International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I1P116
Eureka Vision Publication | Volume 5, Issue 1, 149-171, 2024

Original Article

Correspondent Banking and Nested Relationships: Managing Cross-Border AML/CTF Risk, Due Diligence, and Monitoring Expectations

Mallikarjun Reddy Gouni
University of Illinois Springfield.

Abstract - Correspondent banking remains a critical backbone of cross-border payments, trade finance, and financial inclusion, yet it is also a persistent exposure point for money laundering and terrorist financing (AML/CTF) risk. These risks intensify in nested correspondent relationships where respondent banks provide downstream access to their own clients or other financial institutions because transparency diminishes across the payment chain and accountability for controls can become fragmented. This study examines how financial institutions can manage AML/CTF risk in correspondent and nested relationships while meeting evolving expectations for risk-based due diligence, transaction monitoring, and ongoing oversight across multiple jurisdictions. The research synthesizes regulatory guidance, supervisory enforcement themes, and industry practices to develop a structured framework for (i) risk scoping and customer/relationship classification, (ii) enhanced due diligence (EDD) for nested access, including governance, ownership, sanctions exposure, and AML program effectiveness, and (iii) monitoring and escalation standards that integrate payment-message data quality, typology-driven alerts, and periodic relationship reviews. Methodologically, the study employs comparative policy analysis across key regulatory regimes and a scenario-based assessment using representative nested-relationship typologies (e.g., indirect access to high-risk geographies, fintech/payment intermediary layering, and payable-through account–like structures) to identify practical control gaps and feasible mitigations. The expected contribution is a set of actionable, risk-proportionate recommendations and monitoring expectations that balance financial crime compliance with the operational realities of cross-border banking, supporting safer access to the global financial system without unnecessary de-risking.

Keywords - Correspondent Banking, Nested Relationships, Cross-Border Banking, International Financial Transactions, Foreign Correspondent Accounts, Payable-Through Accounts, Intermediary Banking, Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), Financial Crime Compliance, Regulatory Compliance.

1. Introduction

Correspondent banking is a foundational mechanism that enables cross-border payments, trade settlement, and access to foreign currencies especially for smaller banks and institutions in emerging or low-capacity markets. Through correspondent relationships, a respondent bank can clear transactions, hold accounts, and access payment rails in jurisdictions where it lacks a direct presence. While these arrangements support global commerce and financial inclusion, they also create complex financial crime exposure because funds, counterparties, and underlying customer activity may span multiple institutions, jurisdictions, and regulatory regimes.

These risks become more pronounced in nested correspondent relationships, where a respondent bank provides downstream access to its own clients such as money service businesses (MSBs), fintechs, or even other banks using the correspondent's infrastructure. In practice, nesting can obscure the originator/beneficiary context, weaken visibility into the true nature of counterparties, and complicate accountability for screening and monitoring. The correspondent institution may have limited insight into the nested party's controls, customer base, and transaction behavior, yet is still expected to apply a risk-based AML/CTF framework that is defensible to regulators and aligned with internal risk appetite.

At the same time, supervisory expectations for customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring in correspondent banking continue to rise. Institutions must demonstrate that they can (i) identify and assess cross-border risks, (ii) understand how nested access is structured and governed, (iii) ensure data quality and transparency in payment messages and related information flows, and (iv) calibrate transaction monitoring and periodic reviews to the specific risk profile of the relationship. Failure to achieve this balance has contributed to "de-risking" dynamics, where banks exit correspondent relationships to avoid compliance exposure potentially restricting legitimate access to the global financial system and pushing activity toward less transparent channels.

This research addresses the practical and policy challenge of managing cross-border AML/CTF risk in correspondent and nested relationships without relying on blanket exclusions or overly conservative risk avoidance. It focuses on the control expectations most relevant to nested access: relationship-level risk assessment, due diligence depth and documentation, governance and accountability between institutions, monitoring design and data dependencies, and escalation/remediation pathways when risk changes or transparency deteriorates.

Research objectives

- Define the risk drivers unique to nested correspondent relationships and explain how they differ from standard bilateral correspondent arrangements.
- Examine due diligence expectations for nested access, including what "knowing your respondent" should reasonably include when downstream parties are involved.
- Identify monitoring and oversight approaches that improve transparency and control effectiveness across borders while remaining operationally feasible.
- Propose a structured, risk-proportionate framework that integrates due diligence, monitoring, and periodic review into a coherent lifecycle model for correspondent/nested relationships.

Research questions

- What typologies and structural features make nested correspondent relationships higher risk (or less transparent) than non-nested relationships?
- What constitutes sufficient CDD/EDD for nested access in a risk-based compliance program, and how should responsibilities be allocated between correspondent and respondent institutions?
- What monitoring expectations are realistic given limitations in payment data, jurisdictional constraints, and varying maturity of downstream AML programs?
- How can institutions reduce financial crime exposure while avoiding unnecessary de-risking and preserving legitimate cross-border access?

Significance and contribution

The study contributes a practical perspective that connects regulatory expectations to implementable controls. By organizing nested-risk management into clear components risk scoping, due diligence depth, and monitoring design it aims to help compliance teams, risk managers, and policy stakeholders align on what "reasonable and effective" looks like in nested relationships, including where visibility limits should trigger enhanced controls, restrictions, or exit decisions.

Structure of the paper

Following this introduction, the paper reviews key concepts and risk typologies in correspondent and nested relationships, then examines AML/CTF due diligence expectations and common supervisory themes. It next proposes a lifecycle control framework (onboarding, ongoing monitoring, periodic review, and remediation/exit), and concludes with recommendations for institutions and regulators to strengthen cross-border risk management while supporting sustainable correspondent banking access.

1.1. Background and Context

1.1.1. The Role of Correspondent Banking in Cross-Border Finance

Correspondent banking is a long-established mechanism that allows financial institutions to access payment and settlement services in jurisdictions where they do not maintain a direct presence. In practice, a *correspondent* bank provides a *respondent* bank with services such as foreign currency accounts, international wire transfers, trade finance support, and access to major clearing and settlement systems. This infrastructure underpins everyday cross-border activity remittances, import/export payments, corporate treasury movements, and interbank settlements by connecting domestic institutions to global payment rails. For smaller banks, regional institutions, and banks in developing markets, correspondent relationships are often the only feasible route to participate in international finance. As a result, correspondent banking is closely tied not only to global commerce but also to access to formal financial channels for households and small businesses operating across borders.

1.1.2. Why "Nested" (Downstream) Relationships Increase Opacity and Risk

Nested correspondent relationships arise when a respondent bank provides downstream entities such as other banks, money service businesses, payment intermediaries, fintechs, or high-volume commercial clients access to cross-border payment capabilities through the respondent's own account relationship with its correspondent. This layering expands the payment chain and can substantially reduce transparency for the correspondent bank, which may only see the respondent as its direct counterparty while having limited visibility into the downstream party that is effectively using the correspondent network.

This structure increases opacity and AML/CTF risk in several ways. First, it can dilute the correspondent's ability to understand the *true source and purpose of funds*, particularly when payment messages do not consistently carry complete originator/beneficiary information or when the respondent aggregates flow from multiple downstream clients. Second, nested access creates control dependency: the correspondent must rely on the respondent's AML program effectiveness, governance, and monitoring to manage the risks posed by downstream parties. Where the respondent's controls are weaker or where supervision is inconsistent across jurisdictions nested relationships can become conduits for sanctions evasion, trade-based money laundering, terrorism financing, and other illicit flows. Third, accountability can become fragmented: responsibilities for screening, customer due diligence, and transaction monitoring may be distributed across institutions with different legal obligations, risk appetites, data access, and technology maturity. The result is a heightened need for clear contractual expectations, robust due diligence on the respondent's control environment, and monitoring approaches that compensate for reduced direct visibility.

1.1.3. De-Risking Trends and Financial Inclusion Tradeoffs

Rising compliance expectations, high enforcement costs, and the reputational consequences of AML/CTF failures have contributed to de-risking the withdrawal or restriction of correspondent banking relationships perceived as high risk, unprofitable, or operationally difficult to monitor. Banks may terminate or avoid relationships involving high-risk jurisdictions, weak regulatory environments, or respondent institutions that serve higher-risk customer segments (e.g., MSBs, cash-intensive businesses, certain nonprofit or humanitarian corridors). While de-risking can reduce exposure for individual banks, it can also generate systemic and social costs.

When correspondent lines are curtailed, legitimate cross-border flows such as remittances that support households, payments for essential imports, and humanitarian transfers may become slower, more expensive, or forced into less transparent channels. Smaller institutions can lose access to reserve currencies and international payment systems, and entire corridors may become concentrated among fewer providers, increasing fragility. This creates a persistent policy tension: regulators and banks seek stronger AML/CTF controls and demonstrable oversight, but excessive risk aversion can undermine financial inclusion and the integrity of regulated payment pathways by pushing activity into informal networks.

Against this backdrop, nested correspondent banking sits at the center of a difficult balance. It is often commercially and socially important supporting payment access for downstream institutions and customer groups yet it amplifies opacity and requires more sophisticated, risk-proportionate governance. Understanding how to manage these risks through well-designed due diligence and monitoring, without defaulting to indiscriminate exits, is therefore a central motivation for this research.

1.2. Problem Statement

Correspondent banking is essential for cross-border financial access, yet it is also one of the most scrutinized channels for AML/CTF risk. Financial institutions are expected to maintain robust, risk-based controls covering due diligence, sanctions screening, transaction monitoring, and ongoing oversight despite operating across multiple jurisdictions with uneven regulatory capacity, inconsistent data standards, and varying levels of respondent maturity. This creates a persistent tension: banks must either sustain cross-border connectivity that supports trade, remittances, and financial inclusion, or reduce exposure by limiting relationships that are costly to oversee and difficult to defend to regulators. The dilemma is most acute where respondents service higher-risk corridors or downstream customer types, because the compliance burden rises quickly while commercial returns may remain modest.

Nested correspondent relationships amplify this tension by adding additional layers between the correspondent and the ultimate transacting parties. In nested structures, the correspondent bank typically has a direct relationship with the respondent bank but the respondent may in turn provide payment access to downstream institutions (e.g., other banks, MSBs, fintechs) or aggregated client groups. As the payment chain lengthens, visibility declines and risk ownership becomes less clear, even though supervisory expectations increasingly demand demonstrable control over the relationship's risk profile.

A core problem, therefore, is the gap between regulatory expectations for effective AML/CTF risk management and the practical limitations of oversight in nested arrangements. Three interrelated challenges drive this gap:

- Visibility constraints and incomplete transparency: The correspondent often lacks direct knowledge of the nested entity's customers, products, and transaction purpose. Payment flows may be aggregated or routed in ways that obscure who ultimately benefits or initiates transactions. This reduces the correspondent's ability to assess inherent risk, detect typology-driven anomalies, or validate whether the respondent is applying appropriate controls downstream.
- Data quality and information asymmetry: Cross-border payments depend heavily on the accuracy and completeness of payment message data (e.g., originator/beneficiary details), yet data fields may be incomplete, inconsistently formatted, or truncated across systems and jurisdictions. Where nested access is involved, the respondent may not pass through full

underlying party information, or it may be operationally difficult to preserve context for downstream transactions. As a result, screening and monitoring systems can generate false positives or more critically miss risk signals due to insufficient information.

- Fragmented accountability and control dependency: Nested relationships create shared—but not always clearly defined responsibilities between correspondent and respondent institutions. The correspondent relies on the respondent's governance, AML program effectiveness, and monitoring processes, but may have limited ability to test or validate those controls beyond periodic reviews, questionnaires, or audits. When incidents occur, accountability can be disputed: the respondent may be responsible for customer-level due diligence, while the correspondent is responsible for relationship-level oversight and detection of suspicious activity. This fragmentation complicates escalation decisions, remediation timelines, and defensible documentation of risk-based judgments.

In combination, these issues can drive risk-avoidant outcomes such as de-risking, narrowing service offerings, or imposing blanket prohibitions on nested access even when downstream activity may be legitimate and socially important. The problem this research addresses is how correspondent banks and respondent banks can implement risk-proportionate due diligence, monitoring, and governance that (i) improves transparency and control effectiveness in nested structures, (ii) produces documentation that meets supervisory scrutiny, and (iii) preserves sustainable cross-border access where feasible.

2. Conceptual Foundations and Definitions

2.1. Correspondent Banking: Definition, Business Models, and Payment Flows

Correspondent banking refers to the provision of banking services by one bank (the correspondent) to another financial institution (the respondent), typically to enable the respondent to conduct business and settle transactions in a jurisdiction and/or currency where it has no direct access. This function is widely recognized as a core enabler of cross-border payments, trade, and broader participation in the global financial system.

In operational terms, correspondent relationships are commonly organized around account and messaging arrangements:

- Account-based access (nostro/vostro logic): the respondent maintains accounts with the correspondent (often in foreign currency), allowing it to clear and settle cross-border obligations.
- Payment routing and message-based execution: cross-border transfers frequently travel through chains of intermediaries, creating multi-institution payment flows where each participant may see only part of the transaction context (depending on message standards, data completeness, and routing).
- Service bundles and business models: beyond payments, correspondent banking can include cash management, FX settlement, trade finance support, and liquidity services. Central bank and BIS/CPMI work highlights that these relationships underpin international trade and financial inclusion, but also create risk dependencies across institutions and jurisdictions.

From an AML/CTF standpoint, the defining feature is that correspondent banking often involves reliance on another institution's customer relationships and controls, while still requiring the correspondent to apply risk-based oversight to the respondent relationship. FATF standards explicitly treat correspondent banking as an area requiring enhanced attention because of the cross-border and intermediary nature of the activity.

2.2. Nested Relationships: Definition and Forms

A nested (downstream) correspondent relationship occurs when a respondent bank that receives correspondent services also provides correspondent-like services to other institutions through that same access—effectively extending indirect access to the correspondent's network. The term and definition appear consistently across key guidance (including FATF and Basel/BCBS materials).

2.2.1. "Respondent-Of-Respondent" Structures

In this structure, the correspondent's direct counterparty is the respondent bank, but one or more indirect respondent banks (or other financial institutions) access cross-border clearing via the respondent's account relationship. Regulators characterize this as a heightened-risk arrangement because it expands the chain of reliance and can reduce transparency into the true originators/beneficiaries and the nature of downstream business.

2.2.2. Payable-Through Accounts and Indirect Access Models

Payable-through accounts (PTAs) are a particular form of indirect access where third parties can "use" a correspondent account to transact on their own behalf. FATF standards define PTAs and set a clear expectation that, for PTAs, the correspondent must be

satisfied the respondent has performed CDD on customers with direct access and can provide relevant CDD information upon request. Conceptually, PTAs sit on a spectrum of indirect access: at one end, the respondent conducts transactions strictly for its own customers under tightly controlled arrangements; at the other, downstream parties have a more direct transactional capability that increases opacity and complicates monitoring accountability.

2.2.3. Fintech and Non-Bank Nesting Via Sponsor Banks

A modern variant of "nesting" arises when non-bank payment service providers (PSPs) or fintechs obtain indirect access to payment systems through banks (often described as sponsorship, agency, or settlement-as-a-service). BIS/CPMI work notes that access arrangements often distinguish between direct participation (commonly banks) and indirect participation (including non-bank PSPs), which can create risk concentration and dependency on the direct participant's controls. In some jurisdictions, practical access constraints mean non-banks may be "sponsored" into settlement through a bank relationship, reinforcing the importance of governance, monitoring expectations, and clear allocation of responsibilities.

2.3. AML/CTF Fundamentals

2.3.1. Money Laundering Stages, Terrorist Financing Patterns

Money laundering is commonly described as progressing through three stages: placement, layering, and integration. This model remains useful as a conceptual lens for why cross-border and multi-institution pathways are attractive to criminals particularly in the layering stage, where complexity and distance help obscure the audit trail.

2.3.2. Terrorist Financing (TF)

Differs in that funds may originate from legitimate sources and can involve smaller amounts, diverse channels, and rapid adaptation to controls. FATF's TF risk assessment guidance and subsequent TF risk updates emphasize the variability of methods across contexts and the need for risk-based countermeasures rather than one-size-fits-all rules.

2.3.3. Cross-Border Risk Amplifiers

Cross-border correspondent and nested structures elevate AML/CTF exposure due to several interacting risk amplifiers:

- Jurisdictional risk and weak supervision: criminals can exploit weak AML/CTF regimes; FATF's public identification of jurisdictions with strategic deficiencies reflects how vulnerabilities in one jurisdiction can weaken global safeguards.
- Sanctions and geopolitical constraints: sanctions screening and related controls add complexity to cross-border flows, particularly where payment chains involve multiple intermediaries and inconsistent data quality. (This intersects directly with monitoring design and data standards developed further in later sections.)
- Opacity mechanisms (secrecy, complex ownership, layered intermediaries): nested relationships can compound opacity by adding additional entities and accounts between the correspondent and the ultimate transacting parties.
- Control dependency and uneven compliance maturity: where downstream entities (including PSPs) rely on sponsor banks or respondent banks for access, the overall risk posture depends heavily on governance, program effectiveness, and information-sharing capacity.

2.4. Key Concepts and Frameworks

2.4.1. Risk-Based Approach (RBA)

The Risk-Based Approach is the organizing principle for modern AML/CTF: institutions identify, assess, and understand ML/TF risks, then apply controls proportionate to the risk profile (rather than applying uniform measures everywhere). FATF's banking-sector RBA guidance positions RBA as central to effective AML/CTF implementation and supervisory defensibility.

In correspondent and nested contexts, RBA typically operationalizes as: (i) relationship risk assessment, (ii) proportionate CDD/EDD depth, (iii) monitoring calibrated to products, geographies, and typologies, and (iv) periodic review with triggers for escalation.

2.4.2. The "Know Your Customer's Customer" Debate

A recurring misconception is that correspondents must "KYC" the respondent's underlying customers. FATF's correspondent banking guidance is explicit: there is no expectation, intention, or requirement for the correspondent to conduct CDD on the respondent's customers; rather, correspondents should apply relationship-level due diligence and may request information on specific transactions (RFI) where warranted by risk. This distinction matters because it frames what "reasonable" oversight looks like: correspondents are expected to understand and test the respondent's controls, not replicate respondent-level customer onboarding.

2.4.3. Beneficial Ownership and Control

Beneficial ownership refers to identifying the natural persons who ultimately own or control a customer (and understanding control structures that could obscure accountability). FATF standards embed beneficial ownership expectations as part of a broader transparency agenda and connect them to higher-risk relationship management (including correspondent banking). In nested structures, beneficial ownership is especially relevant when downstream entities include high-risk intermediaries, complex corporate vehicles, or arrangements spanning multiple jurisdictions.

2.4.4. Financial Crime Compliance as Governance + Technology + Data

Modern correspondent/nested AML/CTF control effectiveness is best understood as an interaction of:

- Governance: clear accountability, senior management oversight, escalation/exit decisioning, and defensible documentation—emphasized in Basel/BCBS guidance on ML/FT risk management and correspondent annex expectations.
- Technology: screening and monitoring systems that can operate across high-volume cross-border flows and typology shifts.
- Data: payment message completeness and quality (originator/beneficiary information, identifiers, structured fields) directly shapes screening accuracy and monitoring signal quality. Industry tooling and migration efforts explicitly target payments data quality improvements.

Together, these foundations clarify why nested correspondent risk is not only a "policy" challenge, but also a data-and-controls engineering challenge where the limits of visibility and information-sharing materially shape what monitoring and due diligence can achieve.

Table 1. Key Concepts and Definitions for Correspondent Banking, Nesting and AML/CTF

Concept / Term	Working definition (for this paper)	How it typically appears in practice	Primary AML/CTF risk implications	Core control focus (RBA-aligned)
Correspondent banking relationship	A bank (correspondent) provides cross-border payment/settlement and related services to another institution (respondent)	Nostro/vostro accounts; cross-border wires; FX settlement; trade finance support; intermediary chains	Reliance on respondent controls; cross-border complexity; potential for misuse of payment chains	Relationship risk assessment; respondent due diligence; governance & contractual expectations; monitoring of activity patterns
Payment chain / intermediary flow	A cross-border payment routed through one or more intermediary institutions	Multiple hops; different systems and data standards; truncation risk	Reduced end-to-end transparency; inconsistent originator/beneficiary data; monitoring blind spots	Data quality checks; message standard controls; typology-based monitoring; escalation/RFI processes
Nested relationship	A respondent provides downstream entities indirect access to cross-border services via its correspondent relationship	"Respondent-of-respondent" access; downstream banks or PSPs using the respondent's infrastructure	Additional opacity layer; increased reliance on downstream AML controls; higher typology exposure	Enhanced due diligence (EDD) on respondent's downstream controls; restrictions/conditions on nesting; ongoing oversight triggers
"Respondent-of-respondent"	A nested structure where the downstream entity is itself a financial institution	Small banks accessing major currencies through a respondent	Complex accountability; limited visibility into downstream institution's customers and products	Governance clarity; audit/assurance rights; downstream risk mapping; periodic reviews
Payable-through account (PTA) / indirect access	Arrangement where third parties can initiate transactions "through" the respondent's account	Third parties transact using respondent account access, sometimes resembling direct usage	Elevated risk of disguised beneficial parties; weak traceability if CDD info isn't retrievable	Strong conditions: respondent CDD on direct-access customers; ability to furnish CDD; tighter monitoring and limits
Fintech / non-bank nesting via sponsor bank	Non-bank PSP/fintech gains indirect access to payment systems using a bank sponsor	Sponsorship/agency models; settlement-as-a-service	High-volume/velocity patterns; fast product change; third-party dependency risk	Third-party risk management; monitoring calibration for fintech typologies; strong data/ID requirements
Money	Placement, layering,	Structuring, transfers,	Layering increases with	Typology-driven

laundering stages	integration as a conceptual model of laundering activity	complex routing, trade-based schemes	cross-border chains and nesting	monitoring; anomaly detection; corridor and counterparty risk scoring
Terrorist financing patterns	Funding may be small, mixed with legitimate flows, and rapidly adaptable	Small-value transfers; networked movements; use of intermediaries	Harder to detect via thresholds; relies on intelligence-led typologies	Targeted scenarios; network indicators; sanctions screening integration; rapid escalation pathways
Cross-border risk amplifiers	Factors that heighten ML/TF risk in international contexts	High-risk corridors; weak supervision; secrecy; sanctions exposure	Increased probability of illicit flows and reduced enforcement cooperation	Jurisdictional risk scoring; sanctions/PEP screening rigor; EDD triggers; tighter review cycles
Risk-Based Approach (RBA)	Controls proportionate to assessed risk; risk informs depth of due diligence and monitoring	Tiered onboarding; differentiated monitoring thresholds; periodic review by risk	Avoids both under- and over-compliance; supports defensibility	Documented risk rationale; control mapping; governance oversight; testing/validation
"Know Your Customer's Customer" (KYCC) debate	Extent to which correspondents should understand downstream parties	Often misunderstood as requiring full customer-level KYC	Misinterpretation drives de-risking or unworkable expectations	Clarify scope: focus on respondent program effectiveness and transaction-level RFIs when justified
Beneficial ownership and control	Identifying natural persons who ultimately own/control entities	Multi-layer ownership chains; nominees; trusts/complex structures	Obscures accountability; increases sanctions/ML exposure	BO verification approach; control person identification; higher scrutiny for complex structures
Compliance as governance + technology + data	AML/CTF effectiveness emerges from decisioning structure + systems + information quality	Screening/monitoring engines + data pipelines + documented governance	Poor data reduces detection; weak governance undermines accountability	Data standards and completeness; model tuning; clear roles/SLAs; audit trails and metrics

3. Literature Review

3.1. Academic Research on Correspondent Banking Risk and De-Risking

Academic work generally frames correspondent banking risk and de-risking as an interaction between (i) financial crime and sanctions exposure, (ii) regulatory expectations and enforcement risk, and (iii) profitability/operational cost constraints especially for low-margin corridors and smaller respondents. A recurring conclusion is that CBR withdrawals are rarely driven by a single factor; instead, they reflect bundled incentives (risk, cost, reputational exposure, and supervisory pressure) that make some relationships difficult to justify under a risk-based compliance model. Empirical studies increasingly quantify real-economy impacts. For example, research using firm-level export data links the loss of correspondent access to measurable reductions in trade performance for affected firms, reinforcing that de-risking can produce macro and micro frictions beyond the banking sector. In parallel, scholarship focusing on higher-risk customer segments (e.g., MSBs) finds that de-risking can disrupt remittance and small-value payment corridors often without eliminating underlying demand raising the risk of displacement to less transparent channels.

Across this academic stream, two themes stand out for your paper:

- Outcome measurement is improving (trade/remittance effects, corridor contraction, concentration).
- Mechanisms are still under-specified, especially the operational reality of how limited visibility, data quality constraints, and shared accountability in nested structures translate into monitoring and governance decisions.

3.2. Practitioner and Industry Guidance (Banking Associations, Compliance Surveys)

Industry guidance tends to be more operational than academic work, emphasizing standardized due diligence artifacts, defensible documentation, and pragmatic expectations for "what a good file looks like" during onboarding and reviews.

A central private-sector tool is the Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ), which provides a common structure to gather information on the respondent's AML program, governance, sanctions screening, and (importantly for your topic) processes for identifying and managing downstream/nested relationships. The BAFT "Respondent's

Playbook" reflects the *respondent side* of expectations how respondents can present their control environment to maintain access, reduce friction, and respond to information requests in a consistent format.

National-level practitioner guidance also provides concrete expectations on documentation and ongoing assessment, such as AUSTRAC guidance that explicitly requires pre-relationship and ongoing due diligence assessments with written records. Finally, practitioners increasingly connect AML/CTF effectiveness to payments data quality and standards migration, because monitoring quality is bounded by the completeness/structure of originator and beneficiary fields.

3.3. Key AML/CTF Standards and Regulatory Guidance (Comparative Lens)

3.3.1. International Standard-Setters and Major Jurisdictions

Global baseline expectations are anchored by the Financial Action Task Force standards and its correspondent banking guidance, which emphasizes managing rather than avoiding risk and clarifies that correspondents are not expected to conduct CDD on every downstream customer (a frequent source of KYCC confusion). The Basel Committee on Banking Supervision guidance operationalizes this into bank-wide risk management expectations, including an updated correspondent banking annex that links relationship risk assessment, respondent AML controls evaluation, and proportional monitoring/restrictions.

From a system perspective, the Committee on Payments and Market Infrastructures (under the Bank for International Settlements) frames correspondent banking as a core cross-border payments mechanism and documents structural issues (concentration, fragmentation, and data challenges) that interact with AML/CTF expectations. The Financial Stability Board complements this with an action-plan lens: data monitoring of CBR declines, guidance alignment, and coordination with FATF/BCBS and SWIFT.

Jurisdictional guidance then applies these principles in different ways:

- United States: Examiner and regulator materials (notably the FFIEC BSA/AML manual) explicitly discuss nested correspondent relationships and testing expectations around identifying nested activity and considering AML program information. FinCEN materials on special due diligence programs and Section 312-related requirements set the tone for correspondent account due diligence obligations.
- European Union: the European Banking Authority risk factor guidelines provide a broad RBA framework and risk indicators to adjust CDD intensity (including for higher-risk relationships), reinforcing proportionality while leaving implementation detail to firms and supervisors.
- United Kingdom: the Financial Conduct Authority Financial Crime Guide includes discussion of themes relevant to correspondent banking risk assessment and the use of country-level AML regime strength in decisioning.
- Singapore: Monetary Authority of Singapore Notice 626 and its guidelines establish risk assessment, CDD, and ongoing monitoring expectations for banks operating under MAS supervision.

Comparative insight for your paper: global standards align on RBA and proportionality, but jurisdictional materials differ in operational specificity e.g., examiner testing procedures (US), broad risk-factor guidance (EU), thematic controls guidance (UK), and notice-based compliance requirements (Singapore).

3.4. Gaps in the Literature

3.4.1. Limited Empirical Work on "Nested Visibility" and Monitoring Design

While many sources recognize nested relationships as a risk issue, fewer provide granular, testable models of how data gaps (message completeness, truncation, aggregation) affect detection performance, false positives/negatives, and escalation thresholds in monitoring systems especially across multi-hop payment chains.

3.4.2. Inconsistent Expectations across Supervisors and Market.

The standards emphasize RBA and "manage, don't avoid," yet implementation expectations vary in practice (depth of EDD, acceptable reliance on respondent controls, auditability of downstream activity). This inconsistency contributes to uneven outcomes and can reinforce conservative exits where requirements are perceived as unclear or unbounded.

3.4.3. Data-Sharing Constraints vs. Compliance Demands

A persistent tension is that effective nested-risk oversight often requires timely access to underlying-party context, but real-world constraints (privacy, banking secrecy, contractual limits, technical interoperability) restrict what can be shared, how quickly, and in what structure. Cross-border payments roadmaps and data-quality initiatives highlight the push toward richer, standardized data yet the governance and legal-operational pathways for sharing risk-relevant data remain uneven.

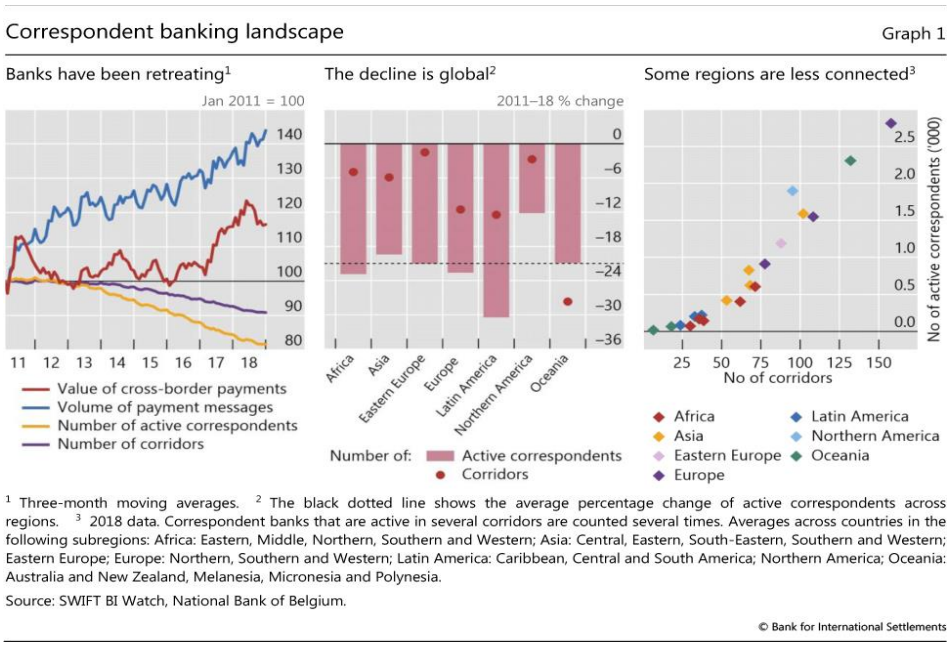

Figure 1. Correspondent Banking Landscape

4. Risk Landscape in Correspondent and Nested Banking

4.1. Risk Typologies Specific to Correspondent Banking

4.1.1. Unclear Originator/Beneficiary Information

A core typology in correspondent banking is **o**pacity created by incomplete, inconsistent, or truncated payment information as transactions pass through intermediaries. This undermines sanctions screening and AML monitoring because detection quality is bounded by what the correspondent can reliably "see" in payment messages and supporting data. Guidance on correspondent banking risk management repeatedly highlights transparency and information availability as central to controlling ML/TF risk. Financial Action Task Force guidance emphasizes managing correspondent risks through proportionate due diligence and monitoring, not "blanket exits," while recognizing that information gaps can increase risk.

4.1.2. High-Volume, Low-Margin Processing Pressures

Many correspondents banking services particularly wire processing and FX settlement operate under thin margins and high throughput. This creates pressure to (i) streamline onboarding and periodic reviews, (ii) manage large alert volumes, and (iii) maintain straight-through processing. Operational realities can weaken controls when monitoring is tuned too loosely to reduce friction, or conversely, drive relationship exits when alert volumes become unmanageable. International payments work also notes that structural factors (fragmentation, concentration, and complexity) contribute to cost and risk pressures in the correspondent ecosystem. Bank for International Settlements / Committee on Payments and Market Infrastructures analysis discusses these systemic constraints in the cross-border payments landscape.

4.1.3. Reliance on Intermediaries' Controls

Correspondent banking is inherently a control-dependency model: the correspondent often must rely on the respondent's AML program effectiveness, governance, and monitoring capacity for customer-level risks. This "reliance risk" is explicitly addressed in Basel Committee on Banking Supervision guidance, which situates ML/FT risk within broader bank risk management and underscores governance, assurance, and defensible risk decisions for higher-risk relationships (including correspondent contexts).

4.2. Risks Amplified By Nesting

4.2.1. Reduced Transparency Over Downstream Customers and Transactions.

Nested relationships extend the chain of access so that downstream institutions or clients effectively use the respondent's correspondent access. This reduces the correspondent's visibility into (i) downstream customer types, (ii) underlying transaction purposes, and (iii) whether downstream screening/monitoring is effective. FATF correspondent banking guidance treats nested activity as a higher-risk feature, requiring proportionate measures (especially clarity on the nature of downstream access and the respondent's controls).

4.2.2. Layering via Multiple Institutions.

Nesting can introduce additional layers of intermediation, which is especially relevant to the "layering" stage of money laundering. Each layer can add friction to traceability (different systems, different data fields, different retention practices) and can dilute accountability for detection and escalation. This is a practical reason nested corridors may exhibit higher risk even when all parties are regulated.

4.2.3. Regulatory Arbitrage and Weak Supervision Corridors.

Nesting can facilitate regulatory arbitrage, where activity is routed through jurisdictions with weaker supervision, inconsistent enforcement, or less mature AML frameworks. International standard setters explicitly maintain public mechanisms for identifying jurisdictions with strategic AML/CFT deficiencies, reflecting the importance of jurisdictional risk in cross-border relationships. In practice, risk intensifies where nested parties serve higher-risk geographies (or customers with higher-risk products), and where requests for additional information (RFI) are slow or incomplete.

4.2.4. Complex Ownership Structures and Shell Entities.

Nested arrangements can be exploited when downstream entities (or their customers) use opaque corporate structures, nominee arrangements, or shell companies that obscure beneficial ownership or control. This complicates both onboarding (what is the "true" counterparty risk?) and monitoring (is the activity consistent with stated business and ownership?). Basel guidance reinforces beneficial ownership transparency and governance expectations as part of sound ML/FT risk management.

4.3. Cross-Border AML/CTF and Sanctions Convergence

4.3.1. Sanctions Screening vs AML Monitoring Overlap.

In correspondent and nested chains, AML/CTF monitoring and sanctions screening increasingly converge operationally:

- Both depend on complete and structured party data (names, identifiers, addresses, purpose codes, entity types).
- Both use risk-based approaches to prioritize higher-risk corridors, counterparties, and patterns.
- Both face the same constraints: missing fields, inconsistent transliteration, and multi-hop routing.

This convergence is one reason the industry focus on richer payments data standards (including ISO 20022) is relevant to both sanctions and AML outcomes. SWIFT explicitly ties screening effectiveness to richer, structured data in the ISO 20022 environment and highlights alert reduction and improved screening quality as key benefits.

4.3.2. Risks from High-Risk Jurisdictions, Conflict Zones, Offshore Centers.

Cross-border relationships are especially sensitive to:

- jurisdictions subject to increased monitoring/deficiencies,
- regions affected by conflict or instability (higher TF and evasion concerns), and
- Offshore centers or secrecy-linked structures that complicate beneficial ownership verification.

Global policy work on cross-border payments recognizes that legal/regulatory and supervisory implementation varies significantly across jurisdictions, shaping both risk and the feasibility of harmonized controls. Financial Stability Board monitoring under the G20 cross-border payments roadmap stresses that implementation of legal/regulatory recommendations remains uneven and progress is still developing.

4.4. Products and Channels

Different products and channels shape risk because they determine speed, data richness, typical counterparties, and typologies.

4.4.1. Wire Transfers

Wires are high-throughput and often time-sensitive. Risks include:

- incomplete originator/beneficiary information,
- rapid movement across jurisdictions,
- structuring via multiple payments, and
- Use of intermediaries to obscure routing.

Controls typically emphasize data quality checks, sanctions screening, typology-driven monitoring, and rapid escalation processes for RFIs.

4.4.2. Trade Finance

Trade finance can be exposed to:

- trade-based money laundering (TBML) typologies (over/under-invoicing, phantom shipments),
- complex document flows, and
- Multi-party structures across borders.

Controls often require stronger integration of customer risk, trade documentation review, and monitoring for anomalies relative to customer profile and corridor.

4.4.3. Cash-Intensive Flows and Remittances

Cash-intensive businesses and remittance corridors can generate:

- higher placement risk (cash introduction),
- fragmentation into many small transfers, and
- Dependency on intermediaries (e.g., MSBs) that may sit "downstream" in nested structures.

This is where the access vs risk tension is sharp: loss of correspondent access can displace legitimate flows and harm financial inclusion an issue FATF explicitly addresses in its broader inclusion-oriented guidance.

4.4.4. Correspondent Accounts, Payable-Through Accounts, Clearing Arrangements

Indirect access models (including PTAs) raise the stakes because third parties may have more direct transactional capability through the respondent's account. FATF standards specify heightened expectations for PTAs (e.g., confidence that the respondent performs CDD on direct-access customers and can provide CDD information when needed). Clearing arrangements and tiered access can also concentrate operational and compliance risk in the correspondent and respondent institutions that sit at the "access points" to major payment systems.

4.5. Emerging Risks and Trends

4.5.1. Crypto/Virtual Assets Exposure through Nested Clients

A growing risk pathway is indirect exposure to virtual assets through nested downstream clients (e.g., fintechs, payment intermediaries, or businesses that interface with VASPs). FATF has repeatedly assessed uneven global implementation of virtual asset standards (Recommendation 15), including travel rule implementation and supervision. The 2025 targeted update continues to flag gaps while noting progress in regulation and supervisory actions. For correspondent/nested frameworks, the practical issue is: does the respondent (and downstream party) have sufficient controls to identify VA-linked flows, counterparties, and typologies and can the correspondent obtain risk-relevant information when needed?

4.5.2. Instant Payments and Cross-Border Interoperability

Cross-border linking of fast payment systems can improve speed and user experience, but it can also compress the time available for compliance intervention and raise dependency on standardized data, governance, and operating procedures. CPMI work on cross-border fast payment system interlinking highlights governance/oversight structures and the operational arrangements required for safe interoperability factors that directly affect monitoring design and escalation feasibility.

4.5.3. AI-Driven Fraud and Financial Crime

AI is accelerating fraud tactics (phishing, impersonation, deepfake-enabled social engineering), which can increase suspicious payment volumes and complicate detection especially in high-speed environments. Europol reporting notes the growing role of generative AI and LLM-assisted fraud communications. INTERPOL also documents global financial fraud trends and evolving scam patterns.

For correspondent/nested settings, this translates into:

- greater pressure on monitoring teams (alert volumes, faster victim-driven transfers),
- more sophisticated "legitimacy camouflage" (high-quality fake documentation and communications), and
- a stronger need for behavioral analytics + typology refresh + rapid RFI/escalation, especially for corridors and counterparties where fraud proceeds are quickly laundered through cross-border chains.

Table 2. Risk Landscape Matrix for Correspondent and Nested Banking

Risk driver / typology	Where it shows up most	What increases it in nested structures	Practical red flags / indicators	Primary controls to mitigate (RBA-aligned)
Unclear originator/beneficiary info	Wire transfers; intermediary chains	Downstream aggregation + incomplete pass-through	Missing/placeholder fields; inconsistent names/addresses; repeated "unknown"; truncated data; frequent repair messages	Payments data quality rules; mandatory fields; structured data standards; RFI playbooks; corridor-based monitoring
High-volume, low-margin processing pressure	Large payment hubs; corridor clearing	Alert suppression pressure increases	Sudden tuning changes; declining SAR/STR vs stable volumes; high straight-through rates in higher-risk corridors	Governance for model tuning; alert quality metrics; periodic independent testing; risk-tiered thresholds
Reliance on intermediaries' controls	All correspondent relationships	Dependency expands to downstream entities	Weak respondent audit trail; slow/incomplete responses to RFIs; limited evidence of downstream oversight	Enhanced due diligence (EDD) on respondent program; audit/assurance rights; periodic reviews; conditional access (limits, exclusions)
Reduced transparency over downstream customers	Respondent-of-respondent; sponsor models	Core feature of nesting	High flow volumes with vague "purpose"; new business lines not disclosed; downstream entity types not documented	"Nesting disclosure" requirement; downstream typology mapping; onboarding attestations; targeted sampling/testing
Layering through multiple institutions	Complex corridors; trade/payment hybrids	Adds hops, increases opacity	Many-to-many routing; frequent intermediary changes; round-tripping patterns	Network analytics; relationship/corridor risk scoring; typology-based scenarios; escalation triggers
Regulatory arbitrage / weak supervision corridors	Higher-risk geographies	Nesting can route via weaker regimes	Disproportionate flows through lightly supervised markets; rapid onboarding of downstream entities	Country/jurisdiction risk scoring; EDD triggers; enhanced periodicity; restrictions on nested access to certain corridors
Complex ownership / shell entities	Trade, corporate payments, PSPs	Downstream onboarding variability	Recently incorporated entities; layered ownership; nominee directors; mismatch between profile and flows	Beneficial ownership verification; control person checks; adverse media screening; profile-to-flow reasonableness testing
AML/CTF and sanctions convergence risk	All cross-border flows	Same data limits apply, multiplied	Frequent name variations; transliteration issues; high false positives; repeated near-miss hits	Integrated sanctions+AML workflow; data enrichment; list management governance; consistent escalation rules
High-risk jurisdictions / conflict zones / offshore centers	Specific corridors	Increases when downstream serves these areas	Activity spikes tied to sensitive regions; routing via offshore nodes	Corridor restrictions/limits; enhanced screening; additional approvals; heightened monitoring frequency
Virtual asset exposure via nested clients	PSPs/fintech sponsor chains	Downstream may interface with VASPs	Payments to/from crypto-related merchants; unusual velocity; "exchange" or "digital asset" descriptors	Targeted typologies; counterparty classification; enhanced KYC for nested PSPs; focused transaction monitoring
Instant payments interoperability	Faster payments links	Less time to intervene	Very short time-to-withdrawal; high-speed mule patterns	Pre-transaction controls; stronger upfront risk scoring; real-time monitoring; automated holds/escalations

				were permitted
AI-driven fraud & synthetic activity	All channels; especially retail-to-cross-border	Downstream channels scale faster	Spike in first-time payees; micro-splitting; mule networks; repeated social-engineering patterns	Fraud–AML coordination; behavioral analytics; rapid typology refresh; improved RFI turnaround SLAs

5. Regulatory and Supervisory Expectations

5.1. Global Standards and Principles

5.1.1. Correspondent Banking Due Diligence Expectations

Global expectations for correspondent banking are anchored in the standards and guidance of the Financial Action Task Force. The core message is risk-based: correspondent banking is often higher risk, but institutions should manage ML/TF risk through proportionate controls rather than indiscriminately exiting whole regions or customer classes ("de-risking").

Across FATF-aligned frameworks, supervisory expectations for correspondents typically include:

- Understanding the respondent (ownership, management, business model, product/customer base, geographic footprint, and AML/CTF program effectiveness).
- Risk-based escalation to EDD when risk drivers are present (e.g., high-risk corridors, poor transparency, nested access, weak supervision).
- Ongoing monitoring and periodic review that is demonstrably aligned to the assessed risk, including the ability to detect significant changes in the respondent's risk profile.
- Clear treatment of payable-through / indirect access: where third parties can transact through a correspondent account, expectations increase (including confidence the respondent performs CDD on direct-access customers and can provide relevant CDD info when requested).

In parallel, the Basel Committee on Banking Supervision frames AML/CTF as a bank-wide risk management obligation emphasizing governance, control testing, escalation/exit decisions, and the need for banks to manage ML/FT risk in line with overall risk appetite.

5.1.2. Reliance, Outsourcing and Third-Party Risk Principles

Supervisors generally draw a bright line between outsourcing/reliance and accountability:

- Reliance on another institution's controls does not remove responsibility. Correspondents can rely on respondents to conduct customer-level CDD, but must still apply relationship-level due diligence and oversight proportionate to risk.
- Third-party and outsourcing principles show up as expectations for governance and assurance: documented control ownership, audit/oversight rights, periodic testing, and clear escalation triggers when downstream risk increases or transparency degrades.
- Where "nesting" exists, the emphasis shifts to validating that the respondent has an effective framework to manage downstream access and can respond to reasonable information requests.

5.2. Jurisdictional Comparison

Below is a practical structure you can use (and repeat) for each jurisdiction: (i) CDD/EDD requirements, (ii) ongoing monitoring expectations, (iii) payable-through/nested treatment, (iv) enforcement themes.

5.2.1. United States

- CDD/EDD for correspondents: The Financial Crimes Enforcement Network links correspondent account due diligence expectations to Section 312 of the USA PATRIOT Act framework, establishing due diligence obligations for correspondent accounts maintained for certain foreign financial institutions.
- Ongoing monitoring: U.S. examiner expectations are operationalized through the FFIEC BSA/AML Examination Manual, which includes testing procedures for correspondent account due diligence and expects banks to evidence a risk-based program (including sampling, documentation, and escalation decisions).
- Payable-through and nested arrangements: U.S. guidance is unusually explicit:
- The FFIEC manual contains specific coverage of payable-through accounts and risk management objectives.
- It also explicitly references nested/downstream correspondent banking, including examiner focus on determining nested relationships and considering respondent AML program information.

- Supervisory priorities: The most consistent U.S. supervisory themes are (a) defensible risk-based EDD decisions, (b) monitoring effectiveness, and (c) documentation that proves the program works in practice especially where foreign respondents, money transmitters, or other higher-risk institution types are involved.

5.2.2. European Union

- CDD/EDD for correspondents: EU expectations are heavily expressed through risk-factor guidance issued by the European Banking Authority, emphasizing how firms should adjust CDD/EDD depth according to customer, product, geography, and delivery-channel risk.
- Ongoing monitoring: Monitoring expectations are framed as a continuous obligation to keep CDD information up to date and ensure transaction behavior remains consistent with the institution's understanding of the customer relationship and risk profile.
- Payable-through / nesting: EU guidance is typically less "product-specific" than the U.S. approach and more risk-factor oriented. The practical consequence is that indirect access and reduced transparency are treated as risk indicators that should drive stronger EDD, enhanced monitoring, and shorter review cycles, rather than a single prescriptive PTA rule-set.
- Supervisory priorities: EU supervision increasingly focuses on (a) quality of risk assessments, (b) beneficial ownership understanding, and (c) effectiveness of monitoring controls particularly for cross-border activity and higher-risk third countries.

5.2.3. United Kingdom

- CDD/EDD and monitoring expectations: UK expectations are frequently visible through enforcement outcomes and supervisory reporting. Recent Financial Conduct Authority materials illustrate strong emphasis on (i) risk identification/assessment, (ii) appropriate EDD where risks are high, and (iii) ongoing monitoring that matches the firm's understanding of customer activity.

Enforcement trends and priorities (illustrative):

- The FCA's published 2025 fines list includes a substantial penalty against Barclays Bank plc tied to failures to identify, assess, monitor, and manage money laundering risks in a corporate banking context.
- The FCA's Final Notice against Nationwide Building Society emphasizes the importance of CDD/EDD and ongoing monitoring expectations over time.
- The FCA's Final Notice against Monzo Bank Limited reinforces the same themes for firms with fast-growing customer bases and operational scaling pressures.

(You can use these outcomes in your paper as evidence of "what supervisors care about" in practice: monitoring effectiveness, risk-based calibration, and documentation/auditability.)

5.2.4. Singapore

- Core requirements: The Monetary Authority of Singapore sets expectations through MAS Notice 626 and related guidance, covering risk assessment, CDD/EDD, ongoing monitoring, and controls relevant to correspondent and trade finance risks.
- Enforcement themes: MAS has publicly documented sizeable AML-related enforcement actions, underscoring supervisory expectations around control effectiveness (not merely policies). For example, MAS announced penalties/actions against multiple financial institutions in 2025 for AML-related breaches.

5.2.5. Hong Kong (Useful Comparator for Cross-Border Hubs)

The Hong Kong Monetary Authority has taken disciplinary actions under Hong Kong's AML/CTF framework, reflecting focus on CDD/EDD and ongoing monitoring failures.

5.2.6. Sanctions Convergence Touchpoint

Cross-border monitoring expectations increasingly incorporate sanctions risk, especially in fast/instant payment contexts. Office of Foreign Assets Control has issued sanctions compliance guidance for instant payment systems that reinforces risk-based compliance design for new payment technologies.

5.3. Key Tension Points

5.3.1. "Reasonable Measures" vs "Full Visibility" Expectations

A central supervisory tension is that correspondents are expected to take reasonable risk-based measures, yet nested structures and cross-border chains inherently limit visibility. FATF guidance is explicit that correspondents are not required to perform CDD on

every downstream customer, but they must still manage risk through proportionate due diligence, monitoring, and information requests where warranted.

In practice, this becomes a defensibility problem: institutions must show how their controls achieve outcomes despite incomplete data.

5.3.2. How Far Downstream Due Diligence Should Extend

The "KYCC" misconception persists because nested arrangements feel like they require deeper downstream insight. Supervisory logic generally supports this boundary:

- Customer-level CDD sits with the respondent (and downstream institutions for their own customers).
- Relationship-level assurance sits with the correspondent, including understanding respondent controls, restricting services if necessary, and escalating monitoring intensity for higher-risk corridors or indirect access.
- For payable-through-like scenarios, expectations sharpen: correspondents should be confident the respondent can identify direct-access customers and provide relevant CDD information when requested.

5.3.3. Documentation and Auditability Standards

Across jurisdictions, supervisors repeatedly return to a shared set of expectations: decisions must be documented, reviewable, and testable. That includes:

- a clear risk assessment rationale for onboarding and for any EDD decisions,
- evidence that monitoring is calibrated and effective (not merely present),
- records supporting changes in risk posture (triggers, RFIs, remediation actions, restrictions, exit decisions),
- and governance proof that senior management oversight exists for higher-risk relationships (correspondent and nested).

6. Due Diligence in Correspondent and Nested Relationships

6.1. Risk-based onboarding framework

A robust onboarding framework for correspondent relationships starts with a clear risk-based approach (RBA): collect enough information to understand the respondent institution, assess inherent and residual risk, and apply CDD/EDD measures proportionate to that risk. FATF guidance emphasizes that correspondent banking requires careful, documented due diligence on the respondent institution and its AML/CTF controls, with the depth calibrated to risk factors such as geography, products, and the nature of access provided. (fatf-gafi.org)

6.1.1. Customer (FI) Risk Assessment (Who is the Respondent?)

Onboarding should establish a defensible understanding of the respondent's identity, legitimacy, and risk profile, including:

- Regulatory status and licensing: licensing/registration type, regulator identity, scope of permitted activities, and any material restrictions.
- Ownership, control, and governance: beneficial ownership (where applicable), group structure, board/senior management oversight, and governance maturity. FATF standards emphasize transparency and beneficial ownership understanding as part of effective CDD. (fatf-gafi.org)
- Business model and products: retail vs corporate, trade finance activity, remittance/MSB exposure, PSP/fintech partnerships, and any high-risk offerings that can affect transaction patterns.
- Geographic footprint: jurisdictions of operation, key corridors, and exposure to regions with heightened sanctions/ML/TF concerns.

6.1.2. AML Program Assessment (Can They Manage Risk?)

Correspondent due diligence should include an assessment of the respondent's AML/CTF program effectiveness not only whether policies exist, but whether controls are credible and governable. Basel guidance frames AML/CTF as a governance and risk management obligation that should be reflected in control design, staffing capability, independent testing, and escalation structures. (bis.org)

Key components to evaluate:

- Policies and procedures: CDD/EDD standards, beneficial ownership approach, sanctions screening, transaction monitoring framework, and suspicious activity escalation processes.
- Staffing and competency: resourcing levels, training coverage, language/corridor expertise, and compliance independence.
- Independent audit/testing: scope, frequency, findings themes, remediation timelines, and governance accountability.
- Technology and data: screening and monitoring tools, model tuning governance, data quality controls, and recordkeeping.

6.1.3. ML/TF Risk Assessment of Corridors and Customer Base (What Will Flow?)
Onboarding should translate business model into expected activity patterns:

- expected corridors and currencies,
- customer segment mix (e.g., corporates, PSPs, MSBs, NGOs),
- Typical transaction purposes and volumes.

This "profile-to-flow" mapping becomes the baseline for monitoring and for later "change detection" during periodic reviews.

6.2. Enhanced Due Diligence Triggers (EDD)

EDD should be activated when risk indicators suggest a higher likelihood of ML/TF/sanctions exposure or reduced transparency. FATF guidance supports tailoring intensity based on risk and emphasizes that higher-risk correspondent relationships require more robust measures and senior oversight. (fatf-gafi.org)

6.2.1. Common EDD triggers include

- High-risk jurisdictions/corridors: operations in, or significant flows to/from, jurisdictions with strategic AML/CTF deficiencies or known typology concerns. FATF's monitored jurisdiction work is commonly used to inform jurisdictional risk scoring. (fatf-gafi.org)
- Weak supervision or adverse media: credible negative reporting, repeated supervisory findings, poor remediation history, or governance instability.
- High-risk products and services: trade finance (TBML exposure), payable-through or direct-access–like arrangements, nested PSP/MSB access, or unusually complex corporate structures. FATF standards highlight payable-through accounts as needing heightened safeguards (e.g., respondent CDD on direct-access customers and ability to provide CDD info upon request). (fatf-gafi.org)
- Unusual volumes/velocity or unclear business purpose: a mismatch between stated business model and observed/expected flows; rapid growth; unexplained corridor concentration; repeated "miscellaneous" payment purposes.

In practice, EDD typically adds: deeper verification of ownership/control, stronger assurance of AML control effectiveness (including audit results), enhanced monitoring design commitments, and higher-level approvals for onboarding/continuation.

6.3. Nested Relationship due Diligence Design

Nested access is not automatically prohibited, but it requires a due diligence design that explicitly addresses opacity and control dependency. FATF guidance specifically calls out nested correspondent activity and frames it as a factor that should drive proportional measures and clear understanding of the access model. (fatf-gafi.org)

6.3.1. Understand the Downstream Access Model and Customer Types
Nested due diligence should document:

- who downstream users are (banks, PSPs/fintechs, MSBs, corporates),
- how downstream customers access cross-border services (aggregation vs segregated flows),
- what information is passed through in payment messages (originator/beneficiary detail, identifiers),
- what products downstream users access (wires only vs trade vs settlement services).

6.3.2. Document Permitted Uses and Prohibited Nesting Tiers
A practical control is to define "nesting rules" in relationship documentation:

- Permitted downstream categories (e.g., regulated FIs only; or regulated PSPs with specified controls),
- Prohibited categories (e.g., unregulated entities; unknown sub-respondents),
- Tier limits (e.g., no respondent-of-respondent-of-respondent chains; no "fourth-party" access),
- Corridor restrictions (e.g., no downstream use for specified high-risk jurisdictions).

This is how "RBA" becomes enforceable: it converts risk appetite into measurable boundaries.

6.3.3. Contractual Clauses: Transparency, Information Rights, Audit Rights
For nested relationships, contractual terms become core risk controls, including:

- Transparency commitments: respondent must disclose existence and nature of nested arrangements and material changes to downstream access.

- Information rights and response SLAs: ability to request information on specific transactions/counterparties and obtain timely responses (especially where monitoring flags anomalies).
- Audit/assurance rights: ability to obtain independent testing results, third-party assurance, or conduct (virtual) audits where feasible. Basel guidance stresses governance and assurance for managing ML/FT risk and supports clear accountability and testing arrangements for higher-risk relationships. (bis.org)

6.3.4. Relying On Respondent Controls: When Acceptable and When Not

The key is bounded reliance:

- Acceptable reliance is most defensible when the respondent is well regulated, has mature AML systems, can evidence independent audit/testing, provides reliable information upon request, and has controls specifically covering downstream/nested access.
- Unacceptable reliance arises when supervision is weak, transparency is poor, information requests are slow/incomplete, nested access is broad or undefined, or when the respondent cannot demonstrate effective monitoring for downstream activity.
- FATF's framing helps here: correspondents are not expected to conduct downstream customer CDD, but must be able to justify their relationship-level confidence in the respondent's program and their own monitoring/controls. (fatf-gafi.org)

6.4. Practical due Diligence Toolkit (What to Include)

This toolkit is designed to produce a file that is both risk-intelligent and audit-ready, and it aligns well with common industry practice.

6.4.1. FI Questionnaires + Validation Steps

Use a standardized FI questionnaire many banks adopt the Wolfsberg Group's CBDDQ as a baseline then validate critical claims with evidence and independent sources. (wolfsberg-group.org)

Validation examples:

- confirm regulator/license details via official registers where possible,
- corroborate ownership and governance claims with reliable corporate filings,
- reconcile declared corridors/products with observed historical activity (if existing relationship).

6.4.2. Independent Verification Sources

- regulator publications and registers,
- reputable corporate registry extracts (jurisdiction-dependent),
- audited financial statements (where available),
- external screening/adverse media tools and reputable press sources (document rationale and dates).

6.4.3. Site Visits / Virtual Audits (Where Appropriate)

Where risk is higher (or transparency is low), virtual audits and structured control walkthroughs can meaningfully improve assurance. These should focus on:

- how CDD/EDD is actually performed,
- how sanctions screening is handled (including alert decisioning),
- how monitoring scenarios are tuned and reviewed,
- how nested access is governed and documented.

6.4.4. Control Testing and Periodic Refresh Cycles

A defensible due diligence program is not "one-and-done." It should define:

- review periodicity by risk tier (e.g., annual for higher risk; longer cycles for lower risk),
- event-driven refresh triggers (regulatory findings, ownership changes, corridor changes, new downstream products, sudden volume shifts),
- ongoing testing/QA (sampled RFIs, monitoring effectiveness checks, sanctions screening quality metrics). This directly supports the documentation/auditability expectations highlighted by supervisory practice in multiple jurisdictions.

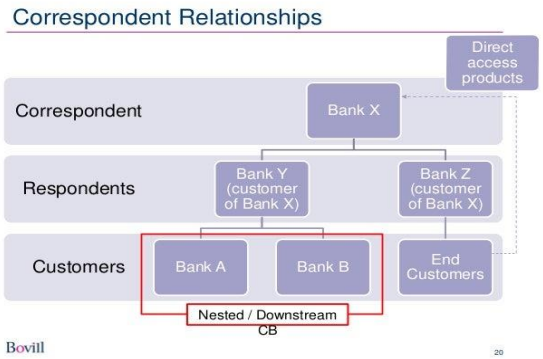

Figure 2. Structure of Correspondent Banking Relationships

7. Ongoing Monitoring and Transaction Surveillance Expectations

7.1. Monitoring Objectives and Risk Model

7.1.1. What "Effective Ongoing Monitoring" Means in Correspondent Contexts

In correspondent banking, "effective ongoing monitoring" means more than running transaction screening tools. It is the ability to detect and respond to changes in risk over time by linking (i) what the bank knows about the respondent's business model and corridors, (ii) what it observes in payment flows and alerts, and (iii) what it can verify through governance and information requests. FATF's risk-based approach guidance reinforces that monitoring must be proportionate to risk and capable of identifying unusual or suspicious activity, while keeping customer/relationship information up to date.

Practically, the monitoring objective set in correspondent banking typically includes:

- Consistency testing: Are flows consistent with the respondent's stated business, customer base, products, and corridors?
- Change detection: Have volumes/velocity/corridors/counterparties changed in a way that indicates increased risk or undisclosed activity?
- Typology detection: Are there patterns consistent with known ML/TF or sanctions evasion methods (layering, round-tripping, use of intermediaries, suspicious trade/payment descriptions)?
- Compliance event response: Can the bank reliably escalate, investigate, document, and (where required) file suspicious activity reports and/or restrict services?

7.1.2. How Monitoring Differs for Nested Access vs Direct Respondents

For direct respondents, monitoring can rely more heavily on stable profiling assumptions (business model and customer segments are better defined), and the bank can reasonably expect faster and more complete responses to information requests.

For nested access, monitoring must explicitly compensate for opacity and control dependency:

- Higher emphasis on "relationship anomaly" monitoring (corridor spikes, new counterparty clusters, unexplained routing changes).
- More structured RFI escalation because clarifying transaction context often requires respondent input.
- Stronger governance triggers (e.g., enhanced review if nesting expands, new downstream types appear, or data quality deteriorates). FATF's correspondent banking guidance highlights nested relationships as a risk factor that should influence proportional monitoring and due diligence expectations.

7.2. Monitoring Architecture

7.2.1. Rules-Based Scenarios vs Analytics/ML Models

A defensible monitoring architecture in correspondent banking is usually hybrid:

- Rules-based scenarios remain essential for regulatory defensibility and targeted typologies (e.g., high-risk corridors + unusual velocity; round-dollar patterns; rapid pass-through; frequent intermediary changes). These are transparent, explainable, and easier to evidence to supervisors.
- Analytics / ML models can improve signal quality for high-volume environments by prioritizing alerts, detecting novel patterns, and reducing false positives but they require stronger governance (model risk management, explainability, drift monitoring, and validation).

Basel guidance emphasizes that AML/CTF controls must be governed as part of enterprise risk management, including appropriate oversight and independent testing principles that become critical when advanced analytics are used.

7.2.2. Network/Link Analysis for Layered Flows

Because correspondent and nested risks often involve layering and interconnected counterparties, network methods can add value:

- identify clusters of beneficiaries/originators linked across multiple respondents, corridors, or intermediaries,
- detect hub-and-spoke pass-through behavior (typical of laundering chains),
- Highlight unusual repetition of entities or routes across apparently unrelated payments.

Network analytics is particularly relevant to nested structures because activity is less interpretable at the single-transaction level; patterns emerge at the corridor/counterparty graph level.

7.2.3. Corridor Risk Scoring and Dynamic Thresholds

A high-performing monitoring program assigns a corridor risk score (country pair, currency, payment type, respondent risk tier) and uses it to adjust:

- thresholds (volume, velocity, value),
- scenario sensitivity,
- Review frequency and sampling depth.

This is one of the most practical ways to operationalize the RBA in a correspondent environment: higher-risk corridors trigger more intensive monitoring and shorter escalation timelines.

7.3. Managing Limited Transparency

7.3.1. Data Quality and Message Standards (Originator/Beneficiary Completeness)

Monitoring quality is constrained by payments data quality. In cross-border flows, missing or poorly structured originator/beneficiary fields reduce screening accuracy and create downstream operational burden. Industry guidance increasingly emphasizes improving payment data quality through structured standards (including ISO 20022 migration and richer field structures), with the goal of improving screening and reducing avoidable alerts.

A practical correspondent monitoring program should therefore include:

- data completeness metrics (missing fields by respondent/corridor),
- quality gates (reject/repair rules for critical fields where allowed),
- trend reporting (deterioration in data quality as a risk trigger).

7.3.2. Handling Missing Information and False Positives

Two competing failures can occur:

- Over-alerting (false positives), which consumes investigator capacity and encourages over-suppression.
- Under-detection (false negatives), where missing data prevents identification of real risk.

To manage this, best practice is to treat missing/low-quality information as a risk signal itself:

- escalate monitoring intensity when data quality is persistently poor,
- impose conditional requirements (e.g., remediation plan, enhanced review cadence),
- restrict certain corridors/products if transparency cannot be improved.

7.3.3. Use of Request-For-Information (RFI) Escalation Pathways

In correspondent and nested monitoring, RFIs are a core control tool. A regulator-ready RFI pathway typically includes:

- standardized RFI templates (what is requested and why),
- service-level expectations (response timelines by risk tier),
- escalation rules for non-response or inadequate response,
- documentation requirements and linkages to alerts/cases.

This aligns with the practical intent of FATF's correspondent banking guidance: correspondents are not expected to conduct full downstream CDD, but should obtain relevant information on a risk basis, especially where transactions appear unusual or inconsistent.

7.4. Alert Management and Investigations

7.4.1. Triage Logic and Investigator Playbooks

Alert handling must be structured to cope with high volumes while remaining defensible:

- Tier 1 triage: rapid disposition of clear false positives using documented rules and rationale.
- Tier 2 investigation: deeper review for alerts linked to high-risk corridors, nested access, poor data quality, or repeat counterparties.
- Tier 3 escalation: enhanced review and RFI activation, possible relationship management escalation, or restrictions.

Investigator playbooks should be typology-oriented and include:

- what data to collect (transaction history window, counterparties, corridor context),
- what patterns trigger escalation (repeat near-misses, unusual routing, rapid pass-through),
- how to document reasoning and outcomes.

U.S. supervisory material (FFIEC BSA/AML manual) is often used as a reference point for the expectation that investigations and decisions be documented and that the institution can evidence how the AML program operates in practice—including in higher-risk contexts such as correspondent relationships and nested activity.

7.4.2. Suspicious Activity Reporting Decisioning

Suspicious activity reporting decisions (e.g., SAR/STR) must be consistent, well-documented, and anchored in:

- the alert facts and supporting evidence,
- the risk profile of the respondent/corridor,
- results of RFIs and internal reviews,
- rationale for filing or not filing.

7.4.3. Documentation and Defensibility for Regulators

Defensibility is typically achieved by ensuring every step is traceable:

- alert generation logic,
- analyst disposition reason,
- investigation notes and supporting records,
- escalation outcomes (RFI requests/responses),
- final decisions (including relationship-level actions such as restrictions or exit).

7.5. Metrics and Effectiveness Testing

7.5.1. Model Validation and Tuning

Whether rules-based or ML-enabled, monitoring systems require ongoing governance:

- documented change control for scenario tuning,
- independent testing/validation (especially for higher-risk corridors and nested access),
- monitoring for model drift and performance degradation.

Basel's emphasis on governance and independent testing supports the expectation that AML/CTF controls are not only designed but also proven effective through oversight and assurance.

7.5.2. Back-Testing, QA, and Outcomes Analysis

A mature correspondent monitoring program measures effectiveness through:

- back-testing (do scenarios detect known historical risk cases?),
- QA sampling of cleared alerts (to estimate false negative risk),
- outcomes analysis (alerts → investigations → RFIs → filings → account actions),
- feedback loops (typology updates and scenario adjustments).

7.5.3. Regulatory-Ready Evidence: Governance, Logs, Audit Trails

Regulatory-ready evidence typically includes:

- governance artifacts (policies, monitoring methodology, committee minutes),
- model documentation (scenario library, thresholds, tuning rationale),
- case management records (timestamps, analyst actions, RFIs, decisions),

- audit trails and reporting dashboards (volumes, outcomes, data quality metrics),
- periodic review outputs for correspondent relationships (including changes in respondent/nested risk posture).

This combination is how institutions demonstrate that monitoring is not a "black box," but a controlled process aligned to RBA and appropriate for correspondent/nested risk.

8. Conclusion

Correspondent banking will remain essential to global payments, trade, and financial inclusion, yet it continues to sit at the center of heightened AML/CTF and sanctions expectations. This paper has shown that risk in correspondent banking is not only a function of geography or customer type, but also a function of structure especially where nested (downstream) access reduces transparency and increases dependence on the respondent's controls. The resulting challenge for banks and supervisors is to apply a risk-based approach that is both effective in preventing illicit finance and practical enough to sustain legitimate cross-border access.

The analysis highlights three findings that shape a defensible compliance posture in correspondent and nested relationships. First, visibility limits are structural, not incidental. Payment chains, inconsistent message quality, and tiered access models constrain what a correspondent can observe directly, particularly in nested arrangements. Second, effective risk management depends on integrating due diligence, contractual governance, and monitoring into a single lifecycle model. Onboarding must establish a clear understanding of the respondent's business model, corridors, and AML control effectiveness; relationship documentation must translate risk appetite into enforceable boundaries (including permitted/prohibited nesting); and transaction surveillance must be designed to detect corridor shifts, layering patterns, and data quality deterioration supported by escalation pathways such as RFIs. Third, the most persistent driver of de-risking is not simply "high risk," but uncertainty and defensibility: where institutions cannot evidence control effectiveness, auditability, and timely access to risk-relevant information, they tend to restrict or exit relationships to reduce exposure.

Based on these findings, the conclusion points to practical implications for both industry and policymakers. For banks, the priority is to strengthen nested-specific governance: explicit nesting disclosures, tier limits, corridor restrictions where necessary, information rights, and risk-tiered review cycles paired with monitoring architectures that combine explainable scenarios with network-aware analytics. Improving payments data quality and standardized information flows is equally critical, because both sanctions screening and AML monitoring are only as effective as the underlying data. For supervisors and standard setters, the key opportunity is greater consistency and clarity around what "reasonable measures" look like when full downstream visibility is not achievable particularly in the treatment of indirect access, data-sharing constraints, and acceptable reliance on respondent controls.

Ultimately, reducing cross-border financial crime risk and avoiding unnecessary de-risking are not competing goals. When AML/CTF expectations are translated into proportionate, testable controls supported by clear documentation and measurable effectiveness banks can better manage correspondent and nested relationships in ways that protect the integrity of the financial system while preserving access for legitimate global activity.

References

[1] AUSTRAC. (2024, January 23). *Due diligence of correspondent banking relationships*. AUSTRAC. https://www.austrac.gov.au/due-diligence-correspondent-banking-relationships

[2] Bank for International Settlements, Basel Committee on Banking Supervision. (2009). *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* (BCBS 154). https://www.bis.org/publ/bcbs154.pdf

[3] Basel Committee on Banking Supervision. (2017). *Revised annex on correspondent banking* (BCBS d389). Bank for International Settlements. https://www.bis.org/bcbs/publ/d389.pdf

[4] Basel Committee on Banking Supervision. (2020). *Sound management of risks related to money laundering and financing of terrorism* (BCBS d505). Bank for International Settlements. https://www.bis.org/bcbs/publ/d505.pdf

[5] Board of Governors of the Federal Reserve System. (2023). *Due diligence programs for correspondent accounts for foreign financial institutions: Examination procedures* (SR 23-6 / CA 23-4).

[6] Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., & Patchipulusu, H. H. S. (2022). Blockchain Technology in Supply Chain and Logistics: A Comprehensive Review of Applications, Challenges, and Innovations. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(3), 72-80.

[7] Attipalli, A., BITKURI, V., Mamidala, J. V., Kendyala, R., & KURMA, J. (2022). Empowering Cloud Security with Artificial Intelligence: Detecting Threats Using Advanced Machine learning Technologies. *Available at SSRN 5741263*.

[8] Routhu, K. K. (2022). From RFID to Geofencing: IoT-Enabled Smart Time Tracking in Oracle HCM Cloud. *International Journal of Science, Engineering and Technology*, *10*(4).

[9] Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. (2022). Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 31-41.
[10] Routhu, K. K. (2022). From Case Management to Conversational HR: Redefining Help Desks with Oracle's AI and NLP Framework. *International Journal of Science, Engineering and Technology*, *10*(6).
[11] https://www.federalreserve.gov/supervisionreg/srletters/SR2306a3.pdf
[12] Borchert, L., De Haas, R., Kirschenmann, K., & Schultz, A. (2023). *Broken relationships: De-risking by correspondent banks and international trade* (EBRD Working Paper No. 285). https://doi.org/10.2139/ssrn.4658618
[13] Committee on Payments and Market Infrastructures. (2016). *Correspondent banking* (CPMI d147). Bank for International Settlements. https://www.bis.org/cpmi/publ/d147.pdf
[14] Committee on Payments and Market Infrastructures. (2020). *Enhancing cross-border payments: Building blocks of a global roadmap* (CPMI d193). Bank for International Settlements. https://www.bis.org/cpmi/publ/d193.pdf
[15] Bank for International Settlements, International Monetary Fund, & World Bank. (2023). Exploring multilateral platforms for cross-border payments (Analytical Notes No. 2023/001). International Monetary Fund. https://doi.org/10.5089/9798400227363.064
[16] Mamidala, J. V., Enokkaren, S. J., Attipalli, A., Bitkuri, V., Kendyala, R., & Kurma, J. (2023). Machine Learning Models Powered by Big Data for Health Insurance Expense Forecasting. *International Research Journal of Economics and Management Studies IRJEMS*, *2*(1).
[17] Bitkuri, V., Kendyala, R., Kurma, J., Enokkaren, S. J., & Mamidala, J. V. (2023). Forecasting Stock Price Movements With Deep Learning Models for time Series Data Analysis. *Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-531. DOI: doi. org/10.47363/JAICC/2023 (2)*, *489*, 2-9.
[18] Singh, A. A. S. S., Mania, V., Kothamaram, R. R., Rajendran, D., Namburi, V. D. N., & Tamilmani, V. (2023). Exploration of Java-Based Big Data Frameworks: Architecture, Challenges, and Opportunities. Journal of Artificial Intelligence & Cloud Computing, 2(4), 1-8.
[19] Routhu, K. K. (2023). AI-driven succession planning in Oracle HCM Cloud: Building resilient leadership pipelines through predictive analytics. *International Journal of Science, Engineering and Technology*, *11*(5).
[20] Tamilmani, V., Namburi, V. D., Singh Singh, A. A., Maniar, V., Kothamaram, R. R., & Rajendran, D. (2023). Real-Time Identification of Phishing Websites Using Advanced Machine Learning Methods. *Available at SSRN 5837142*.
[21] From Fragmentation to Focus: The Benefits of Centralizing Procurement. (2023). International Journal of Research and Applied Innovations, 6(6), 9820-9833. https://doi.org/10.15662/
[22] Routhu, K. K. (2023). Embedding fairness into the digital enterprise, data driven DEI strategies with Oracle HCM Analytics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *9*(8), 266-274.
[23] Routhu, K. K. (2023). AI-driven skills forecasting in Oracle HCM Cloud: From static competencies to predictive workforce design. *International Journal of Science, Engineering and Technology*, *11*(1).
[24] European Banking Authority. (2023). *Guidelines on money laundering and terrorist financing risk factors, including simplified and enhanced customer due diligence, and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions* (EBA/GL/2023/03). https://www.eba.europa.eu/sites/default/files/2023-05/EBA%20GL%202023%2003%20-%20Final%20Report%20on%20ML_TF%20risk%20factors.pdf
[25] Europol. (2023). Internet organised crime threat assessment (IOCTA) 2023. Europol. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023
[26] Financial Action Task Force. (2014, October). *Guidance for a risk-based approach: The banking sector*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf
[27] Financial Action Task Force. (2016). *Guidance on correspondent banking services*. FATF. https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf
[28] Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
[29] Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. *Available at SSRN 5266517*.
[30] Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, V., Enokkaren, S. J., & Attipalli, A. (2021). Systematic Review of Artificial Intelligence Techniques for Enhancing Financial Reporting and Regulatory Compliance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(4), 73-80.

[31] Attipalli, A., Enokkaren, S., BITKURI, V., Kendyala, R., KURMA, J., & Mamidala, J. V. (2021). Enhancing Cloud Infrastructure Security Through AI-Powered Big Data Anomaly Detection. *Available at SSRN 5741305*.
[32] Singh, A. A. S., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Predictive Modeling for Classification of SMS Spam Using NLP and ML Techniques. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 60-69.
[33] Kothamaram, R. R., Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., & Maniar, V. (2021). A Survey of Adoption Challenges and Barriers in Implementing Digital Payroll Management Systems in Across Organizations. *International Journal of Emerging Research in Engineering and Technology*, *2*(2), 64-72.
[34] Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., Maniar, V., & Kothamaram, R. R. (2021). Anomaly Identification in IoT-Networks Using Artificial Intelligence-Based Data-Driven Techniques in Cloud Environmen. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(2), 83-91.
[35] Attipalli, A., BITKURI, V., KURMA, J., Enokkaren, S., Kendyala, R., & Mamidala, J. V. (2021). A Survey of Artificial Intelligence Methods in Liquidity Risk Management: Challenges and Future Directions. *Available at SSRN 5741342*.
[36] Routhu, K. K. (2021). AI-augmented benefits administration: A standards-driven automation framework with Oracle HCM Cloud. *International Journal of Scientific Research and Engineering Trends*, *7*(3).
[37] Routhu, K. K. (2021). Harnessing AI Dashboards in Oracle Cloud HCM: Advancing Predictive Workforce Intelligence and Managerial Agility. *International Journal of Scientific Research & Engineering Trends*, *7*(6).
[38] Financial Stability Board. (2016, December 19). *FSB action plan to assess and address the decline in correspondent banking*. https://www.fsb.org/2016/12/fsb-action-plan-to-assess-and-address-the-decline-in-correspondent-banking/
[39] Financial Stability Board. (2019, May 29). *FSB action plan to assess and address the decline in correspondent banking: 2019 progress report* (P290519-1). https://www.fsb.org/uploads/P290519-1.pdf
[40] Financial Stability Board. (2020, October 13). *Enhancing cross-border payments: Stage 3 roadmap* (P131020-1). https://www.fsb.org/uploads/P131020-1.pdf
[41] Association of Certified Fraud Examiners. (2022). Occupational fraud 2022: A report to the nations on occupational fraud and abuse. Association of Certified Fraud Examiners. https://www.acfe.com/report-to-the-nations/2022/
[42] Kranthi Kumar Routhu. (2020). Intelligent Remote Workforce Management: AI, Integration, and Security Strategies Using Oracle HCM Cloud. KOS Journal of AIML, Data Science, and Robotics, 1(1), 1–5. https://doi.org/10.5281/zenodo.17531257
[43] Routhu, K. K. (2020). Strategic Compensation Equity and Rewards Optimization: A Multi-cloud Analytics Blueprint with Oracle Analytics Cloud. *Available at SSRN 5737266*.
[44] International Monetary Fund. (2016, June). *The withdrawal of correspondent banking relationships: A case for policy action* (Staff Discussion Note SDN/16/06). https://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf
[45] Office of Foreign Assets Control. (2022, September 30). *Sanctions compliance guidance for instant payment systems*. U.S. Department of the Treasury. https://ofac.treasury.gov/system/files/126/instant_payment_systems_compliance_guidance_brochure.pdf
[46] Wolfsberg Group. (2023). *Correspondent Banking Due Diligence Questionnaire (CBDDQ)* (Version 1.4) [Resource page]. https://wolfsberg-group.org/resources/
[47] Routhu, K. K. (2019). Hybrid machine learning architecture for absence forecasting within Oracle Cloud HCM. *KOS Journal of AIML, Data Science, and Robotics*, *1*(1), 1-5.
[48] Routhu, K. K. (2019). Conversational AI in Human Capital Management: Transforming Self-Service Experiences with Oracle Digital Assistant. *International Journal of Scientific Research & Engineering Trends*, *5*(6).
[49] Wolfsberg Group. (2023, February 10). *Publication of the CBDDQ, FCCQ, guidance, glossary and FAQs* [News release]. https://wolfsberg-group.org/news/publication-of-the-cbddq-fccq-guidance-glossary-and-faqs/
[50] World Bank Group. (2017). *The decline in access to correspondent banking services: Trends, impacts, and solutions*. https://thedocs.worldbank.org/en/doc/786671524166274491-0290022018/render/TheDeclineinAccesstoCorrespondentBanking.pdf
[51] Routhu, K. K. (2019). AI-Enhanced Payroll Optimization: Improving Accuracy and Compliance in Oracle HCM. *KOS Journal of AIML, Data Science, and Robotics*, *1*(1), 1-5.
[52] Routhu, K. K. (2018). Reusable Integration Frameworks in Oracle HCM: Accelerating Enterprise Automation through Standardized Architecture. *International Journal of Scientific Research & Engineering Trends*, *4*(4).