



(<https://www.neotas.com>)



Enhanced Due Diligence (EDD) Checklist: A Complete Framework for High-Risk Customer Assessment

Enhanced due diligence (EDD) is a deeper level of customer due diligence applied to high-risk individuals, PEPs, and complex corporate structures. Under UK Regulation 33 of the Money Laundering Regulations 2017 and FATF Recommendation 10, EDD is legally required in specific circumstances.

This enhanced due diligence checklist covers all 9 stages of a compliant EDD assessment, from identity verification to ongoing monitoring.

Jump to a section: What is EDD? | When is EDD required? | EDD vs CDD vs SDD | The 9-Section Checklist | Sector-specific EDD | Regulatory framework | Red flags | Download EDD Checklist PDF

What is an Enhanced Due Diligence Checklist?

**NEOTAS**

(<https://www.neotas.com>) An enhanced due diligence checklist is a structured set of verification steps used to **assess high-risk customers, counterparties, or third parties**. It goes beyond standard customer due diligence (CDD) by requiring source of funds verification, beneficial ownership (UBO) mapping, adverse media research, and enhanced ongoing monitoring. It is legally required under UK MLR 2017 Regulation 33, FATF Recommendation 10, and the US Bank Secrecy Act FinCEN CDD Rule for specific categories of customer.

The EDD checklist covers key areas such as **customer identification, risk assessment, source of funds verification, transaction monitoring, and ongoing compliance measures**.

By following an EDD checklist, businesses and financial institutions can systematically navigate through the various elements involved in the due diligence process, ultimately enhancing the effectiveness and integrity of risk assessments.

What does EDD stand for?

EDD stands for Enhanced Due Diligence (<https://www.neotas.com/enhanced-due-diligence/>). It refers to the heightened scrutiny a regulated firm applies to customer relationships assessed as high risk, either by the firm's own risk assessment or by a specific regulatory trigger such as PEP status or involvement of a high-risk jurisdiction.

Who uses an EDD checklist?

An EDD checklist is used by:

- Compliance Officers and Money Laundering Reporting Officers (MLROs)
- AML Analysts and Financial Crime Teams
- KYC Specialists in banking and financial services
- Risk Managers conducting third-party (<https://www.neotas.com/third-party-risk-management/>) and vendor due diligence (<https://www.neotas.com/vendor-due-diligence-checklist-and-questionnaire/>)
- Legal and accounting professionals subject to MLR 2017
- Corporate TPRM teams assessing high-risk suppliers or business partners (<https://www.neotas.com/glossary/who-are-high-risk-customers-types-of-high-risk-customers/>)

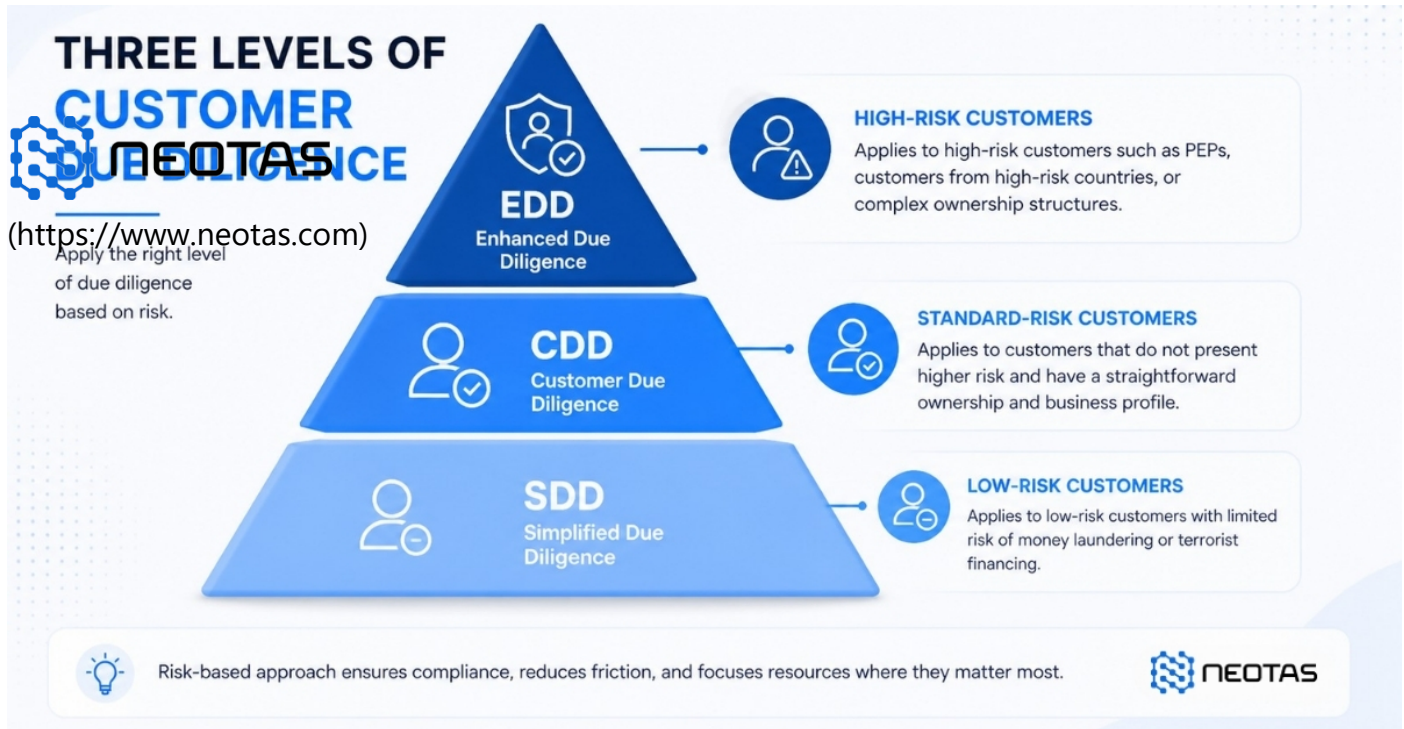


Image: Edd Vs Cdd

When is Enhanced Due Diligence Required?

EDD is required under UK Regulation 33(1) of MLR 2017 and equivalent international frameworks when specific risk conditions are present. It is not optional in these circumstances – **it is a legal obligation for regulated firms.**

The primary triggers are:

- **Politically Exposed Persons (PEPs):** The customer, or their beneficial owner, is a current or former PEP, family member, or known close associate
- **High-risk third countries:** The transaction or business relationship involves a country on the FATF grey or black list, or a jurisdiction identified as high risk by HM Treasury (UK) or FinCEN (US)
- **Unusually large or complex transactions:** Any transaction that is structurally complex or has no apparent economic or legal purpose
- **Firm-identified high risk:** The regulated entity's own risk assessment determines there is an elevated risk of money laundering or terrorist financing
- **Correspondent banking relationships:** Financial institutions maintaining accounts for other financial institutions require EDD under FATF Recommendation 13
- **Opaque ownership structures:** Customers using shell companies, nominee arrangements, or multi-layer corporate structures where the beneficial owner is unclear
- **Negative media associations:** Customers publicly linked to financial crime, corruption, sanctions breaches, or regulatory enforcement

Business relationships requiring EDD

EDD applies across the full lifecycle of a high-risk relationship. That includes onboarding, periodic review, and any triggered reassessment. The obligation continues for as long as the relationship is active and for 12 months after a PEP leaves public function, under UK MLR 2017 Regulation 35.

Manage consent

Transaction-level EDD triggers

At the transaction level, EDD is triggered by: large cash movements above AML reporting thresholds, wire transfers to or from sanctioned jurisdictions, transactions inconsistent with a customer’s declared business profile, and unusual structuring patterns such as multiple near-threshold transactions. (<https://www.neotas.com>)

The Enhanced Due Diligence checklist serves as a streamlined roadmap through the due diligence process (<https://www.neotas.com/due-diligence/>). By offering a systematic approach, it enhances efficiency and reduces the likelihood of errors or omissions. This organised method proves especially crucial when dealing with intricate transactions or partnerships that involve multifaceted considerations.

EDD vs CDD vs SDD: What is the Difference?

Aspect	SDD Simplified Due Diligence	CDD Standard Customer Due Diligence	EDD Enhanced Due Diligence
Who it applies to	Low-risk customers	Standard-risk customers	High-risk customers (e.g., PEPs, high-risk countries, complex ownership)
Purpose	Establish basic identity and assess low risk	Establish identity, understand the customer and assess risk	Obtain deeper understanding and manage higher risk
Information required	Basic identity information	Identity, address, business activity, source of funds/wealth	Additional information on source of wealth, funds, purpose of account, ownership and control, etc.
Verification level	Basic verification	Standard verification	Enhanced verification using reliable and independent sources
Ongoing monitoring	Simplified monitoring	Regular monitoring	Enhanced and more frequent monitoring
Examples	Low-value accounts, limited products/services, low-risk jurisdictions	Retail customers, most business accounts	PEPs, high-risk jurisdictions, complex structures, higher-risk industries

 A risk-based approach ensures compliance, reduces friction, and focuses resources where they matter most.



Feature	SDD (Simplified)	CDD (Standard)	EDD (Enhanced)
Who it applies to	Low-risk customers (e.g., listed companies, regulated financial institutions, government bodies)	All regulated customers by default	High-risk customers, PEPs, high-risk jurisdiction relationships, correspondent banks
Verification depth	Reduced	Full name, address, date of birth or incorporation	All CDD plus source of funds, source of wealth, full UBO mapping
Source of funds check	No	No (unless separately flagged)	Yes, mandatory

Manage consent

Feature	SDD (Simplified)	CDD (Standard)	EDD (Enhanced)
 PEP screening Basic (https://www.neotas.com)		Standard	Enhanced, including family members and close associates
Ongoing monitoring	Periodic	Regular	Enhanced frequency, with trigger-based reviews
Senior management approval	Not required	Not required	Required under UK Regulation 33(5) for PEPs and high-risk third countries
Regulatory trigger (UK)	Regulation 37, MLR 2017	Regulation 28, MLR 2017	Regulation 33, MLR 2017
Regulatory trigger (US)	N/A	FinCEN CDD Rule, 31 CFR 1010.230	BSA / USA PATRIOT Act Section 312, FinCEN guidance
Documentation requirement	Reduced	Standard file	Full audit trail required

When EDD is required, it does not replace CDD. It adds to it. A compliance officer running EDD on a PEP must first complete all standard CDD steps, then apply the additional EDD measures above.

Read more on Simplified Due Diligence (<https://www.neotas.com/what-is-simplified-due-diligence/>), Customer Due Diligence Requirements (<https://www.neotas.com/customer-due-diligence-requirements/>), and EDD for High Risk Customers (<https://www.neotas.com/enhanced-due-diligence-for-high-risk-customers/>)

The Complete Enhanced Due Diligence Checklist

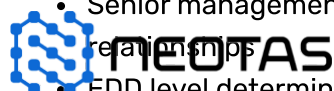
The checklist below covers 9 stages of a complete EDD assessment. Each section maps to specific regulatory obligations under UK MLR 2017, FATF Recommendations, and the US Bank Secrecy Act. Use it as a working reference for client onboarding, periodic review, or triggered reassessment.

1. Pre-Assessment Risk Scoping

Before any verification begins, define the scope and risk parameters of the assessment.

- Subject type: individual, corporate entity, trust, or fund
- Business relationship purpose: onboarding, investment, acquisition, or vendor approval
- Initial risk rating: low / medium / high, based on jurisdiction, sector, and ownership structure
- Countries of incorporation and operation (flag FATF grey and black list countries)
Manage consent

- Applicable regulatory framework: UK MLR 2017, FCA rules, Bribery Act 2010, US BSA, GDPR / UK GDPR
- Senior management approval: required under Regulation 33(5) for PEPs and high-risk third country relationships
- EDD level determination: standard EDD or heightened EDD for very high-risk subjects



(<https://www.neotas.com>)

2. Identity and Beneficial Ownership Verification

- Full legal name, aliases, and trading names
- Date of birth (individual) or date of incorporation (corporate entity)
- Registered address and principal operating address
- Government-issued photo ID verification for individuals
- UBO identification: all beneficial owners above the applicable threshold (10% per FATF Recommendation 10; 25% under UK MLR 2017 for standard CDD, lower thresholds recommended for EDD)
- Corporate registry cross-check for all countries of incorporation
- Nominee director and shareholder screening
- Trust structure mapping where applicable
- Third-country shell company identification

Regulatory note: Beneficial ownership verification requirements were strengthened in the UK by the Economic Crime and Corporate Transparency Act 2023, which introduced identity verification requirements at Companies House. In the US, the Corporate Transparency Act 2024 (CTA) introduced new beneficial ownership reporting obligations to FinCEN.

3. PEP and Sanctions Screening

- Current PEP status across all jurisdictions of relevance
- Former PEP status: under UK MLR 2017 Regulation 35, enhanced monitoring continues for a minimum of 12 months after a PEP leaves public function
- Close associates and immediate family members of current and former PEPs
- Sanctions list screening: HM Treasury Consolidated List (UK), OFAC SDN List (US), UN Security Council Consolidated List, EU Consolidated Sanctions List
- Adverse media screening: minimum 10-year lookback, in the subject's native language where material
- Regulatory enforcement databases: FCA Register, FinCEN enforcement actions, OFSI civil penalties (UK)
- Interpol notices and international law enforcement databases where applicable

4. Source of Funds and Source of Wealth Verification

- Documentation of primary income and revenue streams
 - Verification of asset ownership against declared wealth
 - Audited accounts and tax filings for corporate subjects
 - Cross-referencing declared source of funds with third-party data sources
 - Offshore account identification and assessment
 - Cryptocurrency exposure: wallet history, exchange relationships, and tracing to fiat conversion points
- Manage consent

- Evidence of unusual wealth accumulation relative to the subject's declared profession or business activity

5. Business Activity and Transaction Profile

(<https://www.neotas.com>)

- Detailed description of business model and revenue streams
- Assessment against high-risk sector indicators: gambling, cryptocurrency, precious metals, cash-intensive businesses, arms trade, money service businesses
- Geographic transaction patterns and correspondent banking relationships
- Transaction volume and frequency benchmarked against sector norms
- Unusual transaction pattern flags: structuring, round-dollar amounts, irregular timing, layering indicators

6. Adverse Media and Reputational Screening

- Structured adverse media search: minimum 10-year lookback, in native language where material
- Litigation and regulatory enforcement history across all relevant jurisdictions
- ESG-related risks: modern slavery, environmental crime, human rights abuses, conflict minerals
- Anti-bribery and corruption risk assessed against the UK Bribery Act 2010 and US Foreign Corrupt Practices Act (FCPA)
- Political associations beyond declared PEP status
- Negative judicial outcomes: civil judgments, criminal convictions, director disqualifications

7. Corporate Structure and Ownership Analysis

- Full corporate ownership map to the ultimate beneficial owner level
- Subsidiary and parent company review across all jurisdictions
- Cross-border holding structure analysis
- Identification of opaque ownership arrangements and nominee structures
- UBO declaration verified against corporate registry data
- Assessment of whether the ownership structure has a legitimate commercial rationale or appears designed to obscure control

8. Regulatory and Compliance Posture

- Regulatory registration and licensing verification: FCA Financial Services Register (UK), SEC / FINRA registration (US), equivalent international registers
- AML and compliance programme assessment
- Sanctions and export control compliance review
- Data protection compliance: UK GDPR / EU GDPR, US CCPA
- Evidence of past regulatory breaches, FCA enforcement actions, FinCEN penalties, or OFAC designations
- FATF grey / black list country exposure across the corporate group

9. Ongoing Monitoring Plan

- Adverse media and sanctions re-screening frequency: minimum quarterly for high-risk subjects, continuous for PEPs
- Trigger-based review events: leadership or ownership change, acquisition announcement, regulatory investigation, financial distress, jurisdiction change
- Annual KYC refresh schedule with documented rationale for the assigned risk rating

- Centralised audit log of all EDD activities, decisions, and escalation records
- Continuous monitoring integration: where an automated EDD or TPRM platform is in use, document the monitoring protocol and alert thresholds



Download (from neotas.com)

Download the complete EDD checklist as a printable PDF.

Structured for use in client files and regulatory audit trails. Covers all 9 sections above with checkboxes, regulatory references, and a risk narrative template.

Name

Phone number*

Company Email*

DOWNLOAD NOW

Enhanced Due Diligence Checklist Template

1. Conduct a Risk-Based Assessment

- Define **risk assessment parameters** (e.g., customer type, business sector, country of operation).
- Assign a **risk rating** (low, medium, high) to the customer or transaction.
- Allocate resources **proportionally**—higher-risk cases require deeper scrutiny.

2. Collect & Verify Customer Information

- Full legal name and aliases
- Date of birth (individuals) / incorporation (businesses)
- Nationality or jurisdiction of incorporation
- Residential or business address
- Contact details (phone and email)
- Company registration and corporate structure (if applicable)

[Manage consent](#)

3. Understand the Nature of Business & Activities



- Describe the **customer's business model** and typical transactions.
 - Assess if the industry is **high-risk** (e.g., gambling, cryptocurrency, precious metals).
 - Identify **ultimate beneficiaries** and controlling individuals.
- (<https://www.neotas.com>)

4. Verify Source of Funds & Wealth

- Identify and document the **origin of funds**.
- Ensure funds are consistent with **declared income or revenue streams**.
- Cross-check against **public records, tax filings, and bank statements**.

5. Assess Transaction History & Patterns

- Analyse past transactions for **consistency with expected behaviour**.
- Identify **large, irregular, or high-frequency transactions**.
- Flag any transactions linked to **high-risk jurisdictions**.

6. Conduct a Geographic Risk Assessment

- Assess whether the customer operates in a **high-risk country**.
- Check against **sanctions lists (UK, EU, UN, US OFAC, etc.)**.
- Consider regional AML compliance and regulatory variations.

7. Screen for Politically Exposed Persons (PEPs)

- Identify if the individual holds a **prominent political or public role**.
- Extend screening to **family members and close associates**.
- Assess potential **corruption risks** and relationships.

8. Cross-Check Against Sanctions & Watchlists

- Screen customer details against **government-issued sanctions lists**.
- Monitor against **terrorist watchlists and financial crime databases**.
- Ensure compliance with the **UK Financial Conduct Authority (FCA) guidelines**.

9. Conduct Reputational & Media Reviews

- Investigate **adverse media reports, lawsuits, or regulatory penalties**.
- Use **reliable sources** such as press releases, financial reports, and global databases.
- Assess the **credibility and impact** of any negative findings.

10. Identify High-Risk Indicators

- Unexplained **large transactions** or **multiple accounts** under similar names.
- **Use of intermediaries** or shell companies to obscure ownership.
- **Frequent cash transactions** or movement of funds to offshore accounts.

11. Establish Enhanced Monitoring & Reporting Measures



NEOTAS

- Set up **real-time monitoring** of transactions.
- Establish **thresholds** and **alerts** for suspicious activities. (<https://www.neotas.com/enhanced-due-diligence-checklist/>)
- Regularly update **customer risk profiles**.
- Report suspicious activities to **regulatory bodies** (e.g., FCA, HMRC, NCA).

12. Maintain Thorough Documentation & Records

- Maintain detailed **records of all due diligence steps**.
- Ensure compliance with **UK data protection laws (GDPR)**.
- Store customer files securely for **regulatory audits**.

Download Enhanced Due Diligence Template

Name

Name

Phone number*

Company Email*

Email

DOWNLOAD NOW

How to Use This EDD Checklist

Running EDD is not a linear tick-box exercise. Each step informs the next. Start with scope, let the risk rating guide your depth, and document every decision.

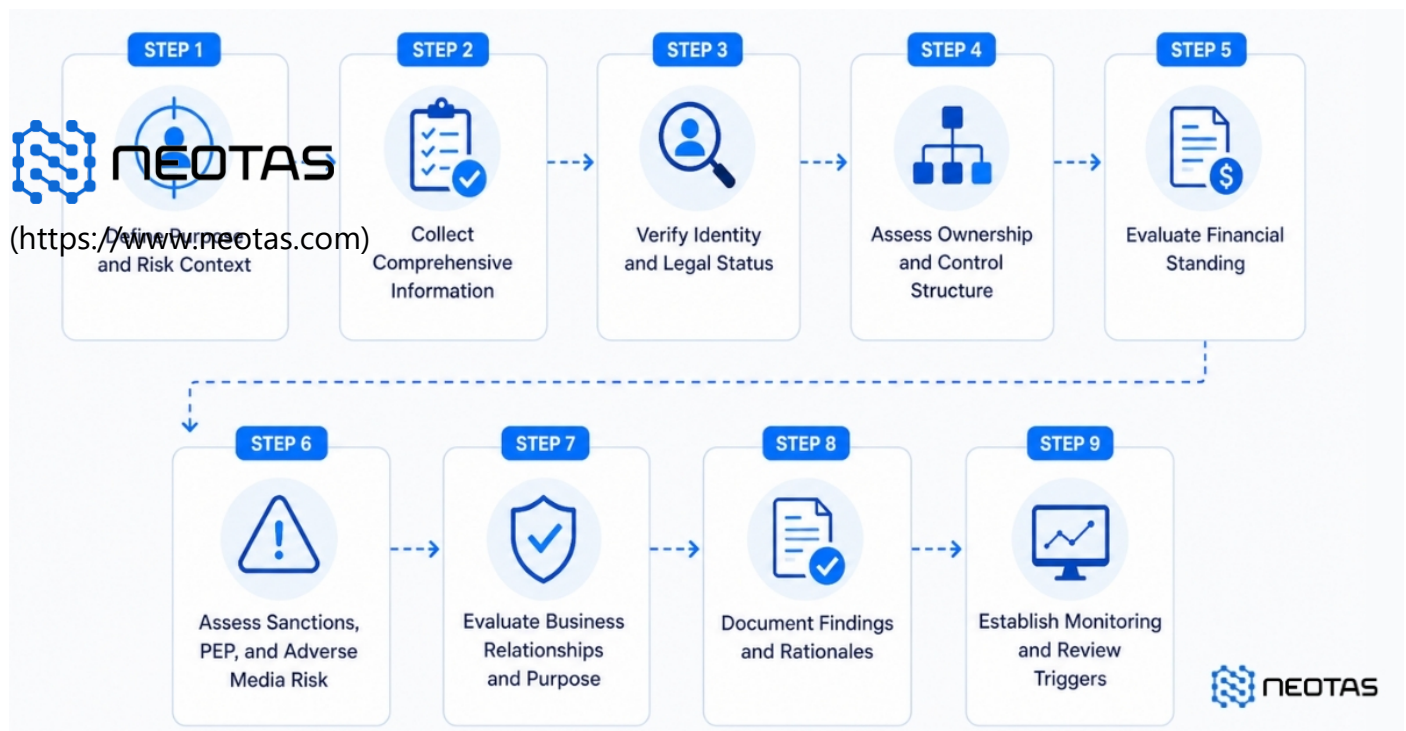


Image: Edd Checklist Steps

Step 1: Define the risk scope before you start any checks

Set the parameters first. Who is the subject? What is the relationship purpose? What jurisdictions are involved?

Assign a preliminary risk rating: low / medium / high. This determines which checklist sections need the most rigour and whether senior management sign-off is required before you proceed.

Key actions:

- Confirm subject type: individual, corporate, trust, or fund
- Flag any FATF grey or black list jurisdictions
- Check whether Regulation 33(5) (UK) or PATRIOT Act Section 312 (US) applies
- Obtain MLRO or senior management approval if required

Step 2: Gather identity and ownership data from primary sources

Work through Sections 2 and 3 of the checklist. Cross-check every key fact across at least 2 independent sources. Document where information is consistent and where it is not.

Reliable sources include: Companies House, FinCEN BOSS system, corporate registries in relevant jurisdictions, government-issued ID, OFAC, HM Treasury Consolidated List, UN Consolidated List.

Watch for: Information that differs between sources, nominee arrangements with no commercial rationale, ownership chains that terminate in unverifiable entities.

Step 3: Trace source of funds, then source of wealth



Source of funds tells you where the money for this transaction came from. Source of wealth tells you how the subject built this over time. Both are required for a complete EDD file.

Obtain documentary evidence: audited accounts, sale agreements, tax records, inheritance documents. Cross-reference against the subject's declared profile.

For corporate subjects, map the full ownership structure to UBO level before drawing conclusions. Multiple holding layers across jurisdictions without clear commercial logic is a red flag, not just a complexity.

Step 4: Configure ongoing transaction monitoring before sign-off

Do not set generic monitoring thresholds. Calibrate alert parameters to the specific risk profile of this customer: sector, geography, expected transaction volume, and declared business purpose.

Document: the monitoring configuration, the review frequency, and who is responsible for triage.

Where automated alerts fire, a trained analyst must review them. Both the alert and the review decision need an audit trail.

Step 5: Run structured adverse media screening

Search on: full legal name, known aliases, associated entities, and key individuals. Cover a minimum 10-year lookback. For subjects with operations in non-English-speaking markets, search in the relevant native language.

When a finding appears, assess two things: **relevance** and **credibility**. A resolved civil matter from 12 years ago is not the same as a live regulatory investigation. Document your assessment either way.

If a finding is material and cannot be resolved: escalate to the MLRO before proceeding.

Step 6: Conduct an on-site visit for high-risk entities

Remote verification has limits. For relationships assessed as high risk, an on-site visit confirms that the business exists, operates as declared, and that the people controlling it are who they say they are.

Document: attendees, premises inspected, documents reviewed, and any observations inconsistent with the declared business profile. The on-site record is part of the EDD file and may be reviewed by a regulator.

This step is standard practice for high-value correspondent banking relationships, complex corporate structures, and any case where remote checks have left material gaps.



Step 7: Write the report and lock in the monitoring schedule

The EDD report is a legal document. It may be reviewed by the FCA, FinCEN, an auditor, or a court.

Every report must cover:

- Subject and scope of the assessment
- Methodology and sources used
- Key findings across all checklist sections
- Risk rating assigned and the reasoning behind it
- Any unresolved issues, escalation decisions, or SAR referrals
- Ongoing monitoring plan: frequencies, trigger events, next review date

Write conclusions that are supported by evidence in the file. Where a judgment call was made, explain the reasoning. Sign it off before the relationship proceeds.

Sector-Specific EDD Considerations

EDD requirements and practical application vary by sector. The triggers are the same, but the depth, focus, and documentation differ.

EDD for financial institutions and banks

For financial institutions, EDD obligations extend beyond individual customer relationships. Correspondent banking relationships require EDD under FATF Recommendation 13, regardless of perceived risk level. This includes establishing the nature and purpose of the relationship, gathering information about the respondent institution's AML controls, and obtaining senior management approval before opening the account.

In the US, financial institutions are subject to the Bank Secrecy Act, FinCEN's CDD Rule (31 CFR 1010.230), and enhanced scrutiny requirements under USA PATRIOT Act Section 312 for foreign correspondent and private banking accounts.

In the UK, FCA-regulated firms must comply with MLR 2017 and the FCA's Financial Crime Guide, which provides sector-specific guidance on EDD documentation and risk assessment standards.

EDD for corporate and third-party risk management (TPRM)

EDD principles apply directly to corporate vendor and supplier risk programmes. High-risk third parties – those operating in sanctioned jurisdictions, holding government contracts, or acting as intermediaries in regulated industries – warrant EDD-equivalent checks as part of any TPRM framework.

Manage consent

UK companies are subject to Section 7 of the Bribery Act 2010, which requires adequate procedures to prevent bribery by associated persons. The UK Modern Slavery Act 2015 and the EU Corporate Sustainability Due Diligence Directive (CSDDD) extend due diligence obligations into supply chains. EDD supports compliance with all three.



(<https://www.neotas.com>)

EDD for private equity, investment, and M&A

In investment contexts, EDD is applied to target companies, management teams, and co-investors. The focus shifts from AML compliance to reputational risk, undisclosed litigation, UBO verification, and anti-bribery exposure in emerging markets. EDD conducted before deal close reduces post-acquisition liability and supports warranty and indemnity insurance underwriting.

EDD for professional services firms

Legal, accounting, and consulting firms subject to UK MLR 2017 must apply EDD when establishing client relationships involving high-risk factors. The ICAEW and Law Society publish AML guidance that specifies EDD triggers and documentation standards for their respective professions. Client file opening procedures must reflect these standards.

Regulatory Framework: When EDD is Legally Required

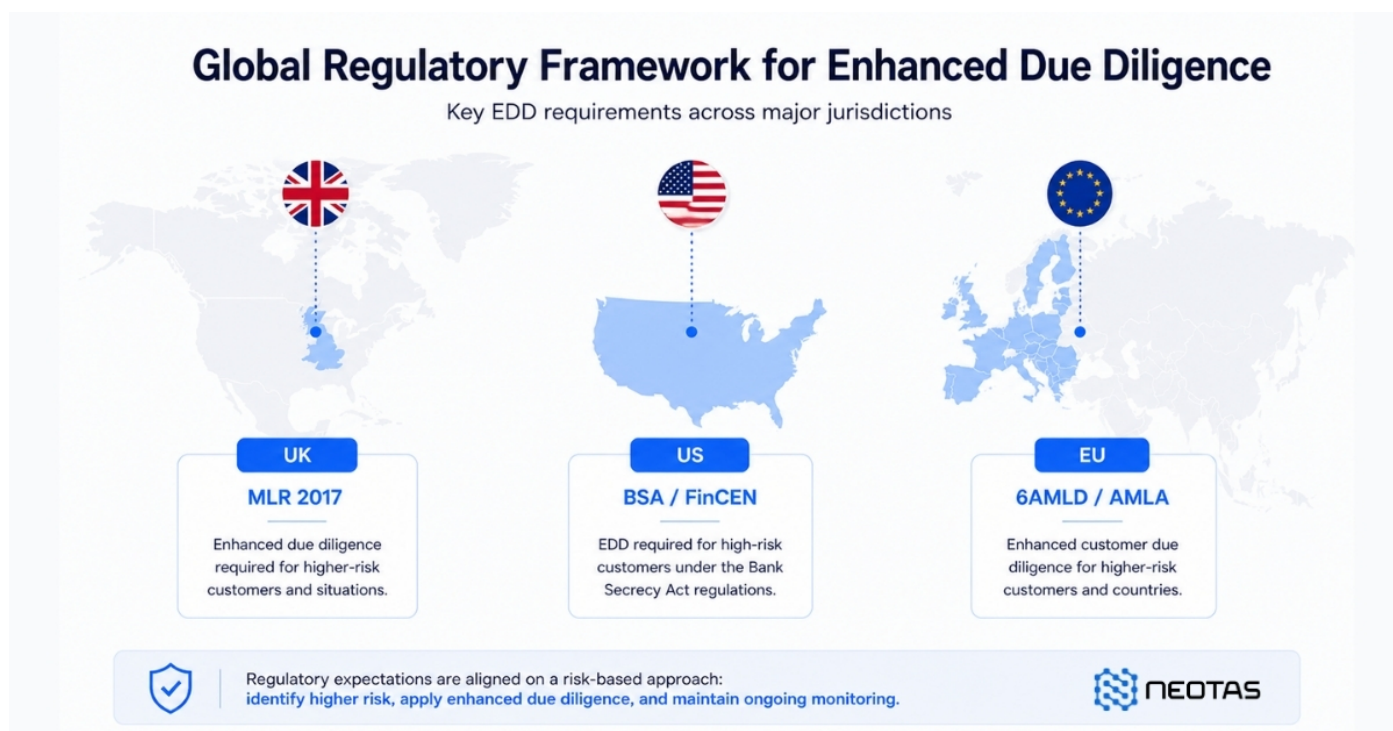


Image: Global Regulatory Framework For Enhanced Due Diligence

UK: Money Laundering Regulations 2017 (MLR 2017)

Under Regulation 33(1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, enhanced due diligence and enhanced ongoing monitoring are legally required when:
(<https://www.neotas.com>)

- The customer or beneficial owner is a PEP, family member, or close associate
- The transaction or business relationship involves a high-risk third country identified by HM Treasury
- Any transaction is unusually large, complex, or has no apparent economic or legal purpose
- The regulated entity identifies a high risk of money laundering or terrorist financing through its own risk assessment

Regulation 33(5) additionally requires senior management approval before establishing or continuing a business relationship with a PEP or a customer from a high-risk third country.

Full regulatory text is available from the UK government: The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 – Regulation 33

FATF Recommendations: the international standard

The Financial Action Task Force (FATF) sets the international standard for AML and counter-terrorist financing. The key Recommendations for EDD are:

- **Recommendation 10:** Requires financial institutions to understand the nature and purpose of customer relationships and conduct continuous due diligence, with enhanced measures for higher-risk situations
- **Recommendation 12:** Specifies EDD measures for Politically Exposed Persons, including source of funds verification and senior management approval
- **Recommendation 13:** Requires EDD for all correspondent banking relationships, including respondent institution assessment and prohibition on shell bank relationships
- **Recommendation 19:** Requires enhanced measures for transactions and relationships involving FATF-monitored jurisdictions (grey and black lists)

FATF Recommendations are available at: <https://www.fatf-gafi.org/en/topics/fatf-recommendations.html>

US: Bank Secrecy Act and FinCEN CDD Rule

Under the Bank Secrecy Act and FinCEN's Customer Due Diligence Rule (31 CFR 1010.230), covered financial institutions must:

- Verify the identity of beneficial owners of legal entity customers
- Understand the nature and purpose of customer relationships
- Conduct ongoing monitoring for suspicious activity
- Apply enhanced scrutiny under USA PATRIOT Act Section 312 for foreign correspondent and private banking accounts

FinCEN's CDD Rule requires identification of beneficial owners holding 25% or more of equity and one individual with significant control. EDD applies where risk assessments identify elevated exposure.

FinCEN CDD Rule guidance: <https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule>

EU: 6th Anti-Money Laundering Directive (6AMLD) and AMLA



The EU's 6th Anti-Money Laundering Directive aligns materially with UK MLR 2017 obligations. The forthcoming European Anti-Money Laundering Authority (AMLA), expected to become operational in 2027, will introduce a unified AML supervisory framework across EU member states with additional cross-border EDD provisions for high-risk entities.

EDD Red Flags and Escalation Triggers

The following indicators require an immediate EDD review or escalation to the MLRO for SAR consideration under UK POCA 2002.

Customer-level red flags

- Reluctance or refusal to provide identity documentation or source of funds information
- Inconsistency between declared income, lifestyle, and transaction behaviour
- Beneficial ownership structure that appears designed to obscure true control
- Prior adverse media findings inconsistent with the customer's explanation
- Undisclosed political connections or relationships with sanctioned individuals or entities
- Significant discrepancy between declared business activity and actual transaction patterns

Transaction-level red flags

- Cash transactions above AML reporting thresholds without clear economic rationale
- Wire transfers to or from FATF grey or black list jurisdictions without documented business purpose
- Round-dollar transactions or structuring patterns that suggest deliberate threshold avoidance
- Payment methods inconsistent with the customer's stated business profile
- Rapid movement of funds across multiple accounts or jurisdictions (layering indicators)

Business relationship red flags

- Corporate structure with excessive layers relative to the size and nature of the business
- Nominee arrangements with no legitimate commercial justification
- Requests for unusual payment routes, currencies, or payment intermediaries
- Unwillingness to accept standard contractual compliance terms
- Significant unexplained changes in transaction volume or business activity

Escalation rule: Where 3 or more of these red flags apply to a single customer, an immediate EDD review and MLRO consultation is warranted. Where the review identifies known, suspected, or reasonably suspected money laundering, a Suspicious Activity Report (SAR) must be submitted to the National Crime Agency (UK) or FinCEN (US) before proceeding.

Ongoing Monitoring: Turning EDD from a Point-in-Time Check into a Continuous Control



NEOTAS

<https://www.neotas.com>

Ongoing monitoring is not optional. It is a legal requirement under UK MLR 2017 Regulation 28(11) and Regulation 33(1)(c). The frequency and depth of monitoring must be proportionate to the assigned risk rating and updated when circumstances change.

Monitoring frequencies by risk level

Risk Level	Adverse Media Screening	Sanctions Rescreening	KYC Refresh
High risk (including PEPs)	Continuous or monthly	Continuous or weekly	Annual minimum
Medium-high risk	Quarterly	Monthly	Every 2 years
Standard high-risk	Semi-annual	Quarterly	Every 3 years

Trigger-based review events

Regardless of the scheduled review cycle, an immediate reassessment is required when:

- A key director, UBO, or controlling person changes
- The customer announces or completes a merger or acquisition
- A regulatory investigation or enforcement action is reported in any relevant jurisdiction
- A significant adverse media finding is identified that is inconsistent with the prior risk rating
- The customer moves operations to or from a FATF-monitored jurisdiction
- Significant changes in transaction volume, pattern, or counterparty profile occur

About Neotas Enhanced Due Diligence

Neotas Platform covers **600Bn+** archived web pages, **1.8Bn+** court records, **198M+** corporate records, global social media platforms, and **40,000+** Media sources from over 100 countries to help you build a comprehensive picture of the team. It's a world-first, searching beyond Google. Neotas' diligence uncovers illicit activities, reducing financial and reputational risk.

How Neotas Conducts Enhanced Due Diligence

Neotas conducts enhanced due diligence investigations for financial institutions, corporate risk teams, private equity firms, and professional services firms. Each investigation is carried out by an experienced analyst using OSINT, proprietary data sources, and structured adverse media research.

Manage consent

Due Diligence Solutions:



- Enhanced Due Diligence (<https://www.neotas.com/enhanced-due-diligence/>)
- Management Due Diligence (<https://www.neotas.com/management-due-diligence/>)
- Customer Due Diligence ([https://www.neotas.com/customer-due-diligence/?source=about_page--\(https://www.neotas.com\)-----](https://www.neotas.com/customer-due-diligence/?source=about_page--(https://www.neotas.com)-----))
- Simplified Due Diligence (<https://www.neotas.com/what-is-simplified-due-diligence/>)
- Third Party Risk Management (<https://www.neotas.com/third-party-risk-management/>)
- Open Source Intelligence (OSINT) (https://www.neotas.com/open-source-intelligence-osint/?source=about_page-----)
- Introducing the Neotas Enhanced Due Diligence Platform (<https://www.youtube.com/watch?v=StowdIU8Cs>)

Due Diligence Checklists:

- Due Diligence Checklist (DD) (<https://neotas.com/due-diligence-checklist/>)
- Customer Due Diligence Checklist (CDD) (<https://neotas.com/customer-due-diligence-checklist/>)
- Vendor Due Diligence Checklist (VDD) (<https://neotas.com/vendor-due-diligence-checklist/>)
- Third-Party Risk Management Framework (<https://www.neotas.com/third-party-risk-management-framework/>)
- ESG Due Diligence Checklist (ESG) (<https://neotas.com/esg-due-diligence-checklist/>)
- Investment Due Diligence Checklist (IDD) (<https://www.neotas.com/investment-due-diligence-checklist/>)
- Private Equity Due Diligence Checklist (PE DD) (<https://www.neotas.com/private-equity-due-diligence-checklist/>)
- AML Compliance Checklist (AML) (<https://neotas.com/aml-compliance-checklist/>)
- Risk-Based Approach Checklist (RBA) (<https://neotas.com/risk-based-approach-rba-checklist-for-banking-sector/>)
- Vendor Risk Assessment Template (VRA) (<https://www.neotas.com/vendor-risk-assessment-template/>)
- Vendor Due Diligence Questionnaire (VDDQ) (<https://www.neotas.com/vendor-due-diligence-checklist-and-questionnaire/>)



(<https://www.neotas.com/>)

Manage Financial Compliance and Business Risk with Enhanced Due Diligence

(<https://www.neotas.com/enhanced-due-diligence/>) and OSINT (<https://www.neotas.com/open-source-intelligence-osint/>).

Neotas is an Enhanced Due Diligence Platform (<https://www.neotas.com/>) that leverages AI to join the dots between Corporate Records, Adverse Media and Open Source Intelligence (OSINT).

Schedule a Call (<https://www.neotas.com/schedule-a-call/>) or Book a Demo (<https://www.neotas.com/request-a-demo/>) of Neotas Enhanced Due Diligence Platform.

FAQs on Enhanced Due Diligence Checklists

1. What is enhanced due diligence (EDD)?

Enhanced due diligence is a deeper level of customer assessment applied to high-risk individuals, corporate entities, and transactions. It goes beyond standard CDD by requiring source of funds verification, full beneficial ownership mapping, PEP and sanctions screening, adverse media research, and ongoing monitoring. Under UK MLR 2017 Regulation 33 and FATF Recommendation 10, EDD is a legal obligation for regulated firms in specific circumstances, not an optional upgrade.

2. What is an enhanced due diligence checklist?

An enhanced due diligence checklist is a structured set of verification steps used to assess high-risk customers, counterparties, or third parties. It covers 9 stages: pre-assessment risk scoping, identity and UBO verification, PEP and sanctions screening, source of funds verification, business activity profiling, adverse media screening, corporate structure analysis, regulatory compliance assessment, and an ongoing monitoring plan. It is legally required under UK MLR 2017 Regulation 33, FATF Recommendation 10, and the US Bank Secrecy Act.

3. When is enhanced due diligence required?

EDD is legally required when a customer is a PEP or family member, when the relationship involves a FATF grey or black list country, when a transaction is unusually large or has no clear economic purpose, or when the firm's own risk assessment identifies elevated money laundering risk. In the US, USA PATRIOT Act Section 312 also requires EDD for foreign correspondent and private banking relationships.

4. What is the difference between EDD and CDD?

CDD (Customer Due Diligence) is the standard verification process applied to all customers. EDD applies to high-risk customers only and adds source of funds verification, full UBO mapping, enhanced adverse media searches with a minimum 10-year lookback, senior management approval requirements, and more frequent ongoing monitoring. EDD does not replace CDD – it builds on it. All EDD investigations must complete standard CDD steps first.

5. What does an EDD checklist include?

A complete EDD checklist covers: pre-assessment risk scoping, identity and beneficial ownership verification, PEP and sanctions screening, source of funds and source of wealth verification, business activity and transaction profiling, adverse media and reputational screening, corporate structure analysis, regulatory and compliance posture review, and an ongoing monitoring plan. The Neotas EDD checklist covers all 9 sections across 48 individual verification points.

6. What are the FATF requirements for enhanced due diligence?

FATF Recommendation 10 requires continuous due diligence with enhanced measures for high-risk customers. Recommendation 12 mandates EDD for all PEPs, including source of funds verification and senior management approval. Recommendation 13 requires EDD for every correspondent banking relationship. Recommendation 19 requires enhanced measures for transactions involving FATF grey or black list jurisdictions. These four Recommendations form the international baseline that UK, US, and EU domestic regulations implement.

7. What triggers an EDD review mid-relationship?

A triggered EDD review is required when: a key director, UBO, or controlling person changes; a regulatory investigation or enforcement action is reported in any relevant jurisdiction; significant adverse media findings emerge that are inconsistent with the prior risk rating; the customer moves operations to or from a FATF-monitored jurisdiction; or transaction patterns change materially without explanation. Scheduled reviews alone are not sufficient for high-risk relationships.

8. What are the EDD red flags that require escalation to the MLRO?

Key EDD red flags include: refusal to disclose source of funds, beneficial ownership structures designed to obscure true control, transactions to or from FATF-listed jurisdictions without documented business purpose, adverse media findings the customer cannot explain, and unusual transaction patterns such as structuring or rapid fund layering. Where 3 or more red flags apply to a single customer, immediate MLRO consultation is required under UK POCA 2002.

9. Does enhanced due diligence apply to third-party suppliers and vendors?

Yes. EDD principles apply to any third-party relationship presenting elevated risk. For corporate risk teams, this includes high-risk vendors, suppliers in sanctioned jurisdictions, and M&A counterparties. The UK Bribery Act 2010, Section 7 creates corporate liability for bribery by associated persons where adequate due diligence has not been conducted.

diligence was not conducted. The US Foreign Corrupt Practices Act (FCPA) applies the same logic. EDD is a core requirement of any compliant TPRM programme.

10. How does EDD support anti-bribery and corruption (ABC) compliance? (<https://www.neotas.com>)

EDD is a required component of any ABC compliance programme under the UK Bribery Act 2010 and US FCPA. It applies to high-risk third parties including agents, distributors, and intermediaries with government connections. An EDD investigation for ABC purposes covers PEP relationships, political donations, regulatory enforcement history, and jurisdictional corruption risk. Without it, adequate procedures defences under Section 7 of the Bribery Act are materially weakened.

11. How does EDD address ESG risks including modern slavery?

As ESG legislation expands – UK Modern Slavery Act 2015, EU Corporate Sustainability Due Diligence Directive, and emerging US supply chain laws – EDD checks are required to confirm a company is not exposed to modern slavery, human rights abuses, conflict minerals, or environmental crime through its supply chain or business partners. Open source intelligence (OSINT) surfaces ESG risks that structured database screening consistently misses, particularly in emerging markets and complex supply chains.

12. What is the difference between source of funds and source of wealth in EDD?

Source of funds confirms where the money for a specific transaction came from – a business sale, property disposal, or inheritance. Source of wealth establishes how a subject accumulated their total assets over time. Both are required in a complete EDD investigation. They are not interchangeable. A customer can have a clean source of funds for one transaction while the underlying wealth carries unexplained or undocumented elements that require further scrutiny.

Share:



**NEOTAS**

(<https://www.neotas.com/>)
(<https://www.neotas.com/>)

Neotas Enhanced Due Diligence

(<https://www.neotas.com/>)

Neotas Enhanced Due Diligence covers 600Bn+ Archived web pages, 1.8Bn+ court records, 198M+ Corporate records, Global Social Media platforms, and more than 40,000 Media sources from over 100 countries to help you screen & manage risks.

New Whitepaper and Checklist (<https://www.neotas.com/financial-crime-compliance-and-risk-management/>)

A detailed guide to TPRM and a downloadable checklist to implement the TPRM Framework in 2026

DOWNLOAD NOW →
([HTTPS://WWW.NEOTAS.COM/THIRD-PARTY-RISK-MANAGEMENT-FRAMEWORK/](https://www.neotas.com/third-party-risk-management-framework/))

Related Blog Posts



(<https://www.neotas.com>)

Vendor Risk Assessment Template

A repeatable control framework, anchored in governance and capable of standing up to regulatory or audit scrutiny.



(<https://www.neotas.com/vendor-risk-assessment-template/>)

Vendor Risk Assessment Template (<https://www.neotas.com/vendor-risk-assessment-template/>)



Risk Management Framework

A practical playbook for governance, compliance, and strategic resilience. Reduce blind-spots, cut decision-latency, and unlock risk-adjusted growth.



(<https://www.neotas.com/risk-management-framework/>)

Risk Management Framework: The Complete 2026 Guide (<https://www.neotas.com/risk-management-framework/>)

Manage consent



(<https://www.neotas.com>)

Social Media Background Checks

*Legal and Ethical Considerations in
Social Media Background Screening*



(<https://www.neotas.com/social-media-background-checks/>)

Social Media Background Checks – Are Your Social Media Background Checks Legally Sound? (<https://www.neotas.com/social-media-background-checks/>)



Third-Party Risk Management (TPRM) Methodology

*Key components, best practices, and
challenges in TPRM Methodology*



(<https://www.neotas.com/tprm-methodology/>)

TPRM Methodology – Comprehensive Guide to Third-Party Risk Management (TPRM) (<https://www.neotas.com/tprm-methodology/>)



(<https://www.neotas.com>)

Financial Crime Compliance Framework

Best Practices for Financial Crime Compliance



(<https://www.neotas.com/financial-crime-compliance-framework/>)

Financial Crime Compliance Framework

(<https://www.neotas.com/financial-crime-compliance-framework/>)



Financial Crime Compliance and Risk Management

Guide to countering Financial Crime Risks and Business Risk Management



(<https://www.neotas.com/financial-crime-compliance/>)

Financial Crime Compliance & Risk Management – Guide to countering financial crime risks (<https://www.neotas.com/financial-crime-compliance/>)

Manage consent



(<https://www.neotas.com>)

What is Risk Intelligence?

Strategic Risk Intelligence solutions, risk management framework and implementing risk intelligence to manage your business risk.



(<https://www.neotas.com/what-is-risk-intelligence/>)

Risk Intelligence: Strategic Risk Intelligence Software and Advisory Services (<https://www.neotas.com/what-is-risk-intelligence/>)



Third-Party Risk Management (TPRM) Lifecycle

Adopting a Maturity Model for Third-Party Risk Management (TPRM)



(<https://www.neotas.com/third-party-risk-management-tprm-lifecycle/>)

Third-Party Risk Management (TPRM) Lifecycle: Key Stages & Best Practices (<https://www.neotas.com/third-party-risk-management-tprm-lifecycle/>)



(<https://www.neotas.com>)

Anti-Money Laundering (AML) Law and Regulations



(<https://www.neotas.com/anti-money-laundering-regulations/>)

Anti-Money Laundering Regulations, AML Checks and Compliance (<https://www.neotas.com/anti-money-laundering-regulations/>)



AML Transaction Monitoring

*Regulatory Requirements
and Best Practices*



(<https://www.neotas.com/aml-transaction-monitoring/>)

AML transaction monitoring – Regulatory Requirements and Best Practices (<https://www.neotas.com/aml-transaction-monitoring/>)

Manage consent



(<https://www.neotas.com>)

AML Compliance Checklist for Banks

*AML Compliance Requirements,
AML Regulations and Best Practices
for Anti-Money Laundering*



(<https://www.neotas.com/aml-compliance-checklist-for-banks/>)

AML Compliance Checklist for Banks: Best Practices for Anti-Money Laundering (<https://www.neotas.com/aml-compliance-checklist-for-banks/>)



AML Compliance Checklist

*AML Compliance Requirements,
AML Regulations and Best Practices
for Anti-Money Laundering*



(<https://www.neotas.com/aml-compliance-checklist/>)

AML Compliance Checklist: Best Practices for Anti-Money Laundering (<https://www.neotas.com/aml-compliance-checklist/>)



(<https://www.neotas.com>)

Subscribe to our newsletter

Stay up-to-date on the latest trends and insights

Please enter your email address*

SUBSCRIBE



(<https://www.neotas.com>)

The Neotas Platform covers **600Bn+** archived web pages, **1.8Bn+** court records, **198M+** corporate records, global social media platforms, and **40,000+** media sources from over 100 countries to help you build a comprehensive risk assessment of individuals, entities, and their networks. AI speed. Analyst depth. Every vendor risk covered.

COMPANY

Manage consent

About Us(<https://www.neotas.com/about-us/>)

Awards and Recognition(<https://www.neotas.com/awards/>)

Blogs and Whitepapers(<https://www.neotas.com/whitepaper/>)

News and Press Releases(<https://www.neotas.com/news/>)



(<https://www.neotas.com>)

Life at Neotas(<https://www.neotas.com/life-at-neotas/>)

SOLUTIONS

Third-Party Risk Management(<https://www.neotas.com/third-party-risk-management/>)

Enhanced Due Diligence(<https://www.neotas.com/enhanced-due-diligence/>)

Employment Screening(<https://www.neotas.com/employment-screening/>)

Investigative Platform(<https://www.neotas.com/osint-investigation-platform/>)

KYC & Customer Due Diligence(<https://www.neotas.com/kyc-and-customer-due-diligence/>)

Third-Party Risk Management in Healthcare(<https://www.neotas.com/tpm-in-healthcare/>)

CASE STUDIES

TPRM Using Open-source intelligence (OSINT) (<https://www.neotas.com/case-study/third-party-risk-management-tpm-using-osint/>)

Third-Party Due Diligence for Partner Risks (<https://www.neotas.com/case-study/third-party-due-diligence-for-partnership-risks/>)

ESG Risks: Private Equity Investigation (<https://www.neotas.com/case-study/esg-risks-uncovered-in-investigation-for-global-private-equity-firm/>)

OSINT for Enhanced Due Diligence (<https://www.neotas.com/case-study/open-source-intelligence-osint-for-enhanced-due-diligence-aml-compliance/>)

Supply Chain Risk: Modern Slavery Detection (<https://www.neotas.com/case-study/open-source-intelligence-for-supply-chain/>)

RESOURCES

Third-Party Risk Management Framework (<https://www.neotas.com/third-party-risk-management-framework/>)

Vendor Due Diligence Checklist (<https://www.neotas.com/vendor-due-diligence-checklist-and-questionnaire/>)

Supply Chain Risk Assessment Template(<https://www.neotas.com/supply-chain-risk-assessment/>)

Vendor Risk Assessment Template(<https://www.neotas.com/vendor-risk-assessment-template/>)

Due Diligence Checklist(<https://www.neotas.com/due-diligence-checklist/>)

Enhanced Due Diligence Checklist(<https://www.neotas.com/enhanced-due-diligence-checklist/>)

ESG Due Diligence Checklist(<https://www.neotas.com/esg-due-diligence-checklist/>)
Manage consent

[Customer Due Diligence Checklist](https://www.neotas.com/customer-due-diligence-checklist/)

[Private Equity Due Diligence Checklist](https://www.neotas.com/private-equity-due-diligence-checklist/)



NEOTAS

[Investment Due Diligence Checklist](https://www.neotas.com/investment-due-diligence-checklist/)

[DORA Compliance Requirements](https://www.neotas.com/dora-compliance-requirements/)

GET IN TOUCH

Address:

Neotas Limited,
Coppergate House
10 Whites Row, London,
E1 7NF, United Kingdom

Email: [info\[at\]neotas\[dot\]com](mailto:info@neotas.com)

Phone: +44 (0) 208 0902 622

 [\(https://www.linkedin.com/company/neotas/\)](https://www.linkedin.com/company/neotas/)

 [\(https://www.facebook.com/Neotas/\)](https://www.facebook.com/Neotas/)

 [\(https://www.youtube.com/@neotas/videos\)](https://www.youtube.com/@neotas/videos)  [\(https://x.com/NeotasLtd\)](https://x.com/NeotasLtd)

One platform. Every third-party risk, screened, monitored, and audit-ready.

SCHEDULE A CALL
([HTTPS://WWW.NEOTAS.COM/SCHEDULE-A-CALL/](https://www.neotas.com/schedule-a-call/))

© 2026 Neotas. All rights reserved. (<https://www.neotas.com>)

[Client Login](https://portal.neotas.com/client/login) | [Cookie Policy](https://www.neotas.com/cookie-policy/)

[Privacy Policy](https://www.neotas.com/privacy-policy/) |

[End User License](https://www.neotas.com/end-user-license-agreement/)

[Manage consent](#)