Jersey Financial Services Commission

Feedback from 2021 financial crime examinations

Issued: June 2022

Contents

1 Introduction

Jersey's reputation as a sound, well-regulated jurisdiction remains a critical element in continuing to enable the financial services industry to attract legitimate customers with funds and assets that are clean and untainted by criminality.

The key to the prevention and detection of money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction (**proliferation financing**) (together **financial crime**) lies in the implementation of, and strict adherence to, effective systems and controls (including policies and procedures) based on international standards. These standards are implemented in Jersey through legislation and the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism (the **Handbook**).

Given the critical importance of implementing and complying with effective systems and controls (including policies and procedures) designed to prevent, detect and report financial crime, we regularly undertake examinations of supervised persons to assess the extent to which statutory and regulatory requirements are being complied with.

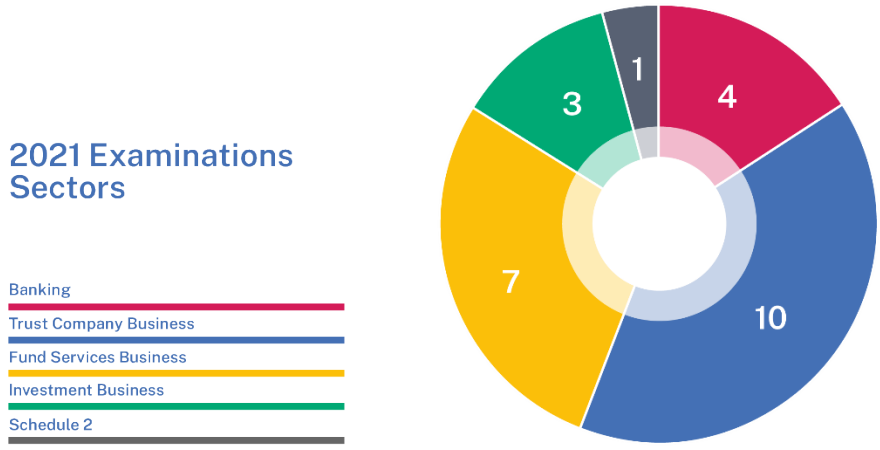
This feedback paper summarises findings and key themes arising from financial crime examinations carried out by us in 2021. Financial crime examination activity in 2021 involved a total of **289** employees of supervised persons taking part in **582** meetings with our officers, who reviewed records relating to **325** customers and their activities.

A number of key themes and detailed findings in this feedback paper are similar in nature to those contained within previous feedback papers issued by us. We expect the board and senior management of all supervised persons to:

- monitor for feedback papers and similar guidance notes published by us from time to time; and
- consider their own arrangements against the matters set out in feedback papers; and
- take prompt action where appropriate to remedy any deficiencies identified.

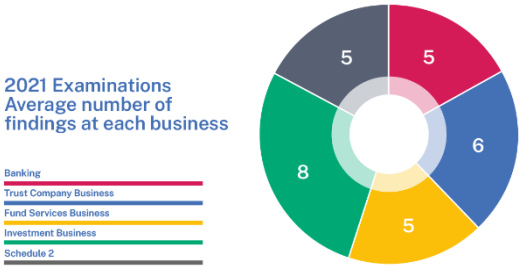
2 Overview of 2021 financial crime examinations

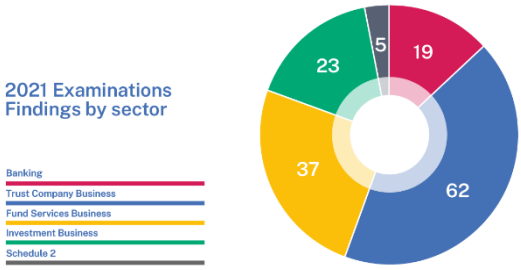
A sample of **25** businesses, comprising **24** carrying on regulated financial services business (**96** individual supervised persons) and **one** carrying on a business described in Part B of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999 (referred to in this paper as a **schedule 2 business**) were selected to be examined in 2021. The industry sectors represented in our selection were as follows:



Our review of these **25** businesses resulted in our officers highlighting **146** findings. At **two** businesses, there were **no findings** arising from the financial crime examinations.

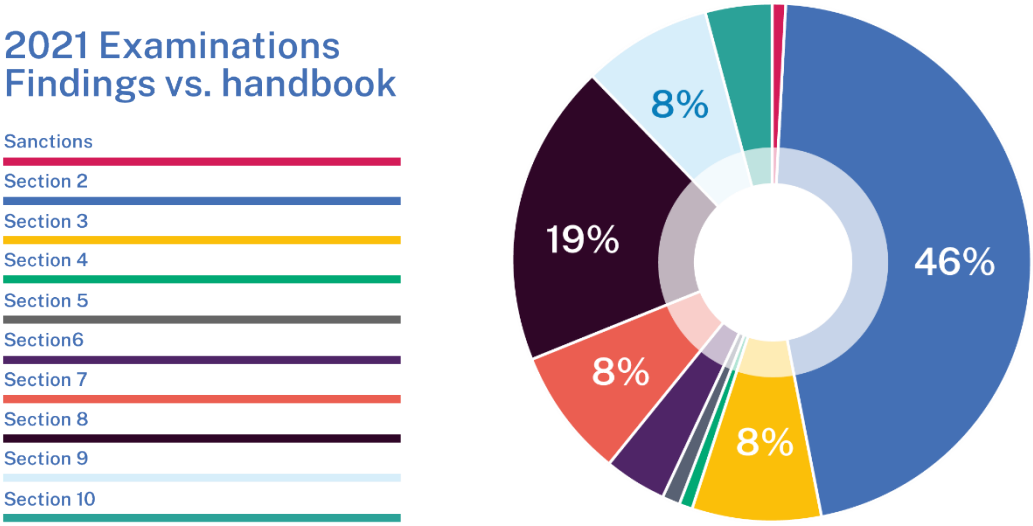
As can be seen from the information below, findings were not concentrated in any particular industry sector:





Analysis of the 146 findings arising from the 25 2021 financial crime examinations highlights that findings most commonly arose as a result of non-compliance or partial non-compliance with the sections of the Handbook that set out statutory and regulatory requirements concerning:

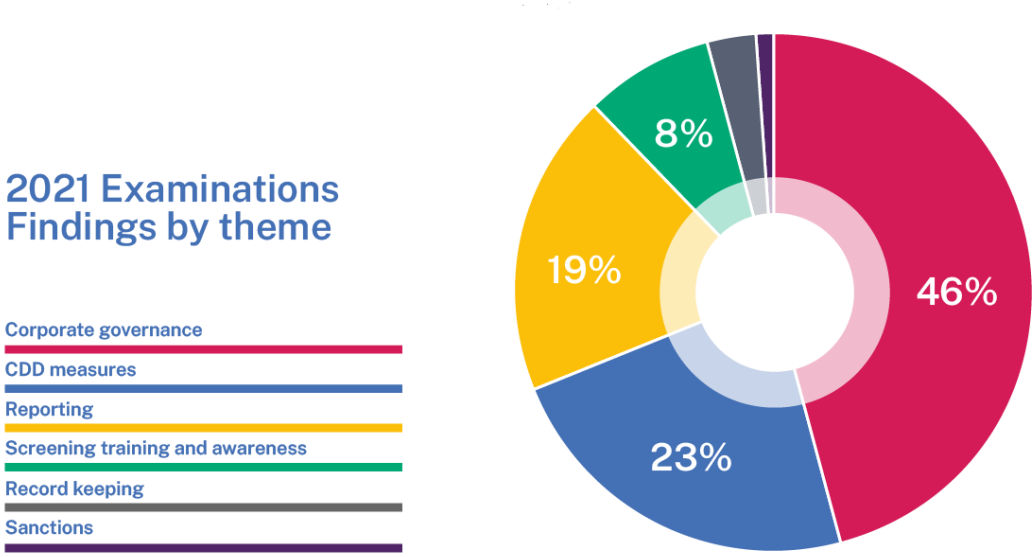
- corporate governance - **Section 2**
- identification measures - **Sections 3 and 4**
- enhanced and simplified customer due diligence (enhanced CDD and simplified CDD) and exemptions - **Section 7**
- reporting suspicions of money laundering or the financing or terrorism - **Section 8**
- screening, awareness and training of employees – **Section 9:**



The findings of the 2021 examination activity can also be categorised into 4 main themes:

- corporate governance (Section 2 of the Handbook)
- CDD measures (Sections 3, 4, 5, 6 and 7 of the Handbook)
- reporting suspicions of financial crime (Section 8 of the Handbook)
- screening, awareness and training of employees (Section 9 of the Handbook)

96% of our 146 financial crime examination findings in 2021 fall in these 4 broad themes:



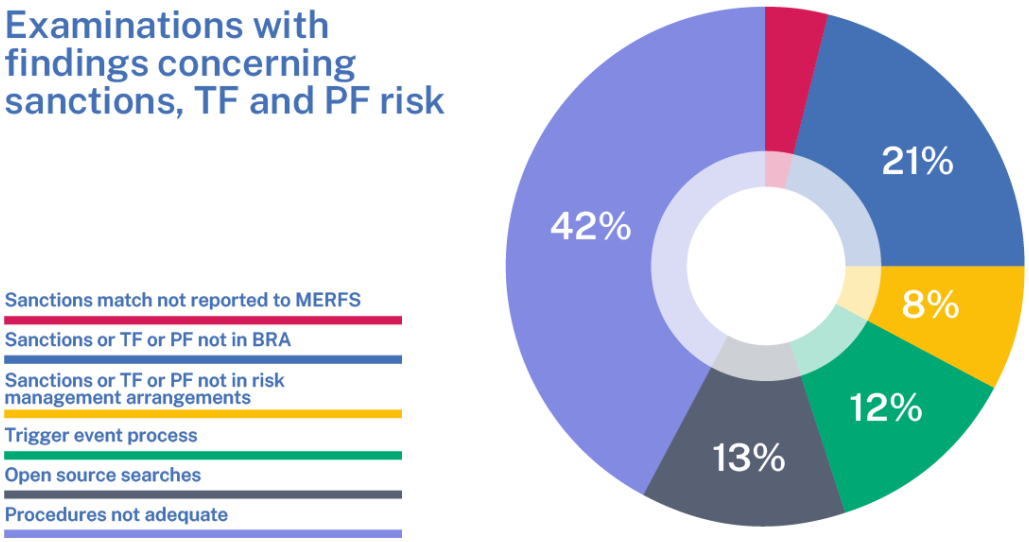
3 Targeted financial sanctions including terrorist financing (TF) risk and proliferation financing (PF) risk

The results of the 2021 examinations set out above include one case where a business had correctly identified a sanctions match and had frozen assets held at an overseas branch of the Jersey

incorporated business. However, the supervised person in Jersey had not met its obligations under the Sanctions and Asset-Freezing (Jersey) Law 2019 and the Sanctions and Asset Freezing (Implementation of External Sanctions) (Jersey) Order 2021 (the **terrorist sanctions measures**) to make a report to the Minister for External Relations and Financial Services (**MERFS**).

Despite the isolated nature of this finding, it nonetheless represented a serious breach of Jersey's legal framework regarding sanctions, TF and PF.

In addition to making reports required by terrorist sanctions measures where matches are identified, examination findings indicate that systems and controls (including policies and procedures) at the selection of 25 businesses visited in 2021 may have benefited in some cases from enhancement to ensure that targeted financial sanctions, including TF and PF risks were managed more effectively:



As can be seen from the chart above, at nearly half of the 25 businesses examined, policies and procedures did not contain adequate guidance for employees concerning action to be taken when screening processes or tools identified a potential sanctions match. This included how to make a report to MERFS, if a match was subsequently confirmed.

Over a quarter of the 25 businesses did not include at least one of sanctions or TF or PF risks in their business risk assessment or risk management arrangements.

Examination activity also highlighted 'trigger event' processes that were ineffective, or inspection of customer records identified a review of customer activity had been commenced by the supervised person but was not completed.

CDD processes established by businesses commonly include the use of open source internet searches. Customer records examined by us as part of the 2021 financial crime examinations did not always include records that indicated the date on which the search was executed, the criteria used or the reasons why potential matches against adverse information had been discounted by employees.

We strongly encourage the boards and senior management of supervised persons to examine their own systems and controls associated with targeted financial sanctions, TF and PF risk to identify and remedy any similar deficiencies.

4 Findings and conclusions

The distribution of findings arising from the 25 financial crime examinations undertaken by us in 2021 was similar to that seen in the 15 examinations of regulated financial services businesses carried out

the previous year. In 2020, 40% of the 120 findings related to corporate governance, 30% concerned CDD measures, 15% related to reporting suspicions of financial crime and 10% were connected to the screening, awareness and training of employees.

As in 2020, our officers identified findings at certain businesses in 2021 that were similar to those highlighted during previous examinations of those businesses, indicating that senior management action to address those historic findings had not been fully completed or was ineffective in addressing the root cause of the matter in question.

Additionally, a number of the key themes and detailed findings in this feedback paper are similar in nature to those brought to the attention of boards and senior management in previous feedback papers issued by us. These are published on our website:

https://www.jerseyfsc.org/industry/examinations/examination-findings-and-questionnaires/

In the event that we identify findings during examinations that indicate prior remediation has been ineffective or known deficiencies exist but have not been addressed by the board and senior management, supervised persons can expect our regulatory strategy to be positioned accordingly.

Of particular concern to us is that non-compliance or partial non-compliance with statutory or regulatory requirements regarding the reporting of suspicions of financial crime has continued to feature prominently in examination findings for a second consecutive year. The **25** examinations completed in 2021 resulted in **28** separate findings being raised.

There were also **24** findings raised relating to governance arrangements concerning Key Persons and their deputies, such as ensuring that sufficient resources are in place and that independence from customer facing and business development roles can be evidenced. In seven examinations, findings highlighted that deputy Money Laundering Reporting Officers were not aware of all statutory or regulatory requirements that were relevant to their role.

As was the case in 2020, examination activity in 2021 found that employee awareness of key legislation and their personal obligations to report suspicions of financial crime was generally of a high level. However, the awareness of financial crime risks inherent in a supervised person's business and risk profile and how those risks may manifest themselves in day-to-day activities was less well embedded.

Given the findings of 2020 and 2021 financial crime examinations, as part of ongoing supervisory engagements, we will continue to:

- assess employee awareness of financial crime risks
- focus on the adequacy and effectiveness of systems and controls (including policies and procedures) to report suspicions of financial crime

As demonstrated by the detailed analysis of the findings arising from the 2021 examinations set out in Part 7 of this feedback paper, a number of the businesses examined need to make comprehensive changes to internal systems and controls (including policies and procedures), to fully comply with the regulatory framework.

Where serious findings were brought to the attention of supervised persons, this will have resulted in escalation. In some cases, further regulatory action has been taken or may still be underway.

All businesses examined have received direct feedback and were required to submit a formal remediation plan setting out actions to be taken to address any findings including timescales for completion.

5 Remediation of deficiencies highlighted by examinations

When conducting remediation activity, we expect that matters set out in findings are not reviewed in isolation. Consideration should be given to the wider implications of the findings detailed in individual examination reports. In addition, understanding and addressing the root cause of findings will generally result in better outcomes and a more robust control framework.

A key component of regulatory effectiveness is to ensure that where a supervised person has completed remediation activity, they have done so in a way that is sustainable and addresses any deficiencies identified. Therefore, we undertake a programme of remediation effectiveness testing on a risk-based approach, following confirmation from supervised persons that action plans have been completed.

Examination findings form part of a supervised person's regulatory track-record and the manner in which a supervised person addresses the findings and engages with us are key to informing our supervisory strategy. Where appropriate, we may consider the implementation of heightened risk supervisory engagement strategies, the use of statutory powers and the imposition of regulatory sanctions.

6 Next steps

We expect boards and senior management of supervised persons to consider the findings highlighted in this paper and their own arrangements to ensure their business is complying with all relevant statutory and regulatory requirements.

Where supervised persons identify any deficiencies in systems and controls, we expect them to:

- prepare a remediation plan and discuss this with their supervisor
- consider the notification requirements under the AML/CFT Codes of Practice within Section 2.3 of the Handbook and Principle 6 of the relevant Codes of Practice
- remedy any identified matters in the manner set out in the documented remediation plan agreed with their supervisor
- consider what assurance activities may provide comfort to the board/senior management that deficiencies identified have been addressed effectively

In future engagements with us, supervised persons may be asked to evidence steps taken to address identified deficiencies in the control environment.

Where this action is not considered to be adequate or where we identify deficiencies of a similar nature to those highlighted in our feedback papers, we will consider future supervisory strategy and where appropriate, regulatory action.

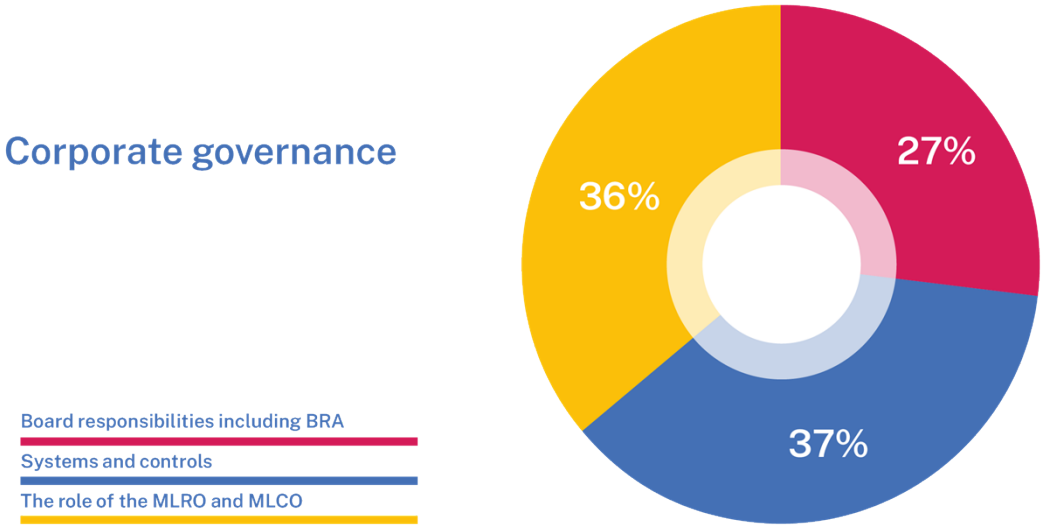
7 Detailed analysis of key themes identified by examination findings

On completion of financial crime examination activity, we set out our findings in detailed reports that are arranged according to the relevant sections of the Handbook. Each finding will detail the circumstance or oftentimes, multiple circumstances, instances or examples that led to our assessment that the supervised person was unable to demonstrate that it was fully complying with all statutory and regulatory requirements included in the financial crime examination scope.

This section also includes feedback on best practices observed during the examinations and other feedback, which supervised persons may find of assistance in assessing the effectiveness of their own control environment.

7.1 Corporate Governance

The **67** findings relating to corporate governance fell into three main categories, as follows:



Board responsibilities

In documenting its Business Risk Assessment (**BRA**) the board of a supervised person must ensure that relevant financial crime risks are assessed 'in the round' and that the conclusions of the BRA drive an appropriate and consistent risk-based approach to managing its financial crime risks.

In nearly half of the 25 examinations, businesses were unable to evidence that an adequate assessment of those risks and the organisation's control environment had taken place. In these 11 examinations, the effectiveness of the supervised person's risk assessment was adversely impacted by one or more of the following:

- lack of relevant supporting data
- absence of proportionate criteria to consistently determine the likelihood, impact and levels of inherent and residual risk
- all customer segments or business locations were not included
- the risks of TF or PF were not considered by the supervised person's BRA
- targeted financial sanctions had not been considered as a risk factor
- external factors impacting customer business and risk profiles had not been considered. For example, the Cayman Islands being added to the FATF 'Grey List'
- an ineffective assessment of the adequacy of the supervised person's control environment to determine if levels of residual financial crime risk were within the supervised person's risk appetite
- the supervised person's risk appetite was not aligned with data set out in the BRA. For example, data in one BRA indicated a significant proportion of the customer base was rated 'high-risk' but the risk appetite statement indicated the supervised person's tolerance for high-risk customers in its book of business was much lower

There were four examples identified where senior employees of a supervised person were not familiar with the business' risk appetite statement or were unaware of how it was used by the firm to manage key financial crime risks set out in the BRA.

There were three examples where directors of supervised persons were unable to demonstrate their involvement in the risk assessment process or were not able to articulate the key financial crime risks set out in the BRA.

At 14 out of the 25 of the businesses examined, boards or senior management were not routinely provided with adequate management information to enable the supervised person to demonstrate that its board or senior management was informed of and was acting upon any indicators of changing financial crime risks in its business and risk profile.

Examples of best practice and other resources to help firms improve compliance in this area

Review your business risk assessment to ensure it captures all relevant risks and that the assessment includes a consideration of the effectiveness of the control environment at managing the risks identified. Control environment effectiveness may be evidenced by the findings of assurance activities, such as periodic testing and other supporting data. Action plans to enhance key controls or to address the emergence of new or external risk factors should form part of the BRA.

Ensure that the conclusions of your business risk assessment and risk appetite statement are aligned and are being used to manage risk on a day-to-day basis.

Some businesses had difficulty in demonstrating that the board received reports from the MLCO on compliance matters and the MLRO on suspicious activity reporting, due to:

- the nature of consolidated compliance function reports presented at board meetings
- the MLCO or MLRO not attending board meetings to present reports
- reporting of financial crime matters being made via a regional financial crime risk report, which did not readily identify content relating to the supervised person

Examination activity also highlighted:

- eight examples where risk management arrangements were not operating as intended;
- six instances where the board had not carried out an assessment of its effectiveness or had not completed an assessment in line with the frequencies set out in its stated policy;
- nine instances where corporate governance records did not adequately reflect:
    - matters being considered and decisions taken
    - escalation of matters within the governance structure as required by terms of reference
    - actions being taken to manage risk
- at nine businesses, systems and controls in place to record and manage conflicts of interest:
    - were not in place
    - records were incomplete
    - did not record how an identified conflict of interest was being managed by the supervised person

We highlighted unidentified potential conflicts of interest to supervised persons during six examinations.

Examples of best practice and other resources to help firms improve compliance in this area

Records of board and senior management meetings should reflect matters discussed, reports or documents considered, scrutiny and challenge of key items, decisions taken and actions arising. Records should also reflect action plans in place to remedy any deficiencies and also evidence that such plans were tracked to completion. Minutes should be taken at all meetings that involve the management of risk.

Review risk management arrangements such as risk management committees, business acceptance committees and other forums with delegated powers to manage risk, to ensure that they are operating as intended and are effective. This should include consideration as to whether escalation of matters is taking place as required by terms of reference and whether there is adequate reporting to the board on matters escalated and on the wider activities of the committees to which it has delegated powers.

Ensure that all employees are aware of your arrangements for the management of potential conflicts of interest and arrange for the conflict of interest register to be regularly updated and reviewed by the board or senior management.

Systems and controls

Supervised persons are required by the Order and the AML/CFT Codes of Practice to establish and maintain appropriate and consistent systems and controls (including policies and procedures) to prevent, detect and report financial crime.

Financial crime examinations in 2021 identified 25 findings relating to non-compliance or partial non-compliance with the statutory and regulatory requirements relating to systems and controls (including policies and procedures) set out in Sections 2.3 and 2.4 of the Handbook.

Many of those findings were similar in nature to those highlighted in previous examination feedback papers we have published.

Circumstances that were identified by our officers included policies and procedures that:

- had not been established
- did not capture updates to the regulatory framework or had not been reviewed in line with the supervised person's stated policy to do so
- did not consider all relevant Jersey regulatory requirements
- were not being complied with

Examples of best practice and other resources to help firms improve compliance in this area

The Order and the Handbook set out systems and controls (including policies and procedures) that must be established by all supervised persons. As a minimum, ensure that the listed policies and procedures are in place and appropriate, taking into account your business and risk profile.

Make sure policies and procedures are regularly reviewed to ensure they facilitate compliance with the latest regulatory developments. Where you utilise policies and procedures developed by your wider group, check that they enable you to meet all local statutory and regulatory requirements.

Supervised persons are also required to check that systems and controls (including policies and procedures) are operating effectively and test that they are being complied with. Boards and senior management must take prompt action to address any deficiencies.

Our officers observed that in 11 examinations the business' compliance monitoring arrangements were not operating as intended and in five of those examples the board of the supervised person had not fully considered those arrangements.

In seven instances, the supervised person could not evidence that its compliance monitoring activity was aligned to a compliance risk assessment of applicable statutory and regulatory requirements.

In 11 examinations, reporting generated as a result of monitoring and testing activity was ineffective, which meant the supervised persons concerned were not always able to evidence that their board or senior management understood one or more of the following:

- the nature and status of monitoring arrangements
- deficiencies or risks that were identified by monitoring activity

- any impact on the supervised person's business and risk profile
- the effectiveness of action taken to remedy deficiencies or manage risk

Examples of best practice and other resources to help firms improve compliance in this area

Feedback was also provided by us on 17 December 2020 following our thematic examination 'compliance monitoring plans'.

The Money Laundering Compliance Officer (MLCO) and Money Laundering Reporting Officer (MLRO)

Financial crime examinations undertaken in 2021 identified 24 findings regarding non-compliance or partial non-compliance with the statutory and regulatory requirements relating to Key Persons that are set out in Sections 2.5 and 2.6 of the Handbook. Again, many of those findings were similar in nature to those highlighted in previous feedback papers we have published.

Circumstances that contributed to examination findings included:

- five examples where the supervised person could not evidence that the compliance function had been provided with sufficient resources to undertake all of its duties;
- independence of the function or the Key Person(s) could not be demonstrated at five supervised persons; and
- eight instances where the MLRO was not routinely monitoring the activities of the deputy MLRO (**DMLRO**)

Of particular concern to us is the fact that during seven examinations, DMLRO's were not aware of all of the responsibilities of the role or were not fully aware of relevant statutory and regulatory requirements. In six instances, we identified individuals acting as a DMLRO who had not been formally appointed by the supervised person to deputise for its MLRO, or where the responsibilities of the role had not been acknowledged by the employee.

Further information is provided at Section 7.3 below regarding the function of the MLRO and DMLRO in the evaluation of internal suspicious activity reports (**iSAR**s) and the submission of external SARs (**eSAR**s) to the Joint Financial Crimes Unit (**JFCU**)

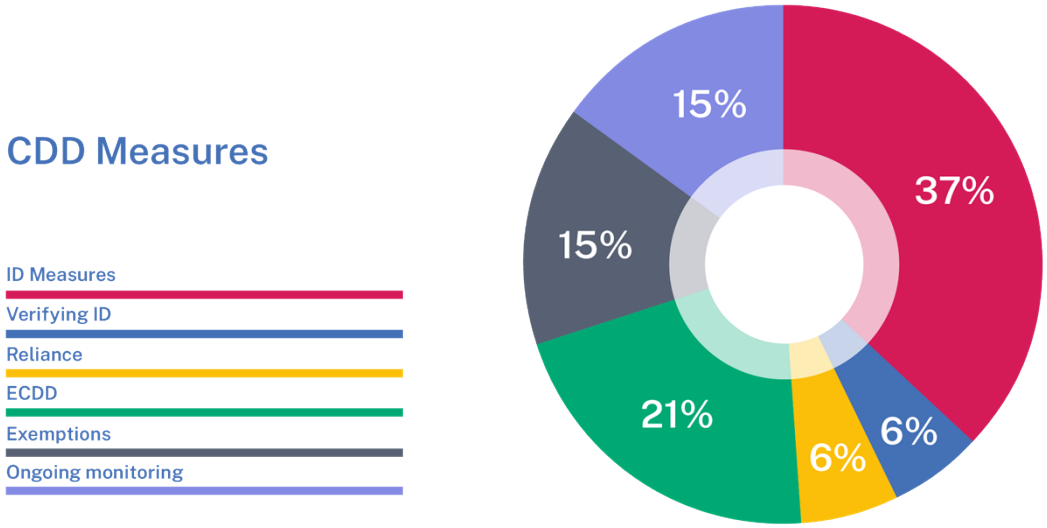
Examples of best practice and other resources to help firms improve compliance in this area

Review the responsibilities of the compliance function to ensure that MLCOs and MLROs have sufficient resources to carry out all required tasks in a timely manner. Consider whether tasks executed by the MLCO or MLRO that form part of day-to-day customer activities could impact on the ability of the function to demonstrate its independence. Such activities may potentially include on boarding processes, payment or other transactional processes and the ability to commit your firm to risk.

Ensure that any DMLROs have been formally appointed and the responsibilities of the role are fully understood by the individual. Training and support should be provided to DMLROs to ensure they are aware of the relevant statutory and regulatory requirements. This will also help to provide assurance that they are able to effectively carry out their role, should the MLRO be unavailable.

7.2 CDD measures

There were **33** findings arising from the 25 examinations conducted in 2021 concerning CDD measures, as follows:



The Order requires supervised persons to apply CDD measures and goes on to set out that CDD measures involve identification measures and ongoing monitoring. Sections 3, 4, 5, 6, and 7 of the Handbook set out statutory and regulatory requirements relating to CDD measures which must be complied with. These sections of the Handbook also provide guidance notes that present ways in which a supervised person may demonstrate that it has complied with the regulatory framework.

Identification measures (Sections 3 and 4 of the Handbook)

There were **12** findings relating to identification measures and **2** that related to the verification of identity.

The majority of the 14 findings related to the assessment of the financial crime risks inherent in customer relationships. For example, matters included:

- in three examples, source of funds (**SoF**) or source of wealth (**SoW**) was not adequately documented
- in three instances, policies and procedures for establishing beneficial ownership and control (the '**three tier test**') were not effective or were not well understood by business development or customer facing employees
- customer risk assessments in six instances were not fully effective as they did not consider the accumulation of risk from multiple risk factors
- there were two instances where supervised persons had implemented E-ID solutions, but had not assessed the risk of doing so and had not included the use of E-ID in their BRA

In one case, customer on-boarding was completed by group entities in the UK for some lower-risk categories of customer. However, the supervised person had not established systems and controls in Jersey to assess whether the customers accepted and booked directly into the Jersey supervised person's platform by group entities were consistent with its business risk appetite and that CDD measures applied were appropriate.

There were three examples where customer records reviewed during examinations indicated that policies and procedures relating to establishing and verifying the identity of customers, beneficial owners and controllers of customers, third parties acting for the customer, or third parties for whom the customer was acting had not been complied with.

Examples of best practice and other resources to help firms improve compliance in this area

Ensure your CDD policies and procedures, including those that relate to SoF, SoW and the three tier test, are well understood by those undertaking business development and customer facing roles. Supporting information that is aligned to your risk based approach to CDD measures should be retained on customer records.

Consider if and how effectively your customer risk assessment assesses the cumulative impact of multiple risk factors. For example, a single customer relationship may reflect multiple country risk factors in different contexts.

Consider your own arrangements against prior feedback provided by us, including the paper published on 3 February 2022 following our thematic examination 'customer risk assessments'.

Reliance on obliged persons (Section 5 of the Handbook)

In some strictly limited cases the Order and the AML/CFT Codes of Practice allow a supervised person to place reliance on measures that have been applied by an 'obliged person' or 'external person' to find out the identity of a mutual customer and to obtain evidence of identity. Reliance on an obliged person or external person is subject to a number of conditions that are set out in the Order and Section 5 of the Handbook. Supervised persons must also carry out testing that establishes whether the use of reliance identification measures enables the supervised person to meet its statutory and regulatory obligations.

In two of the 25 examinations, businesses were unable to evidence that the conditions for placing reliance on an obliged person or an external person had been fully met, due to one or more of the following circumstances:

- no risk assessment had been carried out concerning the use of reliance identification measures
- assurance letters did not enable the supervised person to evidence compliance with regulatory requirements
- policies and procedures to carry out required testing had not been established
- testing had not been carried out

Examples of best practice and other resources to help firms improve compliance in this area

Review your reliance arrangements to gain assurance that you are able to meet the six conditions set out in the Order and in Section 5 of the Handbook. The Handbook also provides guidance on how supervised persons may demonstrate they have met these six conditions.

Consider the prior feedback provided by us, including the paper published on 10 August 2020 following our thematic examination 'reliance on obliged persons'.

Ongoing Monitoring (Section 6 of the Handbook)

The Order sets out that on-going monitoring is to involve scrutinising transactions and activity. Supervised persons must implement policies and procedures to monitor transactions and activity. They are also required to recognise and examine notable transactions and activity to ensure that they are consistent with the supervised person's knowledge of the customer, including the customer's business and risk profile. As part of its examination of such transactions and activity, a supervised person must examine their background and purpose and record its findings in writing.

Supervised persons are also required to keep documents, data or information up to date and relevant, particularly in relation to higher risk categories of customer.

Ongoing monitoring of customer relationships and changes to a customer's business and risk profile are critical to ensure:

- indicators of increasing risk are recognised and examined
- financial crime risks are managed appropriately by supervised persons on an ongoing basis

There were five findings in respect of ongoing monitoring that included one or more of the following circumstances:

- in two examinations the supervised person's customer screening activities were carried out or partly carried out by a group function outside of Jersey. Reliance was placed on internal audit functions to provide assurance that those screening activities were carried out to the required standard. However, the supervised persons had not received the internal audit function's report
- in three examples trigger event processes were ineffective at identifying the indicators of increasing financial crime risk, which were reflected in customer records examined by us
- in four instances periodic review processes were behind schedule or there was ineffective reporting of their status to the board

Examples of best practice and other resources to help firms improve compliance in this area

In respect of customer screening and transaction monitoring, consider:

- the integrity and completeness of data that is screened
- the effectiveness of tools and processes employed to screen customers and scrutinise transactions and activity
- if processes allow for timely escalation of potential matches or transactions and activity which are not in keeping with the customer's business and risk profile
- whether monitoring is tested to provide assurance that it is being undertaken appropriately
- if senior management understand any limitations in the tools or procedures used and whether these are documented, along with any mitigating actions

Ensure trigger event and periodic review processes are operating effectively and policies and procedures are being complied with. Where there are backlogs in processes to keep documents, data and information up to date, a risk-based remediation plan should be in place.

Enhanced and simplified CDD measures and exemptions (Section 7 of the Handbook)

The Order requires supervised persons to apply enhanced CDD measures on a risk-sensitive basis in a number of circumstances, including any situation which by its nature can present a higher risk of money laundering.

The Order also provides for a number of exemptions from CDD requirements that apply in some strictly limited circumstances. These include, for example, exemptions from the need to apply third party identification measures in relation to the underlying customers of certain regulated businesses. In addition, specified exemptions from CDD requirements are provided, for example, in respect of regulated business or persons acting on behalf of a regulated business as part of their employment.

There were 12 findings in relation to this section of the Handbook in 12 of the 25 businesses examined. However, the 12 individual findings were varied in nature and circumstances that contributed to findings included:

- in five instances, policies and procedures relating to enhanced CDD or the application of exemptions from CDD measures:
  - were not in place
  - did not align with Jersey regulatory requirements

- provided incorrect guidance to employees regarding exemptions from CDD measures

› four customer records reviewed indicated procedures relating to the application of enhanced CDD measures had not been complied with. In one instance the required enhanced CDD measures had not been applied by the supervised person

› at two supervised persons, politically exposed persons (**PEP**s) had been de-classified based on the length of time they had been out of office. Declassification of PEPs is not provided for by the Jersey legal and regulatory framework

› in two examples, records confirming that it was appropriate to apply exemptions from CDD requirements were not retained

› in one instance an exemption had been incorrectly applied in respect of third parties connected to a 'relevant customer' that was not regulated

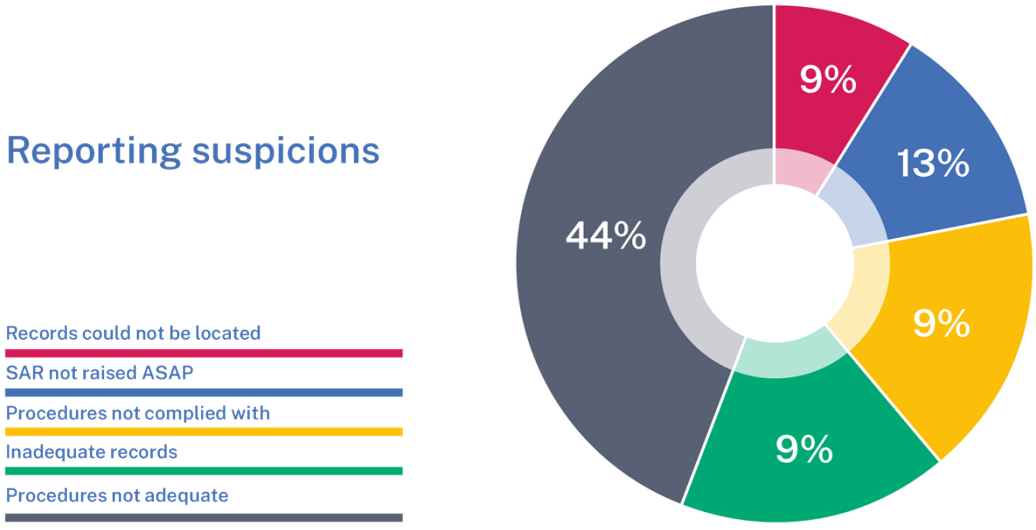
Examples of best practice and other resources to help firms improve compliance in this area

Ensure that policies and procedures relating to enhanced CDD, simplified CDD and exemptions are in place, are operating effectively and are being complied with. Policies and procedures should be reviewed regularly to incorporate any regulatory developments and to provide ongoing assurance that they enable you to comply with statutory and regulatory requirements.

Consider your own arrangements against prior feedback provided by us, including the paper published on 20 September 2021 following our thematic examination 'ECDD, SCDD and exemptions'.

7.3 Reporting suspicions of financial crime

There were **28** findings arising from the 25 examinations conducted in 2021 concerning reporting suspicions of money laundering or terrorist financing, as follows:



Employees must know (i) where to locate a supervised person's procedure for making an internal suspicious activity report (**iSAR**); (ii) how to make a report; and (iii) the identity of the MLRO or deputy MLRO.

As well as ensuring employees are: (i) alert to financial crime risks; and (ii) well trained in the recognition of notable transactions or activity which may indicate money laundering or TF activity,

supervised persons must also take steps to ensure that employees are aware of the importance of submitting an iSAR to the MLRO as soon as practicable.

Reporting procedures must be clear and easy for employees to follow, whilst enabling the employee, the MLRO/DMLRO and the supervised person to all meet their statutory and regulatory requirements.

Supervised persons also need to ensure that robust procedures are in place concerning iSARs and external SARs (**eSARs**) handled by MLROs. This includes the retention of records regarding the steps taken by the supervised person's MLRO to determine whether or not an eSAR is required to be submitted to the JFCU. Procedures are also required for the ongoing management of relationships, including the need to submit 'continuation reports' to the JFCU when further information is identified.

Examination findings concerning the reporting of suspicions of financial crime included the following circumstances:

- 19 instances where policies and procedures reviewed by our officers did not adequately ensure that information required to be retained or recorded was collected or consistently recorded
- in one example, procedures did not include controls to ensure that 'consent' was sought from the JFCU when required and that the relationship was managed appropriately thereafter
- examination activity highlighted eight instances where a supervised person's policies and procedures had not been complied with. In two of these cases, accounts of customers that had been the subject of an eSAR had been closed and funds paid away to a destination outside of Jersey without the MLRO being aware of the matter and without prior consent for the transactions being sought from the JFCU
- four supervised persons could not locate all of the records relating to iSARs or eSARs that our officers wished to review
- in four instances supervised persons were not able to evidence that iSARs or eSARs were raised as soon as practicable
- in eight examples, records relating to iSARs or eSARs did not evidence one or more of the following:
    - all enquiries made by the MLRO
    - the rationale for making or deciding not to make a report or continuation report to the JFCU
    - whether all parties connected with the customer or proposed transactions had been taken into account as part of the MLRO or DMLRO's enquiries
    - guidance provided to employees by the MLRO on how to manage a relationship after an eSAR had been submitted
    - the reasons why certain information included in an iSAR had not been included in the eSAR submitted to the JFCU by the MLRO
- In two instances, reviews of customer records by our officers identified adverse information that suggested there may have been reasonable grounds to suspect money laundering or terrorist financing. However, there was an absence of information in the supervised person's records to indicate whether the employee had considered if the submission of an iSAR was appropriate or not, at the time.

Examples of best practice and other resources to help firms improve compliance in this area

Policies and procedures should be readily available and easy for employees to understand. Ensure that records relating to iSARs and eSARs are retained which evidence:

- whether reports were raised as soon as practicable and the reasons for any delays
- enquiries made

- action taken
- the rationale for making or deciding not to submit an eSAR to the JFCU

Records must be retained that reflect ongoing interaction with customer-facing employees regarding future activity and with the JFCU, including the rationale for making or deciding not to make 'continuation reports'.

Consider your own arrangements against prior feedback provided by us, including the paper published on 21 February 2020 following our thematic examination 'the role of the MLRO'.

7.4 Screening, Awareness and Training of Employees

There were **12** findings relating to the screening, awareness and training of employees.

Supervised persons are required to screen the competence and probity of certain employees at the time of recruitment and where there is a subsequent change of role.

Three supervised persons did not have procedures in place to ensure that employees were re-screened, where it was appropriate to do so when their role changed.

The Order and the AML/CFT Codes of Practice require supervised persons to promote the awareness of procedures to prevent, detect and report financial crime and to provide training at appropriate frequencies. Such training must be tailored to the supervised person and be relevant to the employees to whom it is delivered. Training must cover key aspects of legislation, key policies and procedures and the recognition and handling of transactions, activity and other conduct that indicates that a person is or appears to be engaged in financial crime.

Examination activity highlighted:

- one instance where training had not been completed by one of the supervised person's Principal Persons
- three instances where policies and procedures had not been complied with and another three where training had not been delivered to new employees in a timely manner
- in four examples, records had not been retained regarding the nature and content of training provided to employees
- one business had engaged a third party to provide training to its employees, but had not retained records relating to due diligence carried out on the third party provider, nor concerning the content of the training delivered by the third party provider
- in three instances, businesses were unable to evidence that employees of third party service providers had received information or training on procedures to prevent, detect and report financial crime, when it was appropriate for them to have done so

Examples of best practice and other resources to help firms improve compliance in this area

Review your arrangements to ensure that they enable you to meet the statutory and regulatory requirements set out in Sections 9 and 10 of the Handbook. Section 9 of the Handbook provides guidance to supervised persons on how they may demonstrate that they have complied with statutory and regulatory requirements regarding screening, training and awareness of employees.

In addition, consider the prior feedback provided by us, including that issued on 24 March 2022 the responses provided to our thematic questionnaire 'AML/CFT Training'.

Scope and Methodology regarding

The scope and methodology for visits and examinations we carry out is published on our website.

Glossary of Terms

Board	Board of Directors the function described in Section 2.1 of the Handbook
Customer	Means a customer of a supervised person as defined in the Order and the Handbook.
FATF	The Financial Action Task Force
Guidance	The Guidance provided to supervised persons in the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism.
Handbook	Means the relevant Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism
Key Person	Has the same meaning as provided in Article 1 of the Financial Services (Jersey) Law 1998.
Person	Means any natural or legal person (including a body of persons corporate or unincorporated)
Principal Person	Has the same meaning as provided in Article 1 of the Financial Services (Jersey) Law 1998.
Supervised person	Means a person carrying on financial services business in or from within Jersey as defined under Article 1(1) of the Order