BUSINESS INTELLIGENCE
RISK INTELLIGENCE

GUIDE

Citizenship by Investment Due Diligence Guide

A Practical Framework for Assessing Applicant Risk, Wealth, Reputation and Compliance

CBI applicants often carry wealth, business interests and connections across multiple jurisdictions. This guide sets out Cedar Rose's risk-based framework for assessing that risk, from identification through to ongoing monitoring.

Contents

SECTION 01

Executive Summary

Citizenship-by-Investment (CBI) programmes assess applicants whose wealth, business interests, residency history and personal connections may span multiple jurisdictions. This cross-border profile, together with varying levels of public-record transparency and the potential involvement of intermediaries, means that CBI risk assessment requires a deeper and more tailored approach than routine customer due diligence.

Identity verification confirms that an applicant is who they claim to be. It does not establish how their wealth was built, whether the funds being used are legitimately sourced, who they are connected to, or whether their background carries reputational, political, regulatory or programme-related risk that a programme operator, financial institution or advisory firm needs to understand before onboarding.

> A defensible CBI due diligence process should extend beyond database screening and document collection. Using a risk-based approach, it should independently corroborate **Source of Wealth**, trace the **Source of Funds** for the proposed transaction, assess reputational information in context, map relevant beneficial ownership and corporate relationships, and determine whether Enhanced Due Diligence (EDD), escalation or further clarification is required under applicable law, programme requirements and internal policy.

This guide sets out a practical, risk-based framework for that process, built around six stages: Identify, Verify, Screen, Investigate, Assess and Monitor.

THE CEDAR ROSE FRAMEWORK

Each stage has a distinct objective, a defined set of questions, and a clear output that feeds into the next

01 IDENTIFY	02 VERIFY	03 SCREEN	04 INVESTIGATE	05 ASSESS	06 MONITOR
Who the applicant is and what they claim	Independent evidence for wealth and funds	PEP, sanctions and watchlist coverage	Reputation, media and network mapping	Consolidated, documented view	Rescreening and trigger events

SECTION 02

Why CBI Due Diligence Matters

Many CBI applicants have wealth, commercial interests, residency ties or family connections across more than one jrisdiction and may be applying for citizenship in a country where they have no prior residence, employment or financial history. That profile is not, in itself, a risk indicator. It is, however, a reason why identity verification alone cannot support a defensible onboarding decision.

KYC establishes and verifies identity and, where required, customer profile information. CBI due diligence builds on that foundation by developing the context needed to assess integrity, financial-crime, reputational and wider programme risk.

A due diligence file can be complete in the sense that every required document has been collected, and still be insufficient in the sense that it does not answer the questions a risk committee actually needs answered. A passport copy confirms identity. A bank reference confirms that an account exists. Neither, on its own, explains how the applicant's wealth was generated, whether it survives independent scrutiny, or whether the applicant has any history that a screening database would not surface.

A thorough process extends identity verification into a broader profile covering professional background, business interests, beneficial ownership of related entities, relevant public records, and connected individuals and entities. Each of these adds context that a name-and-document check cannot provide.

FROM IDENTITY VERIFICATION TO RISK INTELLIGENCE

IDENTITY VERIFICATION		RISK INTELLIGENCE
Documents collected Passport, proof of address	*corroborate* →	**Wealth corroborated independently** Registries, filings, public record
Name matched Spelling and dates aligned	*trace* →	**Funds traced to origin** Account to account, with rationale
Database screening run Hits listed, not resolved	*resolve* →	**Network and ownership mapped** Beneficial owners and associates
File complete Administratively, not analytically	*interpret* →	**Findings assessed in context** Verified, alleged or resolved

Depth of enquiry — Defensible decision

SECTION 03

The CBI Applicant Risk Landscape

CBI applicant risk is multidimensional. It should be assessed both by individual risk category and by the way those factors interact. In addition to applicant-level risks, the review should consider application integrity, the role of any authorised agent or intermediary, and programme-specific legal or policy requirements.

APPLICANT LEVEL

Identity, financial, reputational, network, regulatory and jurisdictional exposure.

APPLICATION LEVEL

Declaration consistency, document authenticity, undisclosed control.

PROGRAMME LEVEL

Intermediary conduct and programme-specific legal requirements.

The six risk dimensions in detail

1 • Identity Risk

Whether the applicant's identity can be established with confidence, including lawful name changes, aliases, transliteration variants, multiple nationalities, and prior applications made under different personal details. Further investigation may be required where material discrepancies cannot be satisfactorily reconciled against reliable third-party or public records.

2 • Financial Risk

Whether the applicant's wealth and the specific funds used for the investment can be independently verified and are consistent with their stated background. Further review may be warranted where the wealth narrative cannot be corroborated, or where funds originate from a source unrelated to that history.

3 • Reputational Risk

Whether adverse media, litigation, regulatory action or other public information exists in relation to the applicant, their businesses, or close associates. Findings should be assessed for credibility, relevance and materiality, particularly where they relate to financial conduct.

4 • Network Risk

Whether the applicant's corporate and personal relationships introduce risk not visible from an applicant-only review, including connections to sanctioned parties, politically exposed persons, or entities previously linked to financial crime.

5 • Regulatory Risk

Where the applicant, or entities connected to them, have been subject to regulatory scrutiny, sanctions, enforcement action or professional disciplinary proceedings, the matter should be assessed for relevance, credibility, seriousness, outcome, recency and any evidence of remediation. An allegation, inquiry or discontinued matter should not be treated as proof of misconduct.

6 • Jurisdictional Risk

Whether jurisdictions linked to the applicant's citizenship, residence, wealth, banking activity or business operations present elevated risk indicators. Assessment should consider credible sources such as FATF listings, sanctions exposure, corruption and rule-of-law indicators, AML/CFT effectiveness, and local-record transparency, while avoiding blanket assumptions based solely on nationality or location.

HOW RISK FACTORS COMPOUND

DEPTH OF INVESTIGATION WARRANTED

Isolated, explained factor	Standard due diligence
Ambiguity in one area	Targeted verification
Factors reinforcing each other	**Enhanced Due Diligence**

**Illustrative only, actual depth depends on the facts.*

SECTION 04

Source of Wealth Verification

Source of Wealth (SOW) is the origin and accumulation of an applicant's overall wealth and assets over time. It may arise from employment, business ownership, dividends, investment returns, inheritance, gifts, asset disposals, loans, trusts, family-office arrangements or other legitimate sources. The review should establish not only the stated source, but whether the evidence supports the scale, timing and lawful origin of the wealth claimed.

Assessing the narrative and the evidence

An applicant's account of how their wealth was built should be assessed for internal consistency: does the timeline of income-generating activity match the scale of wealth claimed, does their professional background plausibly support the stated earnings, and are there unexplained gaps. Supporting documentation should be assessed for authenticity, consistency, and whether it genuinely supports the specific claim being made.

Independent corroboration

Wherever possible, the applicant's own account should be corroborated against independent sources: corporate registries confirming ownership and dividend history, public records confirming asset sales, and media or industry sources confirming career or business activity. This is what distinguishes a verified position from an accepted narrative.

CLAIM, EVIDENCE, CORROBORATION

STATED CLAIM		SUPPORTING EVIDENCE		INDEPENDENT SOURCE
Business ownership	→	Shareholder register	→	Corporate registry
Dividend income	→	Financial statements	→	Registry or dividend filings
Asset disposal	→	Sale agreement	→	Land or asset register
Inheritance or gift	→	Will, deed or declaration	→	Probate or court record

WHAT MAY TRIGGER FURTHER INVESTIGATION

A wealth narrative that cannot be corroborated through reliable independent sources

Documents inconsistent with the applicant's career, business or tax history

Wealth that appears to have accumulated rapidly without a clear, verifiable driver

Ownership structures or offshore arrangements that obscure the economic beneficiary

Evidence that depends primarily on private or unaudited transactions

Document authenticity, provenance or completeness that cannot be established

SECTION 05

Source of Funds Verification

Source of Funds (SOF) is often confused with Source of Wealth, but the two answer different questions. Source of Wealth asks how the applicant's overall net worth was built. Source of Funds asks where the specific money being used for this transaction came from.

SOURCE OF WEALTH	SOURCE OF FUNDS
How was the total net worth built?	**Where did this money come from?**
The origin and accumulation of everything the applicant owns, across a career or a lifetime.	The specific funds used for this investment, traced from the originating account to the receiving account.

TRACING THE TRANSACTION

Source of Funds verification should follow the money used for the specific CBI transaction from the originating account to the approved receiving account. The review should establish the account holder, the source and availability of funds before transfer, the transaction path, intermediary banks or parties, the payment purpose, any currency conversion, and whether the payment route complies with programme and financial-institution requirements.

FOLLOW THE MONEY, STEP BY STEP

01	02	03	04	05
Originating account	**Transfer path**	**Payment purpose**	**Currency Conversion**	**Approved account**
Holder identified, funds available	Intermediary banks recorded	Stated and consistent	Conversion explained	Programme-permitted route

Funds that pass through multiple jurisdictions without clear commercial rationale, or amounts that do not reconcile with the applicant's documented income, should be treated as matters requiring further investigation rather than administrative gaps.

Third-party funding

Where third-party funding is permitted, the relationship, rationale and legal basis for the funding should be documented. The funding party should be identified and screened, and, depending on the risk profile, their Source of Wealth and Source of Funds should be independently assessed.

Supporting instruments

Gifts, loans, trust distributions and corporate payments should be supported by relevant agreements, board approvals where applicable, and evidence that the arrangement is genuine and not designed to obscure the origin or control of funds.

SECTION 06

Reputational Risk and Adverse Media

Reputational risk assessment goes well beyond running an applicant's name through a search engine. It requires a structured approach to finding relevant information, and an equally structured approach to assessing what that information means.

A review should cover adverse media, fraud and corruption allegations, financial misconduct, criminal investigations, regulatory enforcement, litigation, business controversies, and associations with other higher-risk individuals or entities, across relevant languages and jurisdictions.

HOW MUCH WEIGHT DOES A FINDING CARRY?

Credibility of the source against materiality to financial-crime or integrity risk

	LOW MATERIALITY	MODERATE MATERIALITY	HIGH MATERIALITY
HIGH CREDIBILITY	**Historic minor litigation, concluded** Record the finding. Limited weight given its age and materiality.	**Regulatory notice, remediated** Weigh the outcome, recency and remediation before assessing impact.	**Court judgment for financial misconduct** A verified, material finding. Weighs heavily in the overall assessment.
MODERATE CREDIBILITY	**Trade or industry press mention** Context only. Note and watch for further developments	**Credible investigative reporting** Corroborate against official records before giving it weight.	**Detailed corruption or fraud reporting** Corroborate carefully. Significant if substantiated.
LOW CREDIBILITY	**Anonymous blog or forum post** Record the search. Do not rely on it.	**Unattributed allegation of misconduct** Seek corroboration or a credible primary source.	**Serious claim, provenance unknown** The trap: neither dismiss it nor treat it as proven. Clarify with the applicant.

Reputational research should use a documented source hierarchy and distinguish verified official records, credible investigative reporting, industry sources, unverified allegations and content of uncertain provenance. Material findings should be corroborated where possible, assessed in context, and, where appropriate, put to the applicant or their authorised representative for clarification before a final risk recommendation is made.

Every finding should be assessed against a consistent set of criteria before it is given any weight: credibility of the source, relevance to the applicant, recency, materiality to financial crime or integrity risk, whether the applicant is directly implicated or connected through a related party, whether the matter is verified or alleged, and whether it has since been resolved.

01 Source credibility

02 Relevance to applicant

03 Recency

04 Materiality

05 Direct or connected

06 Verified or alleged

07 Since resolved

> Negative information should be assessed in context. A screening match, a court filing or an adverse media result is a starting point for analysis, **not proof of wrongdoing**.

SECTION 07

PEP and Sanctions Screening

Politically Exposed Person (PEP) status and sanctions exposure are two of the most consequential risk indicators in CBI due diligence. They are not equivalent and should not be treated as interchangeable findings: PEP status is a risk factor requiring enhanced assessment, while a confirmed sanctions match can create a legal restriction. A screening match is a trigger for investigation. It is not, on its own, a conclusion.

FROM RAW HITS TO TWO DISTINCT OUTCOMES

STAGE 1 · SCREENING UNIVERSE

- **Applicant, family, network and intermediaries**
- **Raw screening hits**
- **Biographical review** DOB, nationality, alias
- **Genuine matches**

WHY HITS FALL AWAY

- **Partial name match**
- **Transliteration**
- **Alias reuse**
- **Genuine**

Each potential match is reviewed against biographical detail before it is accepted or dismissed, and the reasoning is recorded either way.

STAGE 2 · TWO SEPARATE TRACKS

PEP CONFIRMED

A risk factor, not a prohibition. Enhanced assessment is warranted across:

- **Prominence of function**
- **Time since leaving office**
- **Influence retained**
- **Corruption exposure**
- **Source of Wealth, Source of Funds and connected parties**

Outcome: enhanced assessment across SOW, SOF and connected parties.

SANCTIONS CONFIRMED

A legal question, not a risk score. Escalate immediately and assess against:

- **Applicable regimes**
- **Asset-freeze obligations**
- **Programme rules and legal advice**

The application must not proceed except as permitted by law.

Scope of screening

PEP screening should identify the applicant's current or former political exposure, as well as family members and known close associates, in accordance with the definitions and requirements applicable to the programme and relevant jurisdictions. The assessment should consider the prominence of the function, time since leaving office, country risk, influence retained, and any associated corruption or procurement exposure.

Getting the match right

Screening accuracy depends heavily on how names are handled. Common sources of false positive and false negative results include partial name matching, alias and previous name usage, and transliteration differences. Each potential match needs to be reviewed against biographical detail, such as date of birth and nationality, before it is accepted or dismissed.

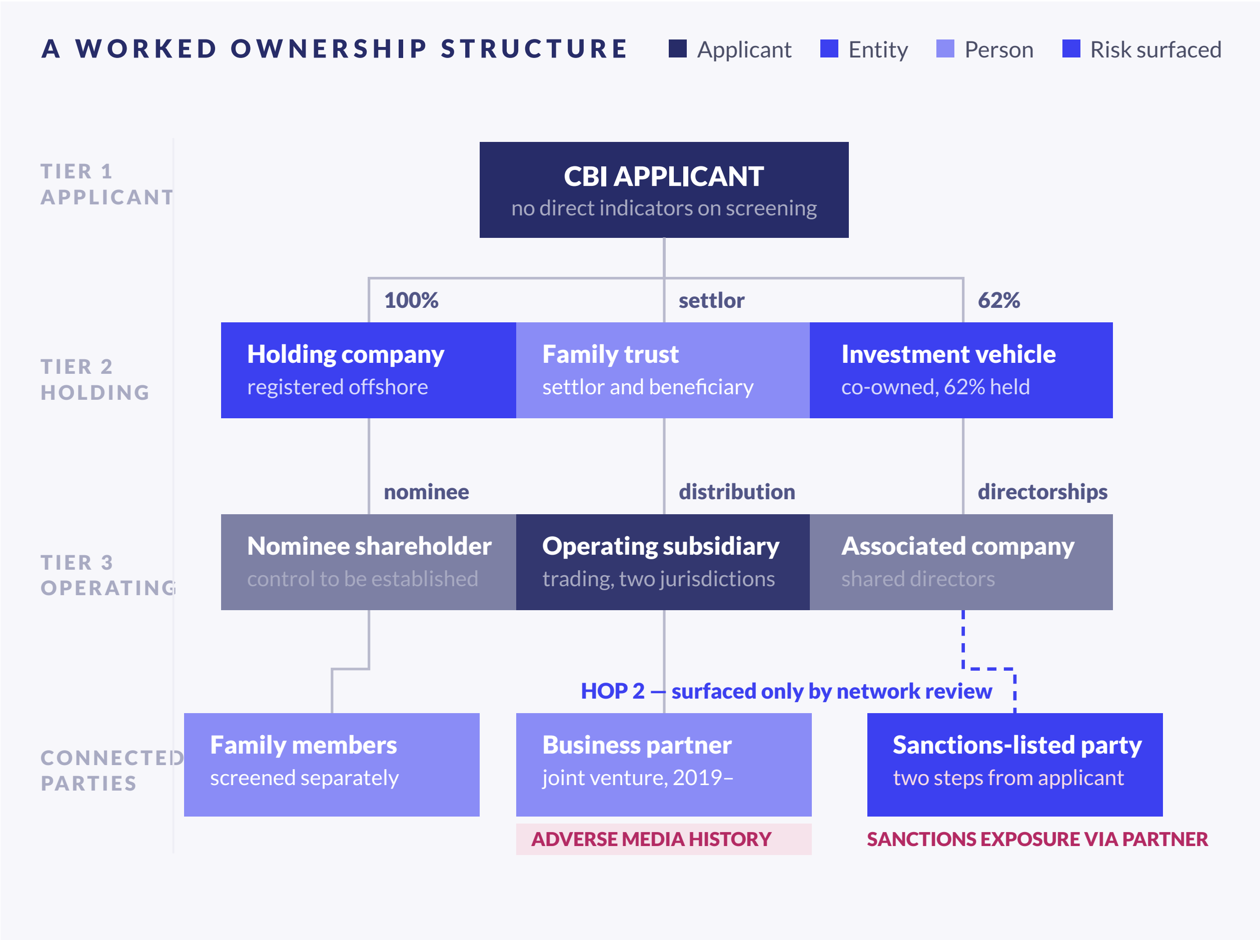
A match is a trigger, not a verdict

A confirmed PEP match doesn't require refusal, but generally warrants enhanced assessment across SOW, SOF, corruption exposure, reputation and connected parties. A confirmed sanctions match must be escalated immediately against the applicable regime, programme rules and legal obligations — the application must not proceed except as permitted by law.

SECTION 08

Beneficial Ownership and Connected Entities

A network review should identify the natural persons who ultimately own, control or benefit from relevant entities and arrangements. This should include direct and indirect shareholdings, voting rights, contractual control, nominee relationships, directorships, parent and subsidiary links, partnerships, trusts, foundations, settlors, trustees, protectors, beneficiaries and persons exercising de facto control.



Why the network matters

An applicant's personal profile may present no risk indicators at all, while a company they control, a business partner, or a related entity carries a sanctions listing, adverse media history or regulatory enforcement record. Without mapping the applicant's wider network, this exposure would not surface through applicant-only checks.

Establishing ownership

Beneficial ownership should be established using a combination of reliable sources, which may include corporate registries, constitutional documents, shareholder registers, annual returns, trust documentation, financial statements, regulatory filings and corroborated open-source information. Registry data alone may not be sufficient where disclosure requirements are limited, outdated or inconsistent with other evidence.

SECTION 09

Application Integrity, Intermediaries and Document Controls

CBI applications frequently involve authorised agents, introducers, wealth advisers, legal representatives and document preparers. Their role, incentives and reputation can materially affect fraud, bribery, conflicts of interest, document manipulation or undisclosed-control risk. Due diligence should therefore extend beyond the applicant to the integrity of the application itself.

Intermediary due diligence

Where agents, introducers, legal representatives, wealth advisers or other intermediaries are involved, the programme operator should understand their role, authority, remuneration, ownership, regulatory status and any relevant adverse information. Particular attention should be given to undisclosed intermediaries, unusual fee arrangements, document-preparation concerns, conflicts of interest and attempts to influence or bypass standard review procedures.

Document authenticity

Documents should not be treated as reliable solely because they appear complete or have been notarised. Depending on risk, verification may include confirming issuers, reviewing metadata and format consistency, obtaining records directly from authoritative sources, comparing information across independent documents, and investigating anomalies such as unexplained amendments, inconsistent dates, identical wording across unrelated documents or unusual certification patterns.

FOUR CHECKPOINTS FOR APPLICATION INTEGRITY

LAYER 01

Declarations

Complete, internally consistent, and tested against evidence

LAYER 02

Documents

Issuer confirmed, metadata and format checked, anomalies investigated

LAYER 03

Intermediaries

Role, authority, fees, ownership and regulatory status established

LAYER 04

Governance

Discrepancies, clarifications and escalation decisions documented

WATCH FOR Undisclosed intermediaries · unusual fee arrangements · identical wording across unrelated documents · unexplained amendments · attempts to influence or bypass standard review procedures.

SECTION 10

When Enhanced Due Diligence Is Required

The appropriate level of due diligence should be determined through a documented risk assessment and in accordance with applicable laws, programme rules and institutional policy. CDD may be sufficient where the risk assessment supports that conclusion. EDD is required where heightened risk indicators, legal obligations or programme-specific requirements warrant additional scrutiny.

COMMON EDD TRIGGERS

01 Confirmed or unresolved PEP exposure, or potential sanctions exposure	**05** Business activity in corruption-prone sectors
02 Links to higher-risk jurisdictions, or complex or opaque ownership structures	**06** Use of third-party funders or intermediaries
03 Unexplained wealth or transaction patterns	**07** Inconsistent application information or document authenticity concerns
04 Material adverse media, litigation or enforcement history	**08** Unexplained changes in citizenship, residency, ownership or payment arrangements

No single trigger automatically means an applicant is unacceptable. EDD is about applying a deeper level of investigation and analysis before a risk decision is made, not about pre-judging the outcome.

WHAT EDD ADDS TO THE STANDARD PROCESS

Enhanced Due Diligence typically extends the standard process through additional independent verification of wealth and funds, wider reputational research, closer examination of the applicant's network, and senior management or risk committee review before a decision is made.

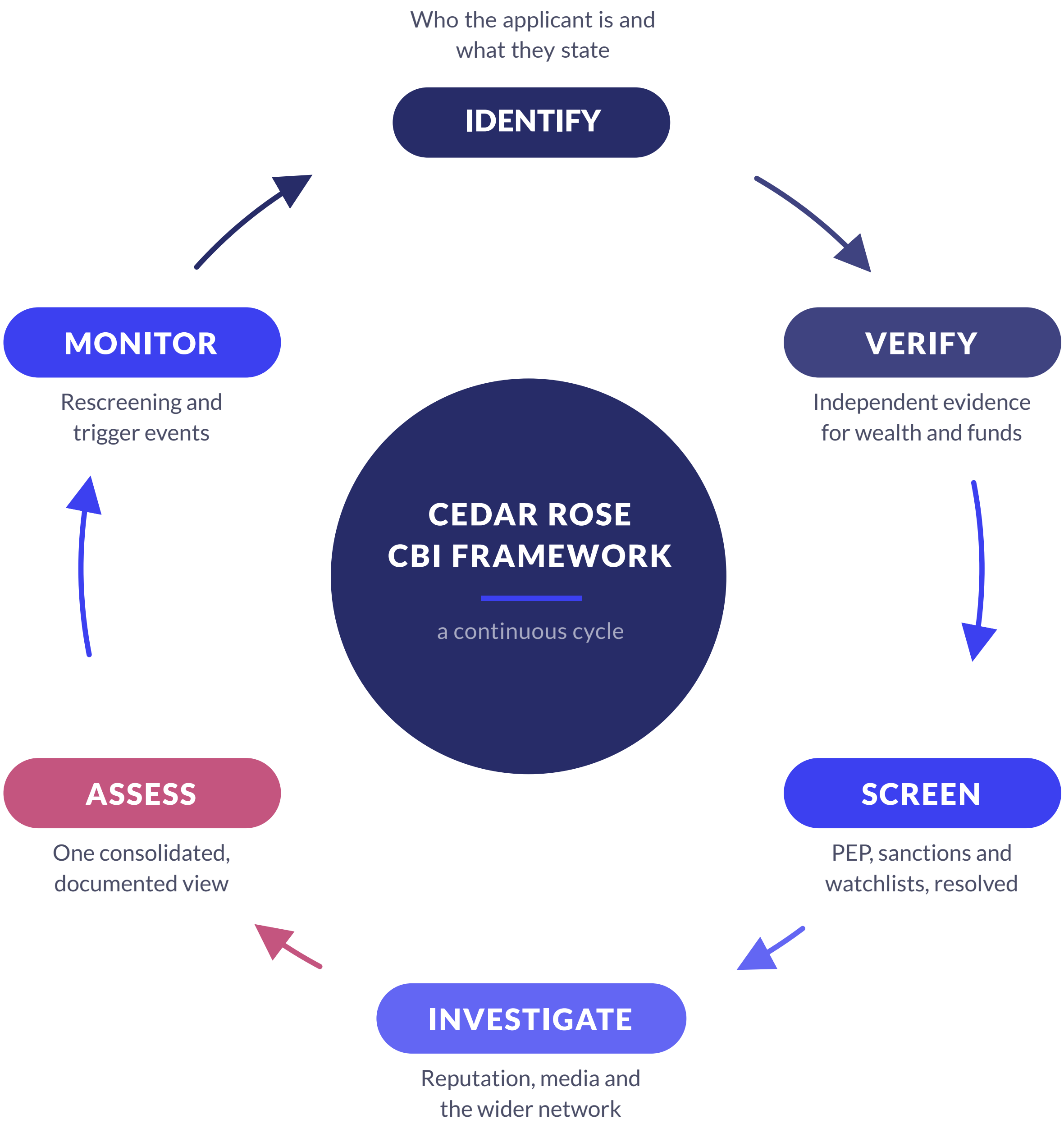
STANDARD CDD	ENHANCED DUE DILIGENCE ADDS
Identify and Verify	Additional independent verification of wealth and funds
Screen	Wider reputational research across languages
Assess	Closer examination of the applicant's network
	Senior management or risk-committee review

SECTION 11

The Six-Stage Due Diligence Framework

The six stages below bring together the areas covered in this guide into a single, repeatable process, so a file can be reviewed at any point and its current state understood without ambiguity.

Each stage has a distinct objective, a defined set of questions, and a clear output that feeds into the next.



Stages 01 – 03 in practice

01 IDENTIFY

Establish who the applicant is, and build an initial profile of their background and stated wealth.

KEY QUESTIONS	REVIEWS	OUTPUT
Is identity fully documented? What is their professional background? What is the stated basis for the investment funds?	Identity documents; application form and declarations.	An initial applicant profile with areas flagged for verification.

02 VERIFY

Independently confirm identity, and corroborate Source of Wealth and Source of Funds against evidence.

KEY QUESTIONS	REVIEWS	OUTPUT
Does independent evidence support the stated identity? Can Source of Wealth and Source of Funds be corroborated?	Financial statements, tax filings, bank statements; corporate registry records.	A verified profile with documented evidence and any unresolved gaps listed.

03 SCREEN

Run PEP, sanctions and watchlist screening across the applicant, family, connected entities and intermediaries.

KEY QUESTIONS	REVIEWS	OUTPUT
Does the applicant or anyone connected appear on a PEP, sanctions or watchlist database? Are matches genuine, based on biographical detail?	PEP, sanctions and watchlist results for applicant, network and intermediaries.	A documented screening outcome, with matches resolved or flagged and escalated.

Stages 04 – 06 in practice

04 INVESTIGATE

Conduct reputational and adverse media research, and map beneficial ownership and connected parties.

KEY QUESTIONS	REVIEWS	OUTPUT
Does adverse media, litigation or regulatory history exist? What does the ownership and directorship network look like?	Adverse media, litigation and regulatory records; corporate ownership mapping.	A reputational risk summary and a mapped applicant network.

05 ASSESS

Bring together findings from every stage into a single, documented risk assessment.

KEY QUESTIONS	REVIEWS	OUTPUT
What is the overall risk profile once all findings are considered together? Does the file support standard processing, EDD or escalation?	A documented risk assessment and recommendation. Final decision rests with the programme operator or other authorised decision-maker.	A documented risk assessment, evidence summary, outstanding-information log and reasoned recommendation. The final decision remains with the programme operator or other authorised decision-maker.

06 MONITOR

Maintain risk-based, ongoing visibility of the applicant's risk profile before and after onboarding.

KEY QUESTIONS	REVIEWS	OUTPUT
Has anything changed in PEP, sanctions or adverse media exposure? Has a trigger event occurred, such as a change in ownership, directorships or payment arrangements?	Periodic rescreening, event-driven screening, and review following material changes.	An updated risk position, with escalation where a trigger event or new information warrants it.

SECTION 12

CBI Applicant Due Diligence Checklist

A practical reference for building or reviewing a CBI applicant file.

IDENTITY AND BACKGROUND

- [ ] Identity documents collected and independently verified, including aliases and transliteration
- [ ] Professional and business history documented and consistent with stated wealth
- [ ] Directorships, shareholdings and beneficial ownership mapped

WEALTH AND FUNDS

- [ ] Source of Wealth narrative documented, evidenced and independently corroborated
- [ ] Source of Funds traced to the originating and receiving account, with third-party funding explained
- [ ] No unexplained transfers or inconsistencies outstanding

SCREENING AND REPUTATION

- [ ] PEP and sanctions screening completed for applicant, family, connected entities and intermediaries, all matches resolved
- [ ] Adverse media, litigation and regulatory records reviewed and assessed for credibility, relevance and materiality

APPLICATION INTEGRITY AND GOVERNANCE

- [ ] Application declarations are complete, consistent and independently tested where necessary
- [ ] Any authorised agent, introducer or intermediary has been identified, screened and assessed in accordance with programme requirements
- [ ] Material discrepancies, clarifications and escalation decisions are documented
- [ ] The file contains an auditable record of sources consulted, evidence relied upon, quality review and final decision authority
- [ ] Personal data is collected, processed, retained and shared in accordance with applicable data-protection and confidentiality requirements

ESCALATION AND MONITORING

- [ ] EDD triggers assessed against the completed file, and EDD completed where triggered
- [ ] Monitoring frequency and scope defined on a risk basis, with re-screening scheduled
- [ ] Process in place to escalate trigger events and material post-approval findings

> A file that satisfies every line above can still require judgement. The checklist records completeness; the risk assessment records reasoning.

SECTION 13

Applying a Risk-Based Approach

Not every applicant requires the same depth of investigation. A risk-based approach allocates investigative effort in proportion to the risk indicators identified at each stage of the framework, rather than applying uniform scrutiny to every file.

EFFORT IN PROPORTION TO RISK

LOWER RISK
Standard due diligence and proportionate verification

MODERATE RISK
Targeted additional verification and focused investigative due diligence

HIGHER RISK
Enhanced Due Diligence, senior review and, where applicable, legal or compliance escalation

A confirmed sanctions match should be handled under the applicable sanctions policy and legal framework, rather than treated solely as an EDD trigger.

Where CBI due diligence commonly falls short

The most frequent gaps are treating identity verification or database screening as a complete investigation, focusing only on the applicant rather than their wider network, overlooking the role of intermediaries and application integrity controls, confusing Source of Wealth with Source of Funds, dismissing unconfirmed adverse media rather than assessing it, and treating due diligence as a one-time exercise rather than something that continues after approval.

01 Treating identity verification or database screening as a complete investigation	**02** Focusing only on the applicant rather than their wider network	**03** Overlooking intermediaries and application-integrity controls
04 Confusing Source of Wealth with Source of Funds	**05** Dismissing unconfirmed adverse media rather than assessing it	**06** Treating due diligence as a one-time exercise that ends at approval

SECTION 14

Decision Governance, Record Keeping and Data Protection

A defensible framework requires a clear audit trail, approval authority, escalation steps and retention requirements, together with appropriate safeguards for the sensitive personal, financial and reputational information the process relies on.

THE DECISION TRAIL A REVIEWER SHOULD BE ABLE TO FOLLOW

- **Evidence** — Sources consulted
- **Open items** — Unresolved issues
- **Rationale** — Risk reasoning
- **Quality review** — Independent check
- **Approval** — Named authority

SENIOR OR RISK-COMMITTEE REVIEW

Material decisions — EDD outcomes, sanctions concerns and high-risk PEP cases — should be subject to defined senior review, with records retained per applicable legal, regulatory, programme and data-protection requiremen

Decision governance and record keeping

Each case should have a clear decision trail showing the evidence reviewed, sources consulted, unresolved issues, risk rationale, escalation history, quality-assurance checks and final approval authority. Records should be retained in accordance with applicable legal, regulatory, programme and data-protection requirements. Material decisions, particularly EDD outcomes, sanctions concerns and high-risk PEP cases, should be subject to defined senior review or risk-committee governance.

Data protection and fair treatment

CBI due diligence involves the processing of sensitive personal, financial and reputational information. Information collection and use should be lawful, necessary, proportionate and secure. Findings should be recorded accurately, with a clear distinction between verified facts, credible allegations and unsubstantiated claims. The process should include appropriate confidentiality controls and a mechanism for clarifying material discrepancies where permitted and appropriate.

SECTION 15

Conclusion

Effective CBI due diligence is not limited to clearing a name against a list or collecting a complete set of documents. It is a risk-based process for establishing a defensible understanding of the applicant's identity, wealth, transaction funds, corporate and personal connections, reputation, and eligibility-related risk factors.

The process should distinguish verified facts from allegations, corroborate key claims through reliable independent sources, and apply greater scrutiny where risk indicators, programme requirements or legal obligations warrant it. It should also recognise that PEP exposure, sanctions concerns, complex structures or adverse information require different forms of escalation and cannot be treated as interchangeable findings.

A structured six-stage framework, Identify, Verify, Screen, Investigate, Assess and Monitor, helps compliance and risk teams maintain consistency, document their reasoning, and make decisions that can be explained and defended. Cedar Rose supports this process through factual research, corporate intelligence, ownership mapping, screening, reputational analysis and ongoing risk monitoring, while final decisions remain with the authorised programme operator or client decision-maker.

IDENTIFY | VERIFY | SCREEN | INVESTIGATE | ASSESS | MONITOR

SPEAK WITH CEDAR ROSE

Speak with Cedar Rose about CBI Due Diligence

Cedar Rose provides factual research, risk intelligence and documented due diligence assessments to support client decision-making. Our work is designed to inform, not replace, the legal, regulatory, compliance or immigration determinations of programme operators, regulated institutions, legal counsel or other authorised decision-makers. We help clients gain deeper visibility into the individuals and entities behind a CBI application, including:

- **Individual and corporate background verification**
- **PEP, sanctions and watchlist screening**
- **Beneficial ownership and corporate relationship mapping**
- **Intermediary and application-integrity research**
- **Adverse media and reputational research**
- **Risk indicator identification to support Enhanced Due Diligence**
- **Ongoing, risk-based monitoring of applicant and corporate risk profiles**

CEDAR ROSE
a coface company

BUSINESS INTELLIGENCE · RISK INTELLIGENCE

info@cedar-rose.com | cedar-rose.com