QUANTUM GROUP LLC

US FL REG: L19000273186

QUANTUM GROUP LLC

ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

Sanctions compliance and responsible precious metals sourcing

Version 2.0 | Updated 29 October 2026

Policy owner and designated Compliance Officer: Carlos Ortega

Purpose and scope

Quantum Group LLC requires its business to be conducted in a manner that prevents the use of its products and services for money laundering, terrorist financing, sanctions evasion, and related criminal activity. This policy governs the purchase and sale of physical gold and silver coins and bars, principally for individual investors, including transactions arranged for third-party storage.

The policy applies to all Quantum operations and to every manager, employee, contractor, and agent carrying out work for Quantum within this scope. Customer, supplier, payment, and storage arrangements must meet the controls set out below. Commercial objectives do not override compliance decisions.

Operating requirements

- Know and verify the parties to a transaction, the people who own or control them, and the legitimate purpose and source of funds or metals.
- Assess financial crime risk, screen relevant parties and transactions for sanctions, and apply additional review where risk is higher.
- Pause and escalate unresolved concerns before committing to or completing a transaction. Make required reports and protect confidential information.
- Keep evidence of checks and decisions, train relevant personnel, independently test the program, and correct deficiencies.

Legal framework

The program addresses applicable United States Bank Secrecy Act requirements, including 31 CFR Parts 1010 and 1027, and sanctions administered by the United States Treasury Office of Foreign Assets Control (OFAC). The Compliance Officer must assess other laws that apply to the actual parties, locations, and transactions involved. Applicable law prevails over an inconsistent policy provision; any conflict must be escalated and resolved before the affected activity proceeds.

Customer verification standards, ownership thresholds, review intervals, and controls identified as company requirements are mandatory within Quantum even where they exceed a legal minimum. The Compliance Officer must maintain the supporting procedures and records needed to put this policy into practice.

Legal basis: 31 CFR Part 1027

1. Governance and accountability

Senior management

Senior management is responsible for approving this program and material amendments, providing adequate resources, and overseeing its effectiveness. Approval must be recorded in company governance records. Management must receive a compliance report at least quarterly covering material risks, control failures, overdue reviews, training, independent testing, and corrective actions. Urgent issues must be escalated immediately.

Management must support compliance decisions and require timely remediation. It must appoint a competent, trained alternate to cover the Compliance Officer when unavailable, document that delegation internally, and ensure reporting and transaction controls remain effective during absences.

Compliance Officer

Carlos Ortega is Quantum's designated Compliance Officer. He has direct access to senior management and the information, personnel, and records necessary to carry out the role. His responsibilities are to:

- Maintain this policy, the business risk assessment, operational procedures, and a register of applicable legal obligations and reporting deadlines.
- Oversee due diligence, sanctions screening, risk ratings, monitoring, investigations, and regulatory reports; approve or decline matters requiring compliance review.
- Require additional information, suspend transactions, restrict activity, and recommend termination of relationships when risk cannot be adequately controlled.
- Arrange training, oversee record retention, support independent testing, and track corrective actions through verified completion.

Regulatory reports must be made within the applicable deadline without commercial interference. Management must not override a legal prohibition or require the Compliance Officer to clear an unresolved sanctions or financial crime concern. Conflicts involving the Compliance Officer must be referred directly to an unconflicted member of senior management.

Responsibilities of personnel

Personnel must complete required training, follow approved procedures, record checks accurately, and escalate concerns promptly. Staff must not omit required information, alter evidence, structure transactions to evade controls or reporting, or suggest ways to circumvent due diligence. Failure to follow this policy may result in corrective or disciplinary action, including termination of employment or engagement.

Controlled exceptions

An exception to a company control requires the Compliance Officer's prior written approval, a documented reason, compensating controls, an expiry date, and management approval where the residual risk is high. Exceptions cannot waive law, required reporting, essential identity verification, or resolution of a potential sanctions prohibition. Recurring exceptions must trigger a review of the control.

Required evidence. Management approvals, designation and delegation records, quarterly reports, exception decisions, and a corrective action register showing owners, deadlines, and closure evidence.

2. Assessment and classification of risk

Business risk assessment

The Compliance Officer must prepare a documented business risk assessment at least annually and when material changes occur. It must consider actual activity and the effectiveness of controls, including customer and supplier profiles, products, transaction values and volumes, payment channels, remote interactions, geographic exposure, and delivery and custody arrangements.

The assessment must address money laundering, terrorist financing, sanctions evasion, proliferation financing, fraud, corruption, tax crime, and illicit sources of metals. Terrorist financing may involve lawful sources of money and small transactions; value alone does not determine risk. Management must approve the assessment and the actions needed to address material residual risks.

Relationship and transaction risk

Each customer and supplier must receive a documented low, standard, or high risk rating before the relationship is approved. The reasons must be recorded using a consistent assessment method maintained by the Compliance Officer. A transaction must also be reviewed for features that are inconsistent with the approved relationship profile.

- Customer and ownership risk includes identity reliability, occupation or business, beneficial ownership transparency, political exposure, credible adverse information, and unexplained use of representatives.
- Geographic risk includes residence, incorporation, operations, payment banks, metal origin, transit, and storage locations. Assess current sanctions, applicable Treasury special measures, and relevant official financial crime advisories.
- Transaction risk includes economic purpose, source of funds and metals, unusual pricing or frequency, unexplained payment routing, and changes to delivery or custody instructions.

High risk relationships require enhanced due diligence and approval under section 5. An unresolved identity, ownership, sanctions, or criminal activity concern cannot be accepted merely by assigning a high risk rating. A low risk classification does not remove minimum verification or screening requirements.

Ongoing review

As company requirements, high risk relationships must be reviewed at least annually, standard risk relationships at least every two years, and low risk relationships at least every three years. An earlier review is required when ownership, control, identity, business activity, payment arrangements, political exposure, sanctions status, or expected activity changes, or when a concern arises. Trading must be restricted where information essential to a decision is missing or unreliable.

Regulatory applicability

At least annually, the Compliance Officer must document the application of the precious metals dealer rules using actual prior-year purchases, sales, and supplier classifications under 31 CFR 1027.100. Any reliance on the retailer exception must be supported by evidence. This policy applies across Quantum's covered business regardless of whether a particular activity falls within that exception. New or materially changed activity requires a risk and legal review before launch.

Required evidence. Approved business risk assessment, relationship ratings and reasons, review dates, change assessments, regulatory applicability analysis, and management actions.

Legal basis: 31 CFR 1027.100 and 1027.210

3. Customer identification and verification

Checks before business is accepted

Quantum must identify and verify each customer before entering into a binding transaction or releasing funds or metals. Required checks must establish who the customer is, whether the customer acts for another person, the purpose and expected activity of the relationship, and the source of the funds used. Anonymous accounts and transactions using false identities are prohibited.

If funds arrive before checks are complete, staff must notify the Compliance Officer and prevent their application to a trade or onward release until the matter is resolved. Any return of funds must first be reviewed for sanctions and other legal restrictions.

Information for individual customers

- Obtain the full legal name, date of birth, nationality, residential address, reliable contact details, and a valid government-issued identity document showing its number, issuing authority, and expiry date where applicable.
- Record occupation or business activity, the purpose of the purchase, expected transaction size and frequency, the intended funding account, and delivery or storage instructions. Collect tax identification information where required by law or the approved account process.
- Ask whether the customer is acting for another person and whether the customer has relevant political exposure. Identify and verify any representative and obtain evidence of authority to act.

Verification standards

Identity must be checked against reliable, independent documents, data, or sources. Staff must compare identifying information, confirm that documents are valid and consistent, and resolve discrepancies. Address verification must use independent evidence appropriate to the risk. A declaration alone is insufficient where information is inconsistent or the risk calls for corroboration.

Remote onboarding requires additional measures proportionate to impersonation and document fraud risk. These may include independently verified contact details, secure identity checks, and confirmation of ownership of the funding account. Staff must retain the method used, the sources checked, the date, the reviewer, and the conclusion. Copies must be readable and handled securely.

Purpose and source of funds

The customer must explain the economic source of the purchase money, such as employment income, business proceeds, savings, or a documented asset sale. Naming a bank or describing the payment as a wire transfer does not establish the source of funds. Supporting evidence must be obtained when risk, transaction size, or inconsistency warrants it, and in all enhanced due diligence cases.

Customers must provide accurate information, confirm that funds and metals have a lawful origin and intended use, and promptly notify Quantum of material changes. Quantum must obtain updated information when needed. If essential information cannot be verified or a material inconsistency remains unresolved, the Compliance Officer must decline or restrict the relationship and assess whether reporting is appropriate.

Required evidence. Customer identification, verification results, purpose and expected activity, source of funds assessment, representative authority, risk rating, screening, and acceptance or refusal decision.

4. Legal entities and beneficial ownership

Entity due diligence

For each legal entity customer or supplier, staff must establish its legal existence, business activity, ownership, control, and authority to transact. The file must contain its legal and trading names, incorporation jurisdiction, registration number, registered and operating addresses, reliable contact details, and tax or business licence details where applicable.

Verification must use current registry information, formation documents, licences, or other reliable independent evidence. Staff must identify directors and persons authorized to instruct Quantum, verify the identity of the relevant representatives, and obtain evidence that they have authority to act for the entity. The entity's expected trading activity, funding arrangements, and purpose must be consistent with its business.

Ownership and control

As a company due diligence standard, Quantum requires identification and verification of every natural person who directly or indirectly owns 10 percent or more of an entity. Staff must also identify and verify persons who exercise ultimate effective control and at least one senior person with significant management responsibility, regardless of ownership percentage.

Staff must obtain an ownership chart or equivalent reliable information that traces intermediate entities to the relevant natural persons. Ownership calculations must combine relevant interests, and nominee arrangements must be examined to identify the persons behind them. A statement that no individual meets the ownership threshold does not remove the requirement to identify control and management.

Where an arrangement separates legal title from beneficial enjoyment or decision-making power, the Compliance Officer must identify and verify the persons who contribute assets, benefit from them, or exercise ultimate control, as relevant to the arrangement. Unclear ownership or control requires enhanced review and must be resolved before acceptance.

Verification and maintenance

Ownership information must be corroborated using suitable independent records and supporting documents. Staff must investigate inconsistencies between customer declarations, public records, payment information, and other evidence. The Compliance Officer must require additional documents or independent confirmation where normal sources are incomplete or unreliable.

Customer and supplier entities must promptly disclose changes to ownership, control, authorized representatives, legal status, or business activity. Quantum must update its records, repeat relevant screening, and reassess risk before accepting instructions materially affected by a change.

Separate sanctions ownership analysis

The 10 percent threshold is Quantum's identification standard. Sanctions review must separately assess all ownership information needed to apply OFAC's 50 Percent Rule and other applicable restrictions, including aggregated ownership and indirect ownership through blocked entities. Staff must not assume that a person below the identification threshold is irrelevant to sanctions compliance.

Required evidence. Registry and formation evidence, ownership and control information, identification and verification records, authority documents, discrepancies and resolutions, and dated approval and review decisions.

Sanctions ownership authority: OFAC guidance on the 50 Percent Rule

5. Enhanced due diligence and political exposure

When enhanced review is required

Enhanced due diligence is required for high risk relationships and transactions. Triggers include political exposure, complex or opaque ownership, material exposure to high risk jurisdictions, credible adverse information, unexplained wealth or payment routing, and activity that is unusually large, complex, or inconsistent with the customer's profile. Several smaller concerns may together justify enhanced review.

Politically exposed persons

Quantum must identify whether a customer, relevant beneficial owner, or controlling person holds or has held a prominent public function, domestically, abroad, or in an international organization. The assessment also covers close family members and known close associates whose relationship creates relevant corruption or financial crime risk.

Political exposure requires enhanced assessment; it does not by itself establish wrongdoing. The Compliance Officer must assess the position, influence, access to public resources, jurisdiction, connected parties, source of wealth, and source of funds. Former officeholders remain subject to controls appropriate to continuing risk; the passage of time alone does not establish that risk has ended.

Required enhanced measures

- Obtain a clear explanation of the relationship, economic purpose, expected activity, and reason for the proposed payment and custody arrangements.
- Establish and corroborate source of funds. For politically exposed persons and other cases where wealth is relevant to risk, establish and corroborate the source of wealth, meaning how overall assets were accumulated.
- Obtain additional identity, ownership, business, financial, or provenance evidence sufficient to resolve the identified concern. Use reliable independent sources and assess the credibility, relevance, and age of adverse information.
- Set documented transaction restrictions, review intervals, and monitoring measures appropriate to the remaining risk.

The Compliance Officer and an unconflicted member of senior management must approve a high risk relationship before business begins or continues after a material risk increase. The approval must explain the remaining risk, the evidence supporting acceptance, and any conditions. Approvals must be reconsidered at least annually and whenever circumstances materially change.

Unacceptable risk

Quantum must decline, suspend, or terminate business where essential verification cannot be completed, a legal prohibition applies, or the risk of criminal activity cannot be adequately addressed. Staff must not assist a party in avoiding a restriction by changing names, payment routes, ownership descriptions, or intermediaries. Decisions concerning funds or metals already held must comply with blocking, reporting, contractual, and other legal obligations.

Required evidence. Enhanced review findings, source of funds and wealth evidence, political exposure and adverse information assessment, compliance and management approvals, conditions, and subsequent monitoring results.

6. Sanctions screening and assessment

Scope of screening

Quantum must comply with applicable OFAC prohibitions and restrictions. Screening must cover customers, suppliers, relevant owners and controlling persons, authorized representatives, payment parties and banks, and storage and other material intermediaries. The transaction review must also consider relevant countries, territories, goods, origin, transit, destination, and services.

Checks must use current OFAC lists and relevant program information. Quantum also screens against the United Nations Security Council Consolidated List as a company control and must assess additional sanctions regimes where they legally apply to the transaction. A list result must be interpreted under the applicable legal regime; the Compliance Officer determines the required action.

Timing and reliable operation

Screening is required at onboarding, before a binding trade, before releasing funds or metals, and following material changes to parties or instructions. The Compliance Officer must arrange prompt rescreening of active relationships when relevant sanctions lists change and confirm that screening sources are current. Staff must not rely solely on a bank, supplier, or custodian to perform Quantum's checks.

Screening must use available identifiers, relevant aliases, and sufficient party information to resolve possible matches. The Compliance Officer must document the basis for clearing a potential match or treating it as confirmed. Unresolved possible matches must be escalated immediately, and the affected activity must remain on hold pending a decision.

Ownership and other restrictions

An entity may be blocked even when it does not appear by name on a sanctions list. OFAC's 50 Percent Rule covers entities owned, directly or indirectly, 50 percent or more in the aggregate by one or more blocked persons. Ownership through blocked entities must be assessed under OFAC guidance, rather than by a simple multiplication of percentages through the chain.

The Compliance Officer must also assess restrictions that depend on a transaction, sector, territory, service, or other program-specific condition. A clear name search alone is insufficient to authorize a transaction. Control by a sanctioned person, even below a relevant ownership threshold, requires review of the applicable program and heightened evasion risk.

Licences and exceptions

Staff must not assume that a licence or exception permits a transaction. The Compliance Officer must verify the applicable authorization, its scope, conditions, validity, and reporting requirements before approval. Uncertain legal questions must be referred for qualified advice or authoritative clarification, and the affected activity must remain suspended until a lawful decision can be made.

Required evidence. Parties and identifiers screened, sources and list currency, dates, results, ownership analysis, match decisions, reviewer identity, and any applicable licence or other authorization.

OFAC 50 Percent Rule and indirect ownership guidance

OFAC sanctions compliance framework

7. Sanctions response and reporting

Immediate response

A possible prohibition requires an immediate pause and escalation to Carlos Ortega. Staff must preserve the relevant records and prevent unauthorized movement of funds or metals. The Compliance Officer must establish the identity of the parties, the relevant legal authority, Quantum's possession or control of property, and the action required.

Where the law requires blocking, Quantum must block the property without delay and prevent dealing in it unless authorized. Blocked property must not be returned to the sender merely because the transaction is declined. Where a transaction is prohibited but no blocking requirement applies, the Compliance Officer must arrange rejection as required by the relevant sanctions program.

An internal risk hold or commercial refusal does not automatically constitute legal blocking or a reportable sanctions rejection. The Compliance Officer must record the distinction and the basis for the decision. Staff must not improvise a transfer or refund while a sanctions issue remains unresolved.

Required OFAC reports

Event	Required action and timing
Property becomes blocked	Submit the initial blocking report within 10 business days.
Transaction rejected under an applicable sanctions prohibition	Submit the required rejected transaction report within 10 business days.
Blocked property held on 30 June	Submit the annual blocked property report by 30 September.
Blocked property unblocked or transferred	Assess the reporting duty under 31 CFR 501.603 and the authorization; file within 10 business days where required.

Reports must be filed through the OFAC Reporting System as required. The Compliance Officer must include the applicable legal basis, parties, property or transaction details, and supporting documents; retain the filing and submission confirmation; and record the deadline and completion date. Any regulatory exception or alternative filing arrangement must be verified and documented.

Property and follow-up controls

The Compliance Officer must maintain an accurate inventory of blocked property and coordinate lawful custody with the relevant bank or custodian. Release or transfer requires verification of the legal authority and satisfaction of all conditions. Licences, list changes, and correspondence affecting the property must be reviewed promptly.

A missed filing, screening failure, unauthorized release, or suspected sanctions breach must be escalated immediately to senior management. The Compliance Officer must preserve evidence, arrange appropriate legal advice, assess reporting and voluntary disclosure, and implement corrective action. Records must be retained for the periods in section 12.

OFAC reporting deadlines and submission method

31 CFR 501.603 on blocked property and release reports

8. Payments transactions and storage

Approved payment arrangements

Quantum accepts payment by approved bank wire or ACH transfer through verified accounts. Cash payments are prohibited. Staff must verify the account holder, bank details, and relationship to the approved customer or supplier before relying on payment instructions. Incoming and outgoing transfers must be consistent with the verified party and the documented transaction.

A payment involving a different account holder requires prior Compliance Officer approval, verification of that party and its authority, and a documented legitimate explanation. Undisclosed third-party funding or payment to an unrelated beneficiary is prohibited. Unexpected receipts, mismatched names, split payments, and unusual routing must be escalated before the funds are applied or released.

Transaction controls

Each trade must be supported by an accurate order or agreement and records identifying the parties, date, metal and product, weight or quantity, purity where applicable, price, payment, and delivery or storage instructions. Material departures from expected pricing, volume, or customer activity require explanation and review.

Before settlement or release, staff must confirm that due diligence and screening are current, risk approvals are in place, funds are confirmed through reliable banking records, and the recipient or custodian is authorized. A payment screenshot or unverified message is insufficient proof of cleared funds. Completion and authorization must be recorded.

Changes to banking, refund, delivery, or storage instructions require independent confirmation using a previously verified contact channel and approval by a second authorized person. Staff must resolve inconsistencies and assess fraud and sanctions risk before acting. Urgency does not remove these requirements.

Refunds and sale proceeds

Refunds must normally return to the verified originating account. Sale proceeds must be paid to the verified account of the entitled customer. Any alternative requires Compliance Officer approval, evidence of entitlement, and a documented reason. A refund or other release must not proceed where blocking, legal restraint, or an unresolved financial crime concern prevents it.

Third-party storage

Storage arrangements must use an approved custodian with appropriate due diligence and written terms. Records must establish the customer's interest in the metals, the custodian, location, product and quantity, and the authority for receipts, transfers, or withdrawals. Product identifiers, including bar serial numbers where applicable and available, must be linked to transaction and custody records.

Quantum must obtain and reconcile confirmations for each receipt, transfer, or release and reconcile continuing customer custody records with custodian statements at least monthly. Differences in ownership, quantity, location, or instructions must be investigated promptly, with affected releases suspended until resolved. Staff must describe storage and ownership arrangements accurately to customers.

Required evidence. Verified bank details, payment and trade records, release approvals, instruction change confirmations, custody agreements and statements, reconciliations, and discrepancy resolutions.

9. Suppliers and responsible sourcing

Supplier approval and review

Quantum must complete due diligence on suppliers before trading, including legal existence, ownership and control, authorized representatives, licences where applicable, business activity, bank account ownership, sanctions, and credible adverse information. The Compliance Officer must assess the supplier's AML controls, reputation, supply relationships, and ability to provide reliable provenance information.

Supplier risk ratings and review intervals must follow section 2. Higher risk suppliers require enhanced due diligence and management approval. Supplier status under the United States precious metals dealer rules must be recorded where relevant to Quantum's regulatory applicability assessment; location or a business label alone is insufficient evidence of that status.

Evidence of lawful origin

For each purchase, records must identify the supplier and product and support lawful title and provenance to a degree appropriate to risk. Obtain invoices and available mint, refiner, product, assay, transport, and chain of custody information. Where origin or transit creates sanctions or illicit sourcing risk, obtain sufficient additional evidence to resolve that risk before proceeding.

Supplier declarations must be supported by appropriate checks. Staff must investigate inconsistent documentation, unexplained changes in origin or routing, implausible pricing, unexplained intermediaries, and evidence suggesting substituted or misrepresented metals. Quantum must not make an assurance about origin or sourcing that its evidence does not support.

Prohibited conduct and sourcing risks

Quantum prohibits knowingly sourcing or trading metals connected with money laundering, terrorist financing, theft, smuggling, bribery, corruption, or sanctions evasion. It requires suppliers to respect applicable law and to avoid sourcing linked to forced labour, the worst forms of child labour, serious human rights abuses, or unlawful support to armed groups.

The supplier assessment must consider these risks in the relevant supply chain. Staff must request a lawful origin and responsible sourcing declaration and require suppliers to cooperate with reasonable information requests and promptly disclose material adverse developments.

Response to concerns

Credible evidence of prohibited conduct requires immediate escalation, suspension of affected purchases, and an assessment of legal reporting and property restrictions. Quantum must disengage where the conduct is established or the risk cannot be adequately controlled. A commercial need for supply cannot justify proceeding through unresolved serious concerns.

For a remediable control deficiency that does not require suspension or termination, the Compliance Officer may approve a written corrective plan with defined actions, deadlines, monitoring, and consequences for failure. Progress must be verified with evidence. Failure to improve or new adverse information requires reassessment and may require termination.

Required evidence. Supplier approval file, risk assessment, sourcing declarations, purchase and provenance records, concerns and investigations, remediation decisions, and verified follow-up.

10. Monitoring and investigation

Transaction and relationship monitoring

Personnel must review each transaction against the customer or supplier profile before approval. The Compliance Officer must also arrange a documented monthly review of aggregate activity to identify patterns across related parties, accounts, and transactions. High risk relationships require additional monitoring proportionate to their risks and approval conditions.

Monitoring must use complete and reliable information about purchases, sales, payments, refunds, delivery, and storage movements. The Compliance Officer must review the adequacy of monitoring criteria at least annually and following significant changes or control failures. Automated tools, where used, must be checked for coverage and accuracy; manual review remains required where a tool cannot resolve the issue.

Indicators requiring attention

- Reluctance to identify a customer, beneficial owner, source of funds, source of metals, or the person directing the transaction; false or inconsistent information.
- Requests for unusual secrecy, omitted records, false descriptions, or division of activity to evade checks or reporting.
- Unexplained third-party payments, rapid changes to accounts or destinations, repeated refunds, or purchases followed by rapid resale without a credible economic reason.
- Activity inconsistent with the party's occupation, business, wealth, expected volume, or known trading pattern; unexplained pricing or losses.
- Connections to sanctioned parties, high risk locations, criminal activity, corruption, illicit sourcing, or attempts to conceal ownership, origin, or routes.

An indicator is a reason to investigate, not an automatic finding of wrongdoing. Staff must consider context and combined indicators. Small amounts and long-standing relationships do not remove the obligation to escalate a concern.

Escalation and investigation

Staff must immediately notify Carlos Ortega of suspected sanctions breaches, terrorist financing, imminent loss, or other urgent concerns and pause the affected transaction. Other unusual activity must be escalated promptly, no later than the next business day. Concerns involving Carlos Ortega must go directly to unconflicted senior management.

The Compliance Officer must open a case, preserve evidence, assess urgency and legal deadlines, obtain proportionate information, and record the analysis. The review must cover connected activity and any attempted transaction. Enquiries must be handled carefully to avoid unlawful disclosure or prejudicing an investigation.

Each case must end in a documented decision to clear, apply conditions, decline, suspend, or terminate activity and to make any appropriate report. The file must explain the reasons, approvals, follow-up, and any decision not to report. Open cases must be tracked to closure and overdue actions escalated to management. Legal reporting deadlines take priority over internal review timetables.

Required evidence. Monitoring reviews, alerts and referrals, investigation files, information obtained, decision rationale, reporting assessment, restrictions, and closure or follow-up records.

11. Reporting cooperation and protected disclosures

Suspicious activity

The Compliance Officer must assess whether suspicious activity should be reported voluntarily to FinCEN through its current suspicious activity reporting process and must arrange a report when warranted. The precious metals dealer rules do not themselves impose a dealer-specific mandatory Suspicious Activity Report (SAR) requirement. This does not remove separate mandatory reporting duties or the need to contact appropriate authorities promptly in an urgent case.

A SAR decision must record the relevant facts, rationale, filing date where applicable, and supporting evidence. Filing must use the current authorized system and instructions. A report does not authorize an otherwise prohibited transaction or remove the need to reassess the relationship.

Mandatory transaction reporting

The Compliance Officer must identify and meet reporting obligations arising from actual activity. Sanctions reports are governed by section 7. Any receipt of cash contrary to company policy must be escalated immediately and assessed under the legal definition of cash and the aggregation rules for Form 8300.

Where more than $10,000 in reportable cash is received in one transaction or related transactions, Form 8300 must be filed within 15 days of the receipt that triggers reporting, subject to applicable deadline rules. The required customer statement must be provided by 31 January of the following year. Electronic filing must be used when required. Related payments must be aggregated; staff must not assist in avoiding a filing. Ordinary bank wires are not cash for this purpose.

The Compliance Officer must verify exceptions, relevant monetary instruments, and notice requirements against current instructions. A customer notice is not required for a voluntary Form 8300 filed solely because a transaction is suspicious. Any required notice must not disclose that a transaction was reported as suspicious. Records must include the report, filing confirmation, and evidence of any required notice.

Confidentiality and lawful cooperation

SARs and information revealing their existence must be restricted to authorized personnel and disclosed only as permitted by law. Staff must not tell the subject that a SAR has been or may be filed. Underlying transaction records must be retained separately from restricted reporting material where needed to prevent improper disclosure.

Quantum must cooperate with lawful requests from FinCEN, regulators, courts, and law enforcement. The Compliance Officer must verify authority, preserve relevant records, assess confidentiality and response deadlines, and provide accurate, complete information through an authorized channel. Required reports must not be delayed while unrelated commercial matters are resolved.

Protected reporting

Personnel may report good faith concerns to Carlos Ortega or directly to unconflicted senior management. Quantum prohibits retaliation against anyone who raises a concern, assists an investigation, or makes a legally protected disclosure. Nothing in this policy restricts lawful reporting to a government authority or requires prior company permission for a protected disclosure.

FinCEN guidance for precious metals dealers including voluntary SARs

IRS Form 8300 instructions

12. Records information security and service providers

Complete and retrievable records

The Compliance Officer must ensure that records allow a reviewer to reconstruct each material check, transaction, decision, and report. Records must identify the person performing or approving the action and its date and must preserve the supporting evidence. Entries must be accurate, legible, retrievable, and protected against unauthorized alteration.

Retention periods

Quantum applies the following company retention standards, which may exceed individual statutory minima. A longer applicable legal requirement, regulatory direction, or preservation hold takes precedence. Any conflict with applicable privacy or deletion law must be resolved by the Compliance Officer with appropriate advice before records are removed.

Record category	Minimum company retention period
Identity and relationship due diligence	10 years after the relationship ends.
Transactions payments screening and custody	10 years after the relevant transaction; retain relationship evidence longer where needed to support that transaction.
Investigations and regulatory reports	10 years after the later of case closure or the relevant filing.
Blocked property	Throughout the blocking period and at least 10 years after unblocking.
Policy risk assessments approvals training and testing	10 years after the record is created or the policy or assessment is superseded, as applicable.

OFAC recordkeeping under 31 CFR 501.601 requires covered transaction records for at least 10 years and blocked property records throughout blocking and for at least 10 years after unblocking. Quantum's retention schedule must preserve those requirements. Destruction must stop when litigation, an investigation, or a preservation request requires a hold.

Privacy and security

Personal and confidential information must be collected for legitimate compliance and business purposes, limited to what is needed, and accessed only by authorized persons with a business need. Quantum must use secure transmission and storage, appropriate access controls, backup and recovery measures, and secure disposal when retention ends. Suspected loss, unauthorized access, or disclosure must be escalated immediately and assessed for notification and remediation obligations.

Service providers

Any service provider supporting verification, screening, recordkeeping, or another compliance function requires prior due diligence and a written agreement defining scope, standards, confidentiality, security, access to evidence, escalation, and continuity arrangements. The Compliance Officer must monitor performance and review material providers at least annually. Quantum retains responsibility for its compliance decisions and must obtain the records needed to verify work performed.

When a provider or system is unavailable or unreliable, affected activity must pause unless an approved alternative delivers the required checks and evidence. Reliance on a supplier, bank, or custodian does not replace Quantum's own obligations.

OFAC recordkeeping rule extending relevant retention to 10 years

13. Training independent testing and review

Training

All personnel with relevant responsibilities, including management, must receive training before performing covered work independently, at least annually thereafter, and when material legal, policy, or risk changes affect their role. The Compliance Officer must ensure the content is appropriate to the person's duties.

Training must cover the business's financial crime risks, identification and beneficial ownership, source of funds, political exposure, sanctions, responsible sourcing, payment and custody controls, suspicious activity, escalation, reporting confidentiality, recordkeeping, and protected disclosures. Practical scenarios and a knowledge check must test the ability to apply the requirements. Gaps must be addressed through additional training and supervision.

Independent testing

The program must be independently tested at least annually as a company requirement, with additional testing when risk, significant change, or a material failure warrants it. The tester must be qualified, must not be the Compliance Officer, and must not be involved in operating the program. An independent external reviewer or an eligible internal person may perform the testing.

The reviewer must assess design and operation using a documented, risk-based scope and sample. Testing must cover due diligence and ownership, enhanced reviews, sanctions and ownership restrictions, payments and custody, monitoring and case decisions, reporting, retention, training, and relevant service providers. The reviewer must examine evidence of operation, rather than rely only on policy wording or staff assurances.

Findings must be reported directly to senior management with severity, required action, ownership, and target dates. Management must track remediation, and closure must be supported by verification or retesting. Material unresolved findings must affect the risk assessment and operating restrictions.

Policy and legal review

Carlos Ortega must review this policy at least annually and promptly after material business, risk, regulatory, or sanctions changes. He must monitor relevant official updates, determine effective dates, and arrange timely changes to procedures and training. Proposed rules must be tracked and assessed without being presented as binding requirements before they take effect.

Senior management must approve material revisions in company records. The Compliance Officer must maintain version history, communicate changes to affected personnel, and replace superseded public copies. Public statements and questionnaire responses about compliance must accurately reflect the policy and the evidence of implementation; staff must not claim an audit, certification, control, or capability that cannot be substantiated.

Evidence of performance

The Compliance Officer must maintain training attendance, content, assessment results, and remediation records; independent testing plans and reports; management review and approval records; and evidence that corrective actions were completed. These records must be available for lawful regulatory inspection and independent verification, subject to confidentiality requirements.

This policy is available to customers, suppliers, and other interested parties on request and for publication on Quantum's website. Personal records, investigation files, restricted reports, and detailed security and monitoring procedures remain subject to the confidentiality controls in this policy. Compliance enquiries may be addressed to Carlos Ortega through Quantum's published contact channels.

Program requirements: 31 CFR 1027.210

14. Policy control schedule and legal references

Required control schedule

These intervals are Quantum's minimum operating standards. Legal deadlines and earlier action required by risk take precedence. The Compliance Officer is responsible for tracking completion and escalating overdue actions.

Control	Minimum timing
Due diligence and sanctions assessment	Before acceptance and at the transaction stages specified in sections 3 and 6; repeat on relevant changes.
High risk relationship review	At least annually and on material change.
Standard and low risk relationship review	At least every 2 years and 3 years respectively; earlier when triggered by change or concern.
Aggregate transaction monitoring and custody reconciliation	At least monthly, in addition to transaction checks.
Management compliance reporting	At least quarterly; urgent matters immediately.
Policy business risk and applicability review	At least annually and on material change.
Relevant staff training	Before independent work, at least annually, and on material changes.
Independent testing and material provider review	At least annually; additional work where risk or failures warrant it.

Primary legal references

Legal references were checked on 29 October 2026. The Compliance Officer must use the current text, relevant program restrictions, and official filing instructions when applying this policy. The links below supplement the citations in the relevant sections.

31 CFR Part 1010 General Bank Secrecy Act requirements

31 CFR Part 1027 Precious metals dealer requirements

31 CFR Part 501 OFAC reporting and recordkeeping

OFAC sanctions programs and country information

FinCEN guidance for dealers in precious metals stones and jewels

IRS Form 8300 reporting instructions

Official risk information

FATF high risk and other monitored jurisdictions

United Nations Security Council Consolidated List