



# Third Party & Sales Intermediary Risk: Mastering ABAC and AML Compliance



---

# Executive Summary

---

The world of third party and sales intermediaries (TPIs / SIs) is rapidly evolving, and organizations are increasingly turning to these intermediaries to expand their global reach. While these partnerships offer significant growth opportunities, they also present complex risk and compliance challenges, particularly in the realms of Anti-Bribery and Anti-Corruption (ABAC) and Know Your Customer/ Know Your Business (KYC/KYB) / Anti-Money Laundering (AML) regulations globally.

This guide illustrates how effective compliance programs are vital for mitigating risks associated with third-party relationships, highlighting best practices, notable regulatory actions, as well as the need for technology-enabled solutions.

The dynamic nature of global regulations and risk necessitates a technology-driven approach to compliance. By leveraging emerging technologies such as advanced analytics and AI-powered tools, organizations can enhance due diligence, transaction monitoring, and risk assessment processes, ensuring sustainable growth and maintaining stakeholder trust in an increasingly complex business environment.

---

# Case Study:

## Tech Giant's Counterfeit Crisis

### What happened?

---

Onur Aksoy was sentenced in May 2024 to over six years in prison for running a massive counterfeit trafficking operation. He sold fake Cisco equipment worth **over \$1 billion** through 19 companies, 15 Amazon storefronts, and 10 eBay stores. The counterfeit products ended up in American government systems, including those of the Navy, Air Force, and Army, as well as schools and hospitals. Despite warnings and confiscations as early as 2014, Aksoy continued his fraudulent activities, relying on Chinese suppliers for modified, substandard Cisco products.

### What are the consequences?

---

- **\$100 million** in restitution ordered to be paid by Aksoy.
- **Immeasurable operational and security risks** for affected organizations, potentially compromising government and healthcare systems.
- **Loss of trust** in online marketplaces and third-party sellers of networking equipment.
- Potential for **network failures, data breaches, and performance issues** due to substandard equipment.

### Why did they target Cisco products?

---

- **Scale:** Cisco is one of the largest networking equipment manufacturers globally, with products used by countless organizations worldwide.
- **Function:** Cisco products are critical infrastructure components for many networks, making them a lucrative target for counterfeiters.
- **Trust:** Organizations continued to purchase from unauthorized sellers, assuming products were genuine Cisco equipment due to the brand's reputation.

### How could this have been avoided or mitigated?

---

- **Enforcement** of anti-counterfeiting measures and **stricter oversight** of online marketplaces.
- Strong supply chain management with verified authorized resellers only.
- **Regular audits** and quality checks on purchased equipment, especially from third-party sellers.
- **Robust Third-Party Risk Management (TPRM)** with thorough vetting of suppliers.
- Implementation of product authentication measures by Cisco and education for customers on identifying genuine products.
- **Increased collaboration** between manufacturers, law enforcement, and online platforms to detect and prevent counterfeit sales.



## 2024 Landscape and Scope of Sales Intermediaries

---

The complexity of managing sales intermediaries has increased with expanding global markets. Global companies now collaborate with various partners across different regions who bring their own regulatory and operational challenges. This global presence necessitates a unified framework for ensuring compliance, data security and consistent service quality at scale.

Governments worldwide have tightened the regulatory environment by introducing legislation to secure information, prevent fraud, and promote fair trade practices. In this complex regulatory landscape, sales intermediaries must comply with international standards like FCPA, UK Bribery Act, and sanctions while staying on the right side of laws.

Competition is also now fiercer than ever, with established players continuously being challenged by new entrants and innovative startups. Sales intermediaries must be at the forefront of their competitors using state of the art technology and easily adaptable strategies to keep ahead of the pack and satisfy changing demands.

The modern-day consumer wants personalized real-time interaction and digital experience without any friction, and organizations and their sales intermediaries must adapt to emerging technologies to meet these expectations and stay on-pace with evolving expectations.



---

# Anti-Bribery & Corruption (ABAC): Strategic Imperatives for Intermediary Risk

---

When dealing with sales intermediaries and companies that help sell, promote, and distribute an organization's product, ABAC compliance is of paramount importance. Third parties can create exposure to the organization under regulations such as U.S Foreign Corrupt Practice Act (FCPA) or UK Bribery Act. When strictly adhered to, ABAC compliance ensures that organizational integrity and reputation is protected. Best practices include:

## ✓ Due Diligence:

Conduct thorough background checks on potential intermediaries, including their reputation, qualifications, and any history of corrupt practices.

## ✓ Contractual Safeguards:

Implement strong anti-corruption clauses in agreements with intermediaries, clearly prohibiting bribery, requiring compliance with relevant laws, and enforcing right-to-audit clauses.

## ✓ Training:

Provide comprehensive ABAC training to intermediaries to ensure they understand the company's policies and legal obligations.

## ✓ Monitoring and Payment Controls:

Regularly audit intermediaries' activities and financial transactions to detect any red flags or suspicious behavior, ensuring payments are commensurate with legitimate services rendered.

The enforcement landscape has seen significant activity in recent years, with several high-profile ABAC cases involving major companies. For instance, in 2022, the DOJ and SEC announced two significant settlements under the FCPA, including a \$460 million coordinated settlement. Other notable cases involved companies like Ericsson, with settlements ranging from **tens to hundreds of millions of dollars**.

---

**Framework to navigate the intricate global ABAC landscape:**

### Preventative Measures:

- Maintain and share ABAC policies with third parties as part of onboarding
- Create a configurable due diligence process (rules and criteria-based)
- Share training content both internally and externally
- Collate and store attestations

### Remedial Measures:

- Alert and flag any potential ABAC issues
- Notify all relevant stakeholders
- Identify alternative Third Parties to impacted one
- Ability to react, amend or correct workflows quickly and efficiently

### Reporting

- Full audit trail allows to demonstrate having preventive measures in place
- Continuous tracking of ABAC program
- Ability to respond to regulators reporting requirements quickly and easily

---

# Rising KYC / KYB and AML Scrutiny

---

While operating in high-risk jurisdictions across complex third party ecosystems, the KYC / KYB and AML risks faced by global organizations are critical. These organizations and their intermediaries must have a strong system of identity verification as an underlying step for effective KYC / KYB procedures. The necessity of understanding whom you do business with cannot be overstated. Robust KYC and KYB processes help verify the legitimacy of third-party entities, reducing the risk of fraud and ensuring regulatory compliance. The critical practices for KYC / KYB and AML must include:

✓ **Identity Verification:**

Implement robust processes to verify the identity of intermediaries and their beneficial owners.

✓ **Risk Assessment:**

Conduct risk assessments of intermediaries based on factors such as their location, customer base, and types of transactions they handle.

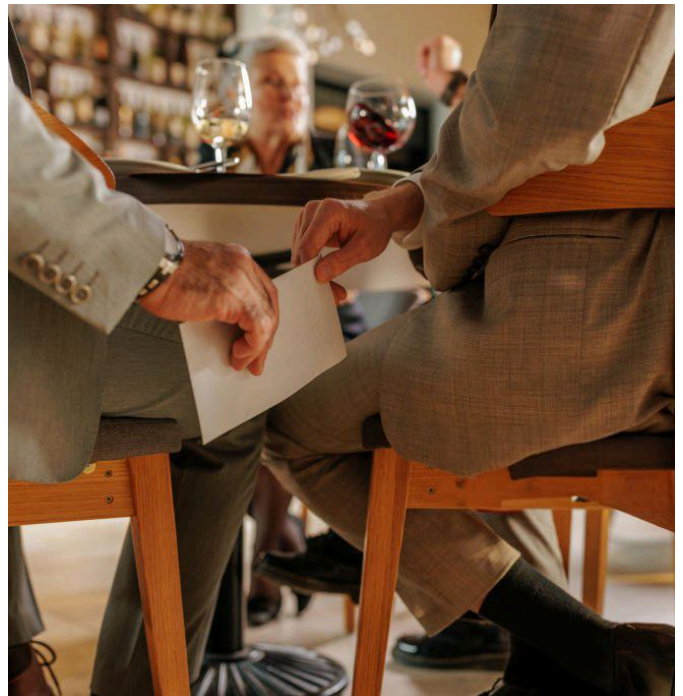
✓ **Ongoing Monitoring:**

Continuously monitor intermediaries' activities for suspicious transactions or changes in their risk profile.

✓ **Screening:**

- Regularly screen intermediaries against sanctions lists and other relevant databases.
- Record Keeping and Reporting: Maintain detailed records of all due diligence efforts, transactions, and communications with intermediaries, and establish clear procedures for reporting suspicious activities to relevant authorities when necessary.

The landscape of anti-money laundering and countering the financing of terrorism (AML/CFT) is continually undergoing significant changes globally. In the European Union, a sweeping package of **new AML rules** has been adopted, introducing a harmonized rulebook and **establishing the European Anti-Money Laundering Authority (AMLA)**. This framework extends coverage to luxury goods dealers, imposes stricter due diligence requirements, and sets a €10,000 limit on cash transactions. Meanwhile, in the United States, the Financial Crimes Enforcement Network (FinCEN) has **proposed a rule** to modernize AML/CFT programs for financial institutions. This proposal emphasizes risk-based approaches, mandates incorporation of government-wide AML/CFT priorities and encourages technological innovation in compliance processes.



---

# Unique Challenges Amid Heightened Dependence on Intermediaries

As organizations continue to globalize by relying more heavily on third parties, sales intermediaries, and distribution channels, failing to have strong ABAC and KYC/KYB/AML at the core of your compliance program poses tremendous risk. Companies operating in this global landscape must continually invest in fortifying their existing compliance programs - and contractually enforcing these policies across their third parties - to mitigate, escalate, and remediate these risks.

Many of these organizations have also developed separate and disparate systems across different functions that make it challenging to run effective programs with a clear view of risks, and this ultimately contributes to the creation of silos across your teams, data, processes, and systems. To successfully handle these issues, organizations require a technology-based approach that unites master data management, risk management, multi-sourced data enrichment and unified due diligence profiles to address these challenges.

## A Deeper Dive into Sales Intermediary Risk

---

The traditional perception about sales intermediaries (SIs) has expanded significantly across a diverse array of channels that now form the backbone of revenue generation for many global enterprises. For instance, over 23% of Amazon's revenue is derived from these expanded channels which include:

➤ **Third party Intermediaries (TPIs)**

Agents, consultants, brokers, distributors, resellers and facilitators.

➤ **Managed Service Providers (MSPs):**

Companies that remotely manage a customer's IT infrastructure and/or end-user systems.

➤ **Independent Software Vendors (ISVs):**

Businesses that develop, market, and sell software that runs on third-party hardware and platforms.

➤ **Marketplaces:**

Online platforms where multiple vendors sell products or services to customers.

➤ **Original Equipment Manufacturers (OEMs):**

OEMs produce parts and equipment which may be marketed by another manufacturer.

➤ **Value Added Resellers (VARs):**

VARs add features or services to an existing product, then resell it like an integrated product or complete solution.

➤ **Traditional System Integrators:**

Traditional System Integrators specialize in bringing together component subsystems into a whole and ensuring they function together.

---

Each one of these channels poses unique compliance challenges. These sales intermediaries are also experiencing rapid growth and expanding their reach and influence throughout global organizations. As they continue to evolve and expand, these channels represent a myriad of new potential risks to organizations. Managing the risks associated with these channels is becoming increasingly complicated and more expansive, requiring that companies re-orientate their regulatory strategies towards managing various developing risks associated with each type of a channel.

Revisiting the Cisco example from earlier, here is a deeper look into the most significant risks and damages incurred from a single bad-acting sales intermediary:

<b>&gt; Compliance Risk</b> Potential violations of US and international law, leading to regulatory scrutiny / investigations	<b>10-year long investigation</b> by the US DoJ and other federal and local agencies.
<b>&gt; Financial Risk</b> Potential for compromised revenue, increased costs, and fines for non-compliance.	\$1B+ lost in direct revenue opportunity. Cisco also estimates an <b>annual loss of \$1.2B</b> to gray market / counterfeit products.
<b>&gt; Business Continuity Risk</b> Service interruption	
<b>&gt; Reputational Risk</b> Damaged brand perception	Incalculable reputational damage as these counterfeit products were sold to both public and private sectors, even impacting critical defense and healthcare systems.
<b>&gt; Operational Risk</b> Decreased control over processes and service levels	
<b>&gt; Cyber Risk</b> Poor data security and over-reliance on third-party safeguards	Pirated Cisco software loaded onto refurbished, often damaged hardware was implemented in sensitive data infrastructure across <b>hospitals, schools, and highly classified military applications</b> such as fighter jets.
<b>&gt; Strategic Risk</b> Misalignment of an organization's strategic objectives	

---

As we move forward, it is clear that third party and sales intermediary compliance must be seen as a strategic imperative, essential for protecting revenue flows, defending brand image and promoting scalable development in an ever more multi-layered global ecosystem. Moreover, with the current international cooperation in enforcement actions, it is necessary for firms to understand how regulatory agencies from various jurisdictions may resolve such investigations thereby warranting robust and adaptable compliance frameworks that keep pace with complexities associated with global operations.



---

# Managing Compliance Risks with Sales Intermediaries

---

Managing compliance risks with sales intermediaries presents unique difficulties to firms. The quick speed at which technology is advancing, in addition to the overwhelming complexities of third party risk management, poses both seen and unseen challenges to the robustness of your compliance program.

---

In order to tackle these challenges, businesses are increasingly adopting digital solutions for compliance that use automated, AI-enhanced platforms to augment due diligence, transaction monitoring and risk assessment processes. Best practices for addressing these challenges include:

✓ **Technology-Driven Compliance:**

Leverage advanced analytics and AI-integrated tools to enhance due diligence, transaction monitoring, and risk assessment processes. Organizations should focus on automation of AML screening, sanctions checks, and KYC / KYB procedures, and leveraging artificial intelligence for ABAC risk detection, updating regulations analysis, managing smart contracts, and enhancing the monitoring of risks and streamline compliance workflows.

✓ **Unified Due Diligence:**

Integrate master data programs, risk program management, multi-source data enrichment and screening for a 360-degree view across enhanced due diligence processes.

✓ **Multi-Source Data Enrichment:**

Validate using multiple compliance-specific data sources, including internal lists.

✓ **Rules-Based Workflows**

Screen entities and all related parties according to your unique business rules and regulations.

✓ **Audit-Ready Documentation:**

Automate the generation of audit evidence, and that evidence should ideally be stored in a single data repository for quick retrieval.

✓ **Remediation and Business Continuity Planning:**

Develop robust strategies for addressing compliance gaps and maintaining operational resilience in today's dynamic landscape. This is carried out through systematic remediation processes, focusing on critical risks, and developing business continuity plans to manage potential disruptions and emerging risks. Repeated testing and updating are indispensable for keeping up with emerging threats and regulatory changes.

---


The adoption of a unified, technology-driven approach to compliance ensures that organizations can effectively manage the unique risks associated with their products and services. Leaning towards technological-based solutions provides an advanced way of real-time risk monitoring and management. Through creating cross-functional collaboration via a unified due diligence process, firms build a culture of compliance which evolves with changing regulations. Hiring a third-party auditor also adds another level of assurance by validating exactly how audit-ready your organization is today.

By promoting a culture of compliance and anticipating regulatory challenges in advance, organizations can mitigate against risks while exploiting opportunities presented by distribution partnerships. In this age of increasing regulation coupled with rapid changes in technology, organizations must be proactive about compliance if they want to grow sustainably as well as retain stakeholder trust in the digital era.





# Unified third party risk & compliance management, powered by AI.

Modern Enterprises rely on 

[Schedule a demo](#) to learn more about cybersecurity compliance from our experts.

**300%**

Faster onboarding

**10x**

Increase in efficiency

**50%**

Savings in operational costs

## Top 5 Compliance Challenges



### Investigation complexity and time

Task variation, multiple databases, and bottlenecks slow down investigators.



### Standardizing inconsistent processes

Variations in policies, procedures, and investigators leave gaps in reports where risk can creep in.



### Fulfilling documentation requirements

Non-standardized investigation reports create audit susceptibility.



### Facilitating managerial oversight

Low visibility over team's processing and volume variances make it hard to commit to SLAs.



### Monitoring ongoing risk

Re-screenings occur intermittently when bandwidth is available, often only for the highest risk entities.

## Certa Compliance Solutions



### Simultaneous Search

All best-of-breed, compliance-specific data sources of your choice, including internal lists, in one place.



### Rules-Based Workflows

Entities and all related parties, screened exactly as business rules and regulations dictate.



### Investigation Reports

Dated and annotated report with all required references.



### Manager's Dashboard

Multiple queue and progress oversight and assignment capabilities.



### Ongoing, Automatic Monitoring of Entities

Daily, monthly, and annual OFAC and adverse news checks.