2025 financial crime examinations feedback

Issued: June 2026

Contents

Welcome 3

Why are financial crime examinations important? 3

Why is this feedback paper relevant to you? 3

1 Executive summary 4

2 Key findings 4

2.1 Corporate governance 4

2.2 Identification measures 10

2.3 Ongoing monitoring 14

2.4 Enhanced and simplified customer due diligence (CDD) measures and exemptions 18

2.5 Reporting requirements 21

3 What story do the findings tell? 23

4 Is our feedback helpful? 24

Welcome

We are pleased to share this feedback paper, which brings together the key themes from our 2025 financial crime examinations.

Why are financial crime examinations important?

Strong financial crime controls are essential to help protect you, your customers, your employees, and Jersey's reputation as a leading international finance centre. Through risk-based and proportionate examinations, we assess how well your systems and controls prevent, detect, and respond to financial crime. We share insights to support industry-wide learning and help strengthen Jersey's regulatory standing.

> "Thank you to all those who engaged openly and constructively during our 2025 financial crime examinations.
>
> Strong financial crime controls are not just a compliance exercise - they are a core component of effective governance and a key safeguard for Jersey's reputation. This paper is intended to be a practical prompt to help boards, senior management, compliance officers and MLROs focus on what good looks like in practice, and to take timely, risk-based action where gaps are identified."
>
> **Jason Carpenter, Director, Supervision - Examinations**

If you want more detail on the examination process, including how to prepare, please visit our website: Effective examination preparation and engagement — Jersey Financial Services Commission

Why is this feedback paper relevant to you?

We encourage boards and senior management to review our feedback and guidance. This paper highlights the most common and higher-risk findings identified in our 2025 examinations. It explains why these matter and shares examples and prompts to help you strengthen your controls.

You can use this paper to identify and address gaps in your control frameworks and take steps to prevent and detect financial crime. Please consider whether the issues identified are relevant to your business and whether they point to isolated weaknesses or more systemic issues.

We hope you find this paper useful and welcome your feedback.

The Examinations Unit

1 Executive summary

This paper highlights five key areas where we found the most common or higher risk issues.

Deficiencies in each area included:

1. **Corporate governance**: gaps in board oversight, BRAs, financial crime strategies, risk appetite, and independence of MLCO and MLRO roles.
2. **Identification measures**: inadequate identification measures, poor evidence of customer understanding, and weak customer risk assessments.
3. **Ongoing monitoring**: overdue or ineffective reviews and poor documentation of screening decisions
4. **Enhanced due diligence and exemptions**: insufficient source of wealth information and unclear rationale for exemptions
5. **Reporting obligations**: failure to record key dates for suspicious activity reports and gaps in money laundering reporting officer (**MLRO**) decision-making evidence

2 Key findings

2.1 Corporate governance

Board responsibilities

Business risk assessment (BRA)

Entities did not consistently review or update BRAs on a regular basis, leaving them misaligned with changes in business models, operating environments, or regulatory requirements.

Some BRAs did not consider all risks relevant to the business and risks required by the Handbook (such as proliferation financing (**PF**) risk).

Entities did not always document mitigating controls for identified risks or provide sufficient detail to demonstrate whether controls were adequate or effective.

The cumulative impact of identified risks was not consistently considered or clearly documented.

Risk

Failing to maintain complete, up-to-date, and well-documented BRAs may mean that senior management has an incomplete understanding of the entity's inherent and residual risks. This may lead to ineffective risk management and may increase the likelihood of financial crime.

Strategy

Some entities had no formal financial crime strategy in place.

Several entities could not demonstrate the financial crime strategy in place was comprehensive, up-to-date or addressed current risks (such as PF or sanctions risk).

Risk

An absent, outdated, or incomplete financial crime strategy may undermine an entity's ability to identify, manage, and respond to financial crime threats.

Risk appetite

Out of those entities with corporate governance findings, just under half lacked a well-defined and consistently applied risk appetite statement. In some instances, the risk appetite was insufficiently clear, meaning it did not provide practical guidance for decision-making, such as for onboarding and managing higher-risk customers. There were instances where customers were taken on despite their risk profiles falling outside the entity's risk appetite, with no documented evidence that the risk appetite statement had been considered.

Risk

An unclear risk appetite may create inconsistency in risk-based decision-making, increasing the likelihood that the entity will accept customers or activities beyond its capacity to manage, thereby heightening financial crime exposure and undermining effective governance and oversight.

Board oversight

Some entities could not demonstrate adequate board oversight because board or committee minutes and action points were either not recorded or did not contain sufficient detail. In some cases, required board meetings were not held. This resulted in insufficient evidence of consideration and approval of:

- the BRA and risk appetite
- key business risk areas such as screening and suspicious activity report (**SAR**) statistics
- policy and procedure (**P&P**) deficiencies and allocation of adequate resources to remediate identified weaknesses

Risk

Deficiencies in oversight limit the board's ability to, monitor, challenge and oversee financial crime risks effectively, thereby increasing the likelihood of control failures.

Overarching risk

As these areas are interconnected, each one relies on and informs the others to create a coherent and effective financial crime risk management framework. A weakness in one area may undermine the effectiveness of others. For example, an unclear risk appetite statement may undermine the effectiveness of the BRA, which in turn may weaken the financial crime strategy, while poor board oversight prevents proper challenge, approval, and monitoring across all three areas.

Practical examples

The methodology used to conduct the BRA is clearly documented and consistently applied. Relevant stakeholders have the opportunity to input into the BRA and clearly understand its relevance and importance.

Mitigating controls in the BRA are proportionate to the level and nature of the risks assessed. Controls are tested, where appropriate, through the CMP and testing results are fed back into the BRA to ensure the assessment remains accurate and up to date.

Questions to ask yourself

?	Are your governance records appropriately maintained? For example, are meeting minutes recorded and approved? Are registers (such as for exceptions, conflicts of interest, and declined business) completed accurately and kept up to date?
?	Are conflicts of interest reviewed on a sufficiently frequent basis to confirm they are still relevant and that the controls used to manage any risks continue to be effective?
?	Have you notified the JFSC of any relevant breaches in line with the Codes of Practice?

Read our guidance

Section 2.3 of our Handbook sets out guidance relating to risk appetite and the BRA.

Adequate and effective systems and controls

Inadequate and ineffective P&Ps

In several instances, systems and controls lacked supporting P&Ps or guidance.

Some P&Ps were not sufficiently detailed, did not address key risks and did not clearly explain key processes such as:

- how to complete a customer risk assessment (**CRA**), interpret risk factors, or determine when overrides are appropriate
- how to identify complex structures
- how and when to conduct adverse media or sanctions screening, including steps for reviewing, discounting, and escalating hits
- when enhanced customer due diligence (**ECDD**) is required, and what forms are acceptable
- processes for politically exposed persons (**PEP**) declassification
- when exemptions may be used, required evidence, and approval pathways
- how to document decision-making rationale, for example, decisions to discount screening or adverse media matches, override risk ratings, applying exemptions, or submitting SARs

There were also instances where P&Ps:

- replicated Handbook text without any contextual tailoring to the entity's operations, making the P&Ps impractical to apply
- were not regularly reviewed, leading to outdated documents not aligned to regulatory or business changes

- were missing version control, preventing the firm from evidencing review, approval, or amendments

Risk

The absence of clear and current guidance which is appropriately tailored increases the likelihood of control failures and financial crime risk.

Compliance monitoring plan (CMP)

CMP tests were not always sufficiently probing, robust or completed in line with intended scheduling. Some lacked guidance on how testing should be conducted.

In two instances, the results of CMP tests were not documented. These failings made it difficult to demonstrate that CMP testing had been conducted, what was tested, or what conclusions were reached.

Actions arising from testing and remediation were not always recorded systematically or completed in a timely manner.

Reports to the board sometimes lacked adequate detail on the CMP tests performed, limiting the board's ability to evidence consideration of system and control effectiveness.

Risk

Without robust CMP processes, deficiencies may go undetected or unresolved, increasing the likelihood of financial crime risks crystallising.

Overarching risk

Weaknesses identified in both P&Ps and CMPs mean an inability to demonstrate that systems and controls are effectively designed, consistently applied, or subject to appropriate oversight and remediation. As a result, deficiencies may go unaddressed, increasing the risk of prolonged non-compliance and exposure to financial crime risks.

Practical examples

- P&Ps are accessible, clearly written, and structured to enable employees to understand and apply them effectively in practice. Guidance is used to supplement the application of P&Ps by offering additional support, such as worked examples.
- P&Ps are developed to reflect processes and are appropriately tailored to the individuals who perform those activities.
- Any deviations from P&P requirements are recorded in an exceptions register, which is monitored and reported upon.

Questions to ask yourself

?	Are all processes regularly completed by the business formally documented in your P&Ps?
?	Are P&Ps maintained and updated when there are changes to internal or external processes and when there is a change in regulation or legislation?
?	Are CMP test results, including the volume and progress of any outstanding findings or actions, regularly reported to the board to enable it to assess whether systems and controls are adequate and operating effectively? Where such information is reported, is the board's consideration of the results and any resulting actions appropriately recorded in the minutes?

Read our guidance

Read our 2025 feedback on compliance monitoring.

Sections 2.4.1 and 2.4.2 of our Handbook sets out guidance relating to systems and controls.

The money laundering compliance officer (MLCO) and money laundering reporting officer (MLRO)

Conflicts of interest

Conflicts of interest held by the MLRO or MLCO were not always recorded in the conflicts of interest register. As a result, entities were unable to demonstrate that they had assessed the associated risks or implemented appropriate mitigating controls to support the role holder's independence.

In one case, although controls to mitigate the identified conflict were documented in the register, they were not operating in practice.

Risk

Such failures undermine the independence of key roles and increase the risk that financial crime issues may not be identified, escalated, or addressed appropriately.

Resourcing

In one instance, insufficient resourcing for the MLRO and MLCO role was identified.

Risk

Insufficient resourcing increases the risk that the MLRO or MLCO would be unable to fulfil their responsibilities or effectively identify, investigate, and escalate financial crime risks.

Oversight and effectiveness

In some cases, an assessment of the MLRO and MLCO's effectiveness had not been completed or recorded.

Reporting by the MLRO and MLCO to the board was also not always formally documented, limiting the board's ability to demonstrate effective oversight of the role holder's performance.

Risk

Such deficiencies increase the risk that weaknesses in the financial crime framework go unidentified and unaddressed.

Overarching risk

The MLCO and the MLRO functions play critical roles in the effectiveness of an entity's financial crime framework. Ensuring that the MLCO and the MLRO roles are clear and distinct, and that the appropriate personnel identifies, investigates, and reports financial crime risks appropriately, depends on effective management of conflicts of interest, adequate resourcing, documented performance assessments, and strong board-level oversight. Weaknesses in these areas increase the likelihood that financial crime risks are not identified, reported, or mitigated in a timely manner.

Practical examples

Where the deputy MLRO (**DMLRO**) has not had the opportunity to act in that capacity, the MLRO provides the DMLRO with a case study to support their development and assess their handling of SARs.

P&Ps are supported by guidance notes which outline practical points and examples to assist in the MLRO and DMLROs consistency of approach in handling SARs.

Questions to ask yourself

Do your minutes reflect that the board has discussed or questioned the information raised in the MLRO and MLCO reports, rather than simply noting them?

Have you considered whether your MLCO and MLRO (and any deputies) have any potential or actual conflicts of interest that may impact on their ability to operate independently in their role? For example, where the roles are held by the same individual, the individual also holds a customer facing role or where the MLRO reports into the DMLRO?

Read our guidance

Read our 2025 feedback on conflicts of interest.

Our Handbook at sections 2.6 and 2.7 sets out guidance relating to the MLCO and MLRO (and any deputy MLRO).

2.2 Identification measures

Application and timing of ID measures

Inadequate documentation

In some cases, identification measures were either not applied at all or not applied consistently.

On occasion the evidence in support of identification measures was insufficient to properly identify or verify customers. For example, address verification showing only a street name instead of a specific property or passports with unclear photographs.

Risk

Insufficient or unreliable identification increases the risk of onboarding customers who are misrepresenting their identity and undermines an entity's ability to properly assess customer risk and detect suspicious behaviour.

Understanding the customer

Deficiencies were identified in respect of the documentation, understanding (and, where relevant, the corroboration) of:

- ownership and control structures (including the application of the three-tier test, resulting in failings to identify all UBOs)
- business activities
- source of funds (and, where relevant, source of wealth).

Risk

Insufficient understanding of customers, together with incomplete or uncorroborated information on business activities and source of funds/wealth, increases the risk that beneficial owners, illicit funds, or high-risk activities go undetected. This undermines the effectiveness of risk assessments, may lead to onboarding customers outside risk appetite, and heightens exposure to financial crime.

Delays in applying identification measures

In one examination, identification measures were delayed until after the establishment of a business relationship. Services were also provided to customers, including higher-risk customers, before the required identification measures had been fully completed. The entity was unable to demonstrate that the specific requirements for this type of arrangement had been met.

Risk

Delaying identification checks creates the possibility that unauthenticated customers may transact or access services, increasing the risk of unknowingly facilitating financial crime.Such deficiencies increase the risk that weaknesses in the financial crime framework go unidentified and unaddressed.

Overarching risk

These weaknesses significantly increase the risk that customers are onboarded and retained without their identities, backgrounds, and financial activities being properly verified or understood. This undermines the effectiveness of risk-based controls and reduces the ability to prevent, detect, and report financial crime.

Practical examples

There is a clear rationale and record of approval documented where identification documents obtained are not in line with internal P&Ps.

Onboarding packs contain a clear audit trail of documentation, review, and sign-off.

Questions to ask yourself

Are the identification documents you hold appropriate for the customer and their risk? Do your P&Ps offer clear guidance on this to enable your staff to undertake adequate KYC?

Do you maintain a comprehensive customer profile throughout the entire customer lifecycle, which supports the ongoing evaluation of whether identification measures should be refreshed, whether the CRA requires updating, and how frequently periodic reviews should occur?

Customer risk assessment

Methodology

Some CRA methodologies or processes did not include key risk factors, such as TF and PF risk and adverse media.

In some instances, changes to CRA methodology were not always followed by reassessment of existing customers or updates to P&Ps.

Risk scores did not always reflect the actual customer risk. For example, CRAs understated risk by omitting known factors outlined in customer profiles such as PF exposure or high-risk jurisdictions.

In several instances CRAs were not consistently completed for all relevant parties. For example, joint customers were assessed through a single CRA, leaving risk factors for one party unassessed.

Risk assessors did not consistently record sufficient rationale to justify risk scores, making ratings subjective, inconsistent, and difficult to independently review.

Risk

Deficiencies in CRA methodology or incorrectly completed CRAs undermine the accuracy and consistency of customer risk assessments. This increases the likelihood that risk factors are omitted, incorrectly weighted, or applied inconsistently, resulting in unreliable risk ratings. As a result, due diligence and monitoring may not be aligned to the customer's actual risk profile, increasing the risk of financial crime exposure.

Oversight and control

Some relationships that were approved would have been outside the entity's risk appetite had risks been properly assessed.

In some cases, CRA results could be manually overridden without required oversight, approval, or audit tracking.

In one instance, some CRAs were approved by the same individual who completed them.

CRAs were also not always updated at trigger events such as where there was new adverse media, or during periodic reviews. This meant risk ratings were quickly outdated and did not reflect emerging risk indicators.

There were entities which did not conduct a formal assessment of the CRA to determine if it was sufficiently comprehensive and produced effective risk ratings.

In one case it was not evident who assigned or agreed the scoring in the CRA, who reviewed and approved it, and the frequency with which it was reviewed.

Risk

Weaknesses in oversight and control reduce the ability to identify, challenge, and remediate deficiencies in CRA processes and outputs. This increases the risk that inappropriate risk ratings, overrides, or outdated assessments persist without detection, leading to customers being onboarded or retained outside risk appetite and emerging risks not being addressed in a timely manner.

Overarching risk

Where CRAs cannot be relied upon to provide an accurate, current, and consistently governed view of customer risk, risk-based decision-making is compromised across onboarding, due diligence, monitoring, and escalation, materially increasing the entity's exposure to financial crime and regulatory failure.

Practical examples

- Responsibilities for CRA review and approval are clearly documented and understood.
- Staff involved in the CRA process are provided with sufficient training to understand the methodology, the purpose and risks related to CRAs. Training is tailored for those who conduct, review, approve or interpret CRAs.
- Training is provided following any methodology changes, P&Ps are updated and customers are re-assessed.

Questions to ask yourself

- Do CRA results align with risk indicators in the customer profile?
- How often do you assess the effectiveness of your CRA? Does the review consider the risk of any human error, inconsistency or inaccuracy? If so, how is that risk mitigated (i.e. by automations, further reviews, escalation or approvals)?
- If any of your CRA questions require a subjective response, have you provided guidelines on what factors should be considered in that assessment? Should any subjective response be subject to a second or escalated review?
- Are CRAs refreshed at periodic review? If not, is this rationale clearly documented (For example, it is clear that there was no need to refresh the CRA because there were no changes in the customer risk profile)?
- Can CRA outputs be manually overridden? If so, is there sufficient evidence of decision making, oversight, approval and tracking?

Read our guidance

Sections 3 and 4 of our Handbook set out guidance relating to identification measures

2.3 Ongoing monitoring

Periodic reviews

Delays and ineffective reviews

In multiple instances, periodic reviews were significantly overdue, sometimes by many months.

Some periodic reviews failed to identify obvious deficiencies, indicating that the review process itself was not sufficiently robust or effective.

When issues were identified during periodic reviews, the resulting remedial actions often remained outstanding for prolonged periods, leaving known risks unmitigated during this time.

In some cases, periodic reviews were not approved promptly or lacked approval altogether, weakening the effectiveness and oversight of the review process.

Risk

Delays in completing reviews, or ineffective reviews prevent timely identification of changes in customer risk profiles or financial crime indicators, allowing financial crime risks to persist unchecked, increasing exposure to financial crime

Level of ongoing monitoring

The level of ongoing monitoring in some cases was not risk based. For example, high-risk customers were subject to the same level of monitoring as low or medium risk customers, meaning higher-risk relationships were not receiving the enhanced scrutiny required.

Risk

Where ongoing monitoring is not risk-based, the financial crime control framework's ability to identify, assess and respond to elevated risks is weakened, which increase the likelihood that elevated risks in higher-risk customer relationships are not identified or addressed in a timely manner.

Overarching risk

Where material changes in customer circumstances or emerging financial crime risks go unnoticed or remain unmitigated due to delays or insufficiently robust monitoring processes, the risk of financial crime crystallising increases.

Practical examples

- Risk-based periodic review cycles ensure the frequency of reviews are adjusted when new risk indicators emerge, such as adverse media, unusual activity, or changes in customer circumstances.
- Periodic reviews include checks that customer risk ratings remain appropriate based on the most current information, and prompt timely updating of the risk rating where necessary. The rationale for maintaining or adjusting risk ratings is also recorded within the periodic review.
- Senior management receives information on periodic review timeliness, quality assurance results and outstanding actions.

Questions to ask yourself

- How do you track periodic reviews and action points? Do you make use of automatic reminders and escalation procedures if matters become overdue? Do you have assigned action owners and deadlines?
- Do you conduct any form of quality assurance to confirm that reviews are thorough and consistently applied? If so, is training and/or feedback provided following quality assessment results?
- Do you maintain clear P&Ps showing how monitoring activities differ depending on the risk rating of the customer?
- Within your periodic review (or other document such as a customer profile) do you outline the monitoring activity conducted and explain why that activity is appropriate to the risks associated with the customer?

Screening

Incomplete screening

In multiple instances, screening for sanctions, PEPs, or adverse media was either not conducted at all, or not performed on all relevant parties.

In one instance, adverse media screening was not consistently carried out as part of periodic reviews.

Risk

Incomplete screening undermines a financial crime control framework, increasing the likelihood that sanctioned individuals, PEPs, or customers linked to adverse media are not identified and are onboarded or retained without appropriate controls, increasing exposure to financial crime risk.

Inconsistent review of screening hits

In multiple instances screening hits were incorrectly discounted. In one case this led to a delay in identifying PEPs.

The failure to adequately record the rationale for discounting screening hits was a common deficiency.

In one examination, adverse media alerts were not consistently reviewed promptly upon detection and were instead left unresolved until the next periodic review.

Risk

Where screening alerts are not consistently addressed, and the rationale for discounting is not adequately recorded, there is an increased risk that relevant information is not identified, appropriately assessed, or acted upon in a timely manner. This could result in breach of the sanctions legislation and heightened exposure to financial crime.

Screening P&Ps

Screening P&Ps did not always cover key processes such as:

- reporting sanctions matches to the Minister for External Relations
- the steps to take following a positive match
- the requirements for annotating screening alerts reviewed

Risk

A lack of comprehensive P&Ps could lead to inconsistent practices and increase the risk of entities failing to identify links to sanctions or financial crime and take appropriate action.

Oversight of backlogs

Multiple backlogs of unreviewed screening hits were identified.

In one case a system limitation meant the full extent of the backlog could not be determined which hampered the board's ability to demonstrate effective oversight and that timely mitigating action was taken.

Risk

Backlogs of unreviewed screening alerts and inadequate oversight of their scale materially increases the risk that sanctions designations or financial crime indicators remain unidentified or unaddressed.

Testing the effectiveness

In multiple cases, there was no assessment of the effectiveness of screening arrangements.

Risk

Where the effectiveness of screening arrangements is not assessed, an entity cannot be confident that its screening controls are operating as intended to identify financial crime risks. This increases the likelihood that deficiencies in screening remain undetected, reducing the reliability of risk identification and heightening exposure to financial crime risks.

Overarching risk

Where material changes in customer circumstances or emerging financial crime risks go unnoticed or remain unmitigated due to delays or insufficiently robust monitoring processes, the risk of financial crime crystallising increases.

Practical examples

- Where screening practices are incomplete or inconsistent, entities cannot rely on their screening frameworks to promptly and reliably identify, assess, and evidence sanctions, PEP, and adverse media risks. This materially increases the likelihood that high-risk or prohibited relationships are onboarded or retained without appropriate controls, heightening exposure to sanctions breaches and other financial crime risks.
- For all screening conducted, details of key information such as the screening date, the reason for the screening (i.e. onboarding, periodic review, trigger event) and the individual who conducted it are recorded and easily audited.
- Senior management receives information on screening backlogs, false positives, and hit resolutions via reporting to enable oversight.

Questions to ask yourself

- Do you conduct effectiveness testing to assess accuracy, timeliness, and completeness of screening outputs? Have there been known instances where your screening tool has not identified PEP or sanctions matches? Have you considered the effectiveness of the screening system and/or its calibration as a result?
- Are screening alerts reviewed promptly (i.e. not left unresolved until periodic review)?
- Do your customer records include the date screening was conducted and how/why results were assessed (i.e. discounting rationale)?
- Do you conduct enhanced screening on your high-risk customers such as deeper adverse media checks?

Read our guidance

Section 6 of our Handbook sets out guidance relating to ongoing monitoring.

2.4 Enhanced and simplified customer due diligence (CDD) measures and exemptions

Periodic reviews

Risk based approach

In one case, ECDD was not applied on a risk-sensitive basis. Measures were applied uniformly across the customer base, resulting in higher-risk customers not being subject to appropriately ECDD measures.

Risk

Applying ECDD uniformly may weaken the ability to identify and assess financial crime risks and reduce the capacity to apply enhanced measures to higher-risk customers.

Enhanced measures

In multiple instances the level and quality of source of wealth information obtained was inadequate and there was often a failure to take reasonable steps to corroborate source of wealth information.

Risk

Insufficient and uncorroborated source of wealth information increases the risk that illicit wealth is not identified.

PEPs

In one instance there were no P&Ps in place to support the identification of PEPs, (including immediate family members or close associates) or to assist the application of appropriate ECDD measures where PEP status was identified at onboarding or acquired during the business relationship.

Risk

The absence of PEP related policies and procedures increases the likelihood that PEP relationships are not identified or managed appropriately, increasing the risk of exposure to bribery, corruption and other financial crime.

Overarching risk

Failing to apply a risk-based approach to enhanced due diligence, or to apply proper scrutiny to source of wealth, weakens the effectiveness of the entity's financial crime control framework and the ability to identify and mitigate specific risks, heightening exposure to financial crime.

Practical examples

P&Ps clearly set practical examples which distinction between CDD and ECDD measures and explain how each should be applied in line with customer risk.

	Details of source of funds and source of wealth, together with a rationale outlining why any supporting evidence is appropriate, is clearly recorded in the client file, such as in the client profile.
	Corroborating evidence of source of funds (and, where appropriate source of wealth) is sufficiently independent and dated to demonstrate when it was created and obtained. All internal assessments and considerations are clearly documented.

Questions to ask yourself

	Do you clearly explain the rationale for the level of due diligence applied to the customer, and how it is proportionate to the risk they present?
	Have you considered the independence of any source of funds/source of wealth evidence obtained? Have you documented those considerations?
	Where the initial source of funds in a structure is difficult to evidence due to the passage of time (i.e. you have legacy customers), have you carried out appropriate searches and applied sufficient scrutiny to gain comfort that the funds were not the proceeds of crime? Have you documented those considerations?

Exemptions

Appropriateness of application

Evidence demonstrating that it was appropriate to use the exemption was not always recorded.

Exemptions from CDD requirements were sometimes applied to customers who had been assessed as higher risk, with no documented consideration of the criteria in Article 17A of the Order and whether it was appropriate to apply the exemption.

Risk

The incorrect use of exemptions increases the risk that customers who should have been subject to full identification and verification measures are onboarded or retained without adequate scrutiny, increasing exposure to financial crime risk.

P&Ps

In another case, P&Ps did not clearly document when exemptions were appropriate or how they should be assessed and applied, increasing the likelihood of inconsistent or incorrect application of exemptions.

Risk

Where P&Ps do not clearly define when exemptions are appropriate or how they should be assessed and applied, exemptions may be used inconsistently or incorrectly with the risk that customers are onboarded or retained without sufficient safeguards.

Overarching risk

Weaknesses in the governance, documentation, and application of CDD exemptions undermine the effectiveness of the due diligence framework, increasing the risk that identification and verification measures are inappropriately reduced. This compromises the entity's controls and its ability to understand and manage customer risk, increasing its exposure to financial crime.

Practical examples

- Records of evidence in support of the application of an exemption are clearly dated to demonstrate when the evidence was obtained.
- The use of exemptions is reflected in customer profiles and risk assessments.
- Exemptions are subject to ongoing assessment, for example at periodic reviews, to confirm that the application of the exemption remains appropriate.

Questions to ask yourself

- Have you completed a full risk assessment to allow you to assess if there is a higher risk of financial crime, and therefore whether it is appropriate to apply the exemption?
- If you are using exemptions, is it clear which exemption is being used, the reasons why and what evidence you hold in support?

Read our guidance

Read our feedback on the 2024 PEP thematic examination.

Look out for our upcoming feedback on the thematic examination regarding exemptions.

Section 7 of our Handbook sets out guidance relating to ECDD and section 8 sets out guidance relating to exemptions.

2.5 Reporting requirements

Reporting requirements

SAR register and form

Despite being **previously** included in both our 'quick wins for financial crime compliance' publications, in the majority of examinations SAR registers and forms did not consistently record **the date on which the information or matter giving rise to knowledge, suspicion, or reasonable grounds for knowledge or suspicion first came to the employee's attention**. The Handbook requirements specify supervised persons must maintain procedures for iSARs to include this date. Instead, entities frequently record the date of suspicion. Whilst the date of suspicion may often coincide with the date the information or matter first came to the employee's attention, it may not always, and an employee may not form a suspicion until later.

Risk

Where this date is not captured, it prevents entities from monitoring any undue delays between employees first becoming aware of information, forming a suspicion, and submitting an iSAR. This may indicate a need for additional training and/or highlight instances where an iSAR has not been submitted as soon as practicable.

SAR P&Ps

Deficiencies included that P&Ps did not:

- document the importance of submitting an iSAR as soon as practicable
- require the date the information came to an employee's attention to be recorded
- explain how the MLRO or DMLRO should review or determine whether to externalise iSARs
- record how the MLRO should exercise oversight and monitoring of the DMLRO.
- cover reporting requirements for declined business or one-off transactions.

P&Ps were not always maintained or reviewed in line with internal expectations.

Risk

The above deficiencies in SAR P&Ps undermine the effectiveness of the SAR reporting framework, increasing the risk that the entity may fail to meet its legal reporting obligations, for example through missed, delayed, or poor-quality iSAR reporting.

SAR handling and consideration

In one examination, the MLRO's enquiries and decision-making regarding whether to externalise iSARs were not recorded.

Reasons for delays in externalising sanctions reports or SARs were not always clearly documented.

In one case, the MLRO permitted transactions to proceed after an iSAR had been made, without any recorded assessment or rationale for allowing the transactions to proceed, and without obtaining prior consent from the FIU.

There was also an instance where an employee failed to identify red flags that should have given rise to suspicion.

In another case, an employee did not use the required iSAR form to raise a suspicion and instead made a phone call to the MLRO, which was not recorded.

Risk

Failures to properly record enquiries, decisions, and actions taken in response to iSARs can undermine the suspicious activity reporting framework and entities are likely to be unable to demonstrate effective oversight by the MLRO or compliance with legal reporting obligations. This increases the risk that suspicious activity is mishandled, reporting is omitted or delayed, and financial crime goes undetected.

Overarching risk

The deficiencies identified present a material risk of non-compliance with regulatory requirements for the timely identification, escalation, and reporting of suspicious activity. Inadequate policies, record keeping, and documentation of MLRO/DMLRO decision making (including failure to record when suspicion first arises) undermine effective oversight and the ability to assess whether SARs are submitted as soon as practicable in compliance with statutory reporting obligations. This limits the identification of training needs and heightens the risk of the entity being used to facilitate financial crime.

Practical examples

Regular, role-appropriate training ensures employees understand:

- indicators of suspicion
- reporting obligations

the importance of timely escalation and accurate documentation

SAR records are subject to appropriate access controls and confidentiality rules (such as use of reference numbers instead of subject names in communication).

Relevant SAR statistics, trends, and insights are reported to senior management and the board to support oversight of financial crime risks.

Questions to ask yourself	
?	Are the following three key dates clearly, consistently, and distinctly recorded in your iSAR forms and SAR registers to support assessment of internal reporting timeliness, regardless of whether the dates are the same or differ (e.g. due to delays between awareness, suspicion, and submission)? › when the information giving rise to knowledge or suspicion first came to the employee's attention › when the suspicion was formed when the iSAR was submitted
?	Do you report to the board on the timeliness of iSAR filing? (Namely, the length of time it takes an employee to submit an iSAR following the date on which the information or matter giving rise to knowledge, suspicion, or reasonable grounds for knowledge or suspicion first came to their attention?)
?	Are SAR records comprehensive, including MLRO evaluations and enquiries?
?	What controls are in place to prevent transactions following an iSAR or eSAR without prior consent from the FIU?

Read our guidance	
	Read our feedback on the 2025 SAR thematic. Section 9 of our Handbook sets out guidance relating to SARs.

3 What story do the findings tell?

While the core risk themes remain broadly consistent with examinations conducted in previous years, the findings identified increasingly point to challenges in embedding and evidencing effective controls rather than the absence of basic frameworks, reflecting a maturing compliance environment and improved understanding of regulatory expectations. Encouragingly, industry engagement during examinations has improved, and feedback on the revised, more risk-focused examination approach has been positive.

While the main finding areas remain similar to previous years, we continue to see more challenges with putting effective controls into practice and showing how they work, than with basic frameworks. This reflects a maturing compliance environment and improved understanding of regulatory expectations. We are pleased to see greater engagement from industry during examinations, and feedback on our more risk-focused approach has been positive.

We encourage industry to continue building on this progress by strengthening oversight, documentation, and responsiveness to emerging risks, and by taking timely action to address identified deficiencies, to maintain robust financial crime controls and protect the integrity of Jersey as an international finance sector.

4 Is our feedback helpful?

Read our guidance

Want to avoid common pitfalls identified in 2024 and 2025 which should be relatively easy to address? Read our seven quick wins for financial crime compliance and our five more quick wins for financial crime compliance.

Our feedback papers are for you. Did you find this paper helpful? Was there enough detail, or would you like more information about our examinations, themes, findings, or practical examples? Would you find more numbers, graphics, or video content useful? How do you use the information in our feedback papers? Please let us know.

Let us know what you think by completing this five-minute survey by 31 July 2026.

Alternatively, you can email us at FSCFCEU@jerseyfsc.org titled 'Financial crime 2025 Feedback '.