screening List with distinct tag suffixes.
- **Beneficial ownership verification** in high-risk jurisdictions; complex ownership structures and nominee arrangements may obscure cartel ties. Conduct human source enquiries.
- **Geographic risk assessment** for Latin American operations; map exposure to known cartel territories and transit corridors.
- **Monitor for extortion payments**, "security fees," derecho de paso, or unexplained cost increases in supply chain; require third-party payment audit trails.
- **Train personnel on cartel-specific red flags**: demands for cash payments, pressure to use particular suppliers, infiltration of logistics or procurement functions, and requests to route shipments through specific intermediaries.

# Legal consequences and implications of FTO designation

## Material Support Liability

- **18 U.S.C. §2339A**: Criminal to provide "material support or resources […] knowing or intending" that they be used by individuals to carry out terrorist activities; no FTO designation necessary.
- **18 U.S.C. §2339B**: Criminal to "knowingly provide[] material support or resources" to designated FTOs.
- "**Material support**" includes money, financial services, lodging, training, transportation, personnel, weapons, equipment, services.
- **Penalties**: Imprisonment up to 15 years for §2339A and 20 years for §2399B; life if death results; no intent to support terrorism required—only intent to provide the resources.

## Third-Party Risk Implications

- **OFAC 50% rule**: Entity owned 50%+ by designated persons is itself blocked—applies to cartel-controlled businesses.
- **Willful blindness is not a defense**: "Conscious avoidance" of red flags can establish knowledge.
- **Chiquita Brands precedent (2024)**: $38.3m verdict for paying Colombian paramilitary groups—demonstrates civil liability for third-party payments reaching violent organizations.
- **DOJ FCPA Guidelines (June 2025)** now prioritize schemes connected to cartels/TCOs—any link, however indirect, increases enforcement risk.

## Example of Cartel Nexus

- European multinational with manufacturing plant in northern Mexico.
- **Potential exposure** to designated cartel through EPC supplier in charge of constructing an extension to a plant.
- EPC provider extorted by a labor union
- **Investigation of the facts** while ensuring business continuity
- **Scenario workshop** with key stakeholders
- **Security component**: keeping everyone safe throughout the process.

# AI Governance: The Emerging Risk

**13%**

Organizations have already experienced a breach of AI models or applications

**97%**

Lacked AI access controls, of the organizations that experienced AI breaches

**83%**

Lack automated controls to prevent sensitive data entering public AI tools

**23%**

Do not monitor whether vendors use AI in service delivery (down from 37% in 2024)

## Key Questions to Ask Vendors

- Does your product or service use AI or machine learning?
- Is our data used to train AI models?
- What controls prevent our data from being exposed via AI tools?
- Do you have a formal AI governance policy?
- How do you detect and manage “shadow AI” within your organization?

## Actions to Take Now

- Add AI-specific questions to vendor assessment questionnaires.
- Review existing contracts for AI usage rights and data training provisions.
- Establish policy on acceptable vendor AI usage.
- Require disclosure of AI sub-processors and fourth-party AI tools.
- Include AI incident notification requirements in contracts.

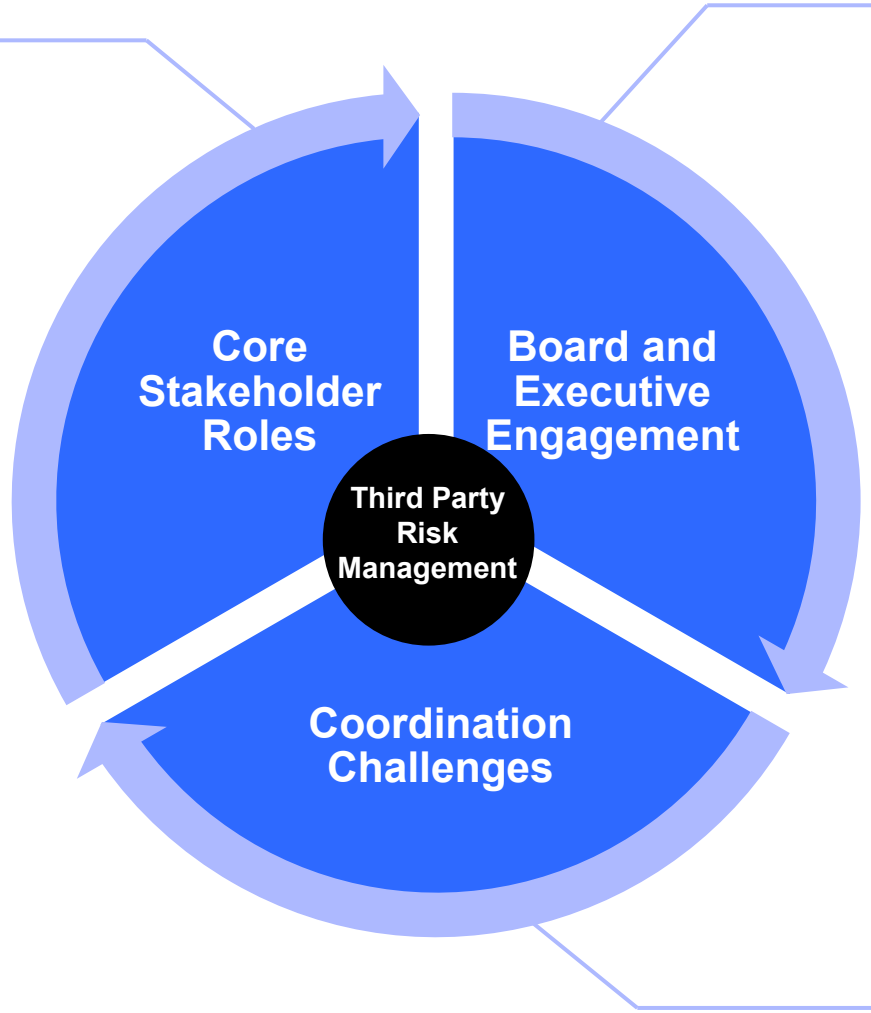
Source: IBM, Cost of a Data Breach Report 2025 (July 2025); Kiteworks, 2025 AI Data Security and Compliance Risk Study; Venminder State of Third Party Risk Management Survey 2025.

# GOVERNANCE FRAMEWORKS

03

# Third Party Risk Is Everyone's Responsibility

- **Procurement/Sourcing**: Vendor selection, contract negotiation, commercial terms, supplier management.
- **Legal**: Contract drafting/review, regulatory compliance, dispute resolution, liability management.
- **Information Security**: Cyber assessments, technical due diligence, security reviews, continuous monitoring.
- **Compliance**: Regulatory mapping, sanctions screening, anti-corruption due diligence, audit coordination.
- **Business Owners**: Relationship management, performance monitoring, operational integration, daily oversight.
- **Finance**: Payments, financial due diligence, spend analytics, budget oversight.
- **Internal Audit**: Independent assessments, control testing, program reviews.




- **Boards have now become significantly more engaged on cybersecurity**, with 77% of directors now discussing the material and financial implications of cyber incidents, a 25-point jump from 2022, according to National Association of Corporate Directors.
- **DOJ ECCP provides** that senior management should set tone of compliance for entire company.
- **DORA requires management body approval** of ICT risk management framework and third-party strategy.
- **SEC cybersecurity rules** require disclosure of board oversight of cybersecurity risk.
- **Personal liability exposure** increasing: directors can face derivative suits for oversight failures.

- **Siloed ownership**: Procurement owns contracts, InfoSec owns security, Compliance owns regulatory—no one owns the whole picture.
- **Conflicting incentives**: Procurement measured on cost savings may resist security requirements that delay deals.
- **Communication gaps**: Business owners may not know what Legal negotiated or what InfoSec assessed.
- **Accountability diffusion**: When everyone is responsible, no one is accountable.

# Risk Management and Compensating Controls

## The Reality: Not Every Vendor Will Meet Every Requirement

- **Critical business need** may require vendor with identified deficiencies.
- **Remediation timelines** may not align with business timelines.
- **Limited alternatives** in specialized markets (*e.g.*, sole-source technology).
- **Cost of control** may exceed cost of risk in low-impact scenarios.

## Formal Risk Management Framework

- **Document the Risk**: Specific deficiency identified, potential impact, likelihood assessment, risk rating.
- **Justify the Need**: Business rationale for proceeding despite risk, alternatives considered and rejected.
- **Define Compensating Controls**: Specific mitigations that reduce residual risk to acceptable level.
- **Set Conditions**: Time-bound acceptance with remediation deadline; trigger conditions for reassessment.
- **Obtain Appropriate Approval**: Risk acceptance authority based on residual risk level.
- **Monitor and Review**: Track remediation progress; validate compensating control effectiveness.

## Compensating Controls Toolkit

- **Enhanced monitoring**: More frequent assessments, real-time security monitoring, increased audit rights, sample testing of invoices, payment pattern analysis.
- **Contractual protections**: Expanded indemnification, cyber insurance requirements, performance bonds.
- **Operational controls**: Data encryption, access restrictions, network segmentation, transaction limits.
- **Probationary periods**: Limited initial scope with expansion contingent on performance.
- **Root cause analysis requirements**: Vendor must provide root cause analysis for any incidents.
- **Exit planning**: Accelerated exit strategy if risk materializes.

# Common Operating Model Approaches in Practice

## Different organizational contexts may favor different approaches to third party risk ownership

| | Centralized | Decentralized | Hybrid |
|---|---|---|---|
| **Ownership** | Dedicated third party risk management team owns entire lifecycle | Business units manage their own vendors | Central team sets framework; business units execute with oversight |
| **Strengths** | Consistency; expertise concentration; clear accountability; efficient for smaller portfolios | Business context; relationship ownership; faster decisions; scalable across large organizations | Combines consistency with scalability; leverages business expertise with central oversight; most flexible |
| **Weaknesses** | Bottleneck risk; limited business context; doesn't scale well; can become disconnected from operations | Inconsistency; duplication; skill gaps; compliance gaps; difficult to aggregate risk view | Complexity; requires clearly defined roles; training burden; potential for confusion on responsibilities |
| **Best For** | Smaller organizations; highly regulated industries; limited vendor portfolios | Large decentralized organizations; diverse business units; mature risk culture | Most organizations; balances control with scalability |

### Hybrid Model Implementation

- **Central team responsibilities**: Framework design, policy setting, tool selection, training, reporting, critical vendor oversight, escalation management.
- **Business unit responsibilities**: Day-to-day relationship management, performance monitoring, operational risk assessment, first-level due diligence for low/medium risk vendors.
- **Clear handoff points**: Critical/high-risk vendors require central team involvement; standard risk vendors managed by business with central oversight.

# Escalation and Dispute Resolution: Illustrative Framework Considerations

## Escalation frameworks will vary based on organizational context and risk appetite

| Escalation | Typical Scope, Potential Triggers, Resolution Considerations |
|---|---|
| **Low** | • **Scope**: Operational (Business Owner to Vendor Account Manager)<br>• **Triggers**: Day-to-day issues; service level agreement misses; minor quality problems<br>• **Resolution**: Typically 5 business days; documented in vendor file |
| **Moderate** | • **Scope**: Management (Department Head to Vendor Senior Management)<br>• **Triggers**: Recurring issues; significant performance failures; contract interpretation disputes<br>• **Resolution**: Typically 15-20 business days; TPRM team engaged |
| **Medium** | • **Scope**: Executive (VP/C-Suite to Vendor Executive)<br>• **Triggers**: Material breaches; strategic relationship issues; significant financial disputes<br>• **Resolution**: Typically 30-45 days; executive sponsor involvement |
| **High** | • **Scope**: Legal/External (GC involvement)<br>• **Triggers**: Contract termination; litigation; regulatory reporting; mediation/arbitration<br>• **Resolution**: Variable timeframe based on complexity; legal counsel leads; board notification if material |

### Illustrative Trigger Examples

- **Security incident affecting company data** → Immediate escalation (typically medium level or higher) with security team engagement
- **Repeated SLA failures** → Moderate
- **Material financial dispute** (threshold varies by organization size/risk appetite) → Medium
- **Regulatory inquiry involving vendor** → High
- **Vendor bankruptcy/acquisition** → Medium + exit planning
- **Unresolved Level 1 issue for >10 days** → Auto-escalate to Moderate

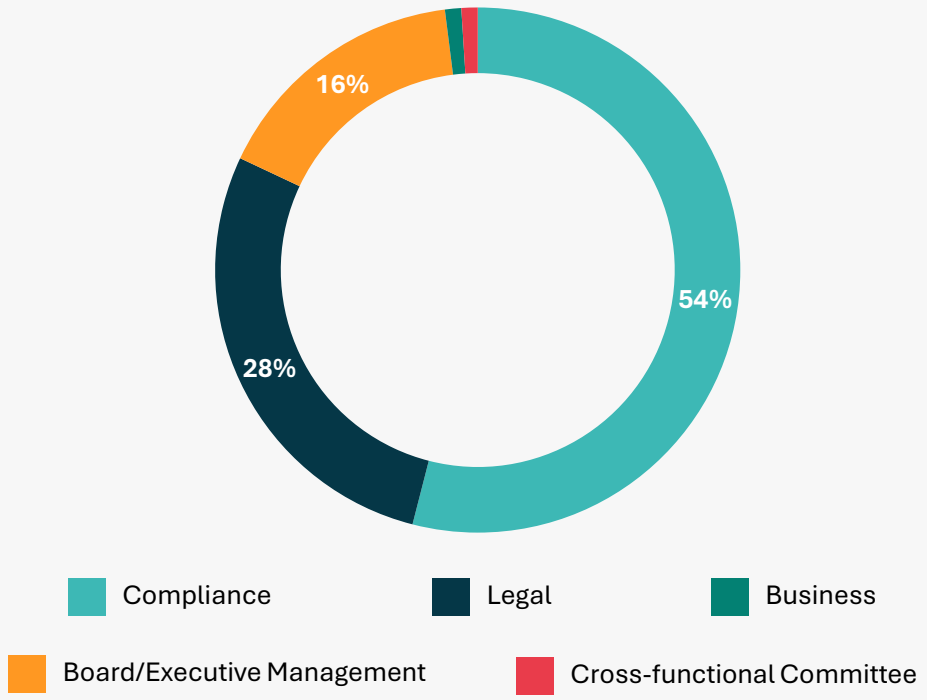
### Common Documentation Elements to Consider

- Issue description and business impact.
- Timeline of events and communications.
- Remediation attempts and vendor response.
- Resolution and root cause analysis.
- Lessons learned and preventive measures.

# Case Study: The Final Say

- Multinational with global operations inquired as to best practices concerning escalation of disputes over the approval or retention of third parties.
- Benchmarking revealed that many companies choose to handle disputes on an **ad hoc and informal basis**.
- Companies typically fall into one of three categories when resolving escalations:
  - First, **business** has final decision-making authority but is exercised with significant input from Legal / Compliance.
  - Second, **Legal / Compliance** has final decision-making authority, especially with respect to high-risk parties.
  - Third, a **multidisciplinary team** has final authority.
- Companies that faced a **serious compliance** event (e.g., resolution or investigation) are more likely to **give greater authority to Legal / Compliance**.
- Legal / Compliance often plays a significant role no matter final authority.

**Figure 3 | Final decision-making function**




**Q7: If there is a disagreement between the business and compliance on an issue (for example, whether to engage with a third-party that is high risk), who has the final decision-making authority**

GIBSON DUNN Control Risks

# INSIGHTS AND OPPORTUNITIES

04

# Monitoring and Analytics: A Case Study

**Analytics-driven segmentation** of a reseller ecosystem for customer offboarding decisions and deep dive audits

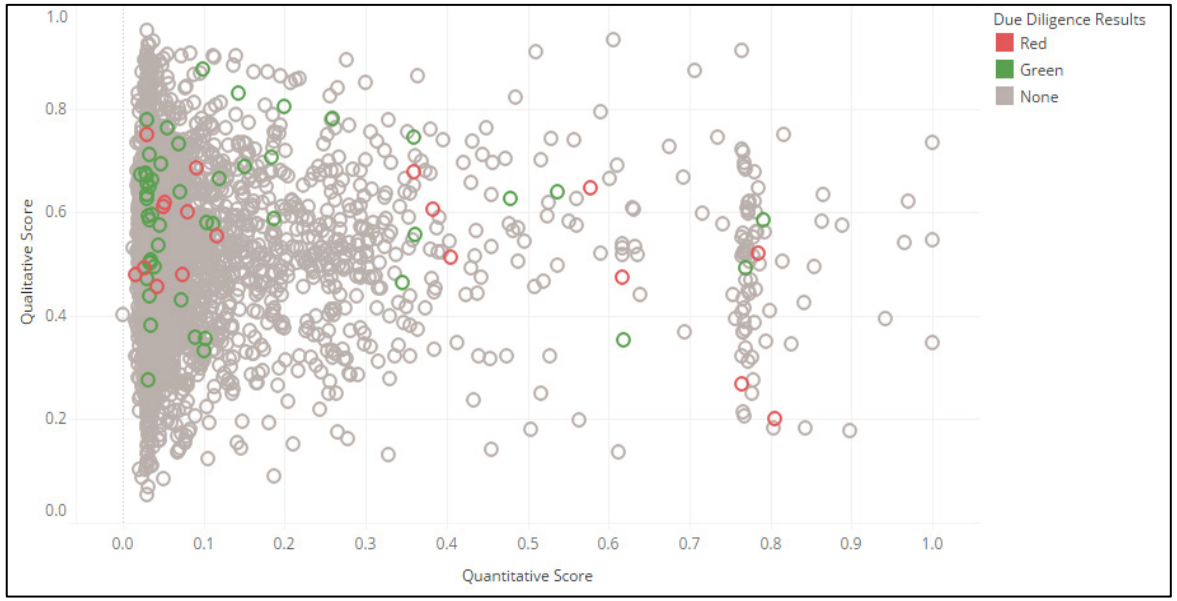
A global technology company sought a more systematic, data-driven way to understand the risk profile of its reseller ecosystem and to prioritize where deeper diligence and monitoring were warranted.

Control Risks developed a simple scoring framework combining:

- A ***quantitative dimension*** reflecting **commercial importance** (e.g. revenue contribution, sales volume, recent growth trends, etc.); and,
- A ***qualitative dimension*** reflecting **early-stage risk indicators** derived from open-source and contextual review, such as potential conflicts of interest, limited or inconsistent digital footprint, mismatches between registered and operating locations.

By viewing these dimensions together, the company was able to segment its reseller population rather than treating all partners uniformly.

In practice, this enabled the company to **identify a long tail of high-risk, low-impact partners appropriate for offboarding**, as well as a smaller set of **high-revenue partners with elevated risk signals that warranted enhanced monitoring or deeper due diligence**. The framework also provided a repeatable screening layer that now supports ongoing, risk-based third-party monitoring across regions.



# Monitoring and Analytics: The Art of the Possible

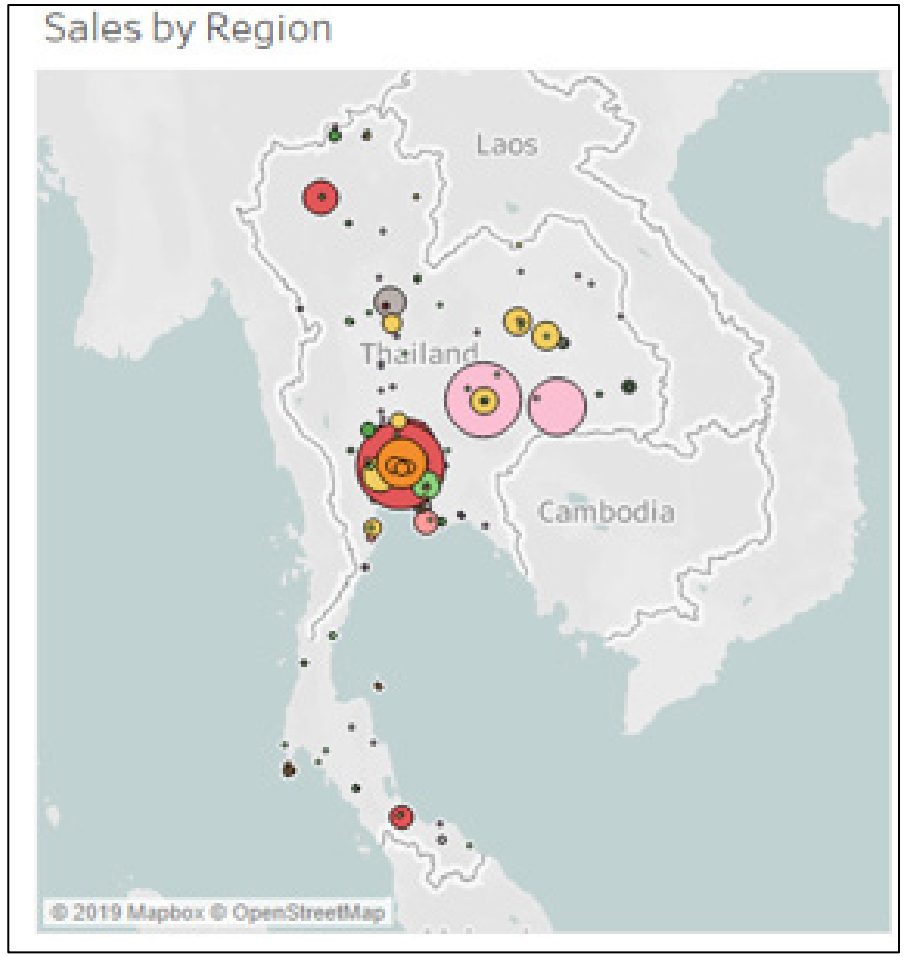
## Rethink your existing data

- Sales & Revenue Data → Concentration risk, dependency risk, continuity/resiliency risk
- Vendor Master Data → Change patterns, Anomalies, Conflicts of Interest
- Payment Data → Behavioral shifts, unusual flows and patterns of payment
- Onboarding and DD Data → Identify emerging risks through living profiles

## Blend and combine data

- *Sales + Customer Master + Onboarding/DD*
  **= Sales Ecosystem Risk**
- *Payments + Vendor Master + Contract Data*
  **= Supplier Payment Risk**
- *Shipping/Logistics + Location Data + OSINT*
  **= Supply Chain Routing Risk**
- *Sales + Distributor Profile + Shipping/Logistics*
  **= Sales Channel Integrity Risk**

## External data enrichment




GIBSON DUNN Control Risks

# Defining the Risks Managed: Red Flags Checklist

## Payment and Financial

- Requests for unusual payment terms (cash, cryptocurrency, third-country accounts)
- Commission rates significantly above market norms for the service
- Requests to split payments across multiple entities/invoices
- Invoices lacking specificity about services rendered
- Requests for large upfront payments or retainers
- Payments to jurisdictions unrelated to where services performed

## Government Connection

- Vendor owned by or employs current/former government officials
- Close family relationship between vendor principals and decision-makers
- Vendor recommended by government officials rather than competitive process
- Vendor's primary qualification is "relationships" rather than technical capability
- Recent formation of entity coinciding with contract opportunity

## Due Diligence Resistance

- Reluctance to disclose beneficial ownership or corporate structure
- Refusal to provide references or allow customer contact
- Objection to audit rights or compliance certification requirements
- Inconsistencies between information provided and independent verification
- Pressure to expedite onboarding and bypass normal processes

## Reputational & Compliance

- Adverse media coverage related to fraud, corruption, or sanctions violations
- History of regulatory enforcement actions or consent orders
- Principals with criminal history or association with sanctioned parties
- Operation in high-risk jurisdictions (CPI <40) without adequate explanation
- Previous termination by other companies for compliance reasons

# Recent Third-Party Incidents

## Exclusive Networks Corporate SAS CJIP (June 2025)

- **Summary:** PNF reached a judicial public interest agreement (CJIP) with Exclusive Networks to resolve allegations that it paid bribes through third parties in India, Indonesia, Malaysia, Thailand, and Vietnam. According to the resolution, the company's former risk and compliance manager reported concerns about the use of third parties to the PNF after he raised concerns internally but the company allegedly took no action.
- **Sanction:** €16.1 million (~$18.5 million).
- **Lesson:** Enforcers expect companies to follow up on and remediate audit findings, and the failure to do so can support charges against a company.

## Liberty Mutual Insurance Company Declination (August 2025)

- **Summary:** DOJ issued a declination letter to Liberty Mutual to resolve allegations that the company's India subsidiary paid bribes to officials at six state-owned banks, including by classifying the payments as marketing expenses and using third-party intermediaries to make the payments to the officials.
- **Sanction:** $4.7 million.
- **Lesson:** Companies should include members of corporate family in risk assessments evaluating controls and policies regarding third-party management.

## Kontrolmatik Teknoloji Enerji Ve Mühendislik A.Ş. World Bank Debarment (December 2025)

- **Summary:** The World Bank Group announced it reached a settlement with Kontrolmatik in connection with fraudulent and obstructive practices. According to the press release, Kontrolmatik submitted fabricated past performance documents to meet bid requirements for a project-financed contract and impersonated a third party to verify these documents.
- **Sanction:** 24-month sanction period, consisting of 12 months condition debarment and 12 months conditional non-debarment.
- **Lesson:** Companies should consider evaluating and enhancing procurement processes and controls as they relate to third parties.

# KEY TAKEAWAYS

05

# Key Takeaways

## 1 Strategic Imperative

Third party risk has evolved beyond compliance—it is now a strategic governance imperative requiring top-level accountability and cross-functional integration to address emerging threats from cartels, AI risks, and supply chain complexities.

## 2 Regulatory Shift

Regulatory convergence globally demands continuous monitoring capabilities rather than point-in-time assessments, with legal and compliance teams increasingly holding final authority on high-risk vendor decisions.

## 3 Emerging Threat

The February 2025 cartel FTO designations create material support liability exposure through third-party relationships, requiring enhanced due diligence for Latin American operations and supply chains.

## 4 Operational Excellence

Organizations must move from reactive vendor management to predictive risk intelligence—leveraging analytics, external data sources, and AI augmentation to identify risks before they materialize.

## 5 Early Warning

Employee concerns and audit findings remain the strongest early warning indicators, but only if organizations establish systematic investigation processes and capture lessons from both internal incidents and peer enforcement actions.

## 6 Implementation Priority

Success requires balancing quick wins (vendor inventory completion, KRI implementation, contract updates) with long-term capabilities (integrated platforms, predictive analytics, fourth-party visibility) while acknowledging that formal risk acceptance frameworks are essential given business realities.

# Upcoming Programs

# 2025/2026 White Collar Webcast Series

| Date and Time | Program | Registration Link |
|---|---|---|
| **Wednesday, February 11, 2026 9:00 AM – 10:00 AM PT 12:00 PM – 1:00 PM ET** | **Crime Fraud Litigation**<br>Moderator: George Hazel<br>Presenters: M. Kendall Day, Karin Portlock, Jeremy Robison | Event Details |
| **Tuesday, February 24, 2026 9:00 AM – 10:00 AM PT 12:00 PM – 1:00 PM ET** | **Commodities Enforcement and the CFTC**<br>Moderator: David Burns<br>Presenters: Amy Feagles, Jeffrey Steiner | Event Details |
| **Thursday, February 26, 2026 9:00 AM – 10:30 AM PT 12:00 PM – 1:30 PM ET** | **State AG Developments**<br>Moderator: Winston Chan<br>Presenters: Karin Portlock, Chris Chorba, Eric Vandevelde, Prerak Shah | Event Details |


GIBSON DUNN
Control Risks