



Isle of Man Financial Crime Partnership e-Gaming Risk Group

Proportionate and Intelligence Led Diligence

Date: 17th September 2026

Reference: FCP-e-Gaming-001

Disclaimer

This document is an industry consultation paper containing illustrative approaches only. It is not statutory, regulatory or legal guidance, and publication does not indicate adoption, approval or endorsement by any participating authority. All legal obligations and guidance issued by the regulators, the Isle of Man Financial Services Authority and the Gambling Supervision Commission, regarding a regulated business's anti-money laundering and countering the financing of terrorism controls must still be followed and cannot be substituted for anything mentioned in this document.

Contents

Introduction 3

Traditional versus Proportionate and Intelligence Led Diligence 4

Situations To Undertake Proportionate and Intelligence Led Diligence..... 5

Methods and Tools 6

Decision Pathway and Risk Considerations..... 13

Typologies 14

Conclusion..... 18

Reporting 19

Contact 19



Introduction

The Isle of Man Financial Crime Partnership (IOMFCP) is the Isle of Man's public private partnership. The IOMFCP e-Gaming Risk Operational Group (OG) is a 'fusion group' consisting of private members from six different sectors and includes public sector representation from both regulators, the Police and the Isle of Man Financial Intelligence Unit (FIU), who operate as the OG's Secretariat. It was formed in November 2025 and discussed potential, collaborative strategic projects.

Following the publication of the Isle of Man's Gambling Sector Money Laundering National Risk Assessments (NRA)¹, the OG examined key threats derived from the report. "Criminal ownership and control of gambling related businesses or software suppliers via companies and complex structures" was a key theme within the findings of the report that was discussed within the OG. From these discussions the OG determined that Isle of Man businesses implementing a robust and pre-emptive Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD) processes was a key mitigant to the risk of criminal ownership via complex structures. The OG therefore undertook a strategic project to produce and propose a best-practice framework for proportionate and intelligence-led diligence across online gambling content supply chains. This framework aims to address possible knowledge gaps in the industry and is intended for businesses that develop, supply, aggregate, resell, host or distribute online casino content, and for firms that provide services to those businesses.

The framework can be applied to regulated and non-regulated counterparties. Regulatory status is a relevant consideration, but it is only one factor in the overall risk assessment. The relevant questions are whether the business is legitimate, whether its ownership and operations are understood, where the content is being used, and whether the relationship creates material money laundering (ML), terrorist financing (TF), proliferation financing (PF), targeted financial sanctions, regulatory or reputational risk.

¹ <https://counteringfinancialcrime.im/reports-and-assessments/sectoral-reports/gambling-sector-report/>

The practical starting point is non-intrusive supply chain assurance. This means reasonable checks using information already held, publicly available information, observable online activity, contractual rights and targeted testing. It does not imply routine access to player data, transaction records, internal systems, detailed source code, or commercially sensitive lists of every downstream customer.

Traditional customer due diligence and any legal or regulatory requirements continue to apply. This framework supplements those obligations and should not be treated as a substitute, safe harbour or legal opinion. Each business remains responsible for determining the checks required by law, its risk assessments, its contractual position and the information reasonably available to it.

Core Principles

- Risk should be assessed proportionately rather than against an expectation that all risk can be eliminated.
- A red flag is an indicator requiring consideration and, where appropriate, corroboration. It is not proof of wrongdoing.
- Non-regulated activity is not automatically unlawful or unacceptable.
- Checks should reflect the firm's role, knowledge, access to information and practical leverage within the supply chain.
- Contractual and technical controls are useful but should not be treated as evidence that the controls work unless they are capable of being tested.
- Escalation should be targeted. Intrusive requests or audits should follow a defined trigger and be limited to what is reasonably needed to address the concern.
- Decisions, rationale and outcomes should be recorded so that the business can demonstrate how it applied a risk-based approach.
- Risk is an ongoing process, and relationships should be reviewed regularly not just at onboarding or trigger events.

A common industry approach can improve visibility without imposing an unrealistic obligation on content suppliers to recreate the due diligence or supervisory work of operators, regulators, banks or law enforcement. It can help businesses identify inconsistencies earlier, direct resources towards genuine risk, support more informed customer risk assessments and create a clearer basis for escalation, restriction, suspension or disengagement where concerns cannot be resolved.

This framework should be read alongside the Isle of Man NRAs, relevant sectoral statements, applicable AML and CFT legislation, sanctions requirements, regulatory guidance and each firm's own business risk assessment.

Traditional versus Proportionate and Intelligence Led Diligence

Traditional diligence and intelligence-led assurance serve different but complementary purposes. The distinction below is important because the same level of access and evidence will not be available or proportionate in every supply-chain relationship.

Approach	Primary purpose	Typical information	Relationship to escalation
Traditional customer due diligence	Establish who the customer or counterparty is and whether the relationship is acceptable at onboarding and review.	Identity, ownership and control, business model, purpose of the relationship, jurisdictions, source of funds should be checked and	Provides the starting risk profile. Gaps or inconsistencies may lead to targeted assurance or enhanced due diligence.

		source of wealth where required, licensing and regulatory status.	
Non-intrusive supply chain assurance	Test whether assumptions remain credible and identify emerging risks after onboarding.	Information already held, licence and registry data, websites, domains, marketing, adverse media, industry announcements, geolocation tests, observable payment methods and other public signals.	The baseline ongoing approach. A concern should normally be corroborated and, if appropriate, put to the counterparty before intrusive measures are considered.
Enhanced or intrusive assurance	Resolve a material concern that cannot be addressed through baseline checks or targeted enquiries.	Independent audit, detailed technical information, activity logs, transaction or payment data, downstream customer information, formal attestations or control testing.	Used only where justified by risk, lawful, contractually available and proportionate. The request should be specific and documented.

1. Complete onboarding and establish the expected business model, markets, distribution chain and use of the content.
2. Apply routine non-intrusive checks at a frequency informed by risk.
3. Where a trigger is identified, use additional public information or targeted testing to corroborate it.
4. Seek a focused explanation or updated information from the counterparty where the concern remains material.
5. Escalate to enhanced or intrusive assurance only where the concern cannot otherwise be resolved and the proposed measure is reasonable and available.
6. Record the outcome and decide whether to continue, monitor, restrict, suspend, terminate or report in accordance with legal obligations.

Situations To Undertake Proportionate and Intelligence Led Diligence

The following indicators may justify additional intelligence-led checks. They should be considered in context and weighted according to the nature of the relationship, the jurisdictions involved, the reliability of the information and whether several indicators are present together.

Structural and Contractual Indicators

- Limited visibility beyond the immediate contracting party, including restrictions on disclosure of onward supply arrangements.
- Use of aggregation, reseller or white-label models which introduce additional layers between the product owner and end user, particularly when the structure appears unnecessarily complex and lacks clear commercial rationale.
- Reliance on contractual assurances without a practical mechanism to test their effectiveness (such as GEO blocking and/or GEO testing).

- Unclear ownership, control, group relationships, intellectual property ownership or distribution rights.
- A commercial footprint that appears materially larger or different from the disclosed structure.
- Structures which employ complex payment systems (multiple Payment Service Providers (PSPs), cryptocurrency or combinations of payment methods)

Licensing and Corporate Indicators

- A licence has expired, been suspended, changed scope or cannot be verified.
- The website, licence, contracting entity and corporate registry information do not align.
- A business describes itself as licensed or regulated where the public record does not support that claim.
- Frequent changes of entity, brand, domain or jurisdiction without a clear commercial explanation.
- A non-regulated business cannot explain why its activity does not require licensing.
- Clients of the subject which have no online presence or are in an industry / sector completely unrelated to gaming.

Jurisdictional and Market Exposure

- Exposure to prohibited, sanctioned, higher-risk or restricted jurisdictions.
- Marketing, language, currencies, payment methods, affiliates or search results suggesting activity outside disclosed markets.
- Changes in regulatory, sanctions or geopolitical risk affecting the expected markets.
- Evidence that users are encouraged to circumvent territorial controls, including the use of VPNs, or alternative domains.

Technical and Operational Indicators

- Discrepancies between expected and observed deployment, traffic, geography or brand usage.
- Geo-blocking or other technical controls cannot be demonstrated or appear ineffective when tested.
- Content appears on websites or domains not previously associated with the counterparty.

Behavioural and Change-Based Indicators

- Material changes in ownership, control, management, business model, partners, PSPs or markets.
- Unexplained growth in revenue, volumes or reach that is not supported by observable activity.
- Repeated reluctance to provide a focused explanation or proportionate information.
- Adverse media, regulatory action, litigation, enforcement, sanctions exposure or credible allegations of criminality.
- Pressure to relax restrictions or accept exceptions in commercially attractive but higher-risk markets.

Methods and Tools

The methods and tools listed below are not an exhaustive list. All checks undertaken should be proportionate to the level of risk and a risk-based approach should always be applied when determining the extent of any additional checks.

Baseline Non-Intrusive Assurance

These checks can usually be completed using public information, information already held by the business and limited testing of public-facing controls.

Method	How the check is conducted	Purpose and expected result	Applicable Scenarios <i>Note: Non-Exhaustive Lists</i>
Licence and corporate status verification	Check relevant licensing registers, company registries and public corporate records. Compare the legal entity, trading names, domains, licence scope and status with customer records.	Confirm that the business and any claimed regulatory status remain current and consistent.	Onboarding, periodic review, material change, new brand or domain.
Website and brand compliance assurance	Review customer and associated websites for ownership details, licence disclosures, terms, brands, payment methods, currencies, restricted territory statements, responsible gambling information and other observable indicators.	Identify inconsistencies, undisclosed brands, misleading claims and signs of activity outside the expected model.	Review at a frequency determined by the firm's documented risk assessment and following relevant trigger events or adverse information.
Adverse media and open-source intelligence	Screen the entity, owners, controllers, brands, domains and known partners against reliable media, regulatory, sanctions and industry sources. Review public announcements, affiliate activity and marketing materials.	Corroborate or challenge existing assumptions and identify emerging financial crime or reputational risk.	Ongoing screening, early risk triage and change-triggered review.
Geolocation and territorial availability testing	Use controlled testing from selected restricted or higher-risk territories to determine whether a public-facing website can be accessed and whether content, registration or play appears available. Record the method and limitations.	Test whether territorial restrictions appear to work in practice and identify possible circumvention routes.	Where territorial controls are important, following go-live and periodically thereafter.
Supply chain mapping using	Combine contractual information, known integrations, corporate	Identify areas of reduced transparency, concentration,	Aggregator, reseller, white-label and multi-layered distribution models.

available information	ownership, websites, partner announcements and other public material to map the immediate and observable supply chain.	dependency or onward supply risk.	
Integration-level visibility already held	Use information generated in the ordinary course of onboarding and technical integration, such as approved domains, deployment environments, jurisdictional settings and access controls. Additional access may be available, but it shouldn't be assumed.	Understand where and how software was intended to be made available and establish a baseline for later comparison.	New Business to Business (B2B) integrations and material technical changes.
Contractual control review	Review restrictions on redistribution, jurisdictional use and onward supply together with notification, audit, suspension and termination rights.	Assess whether the contract provides practical levers if concerns arise and whether the rights remain usable.	Relationships with confidentiality constraints, resellers and long-standing arrangements.
Observable activity and commercial footprint monitoring	Compare public-facing traffic, geography, advertising, affiliates, partner announcements, brands, currencies and payment methods with the expected operating model. Use indicators as signals rather than definitive evidence.	Identify unexpected changes, hidden partnerships or market exposure requiring follow-up.	Post-go-live assurance, rapid growth, new markets or unexplained anomalies.
Business and Transaction Consistency Review	Based on all the information provided is the anticipated transactional activity consistent with the stated business model and markets.	Based on knowledge and experience, is this reasonable, or does it present a red flag requiring more enhanced or intrusive measures?	When establishing a new relationship. Post-go-live assurance, rapid growth, new markets, or unexplained anomalies.
Blockchain Analysis	Public blockchain analytics are used to assess wallet exposure to sanctions, mixers, darknet markets, high-risk Virtual Asset Service Providers (VASPs) and unusual transaction patterns.	Assess crypto source of funds using Open-Source Intelligence. Identify higher-risk wallet exposure. Support proportionate escalation without immediately requesting customer documentation.	Crypto deposits, Crypto PSPs, Customers using self-hosted wallets, VASPs counterparties.

Targeted Follow-Up

Where a baseline check identifies a material inconsistency, the first response should normally be a focused enquiry rather than a broad request for enhanced due diligence.

Method	How the check is conducted	Purpose and expected result	Applicable Scenarios <i>Note: Non-Exhaustive Lists</i>
Focused counterparty enquiry	Put the specific issue to the counterparty and request an explanation, correction or limited supporting information. Avoid generic or open-ended demands where the concern can be framed precisely.	Resolve false positives, refresh assumptions and determine whether the risk is genuine.	Where public information is incomplete, inconsistent or potentially outdated.
Targeted record refresh	Request only the records affected by the change, such as an updated structure chart, licence evidence, list of approved domains, market statement, material partners or explanation of revenue growth.	Bring the customer risk assessment and supply-chain map up to date without repeating the full onboarding exercise.	Material change in ownership, business model, markets, brands or counterparties.
Specific contractual attestation	Seek a written confirmation addressing the identified risk, supported by a named responsible person and a clear statement of the relevant control.	Create accountability and a basis for later testing without demanding unrestricted downstream disclosure.	Commercial sensitivity, limited downstream visibility or isolated exceptions.

Enhanced or Intrusive Measures

These measures should be used only where justified by the nature and seriousness of the unresolved risk. They are not a minimum standard for every content supplier or customer.

Method	How the check is conducted	Purpose and expected result	Applicable Scenarios <i>Note: Non-Exhaustive Lists</i>
Independent or third-party assurance	Commission or rely on a suitably scoped independent review of jurisdictional deployment, redistribution or control effectiveness.	Obtain stronger assurance where direct visibility is limited and the risk cannot be resolved through public information or targeted enquiries.	Opaque distribution chains, repeated contradictions or material higher-risk exposure.
Technical or activity information	Request narrowly defined deployment data, activity logs or technical evidence	Test whether stated controls and actual use align.	Persistent monitoring gaps, suspected unauthorised

	relevant to the identified concern, subject to legal, security and contractual constraints.		deployment or material control failure.
Transaction or payment information	Request or review limited transaction, payment, currency or PSP information only where relevant to the firm's role, lawful and necessary to address a specific risk. Financial institutions will apply their own CDD and transaction monitoring duties.	Understand whether financial activity supports the stated business model and markets.	Unexplained commercial growth, unusual payment routes or concerns about underlying sources of funds.
Restriction, suspension or audit rights	Apply contractual restrictions, limited market permissions, suspension or formal audit where the risk remains material and cannot be mitigated by lesser measures.	Prevent continued exposure while the concern is investigated or resolved.	Serious or repeated breach, sanctions concern, suspected unlawful market access or refusal to address a material issue.

1. Integration-Level Visibility

How the check is conducted

Information is gathered during the technical integration of software into platforms or aggregators, including data relating to deployment environments, jurisdictional settings, platform architecture, and access controls. This visibility is typically strongest at onboarding or during material technical changes.

Purpose / expected result

- To understand where and how software is initially made available.
- To identify inherent jurisdictional or structural exposure at an early stage.
- To inform assumptions made during customer or counterparty risk assessment.

Best scenarios to employ this tool

- Onboarding of new B2B partners.
- Use of aggregator or multi-layered distribution models.

2. Upward-Chain Visibility and Supply-Chain Mapping

How the check is conducted

An entity draws on available information to understand its position within the broader supply chain, including upstream ownership of platforms, technical dependencies, and distribution pathways. This may combine integration insight, contractual information, and open-source material.

Purpose / expected result

- To identify areas of reduced transparency or dependency.
- To understand where influence or leverage exists within the chain.

- To support prioritisation of further intelligence-led measures.

Best scenarios to employ this tool

- Complex reseller or network arrangements.
- Contractual limitations on downstream disclosure.

3. External or Third-Party Audits

How the check is conducted

Independent third parties are engaged to review whether software is being made available in permitted jurisdictions and in accordance with contractual and regulatory restrictions.

Purpose / expected result

- To obtain independent assurance where direct visibility is limited.
- To validate the effectiveness of contractual and technical controls.
- To address uncertainty without conducting full re-performance of due diligence.

Best scenarios to employ this tool

- Use of aggregator platforms or opaque distribution chains.
- Higher-risk jurisdictional exposure.
- Situations where reliance on contractual assurances alone provides insufficient comfort.

4. Activity and Usage Monitoring

How the check is conducted

Targeted monitoring is used to confirm that software usage aligns with agreed terms, expected jurisdictions, and intended operating models. This may include a combination of internal usage or transaction indicators where available, and open-source digital intelligence tools to provide high-level insight into audience geography, traffic patterns, or market reach.

Purpose / expected result

- To identify anomalous or unexpected patterns of use.

Best scenarios to employ this tool

- Post-go-live assurance where visibility diminishes over time.
- Following material changes to business models or partnerships.
- Where historic controls have relied heavily on assumptions.

5. Contractual Controls and Contractual Testing

How the check is conducted

Contractual clauses restricting redistribution, jurisdictional use, or onward supply are reviewed alongside mechanisms for testing compliance, such as audit rights, reporting obligations, or termination provisions.

Purpose / expected result

- To assess whether contractual controls are effective in practice.
- To determine whether contractual rights are exercisable if needed.
- To support proportionate escalation rather than default reliance.

Best scenarios to employ this tool

- Relationships with confidentiality or non-disclosure constraints.
- Long-standing arrangements where assumptions may be outdated.
- Situations involving repeated exceptions or breaches.

6. Currency and Payment Controls

How the check is conducted

Technical measures are used to restrict access to software based on geographic location, either contractually, technologically, or both. Controls may be tested to confirm they function as intended.

Purpose / expected result

- To prevent access to restricted jurisdictions through financial channels.
- To align operational controls with jurisdictional risk assessments.
- To provide preventative safeguards alongside other measures.

Best scenarios to employ this tool

- Exposure to jurisdictions subject to regulatory or legal restrictions.
- Markets where payment channels create elevated risk.

7. Geo-Blocking and Technical Restrictions

How the check is conducted

Technical measures are used to restrict access to software based on geographic location, either contractually, technologically, or both. Controls may be tested to confirm they function as intended.

Purpose / expected result

- To prevent access from prohibited or high-risk jurisdictions.

Best scenarios to employ this tool

- Markets with rapidly changing regulatory or geopolitical risk.
- Situations where visibility is otherwise constrained.

8. Open-Source Intelligence (OSINT)

How the check is conducted

Publicly available information is reviewed, including websites, marketing materials, corporate disclosures, media reporting, and industry announcements, to corroborate or challenge existing assumptions.

Purpose / expected result

- To identify inconsistencies between stated and actual activity.
- To provide additional context without traditional data requests.
- To support proportionate escalation decisions.

Best scenarios to employ this tool

- Where contractual disclosure is limited.
- Early-stage risk triage.
- Ongoing relationship reviews triggered by change.

Decision Pathway and Risk Considerations

The decision pathway should be capable of leading to no further action as well as escalation. The objective is to reach a reasoned outcome which should be recorded, not to ensure that every indicator produces enhanced due diligence.

The following considerations are illustrative only and should not be read as prescribing a particular outcome. The appropriate response will depend on the full risk context, the reliability of the information, legal and regulatory obligations, its contractual position, its role in the supply chain, and whether the concern can be corroborated or mitigated.

Stage	Key questions	Action	Possible outcome
1. Establish the baseline	What is the relationship, expected business model, supply chain, market exposure and legal duty? What information and leverage are reasonably available?	Complete required onboarding and document the expected position.	Risk rating and baseline monitoring plan.
2. Complete routine assurance	Do licences, corporate records, websites, brands, territories, media and observable activity align with the expected position?	Record the results of proportionate non-intrusive checks.	No concern and continue routine monitoring, or an indicator is identified.
3. Corroborate the indicator	Is the information reliable, current and material? Is there a reasonable alternative explanation? Are independent sources consistent?	Use additional public information, a repeat test or another baseline method.	False positive or immaterial issue is closed, or a material inconsistency remains.
4. Engage the counterparty	Can the concern be addressed through a focused explanation, correction, attestation or limited record refresh?	Put the issue clearly to the counterparty and set a reasonable response period.	Risk resolved, monitoring increased, or enhanced assurance is considered.
5. Assess proportionality	What is the seriousness and likelihood of the risk? What appropriate measures are available? Is the requested information lawful, relevant and obtainable? Could the identified risk be addressed through additional intelligence rather than requesting further documentation?	Approve a defined enhanced measure or decide that escalation is not proportionate.	Continue with controls, restrict markets, suspend, audit, terminate or report.
6. Record and review	Does the final decision align with the business risk assessment, legal obligations and risk appetite? Has the rationale been documented?	Record evidence, decisions, owners, timescales and review triggers.	Defensible outcome and clear future monitoring plan.

Risks of Taking No Action

- The business may remain exposed to sanctions, financial crime, regulatory, contractual or reputational risk.
- Inaccurate customer risk assessments may remain uncorrected.
- A pattern of minor indicators may develop into a material issue without being recognised.
- The firm may be unable to demonstrate that it responded reasonably to information available to it.

Risks of Disproportionate Action

- Unnecessary duplication of customer due diligence.
- Routine demands for data that the supplier has no legal right, operational need or technical ability to obtain.
- Unwarranted de-risking of legitimate regulated or non-regulated businesses.
- Commercial, confidentiality, competition, privacy and information security concerns.
- Creation of an industry standard that only the largest firms can satisfy, without evidence that it improves outcomes.

Minimum Record of the Decision

- The trigger or question identified.
- The information and checks considered.
- Any explanation or evidence obtained.
- The assessment of seriousness, likelihood and available mitigation.
- The decision, responsible owner, review date and any restrictions or conditions.

Typologies

The scenarios below illustrate how the framework can be applied. They are not intended to prescribe a single outcome. The same indicator may be mitigated or escalated depending on the surrounding facts.

Scenario 1: Contractual Opacity and Onward Supply Risk

Background

A proprietary game owner licences content to a reputable reseller. Confidentiality clauses limit disclosure of downstream operators and the reseller provides only first-tier information.

Red flags and triggers

- Limited downstream visibility.
- Reliance on a general contractual assurance that prohibited markets are excluded.
- Public partner announcements suggest a wider commercial footprint than disclosed.

Proportionate steps

- Map the observable supply chain using websites, announcements and known integrations.
- Review the reseller agreement and the practical suspension, notification and audit rights.
- Use website and geolocation checks on identified brands.

- Put any specific inconsistency to the reseller before requesting enhanced information.

Possible outcome

On the facts described, one possible outcome may be that the reseller's explanation is accepted, the current approved domain list is retained on file, and quarterly non-intrusive monitoring continues. This would depend on the explanation being credible, supported by public checks and consistent with the wider risk context. A different response may be required where independent information contradicts the explanation or where the opacity gives rise to a material unresolved concern.

Scenario 2: Aggregator Platform and Deployment Geography

Background

Games are distributed through an aggregator. Visibility is good at integration but reduces after go-live and the content owner does not routinely receive a full jurisdictional breakdown.

Red flags and triggers

- The aggregator cannot readily provide a current market breakdown.
- Geo-blocking is relied upon as the main territorial control.
- A third-party website suggests the games are available in a restricted market.

Proportionate steps

- Repeat the public-facing test from the relevant location and confirm whether registration or play is possible.
- Check the website entity, licence and domain against known records.
- Ask the aggregator to explain the deployment and provide a targeted confirmation for the identified domain.
- Escalate to technical evidence only if the contradiction remains.

Possible outcome

On the facts described, one possible outcome may be that the matter is recorded without further escalation where testing confirms that access is limited, registration or play is blocked, and the public listing appears outdated. This should not be read as meaning that website accessibility is irrelevant in all cases. Further enquiry or technical evidence may be appropriate where access, registration, deposits or game play appear available, or where the aggregator cannot provide a credible explanation.

Scenario 3: Contractual Controls Without Practical Testing

Background

A reseller agreement contains strong restrictions on redistribution and jurisdictional access, but the supplier has never considered how it would identify or respond to a breach.

Red flags and triggers

- A set-and-forget contracting approach.
- No defined escalation owner or record of exceptions.
- No routine comparison between approved use and public-facing activity.

Proportionate steps

- Introduce periodic licence, website, brand and territorial checks.
- Map contractual promises to the evidence that can reasonably be observed.

- Create a clear escalation process and identify which contractual rights could be used.
- Reserve requests for activity logs or formal audit for a specific unresolved concern.

Possible outcome

On the facts described, one possible outcome may be that the absence of historic testing is treated as a control improvement point rather than evidence of wrongdoing. Baseline assurance may be introduced, with clear review triggers and escalation routes. A more intrusive review may still be appropriate where there is evidence of breach, repeated exceptions, ineffective controls or an unresolved material concern.

Scenario 4: Technical Controls Used as a Substitute for Risk Understanding

Background

An operator states that geo-blocking and currency blocking address its supply-chain risk but cannot explain why particular jurisdictions are restricted or how the controls are reviewed.

Red flags and triggers

- Technical controls are treated as the risk assessment.
- The restricted territory list has not been reviewed after regulatory change.
- Affiliates appear to target users in a blocked market.

Proportionate steps

- Compare the restricted territory list with the current business and jurisdictional risk assessment.
- Conduct light-touch geolocation and public marketing checks.
- Ask for an explanation of the affiliate activity and evidence of corrective action.
- Escalate only if there is evidence that the controls are knowingly being circumvented.

Possible outcome

On the facts described, one possible outcome may be that the operator updates its jurisdictional risk review, takes corrective action in relation to the affiliate activity, and increases monitoring for a defined period. This would depend on the issue being capable of correction and there being no evidence of deliberate circumvention. A different response may be required where the controls are ineffective, knowingly bypassed or not aligned to current legal, regulatory, sanctions or financial crime risk.

Scenario 5: Financial Institution Onboarding a B2B Software Supplier

Background

An Isle of Man bank receives an application from a licensed or non-regulated B2B software supplier. Funds are expected from PSPs or cryptocurrency wallets and payments will be made within the group for software, intellectual property and dividends.

Red flags and triggers

- Large value flows may occur without the bank seeing underlying player transactions.
- The supply chain may include resellers before the content reaches B2C operators.
- Expected payment routes and counterparties are complex.

Proportionate steps

- The bank completes its own established CDD, source of wealth and source of funds assessment.
- The supplier provides its customer profile, markets, contracting model and supply-chain assurance controls.

- The bank uses transaction monitoring for changes in value, volume, geographies, PSPs and counterparties.
- Targeted information is requested where activity departs from the expected profile rather than assuming all underlying customer data must be provided at onboarding.

Outcome

The framework does not determine the bank's risk appetite or replace its legal duties. It can, however, provide a consistent basis for understanding how the supplier identifies downstream risk and may reduce unnecessary de-risking where risks are understood and capable of management.

Scenario 6: Unexplained Increase in Commercial Performance

Background

A B2B software reseller shows sustained growth in revenue and payment volumes without a corresponding increase in disclosed partners or market activity.

Red flags and triggers

- Financial performance is inconsistent with the expected operating model.
- No obvious public evidence of new partners, brands or markets.
- New PSPs or currencies appear in payment activity.

Proportionate steps

- Review public indicators including advertising, affiliates, partner announcements and market activity.
- Refresh the supply-chain map and compare the growth with known integrations.
- Ask for a targeted explanation and supporting data limited to the period and activity in question.
- Escalate to enhanced payment or activity analysis only if the explanation is unsupported.

Possible outcome

On the facts described, one possible outcome may be that the customer risk assessment is updated without further escalation where the increase is explained by a recent acquisition or migration and that explanation is supported by corporate filings, public announcements or other reliable information. Further monitoring or enhanced payment and activity analysis may be appropriate where the explanation is unsupported, inconsistent with observable activity, or suggests undisclosed partners, markets or payment routes.

Scenario 7: Website Screening Identifies a Material Inconsistency

Background

Routine website assurance identifies a customer brand displaying an expired licence reference and appearing accessible from a core restricted territory.

Red flags and triggers

- The public licence statement is no longer current.
- The website is accessible from a restricted location.
- The domain was not included in the latest approved domain list.

Proportionate steps

- Verify the licence directly on the regulator's register.
- Test whether registration, deposits and game access are available rather than relying on homepage accessibility alone.
- Check the entity and domain and contact the customer with the specific findings.

- Require correction and consider restriction or suspension if the customer cannot explain the use of the domain.

Possible outcome

On the facts described, one possible outcome may be that the issue is treated as mitigated and recorded where the customer confirms the domain is dormant, registration and play are unavailable, the inaccurate licence wording is corrected, and a follow-up check is scheduled. This would depend on the explanation being credible and capable of verification. Restriction, suspension or escalation may be appropriate where the domain is active, the licence position cannot be verified, the customer cannot explain the inconsistency, or access from a restricted territory appears to create a material risk.

Conclusion

Intelligence-led diligence can make a business more agile and effective when it is used to direct attention towards material risk rather than to create a checklist. Non-intrusive assurance provides an achievable baseline because it can test whether the expected position remains credible without requiring routine access to sensitive internal information.

The approach is most effective when the business has clearly documented expectations at onboarding, knows which public and internal indicators it can reasonably observe, and has a defined route for targeted escalation. It should support, rather than replace, traditional diligence and legal obligations.

Gaps and Drawbacks

1. Public information may be incomplete, delayed, inaccurate or deliberately obscured.
2. Website accessibility does not necessarily demonstrate that registration, payment or play is available.
3. Traffic, geography and marketing indicators are estimates and should not be treated as conclusive evidence.
4. A supplier may have limited visibility or leverage beyond its immediate counterparty.
5. Commercial confidentiality and data protection may restrict downstream disclosure.
6. Non-intrusive checks will not identify every instance of hidden use or financial crime.

Foreseen Challenges

1. Agreeing which checks form a reasonable minimum standard for different types of business.
2. Avoiding the framework being interpreted as a regulatory requirement or a zero-risk standard.
3. Maintaining consistency across regulated and non-regulated businesses and jurisdictions with different licensing models or standards.
4. Ensuring smaller firms can implement the approach without disproportionate cost or specialist technology.
5. Establishing reliable escalation and information sharing routes where a concern crosses several layers of the supply chain.
6. AI-generated identities, websites and documents may reduce the reliability of traditional open-source intelligence and require additional corroboration.

Reporting

Should you suspect that ML/TF/PF/ Sanctions evasion risk is occurring, using a structure you administer, and your business falls within the Isle of Man regulated sector, then you are reminded of the obligations to make a Suspicious Activity Report (SAR) to the FIU. In addition, any person can disclose information to the FIU to assist the FIU in exercising its functions (under Section 24 of the Financial Intelligence Unit Act, 2016). If you decide to make a report because of the material contained within this product you should adopt the usual mechanism for doing so, and it will help with FIU analysis if you would include the reference **FCP-e-Gaming-001** within the SAR submitted through the Themis portal.

Contact

Should you have any questions, comments or feedback on this document then please contact the IOMFCP at iomfcp@gov.im