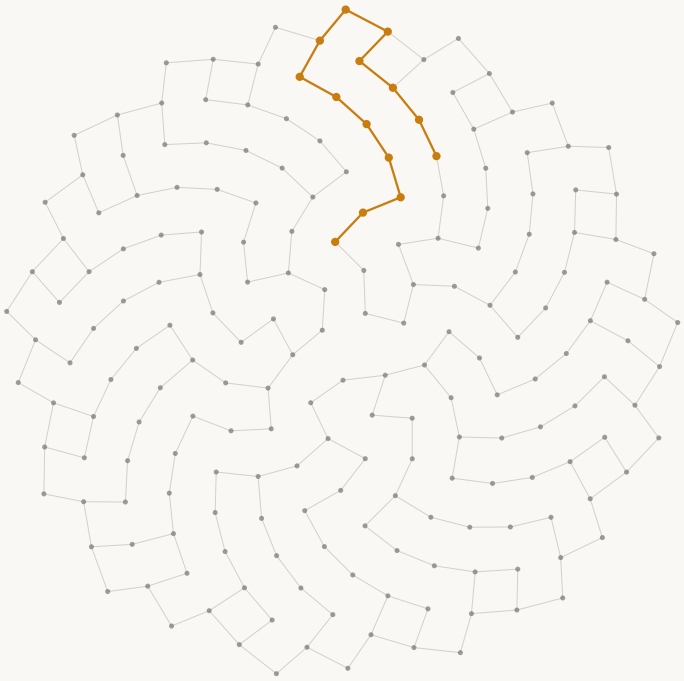
A SAYARI CUSTOMER CASE STUDY . MAY 2026



Counterparty Due Diligence for the BIS 50% Affiliates Rule.

How to prepare for November 10, 2026 reinstatement.

A nine-domain due diligence checklist for exporters preparing for the BIS Affiliates Rule's automatic reinstatement on November 10, 2026.

CUSTOMER CASE STUDY · REGULATORY RESPONSE

Counterparty due diligence for the BIS 50% Affiliates Rule.

How to prepare for the rule's automatic reinstatement on November 10, 2026.

REGULATORY TRIGGER	BIS 50% Affiliates Rule (15 C.F.R. § 744.21)
REINSTATEMENT DATE	November 10, 2026
APPLIES TO	All non-U.S. counterparties receiving EAR-controlled items
SCREENING SCOPE	Entity List + Military End-User List + SDN List
OWNERSHIP THRESHOLD	50% or more — direct, indirect, or in aggregate
VERSION / DATE	May 2026, review annually

How to Use This Checklist

The BIS 50% Affiliates Rule is scheduled to reinstate automatically on November 10, 2026. Under the rule, any non-U.S. entity owned 50% or more (directly, indirectly, or in aggregate) by a party on the BIS Entity List, Military End-User (MEU) List, or certain parties on the Specially Designated Nationals (SDN) List is automatically subject to the same export restrictions as the listed entity itself.

This extends the obligation well beyond name-based list screening. Exporters must now trace and document the full ownership chain of every counterparty.

This checklist provides questions that exporters, procurement teams, and third-party risk managers should ask of every new supplier, vendor, distributor, or other counterparty receiving U.S.-origin controlled items or items subject to the Foreign Direct Product Rule.

It is organized into nine due diligence domains, from corporate identity through transaction transparency. Each section identifies how Sayari's Commercial World Model, built on billions of

records from authoritative government registries worldwide, can independently validate counterparty representations and surface ownership risks that self-reported information alone cannot reveal.

Where standard onboarding forms ask counterparties to disclose their ownership, Sayari independently derives it from primary-source corporate filings, trade data, and financial records across 70+ countries.

WHO SHOULD COMPLETE THIS CHECKLIST

This document is designed for two purposes: (1) as a resource to inform intake questionnaires to be provided to and completed by new counterparties prior to first shipment; and (2) as a resource to inform internal checklists for compliance, procurement, and legal teams conducting independent ownership verification using external data tools.

SECTION 1

Corporate Identity & Legal Formation

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	What is the counterparty's full legal name, including any trade names or doing-business-as (DBA) names?	Alias and name variation risks; Entity List matches may exist under alternate names.
2	In which jurisdiction is the entity incorporated or registered? Provide the company registration number and date of formation.	Opaque or high-risk jurisdictions (e.g., offshore financial centers) require enhanced scrutiny.
3	Provide the registered address, principal place of business, and any other operational addresses.	Shell entity risk; addresses shared with Entity Listed companies may indicate affiliation.
4	Is the entity publicly listed? If so, on which exchange, and what is its ticker symbol?	Public filings provide an independent source of ownership data for cross-validation.
5	Provide copies of official incorporation documents, certificates of registration, and any recent amendments to the corporate charter.	Without primary-source documents, ownership claims cannot be independently verified, requiring exporters to resolve the red flag or apply for a license.
6	Does the entity have a disclosed business purpose?	Disclosed business purposes conflicting with business activity could indicate deceitful practices, including diversion or transshipment risk.

SAYARI VALIDATES

Sayari's Commercial World Model contains authoritative corporate registry records from 250+ jurisdictions. Entity name, registration number, registered address, and legal status are cross-referenced against official government filings, flagging discrepancies between self-reported information and the record of authority.

SECTION 2

Direct Ownership Structure

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Identify all direct shareholders or members holding 10% or more equity interest. For each, provide: full legal name, jurisdiction of residence or formation, and ownership percentage.	The BIS Affiliates Rule triggers at 50% aggregate; any substantial holder requires tracing. BIS explicitly advises that additional time and resources are required to ensure compliance.
2	For each shareholder identified, is that shareholder itself a legal entity (company, fund, trust) or a natural person?	Legal entity holders require further ownership tracing up the corporate tree.
3	Does any government, state-owned enterprise (SOE), or sovereign wealth fund hold a direct equity interest? If yes, identify the government and the nature of its ownership.	State ownership from countries of concern (e.g., China, Russia, Iran, North Korea, Belarus) may indicate Entity List, MEU List, or SDN List exposure.
4	Are any shares held through nominee arrangements, bearer instruments, or undisclosed beneficial owners? If yes, disclose the underlying beneficial owner.	Nominee ownership is a common mechanism to conceal Entity List affiliation from standard screening.
5	Provide a current capitalization table (cap table), shareholder record, or equivalent ownership register certified as accurate as of the date of this certification.	A point-in-time snapshot may be stale; ownership changes between onboarding and re-screening are a key compliance gap.

SAYARI VALIDATES

Sayari's 11B+ record Commercial World Model cross-references self-reported ownership against official corporate registry filings, trade data, and financial disclosures across jurisdictions, surfacing shareholders not disclosed on intake forms. State-linked ownership is flagged against known government entity profiles.

SECTION 3 · CORE BIS AFFILIATES RULE OBLIGATION

Aggregate & Indirect Ownership

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Trace the full ownership chain to the ultimate parent entity. For each intermediate holding company or controlling entity, provide: legal name, jurisdiction, and ownership percentage at each layer.	The BIS Affiliates Rule applies to ownership held directly, indirectly, individually or in aggregate, by listed parties in any foreign country. A clean direct owner may itself be owned by an Entity List company.
2	Does any single entity (when combining direct and indirect ownership stakes) hold 50% or more of the counterparty? (Aggregate rule: multiple minority stakes held by the same ultimate owner must be summed.)	Failure to calculate aggregate percentage is the most common compliance gap under the rule. A 30% direct + 25% indirect = 55% aggregate exposure.
3	Are any intermediate holding companies incorporated in jurisdictions known for corporate opacity (e.g., British Virgin Islands, Cayman Islands, Marshall Islands, Panama, Seychelles)? If yes, provide documentation of their beneficial owners.	Opaque intermediate holders are a recognized mechanism for obscuring Entity List parentage. BIS red flag guidance identifies opaque structures as a trigger for enhanced diligence.
4	Have there been any ownership transfers, equity issuances, or restructuring events in the past 36 months that changed direct or indirect ownership percentages? Provide documentation of any such events.	Ownership restructuring after Entity List designation is a known evasion tactic. Recent changes require retroactive tracing.
5	Do any joint venture partners, consortium members, or co-investors in the counterparty hold an equity stake, directly or indirectly? Identify all such parties and their ownership percentages.	JV structures can create de facto control by a restricted party even below the 50% threshold; board control or veto rights may confer functional ownership.
6	Is the counterparty a subsidiary, affiliate, or division of a larger corporate group? If so, provide the full group structure, including all entities in the group operating in countries of national security concern.	Subsidiary entities inherit Entity List restrictions when their parent is listed. The group structure must be mapped, not just the contracting entity.

SAYARI VALIDATES

Sayari precomputes aggregate ownership risk across multiple corporate layers, automatically surfacing entities majority-owned by Entity List, MEU List, or SDN List entities that name-based screening would never detect. Cross-border corporate chains through opaque jurisdictions are resolved against authoritative local registry records, not reliance on self-reported group charts.

SECTION 4

Beneficial Ownership & Ultimate Beneficial Owner (UBO) Disclosure

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Who are the natural persons who ultimately own or control the counterparty, directly or indirectly, with 25% or more ownership or equivalent control rights? (Provide full legal name, nationality, country of residence, and date of birth.)	UBO opacity is a core risk vector. Undisclosed individual owners may be SDNs or connected to Entity List companies.
2	Are any UBOs current or former government officials, military officers, or state enterprise executives in a country of national security concern? (Politically Exposed Person / PEP status.)	Government or military connections may indicate MEU List exposure or undisclosed state direction of the enterprise.
3	Do any UBOs hold concurrent ownership or management positions in other companies that appear on the BIS Entity List, MEU List, or OFAC SDN List?	Shared UBOs between restricted and clean entities is a known diversion network typology. Sayari routinely surfaces these cross-entity linkages.
4	Provide certified copies of UBO declarations or equivalent filings made to any government registry (e.g., FinCEN BOIR, EU beneficial ownership registers, UK PSC register, Singapore ACRA filings).	Self-reported UBO information without government-registered equivalents cannot be independently verified.

SAYARI VALIDATES

Sayari cross-references disclosed UBOs against OFAC, BIS, and international sanctions databases, and identifies connected entity networks through shared officer, director, and address records from authoritative commercial registries, exposing hidden linkages between disclosed UBOs and restricted parties.

SECTION 5

Entity List, MEU List & Restricted Party Screening

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Confirm that the counterparty's legal name, all known trade names, and all known predecessor names have been screened against the BIS Entity List, MEU List, and OFAC SDN List as of the date of this certification.	Name-based screening alone is necessary but not sufficient. A clean name check does not satisfy the Affiliates Rule ownership obligation.
2	Has any parent company, intermediate holding company, or ultimate beneficial owner been screened against the Entity, MEU, or SDN Lists? Provide the scope and methodology of ownership-based screening performed.	The BIS Affiliates Rule explicitly mandates that restrictions flow through the ownership chain. Screening only the contracting entity's name is legally insufficient after November 10, 2026.
3	Has the counterparty, or any entity in its ownership chain, ever been the subject of a BIS denial order, temporary denial order (TDO), or equivalent export control enforcement action by any government?	Prior enforcement history is a material red flag under BIS due diligence guidance.
4	Has the counterparty, or any of its affiliates or UBOs, ever appeared on the SDN List, Consolidated Sanctions List, EU restrictive measures list, or UK Office of Financial Sanctions Implementation (OFSI) list?	Multi-list exposure is common in relevant enforcement cases. An entity clear of the BIS Entity List may appear on OFAC or allied-nation sanctions lists.
5	Is the counterparty, or any entity in its ownership chain, involved in any industry or program that BIS has flagged for enhanced scrutiny, including: advanced semiconductors, AI chips, military equipment, dual-use technology, or nuclear materials?	Industry and product-type risk factors inform the appropriate depth of ownership screening required. Affirmative findings activate different levels of control depending on the applicable list, item type, destination, and end use.

SAYARI VALIDATES

Sayari's BIS50 Signal Module algorithmically identifies entities majority-owned by Entity List and MEU List companies, delivering a pre-computed restricted affiliate universe that supplements static name screening with ownership-chain intelligence. Sayari's data is derived from the same authoritative source records BIS analysts use.

SECTION 6

Military End-User (MEU) Risk & Defense Connections

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Does the counterparty, or any entity in its corporate group, have contractual relationships with or receive funding from a military, defense, or intelligence agency of any government?	Military end-user relationships may trigger MEU List exposure regardless of the counterparty's name screening status.
2	Is the counterparty involved in research, development, or production of any technology with potential military application (dual-use goods), including: advanced materials, aerospace components, semiconductor equipment, surveillance technology, or communications systems?	Dual-use technology supply chains are a primary BIS enforcement target. End-use declarations must specify ultimate application.
3	Are any of the counterparty's key executives, board members, or technical staff concurrently employed by or seconded from a military or defense research institution?	Shared personnel between commercial entities and defense organizations is an indicator of MEU risk, even when not reflected in formal ownership structures.
4	Does the counterparty or its affiliates participate in any government-designated military-civil fusion (MCF) program, particularly China's MCF strategy or equivalent programs in other countries of concern?	MCF participation is a BIS red flag for MEU List exposure and may indicate undisclosed military ownership or direction.

SAYARI VALIDATES

Sayari maps connections between commercial entities and defense institutions through shared officers, addresses, trade relationships, and corporate filings, revealing MEU risk that does not appear in a formal ownership chart. A series of automated MCF risk indicators, as well as visibility into Chinese provincial registries and defense research institutions, are a core Sayari capability.

SECTION 7

Geographic Footprint & Operational Risk

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	In which countries does the counterparty have operational facilities, offices, manufacturing plants, or research centers? Identify all jurisdictions where physical operations occur.	Operational presence in countries of concern (China, Russia, Belarus, Iran, North Korea, Venezuela, Cuba) elevates the required depth of due diligence.
2	Where are the counterparty's goods manufactured, assembled, or processed? Identify all manufacturing locations, including third-party contract manufacturers.	Manufacturing location affects ECCN classification, de minimis thresholds, and Foreign Direct Product Rule applicability.
3	Does the counterparty use or rely upon any third-party logistics providers, freight forwarders, or transshipment hubs in jurisdictions commonly used to circumvent export controls (e.g., UAE, Hong Kong, Singapore, Malaysia, Turkey)?	Transshipment corridors are the primary BIS enforcement target for controlled semiconductor and dual-use technology diversion.
4	If the counterparty operates or sources from China, identify all Chinese corporate entities in the supply chain, their provincial registration details, and any participation in special economic zones or government-designated innovation programs.	China-linked supply chains require tracing through Chinese provincial registries, where ownership structures are frequently opaque at the top level but resolvable from authoritative local filings.

SAYARI VALIDATES

Sayari's cross-border visibility spans corporate registries across high-opacity jurisdictions, including China's provincial SAMR registries, offshore financial centers, and transshipment corridor jurisdictions. Trade data (bills of lading, customs filings) provides independent corroboration of stated operational locations and logistics relationships.

SECTION 8

Counterparty Export Control Program Assessment

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	Does the counterparty have a documented Export Compliance Program (ECP)? If yes, provide a summary of program scope, ownership screening procedures, and the date of the most recent compliance audit.	An absent or immature ECP is a red flag for diversion risk and may limit your ability to establish effective defense in enforcement proceedings.
2	Does the counterparty's restricted party screening program include ownership-based screening (i.e., tracing the ownership of counterparties, not just their names)? If not, what is the planned implementation timeline?	A program that screens names but not ownership chains will not satisfy the BIS Affiliates Rule, for the counterparty or for you as an exporter relying on their compliance. Screening for entities associated with listed addresses is also now a required feature of due diligence.
3	Has the counterparty's compliance team received training relevant to compliance with the BIS 50% Affiliates Rule, including aggregate ownership calculation methodology and red flag identification?	Counterparty training gaps create downstream compliance exposure for exporters who rely on their representations.
4	What restricted party screening tool(s) does the counterparty use, and at what frequency are counterparties re-screened? Does screening include periodic re-screening for ownership changes?	Screening at onboarding only is insufficient. Entity List, MEU List, and SDN List additions are made continuously. Ownership structures change. BIS best practices include ongoing screening in combination with periodic targeted screening to ensure no transactions with newly listed or newly controlled parties.
5	Has the counterparty ever identified a potential or actual violation of export control regulations? If yes, describe the circumstances and any voluntary self-disclosure or remediation actions taken.	Prior violations, even self-disclosed ones, require enhanced scrutiny. Disclosed violations without remediation evidence are a significant red flag.

SAYARI VALIDATES

Sayari's solutions enable continuous monitoring of counterparty portfolios, automatically alerting compliance teams when changes in ownership, corporate structure, or restricted party status are detected in authoritative data sources. This converts point-in-time onboarding assessments into an ongoing, defensible compliance workflow.

SECTION 9

End-Use & Transaction Transparency

#	DUE DILIGENCE QUESTION	RISK IF UNANSWERED
1	What is the intended end-use of the goods or technology being exported? Confirm that the end-use does not involve: nuclear, chemical, biological, or radiological weapons programs; military applications in countries of concern; or any other prohibited end-use under the EAR.	End-use misrepresentation is the primary mechanism for export control evasion. License conditions and EAR Part 744 end use restrictions require accurate declarations.
2	Who is the ultimate end-user of the exported goods? If the counterparty is an intermediary or distributor, identify all downstream customers to whom the goods will be transferred.	Diversion risk is highest at the distributor level. Ultimate end-user identity must be established even when the exporter's direct counterparty is not itself restricted.
3	Will any goods or technology be re-exported to a third country after delivery? If yes, identify the country of re-export and the ultimate end-user in that country.	Re-export without a license is a common violation. The Foreign Direct Product Rule may apply to re-exports even of non-U.S.-origin goods incorporating U.S. technology.
4	Confirm that neither the counterparty nor any identified end-user intends to use the exported goods in support of a Weapons of Mass Destruction (WMD) program, as described in EAR Part 744.	WMD end-use is an absolute prohibition with criminal penalty exposure. This certification is required regardless of the item's ECCN classification.

SAYARI VALIDATES

Sayari's trade data layer, sourced from global customs and bill-of-lading records, provides an independent validation and check of stated end-use patterns and customer relationships. Trade flow anomalies (e.g., a stated manufacturer with no export history, or goods routed through transshipment hubs inconsistent with declared destinations) are surfaced against global shipping data.

LEGAL NOTICE

Important Notice

> This checklist is an analytical and operational due diligence resource. It does not constitute legal advice. Exporters should consult qualified export control counsel regarding specific licensing obligations, classification questions, and legal interpretations of the BIS Affiliates Rule. Data validation using Sayari is a complement to, not a substitute for, a documented export compliance program.

ABOUT SAYARI

Judgment infrastructure for trustworthy AI in economic security and commercial risk.

The Sayari Commercial World Model resolves 10.6B+ primary-source records from 250+ jurisdictions forming the ground truth of global commerce. A Judgment Ontology, encoding over a decade of investigative tradecraft, and Superconductor, an agentic orchestration platform, deliver AI that reasons like an expert analyst, shows its work, and traces every finding to its source. Trusted by U.S. Customs and Border Protection, the U.S. Treasury, and Fortune 500 enterprises, Sayari is used by thousands of professionals across 35+ countries to secure supply chains and dismantle illicit networks. Headquartered in Washington, D.C.

Sayari's BIS50 Signal Module was purpose-built to address the compliance gap created by the BIS Affiliates Rule: the rule mandates ownership-based screening but does not publish a list of covered affiliates. Sayari algorithmically derives that list from the most comprehensive global corporate database available, providing compliance teams with a defensible, auditable answer to the question the rule demands: **Who owns this counterparty, at what percentage, and across how many layers?**

Learn more at sayari.com