

Financial crime examination feedback 2023 - 2024

This feedback paper sets out the key findings from financial crime examinations conducted from Q4 2023 to the end of 2024.

Glossary

Defined terms are indicated throughout this document as follows:

BRA	Business risk assessment
CDD	Customer due diligence
CMP	Compliance monitoring programme
DMLRO	Deputy Money Laundering Reporting Officer
ECDD	Enhanced customer due diligence
eSAR	External suspicious activity report
FATF	Financial Action Task Force
FCEU	Financial crime examination unit
Handbook	AML/CFT/CPF Handbook
IFC	International finance centre
iSAR	Internal suspicious activity report
MLCO	Money laundering Compliance Officer
MLRO	Money Laundering Reporting Officer
PEP	Politically exposed person
SAR	Suspicious activity report

Contents

1	Executive summary	4
2	Findings.....	7
3	The statistics	17
4	Looking to the future	19

1 Executive summary

1.1 Introduction

- 1.1.1 This feedback paper sets out the key findings from the financial crime examinations conducted from Q4 2023 to the end of 2024. Its purpose is to help supervised persons assess the effectiveness of their own systems and controls in preventing and detecting financial crime and to support compliance with Jersey's legal and regulatory framework.
- 1.1.2 We also cover common or high-risk findings from examinations, along with practical examples of good practice and self-assessment prompts.
- 1.1.3 By reflecting on these findings you can identify any gaps you may have in your own framework and take proactive steps to strengthen your controls to prevent and detect financial crime.
- 1.1.4 This feedback should be read alongside the guidance notes set out in the Handbook.
- 1.1.5 We hope you find this paper useful, and we welcome feedback to help us continue to provide valuable content.

1.2 Background

What is the financial crime examination unit?

- 1.2.1 The financial crime examination unit (**FCEU**) is a dedicated team of examiners who conduct desk-based and onsite examinations of supervised persons' compliance with legal and regulatory obligations, with a specific focus on controls to prevent and detect financial crime.

Why are financial crime examinations important?

- 1.2.2 Robust and effective controls to prevent and detect financial crime are essential to protect supervised persons, their customers, employees and the island as a whole. Individual businesses therefore have a vested interest to ensure that Jersey remains a well-respected international finance centre (**IFC**) which continues to attract vibrant and legitimate business.
- 1.2.3 By analysing supervised persons' controls and compliance with relevant laws and regulations, financial crime examinations enable us to understand, assess and feedback to supervised persons on the significance of risks prevalent in their business. Further analysis undertaken and published by the FCEU in our feedback papers enables us to extend this learning across industry in Jersey.

What does an FCEU examination involve?

- 1.2.4 FCEU examinations have a **three-stage process**.
- 1.2.5 During the **planning stage** a supervised person is informed they have been selected for examination and initial requests for information are made (which may include policies and procedures, registers, a sample of customer files and so on). A preliminary meeting is held during which a supervised person meets the team conducting the examination, who will provide an overview of what to expect.

- 1.2.6 During the **fieldwork stage** examiners undertake a desk-based review of the information received from the supervised person. Examiners also prepare for and attend the supervised person's office for the onsite section of the examination.
- 1.2.7 The **reporting stage** follows the onsite examination and covers the period during which the examination report is drafted, any factual inaccuracies are raised, and the final report is issued to the entity.



Questions to ask yourself

If you are selected for a financial crime examination, have you carefully reviewed the initial information requests and FCEU questionnaire in advance of the preliminary meeting? Any questions on the content of those documents, or what is expected can be discussed during the preliminary meeting.

Have you thought of some questions after the preliminary meeting? Do not hesitate to contact the lead examiner or member of the team at FSCFCEU@jerseyfsc.org for clarification.

Recent changes to our process

- 1.2.8 The Financial Action Task Force (**FATF**) refers to the risk-based approach to preventing money laundering, terrorist financing and proliferation financing as being the cornerstone of its Recommendations. We revised our process in 2023 with an enhanced risk-based approach being central to the changes. We aim to effectively utilise our resources by focusing on those risks that could cause the greatest harm to our guiding principles. These changes to the process were introduced in Q4 2023 and developed in 2024. The key changes introduced are as follows:
- › Previously, financial crime examinations considered an entity's systems and controls against the requirements set out in all relevant sections of the Handbook. Examinations now focus on specific aspects of the regulatory framework. The scope of each examination will differ depending on the known or perceived areas of greatest risk for a supervised person. It will include a selection of the following themes:
 - › business risk assessment (BRA) and governance
 - › systems and controls
 - › the roles of the Money Laundering Compliance Officer (**MLCO**) and Money Laundering Reporting Officer (**MLRO**)
 - › identification measures
 - › reliance and exemptions
 - › ongoing monitoring
 - › sanctions
 - › suspicious activity reports
 - › employee screening
 - › training and awareness
 - › Examiners now send initial questions by email to a supervised person in advance of the onsite section of the examination. This enables us to gain an understanding of a supervised person's business and control framework in advance, allowing for a more focused approach to questions and interviews during the onsite element of the examination.

- › As a result of the more focused scope, the onsite section of the examination generally takes one week, with the end of the onsite examination marked by a meeting (referred to as a “closing” meeting) in the week following the visit.

What happens after the examination?

- 1.2.9 All supervised persons who have been examined receive direct written feedback from the examination team, usually in the form of a report. Once the final report is issued, the supervised person is required to prepare a formal action plan to remediate deficiencies identified and set out timescales for completion. This must be submitted to the supervised person’s supervisor within 20 working days after the FCEU issues the final report.



Read our guidance

When conducting remediation activity, supervised persons are expected to understand and address the root causes of findings and assess whether issues are isolated or systemic.

Read our [guidance on how to approach a remediation action plan](#).

Why should you keep reading?

- 1.2.10 We expect the board and senior management of all supervised persons to:
- › review relevant feedback papers and guidance notes we publish
 - › consider that information against their own arrangements and identify deficiencies or areas for enhancement
 - › take appropriate and prompt action to remedy deficiencies identified

2 Findings

This section provides an overview of the most common findings, and those considered to present the highest risk, identified in the financial crime examinations conducted during Q4-2023 and 2024. Not all examples of good practice highlighted below were identified during the examinations.



Read our guidance

[The Handbook](#) offers a series of suggestions and practical interpretations to assist businesses in complying with regulatory requirements. Keep reading for other practical examples that may assist.

You can also find previous feedback papers on our [examinations findings page](#). Always consider whether guidance remains relevant by reference to current standards and obligations.

2.1 Corporate Governance (section 2 of the Handbook)

Most entities examined had at least one finding relating to corporate governance. The main findings areas were as follows:

2.1.1 Board responsibilities (section 2.3 of the Handbook)

Findings identified

We identified several ineffective risk appetite statements that did not clearly articulate the level of risk businesses were willing to accept. It is essential that a risk appetite statement accurately documents the types and levels of risk to which a business is willing to expose itself. It should not be unrealistic or indicate that the business will not accept any financial crime risk at all or be so ambiguous as to allow the acceptance of any business no matter the associated risks.

In some cases, the business did not cover all financial crime risks to which the business was exposed, for example terrorist financing and proliferation financing risk.

We also identified instances where the BRA had not been kept up to date increasing the risk that the board may be unaware that the level of risk had changed, or a new risk had emerged.

Where risks are not identified in the BRA, businesses may be exposed to those risks crystallising without the benefit of appropriate, tailored mitigating controls.

There were also instances where supervised persons were unable to demonstrate that the board maintained adequate oversight of issues highlighted by, for example, its compliance function or risk committees. Without this oversight there is an increased risk that appropriate or timely action is not taken to address financial crime risks.

Good practice



The BRA defines which member of senior management has responsibility for each risk area.



Senior management has a sound understanding of the main risks identified in the BRA and related mitigating controls.



Board meeting minutes clearly document the discussions, including any scrutiny or challenges raised by board members, and the board's conclusions on these points, along with the rationale behind them.



Clear and effective processes are in place to track action points (such as remedial actions) arising from board or committee meetings.



Questions to ask yourself

Has your risk appetite statement been considered by senior management recently? Is it aspirational? Does it truly reflect the type of customers or business you are willing to accept?

Do you track how often new customer onboarding deviates from your risk appetite? Does senior management regularly review these metrics to assess whether the actual risk being accepted aligns with the agreed risk appetite? Are all the risks your business is exposed to clearly captured in your BRA and addressed via appropriate mitigants and controls?

2.1.2 Systems and controls (including policies and procedures) (section 2.4 of the Handbook)

Findings identified

We identified ineffective compliance monitoring programmes (**CMPs**) which were not tailored, risk-based or informed by the risks outlined in BRAs. This could lead to inadequate testing being performed and the effectiveness of controls not being assessed appropriately, increasing the likelihood of financial crime risks materialising.

There were also several instances where policies and procedures were not assessed, reviewed and updated appropriately or in accordance with review cycles. Where policies and procedures are not maintained there is an increased risk they will no longer be fit for purpose or adhere to current regulatory obligations.

We also identified instances where policies and procedures were deficient, or not consistently applied by employees, increasing the likelihood of avoidable errors arising, which may result in financial crime risks crystallising.

Issues with policies and procedures are often the root cause for other failings. Having comprehensive and easy to use policies and procedures which are applied consistently by staff is therefore essential.

Good practice



Risks identified in the BRA drive the priority and frequency of testing in the CMP. For example, where the business has assessed a risk as high in its BRA, it applies a risk-based approach by testing the associated systems and controls more frequently than others.



Results of testing are reported to senior management and the CMP is reviewed and approved annually.



Results from testing inform amendments to the CMP. For example, the next iteration of the CMP includes testing of the effectiveness and sustainability of remedial actions undertaken.



An index of policies and procedures is maintained, outlining when each policies and procedure was last reviewed, when it is next due to be reviewed, and the individuals with responsibility for reviewing and updating one.



Worked examples of how to use systems and other practical case studies or scenarios are useful for staff to understand how to apply relevant policies and procedures in practice.



Questions to ask yourself

Is your CMP risk-based i.e. informed by the risks identified in the BRA?

Are your CMP tests effective and valuable? Are they checklists or are they more probative? What do you do to test the effectiveness/ value of your CMP tests?

Do the results from your CMP testing inform the control assessments detailed in your BRA?

Do you periodically get feedback from employees on how easy P&Ps are to use and whether they reflect what is undertaken in practice? Is this tested?

Do you have a structured review cycle to help ensure your P&Ps are kept up to date and fit for purpose? Do you monitor updates to the regulatory framework which may necessitate an ad-hoc review?



Read our guidance

Did you know that a [thematic examination on compliance monitoring](#) first took place in 2020 and that another such thematic was conducted in [2024](#)?

2.2 The role of the MLCO and MLRO

Findings identified

In some cases, businesses were unable to demonstrate that the compliance function was adequately resourced. Inadequate resourcing may lead to tasks which are key in preventing financial crime not being conducted, or being completed ineffectively, resulting in a decrease in the efficacy of financial crime controls.

We also identified instances where businesses were unable to demonstrate the independence of the MLCO/MLRO due to, for example, their involvement in customer facing, business development or operational tasks. This was either because there were no mitigating measures in place or those mitigants were not sufficiently robust. Objective decision making is an absolute necessity for the MLCO/MLRO in performing their role.

In addition, we identified instances where oversight and monitoring of the DMLRO's performance by the MLRO could not be evidenced. In these cases, the supervised person was unable to demonstrate how it was comfortable that the DMLRO was handling suspicious activity reports (SARs) in an appropriate and consistent manner, increasing the risk of a failure to report (or adequately report) financial crime.

Good practice



Conflicts or impediments to the independence of key persons are risk-rated and clearly recorded together with associated mitigants. They are reviewed at appropriate frequencies (i.e. annually for high risk) to assess whether the conflict continues and the mitigants remain sufficient.



MLRO's have regular oversight meetings with DMLROs to discuss progress on SAR related matters, discussions with FIU and general workload.



Standing agenda items for the MLCO and MLRO to present key information to the board should be included.



Read our guidance

Want to know more about common findings and good practice relating to the roles of the MLRO and MLCO? Find our [2019 and 2022 feedback papers](#).

2.3 Identification measures (sections 3, 4, 5 and 7 of the Handbook)

Findings which related to identification measures were present in several of the examinations.

2.3.1 Identification measures (sections 3 & 4 of the Handbook)

Findings identified

There were some instances where supervised persons were unable to demonstrate they had taken a risk-based approach to identification measures or where they did take such an approach, that it was adequate or effective.

Deficiencies were also identified in respect of supervised persons' knowledge of their customers, particularly source of funds and source of wealth, most notably with respect to existing or "legacy" customers.

We also identified deficiencies in customer risk assessments. For example, high-risk factors such as connections to sensitive activities or high-risk jurisdictions had insufficient impact on risk scoring resulting in undercalculated risk ratings.

Businesses must know and understand their customers to be able to properly assess risk and apply appropriate due diligence. Different types and levels of customer risk necessitate different forms of customer due diligence (CDD). Failure to apply sufficient mitigants or controls including the right form and level of CDD for a customer (for example, verification of complex ownership structures) may expose a business to the risk of facilitating financial crime.

Good practice



An escalation process or a specific committee to consider and/or monitor high risk customers at onboarding and upon any material change.



A comprehensive, clear and up-to-date customer profile, including details of CDD/enhanced customer due diligence (**ECDD**) held, source of funds and source of wealth, expected activity, the customer risk rating, and noting any recent changes.



Independent verification or corroboration is obtained for source of funds/wealth where appropriate. Handbook guidance outlines examples of what those verifications may consist of and in what circumstances.



A wide range of risk factors considered in a customer risk assessment, and the conclusions reached are clearly articulated.

In addition to the issues identified relating to identification measures more broadly, issues relating to politically exposed persons (**PEPs**) and the use of exemptions were common.

2.3.2 Enhanced and simplified CDD

Findings identified

There were instances where supervised persons failed to identify customers as PEPs and therefore failed to apply appropriate ECDD and enhanced ongoing monitoring to those customers. Where PEPs go unidentified, heightened bribery and corruption risks may be present which have not been considered and mitigated.

There were also instances where supervised persons declassified PEPs without considering whether they continued to present a higher risk of money laundering. Where PEPs are declassified without due consideration, supervised persons may make an incorrect determination and remain exposed to heightened financial crime risks which are not appropriately mitigated.

Good practice



PEP registers are kept up to date and include details such as the date the individual became a PEP and clearly set out why the individual has been assessed as a PEP.



Any ECDD measures applied to PEPs are clearly recorded and reviewed at appropriate frequencies.



Details of any ECDD measures applied, the rationale for applying them and when they next require review, are easily accessible to employees on the customer file.



Declassification of PEPs follows a clear process, and the rationale for declassification is well documented.



Read our guidance

For more information on PEPs, read our [thematic feedback paper from 2024](#).

2.3.3 Exemptions

Findings identified

In some cases, supervised persons were unable to demonstrate that the relevant exemption conditions were met when using an exemption or had not documented the reasons why they could use the exemption in line with Articles 17 and 18 of the Order and section 7.14 of the Handbook.

There were instances where supervised persons had applied exemptions to customers who had been assessed as presenting a higher risk of money laundering. Exemptions are only allowable where customers do not present a higher risk of money laundering.

Good practice



Policies and procedures clearly distinguish between an exception to procedure and an exemption using examples.



A clear rationale and supporting documentation, obtained at the time of applying the exemption, are retained on the customer file.



The eligibility for due diligence exemptions should be reassessed at the time of a periodic review and/or a trigger event.



Questions to ask yourself

Do you have customers to whom any exemptions under Articles 17 or 18 of the Order are applied?

If so, does the customer risk assessment record why no aspect of the customer suggests they might present a higher risk of money laundering? If no such consideration is evidenced, you may be in breach of Article 17A of the Order.

2.4 Ongoing monitoring (section 6 of the Handbook)

More than half of the entities examined had findings in relation to ongoing monitoring. Most of those findings related to periodic reviews or customer screening. Whilst there is a requirement for supervised persons to undertake sanctions screening, most supervised persons will also undertake screening as part of their ongoing monitoring arrangements, for example, to identify any adverse media or PEP connections.

2.4.1 Periodic reviews

Findings identified

There were several instances of backlogs in periodic reviews.

There were also instances where periodic reviews were not being conducted at appropriate intervals in line with the firm's policies and procedures. For example, where periodic reviews for high-risk customers were mandated to be performed every year, they were being performed only every other year.

Where periodic reviews are not completed as planned, or at appropriate intervals, firms may not identify potential areas of risk as soon as practicable. This may result in inappropriate due diligence, and ongoing monitoring measures being applied to customers due to the late identification of changes or issues.

In some cases, periodic reviews did not comprehensively cover all potential risk factors (e.g. did not consider whether there had been changes to jurisdictional risk). This can lead to potential or actual risks associated with individuals or businesses and the nature of their activities going unidentified.

We identified cases where no process was in place to track the resolution of issues raised in periodic reviews, increasing the likelihood that risks are not be mitigated.

Good practice



The frequency of a periodic review is commensurate with the risk assessment of the customer (e.g. the higher the risk rating, the shorter the period between reviews).



There is a process for tracking completion of periodic reviews, including an escalation process for periodic reviews which become overdue. For example, periodic reviews overdue by a defined number of days are escalated to senior management.



Where the periodic review identifies deficiencies in the information maintained on the customer, follow-up actions are tracked and closed in a reasonable time. Escalation processes are in place for actions not closed within set timeframes.



Source of funds and source of wealth records are reviewed and kept up to date on an ongoing basis (not just at onboarding).



Periodic reviews specifically consider whether any changes to the customer necessitate a change to the customer risk rating, and consequently, the level of due diligence or ongoing monitoring applied.



In the event of a backlog of periodic reviews, a prioritisation system is implemented to complete reviews outstanding for higher-risk clients first.



Questions to ask yourself

Is your periodic review process and form/template comprehensive? Does it include consideration of whether the details in a customer profile remain correct, and activity is in line with expectation?

Do you periodically test your trigger event and periodic review processes to assess whether they are operating effectively and whether relevant policies and procedures are being complied with?

Does your board or senior management emphasise the importance of periodic reviews being conducted when they fall due?

2.4.2 Customer screening

Findings identified

There were instances where firms were not screening their customers.

Screening processes (such as the process for discounting adverse media screening hits) were not adequate or effective.

Some screening systems and processes were not periodically tested for effectiveness and consistency.

Where robust and effective screening is not conducted on all customers on a consistent basis, businesses may not be aware of relevant information about a customer. For example, customers could unknowingly be outside of risk appetite or subject to sanctions.

Good practice



Policies and procedures regarding different forms of screening (e.g. adverse media, PEPs, sanctions) are clear, detailed and easy to use. For example, they include specific search terms to be used and guidance on how to narrow search results using open-source search tools such as Google.



Details of who conducted a search, and when, is documented for all screening.



The hits resulting from screening searches are clearly and comprehensively recorded and where hits are discounted, a rationale is documented.



Screening systems are tested for effectiveness, prior to implementation and then on a periodic basis. The results of the tests are reported to senior management. Any deficiencies or limitations identified are understood by senior management, and appropriate action to address those issues is tracked to completion.



Testing is carried out at appropriate intervals to assess that policies and procedures are followed and screening is conducted consistently.



Read our guidance

The Guidance notes in the Handbook may help you in considering whether your ongoing monitoring measures are fit for purpose. Did you know that there is a case study under section 6.2 of the Handbook which illustrates the relationship between the scrutiny of transactions and knowing your customer?

Did you know that there is also screening guidance under section 6.3 of the Handbook? Further detail on good practice relating to ongoing monitoring can be found in our [2021](#) and [2022 feedback papers](#).

2.5 Reporting money laundering and terrorist financing activity (section 8 of the Handbook)

A large proportion of findings related to section 8 of the Handbook, and over three-quarters of entities examined had at least one finding in this area. Common findings related to a lack of comprehensive SAR records (including iSAR forms and registers) and the timely submission of internal suspicious activity reports (**iSARs**) and external suspicious activity reports (**eSARs**).

2.5.1 SAR records

Findings identified

Policies and procedures, as well as related templates, forms or registers, did not detail the requirement to record the name of the individual making the eSAR on the SAR register, or in what capacity that individual was making the report (i.e. as MLRO or DMLRO).

One of the most common deficiencies identified was that iSAR forms did not require employees to record the date the information or matter giving rise to knowledge or suspicion came to their attention, but only the date of the suspicion or date of submission of the iSAR. These three events may occur on different dates. Not only is recording the date the information or matter giving rise to knowledge or suspicion came to the employee's attention a requirement, but capturing this information enables entities to assess whether internal SAR reporting is timely.

Good practice



iSARs are comprehensive, clearly outlining the full details regarding the basis of the suspicion and why the individual is suspicious.



Investigations into iSARs by MLROs and DMLROs are comprehensive and include a documented timeline explaining any delay and set out a clear conclusion.



Appropriate alerts, warnings or restrictions are placed on a customer profile in the event of an iSAR.



A record is maintained of relevant customer activity following an eSAR, which may assist in the prompt provision of information if required.



Comprehensive guidance is provided by MLROs/DMLROs to employees on how to interact with customers following a SAR.

3 The statistics

3.1 Exams conducted in 2023/ 2024

27 
exams conducted

4.5 findings identified per
examination on average

2 exams
had no findings

113 findings
across 25 exams

Number of supervised persons
examined per sector

Banking

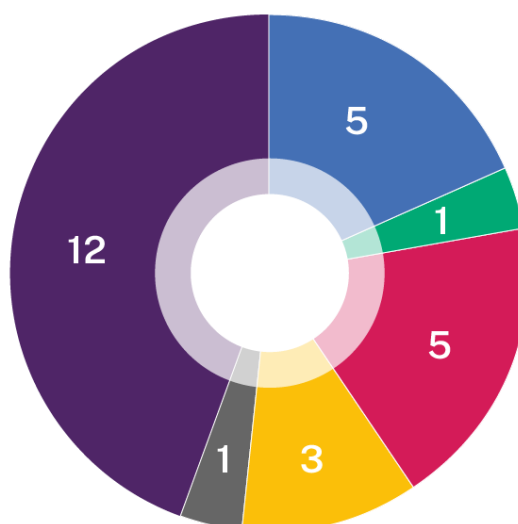
Accountant

Investment business

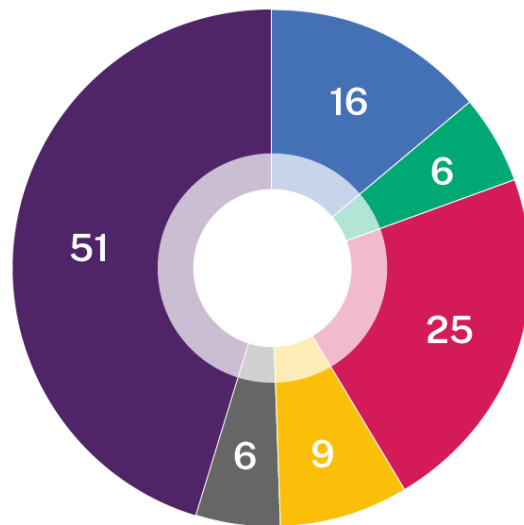
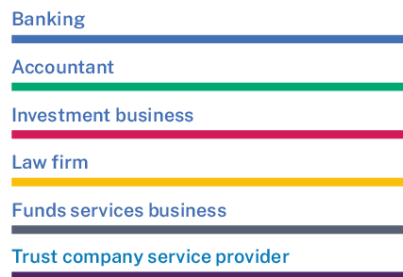
Law firm

Funds services business

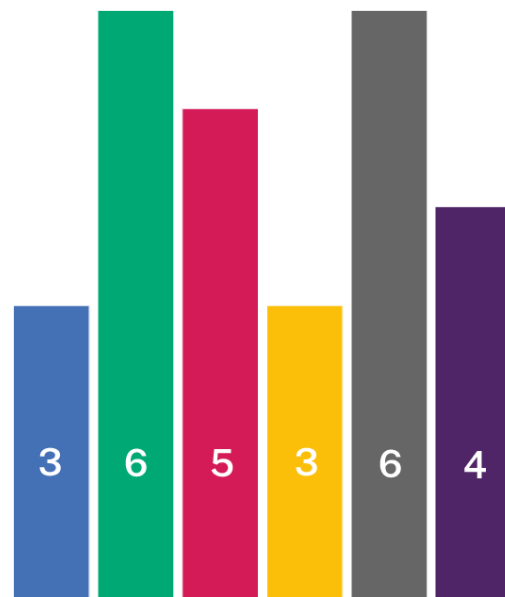
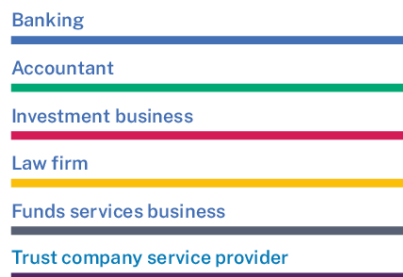
Trust company service provider



Number of findings identified in each sector



Average number of findings identified per examination by sector



Read our guidance

Read our [past feedback papers](#).

4 Looking to the future

Supervised persons are required to remain vigilant and adapt to the ever-evolving ways in which their businesses may be vulnerable to financial crime. Equally, we aim to continually improve our processes for assessing that vulnerability.



Read our guidance

Want to avoid common pitfalls identified in 2024 which should be relatively easy to address? Read our [Seven quick wins for financial crime compliance](#).

4.1 What's next for the FCEU?

- 4.1.1 In addition to the changes to the examination process outlined in section 1, the following enhancements to our processes are planned for 2025.
- 4.1.2 **Report format:** a new look report is being trialled. The intention is to clearly draw out the risks associated with findings identified, remove duplication and make the report more digestible. We will also be introducing a new risk rating system for findings. It is hoped that this will provide greater transparency and assist supervised persons in, among other things, prioritising action points within remediation plans.
- 4.1.3 **The draft report and factual accuracy process:** we have identified that supervised persons may benefit from some clearer guidance on what to do once they receive an examination report. This, together with some changes to the format of the factual accuracy process, is under consideration.
- 4.1.4 **Feedback:** we always seek feedback from supervised persons following examinations. This has historically been requested via a simple questionnaire in a Word document at the time of issuing a final report. We will be enhancing this process so that we can more easily track feedback and suggestions for improvements following an examination. Supervised persons are encouraged to make use of the opportunity to give us your views and be a part of positive change. Feedback is welcome and will assist us in our continued aim to be a high-performing regulator.
- 4.1.5 **Desk-based examinations:** where appropriate to do so, we may make more use of desk-based examinations to help us in taking a risk-based approach to our assessments without the need for an onsite visit. Any further developments will be communicated in due course.
- 4.1.6 Compliance with relevant laws and regulations is not a tick-box exercise. Whilst having appropriate systems and controls is an essential foundation, supervised persons must assess whether those systems and controls are effective. Effectiveness will continue to be an area of focus for examinations.



Read our guidance

Want to know more about what is happening in Examinations or Supervision? Watch our [Supervision monthly updates](#).

Look out for further updates from FCEU (and the examinations teams more generally) in due course.

4.2 Was this feedback paper helpful?

- 4.2.1 Our feedback papers are for you. Did you find this feedback paper informative? Was it sufficiently detailed, or would you like to know more about the examinations conducted, the themes, findings, or good practice? Do you want more numbers or graphics? Would you prefer video content? What do you do with the information in our feedback papers?
- 4.2.2 Let us know what you want to see and give us your feedback by completing this [five-minute survey](#) by the 1st August 2025. Alternatively, you can email us at FSCFCEU@jerseyfsc.org.