Jersey Financial Services Commission

Guidance Note: Compliance Monitoring

Issued: 6 December 2013

Last revised: 4 June 2026

1 Introduction

1.1 This guidance is issued to support registered and supervised persons develop and maintain a risk-based compliance monitoring plan (CMP). The CMP should reflect regulatory expectations, demonstrate good governance standards and provide informed data to the board and/or senior management on the compliance risks in the business.

1.2 The role of the compliance function is critical to the implementation of compliance monitoring and, for the purpose of this guidance, includes the:

1.2.1 compliance officer

1.2.2 money laundering reporting officer

1.2.3 money laundering compliance officer

1.3 The compliance function covers all legal and regulatory obligations including operation of the business, conduct, prudential and financial crime obligations relevant to the type of business and licence type.

1.4 While legislation and codes require compliance monitoring, entities have latitude to design their arrangements in line with their specific circumstances. This guidance is designed to help entities meet our expectations and ensure the CMP is appropriately documented, risk-based, and subject to adequate and effective oversight.

2 What is compliance monitoring?

2.1 Compliance monitoring is the process of assessing your firm's adherence to the legislative and regulatory requirements applicable to your business and licence type. It should operate in conjunction with the controls designed to mitigate risk.

2.2 Effective compliance monitoring provides assurance to the board and senior management that the controls designed to mitigate risk are operating as intended. It also enables the identification of gaps in the control framework, confirms that policies and procedures are being followed, and supports timely action to address any deficiencies.

2.3 Compliance monitoring should form an integral part of your risk management framework, particularly in relation to regulatory and financial crime risk. It should be dynamic, data-driven, and proportionate to the nature, scale, and complexity of the business.

2.4 Monitoring activities may occur across the business and need not be limited to the compliance function. However, the compliance function remains responsible for providing the board or senior management with an accurate understanding of the strengths and weaknesses across the control framework in place, to manage and mitigate compliance risks.

2.5 An effective CMP enables you to demonstrate compliance with:

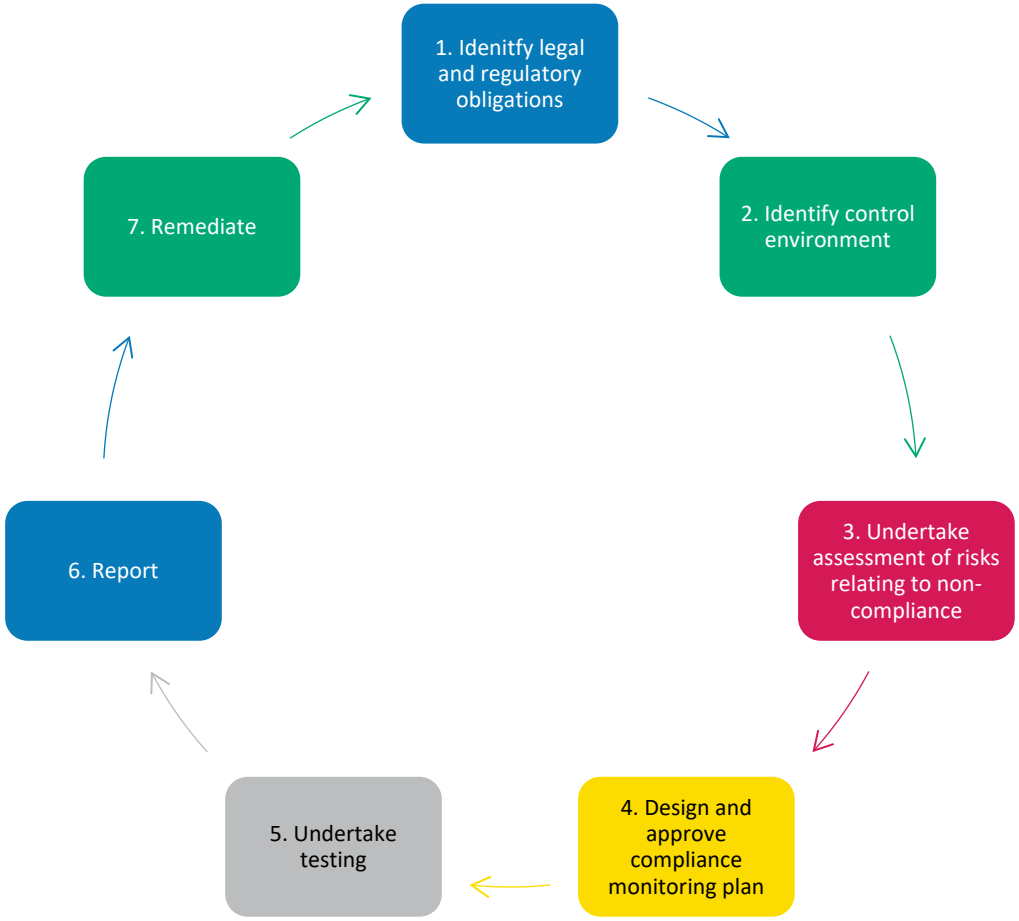
2.5.1 Principle 3 of the sector specific Codes of Practice relevant to your licence type(s)

2.5.2 the Money Laundering (Jersey) Order 2008 (as amended)

2.5.3 the AML/CFT/CPF Code of Practice set out in the Handbook

2.5.4 all other relevant financial services and financial crime frameworks noted in 3.3 below.

2.6 The determination of a risk-based CMP should involve a cyclical feedback process consisting of the following seven steps:



3 How to approach compliance monitoring and your compliance monitoring plan (CMP)

3.1 Compliance functions have finite resources subject to competing demands. As a result, you may adopt a risk-based approach to develop your CMP and focus on the areas that present the highest perceived compliance risks to your business.

Step 1: Identify legal and regulatory obligations

3.2 While set out above as integral to the CMP, the compliance function should remain alert to changes in the regulatory environment and report relevant developments to the board and/or senior management as part of your overall compliance function. This is not limited to the CMP.

3.3 When establishing and reviewing the CMP it is important for you to identify all relevant legislative and regulatory requirements applicable to your business. This includes requirements covering the operation of the business, the regulatory obligations and countering financial crime obligations.

3.4 The relevant legislative and regulatory requirements will depend on your licence type and whether you are registered and supervised or only supervised for financial crime. The following table sets out some of the sources which need to be considered:

Regulatory Laws (including all issued subordinate Regulations and Orders)	**Alternative Investment Funds (Jersey) Regulations 2012** **Collective Investment Funds (Jersey) Law 1988** **Banking Business (Jersey) Law 1991** **Financial Services (Jersey) Law 1998** **Insurance Business (Jersey) Law 1996**
Financial Crime Laws (including all issued subordinate Regulations and Orders)	**Money Laundering (Jersey) Order 2008** **Proceeds of Crime (Jersey) Law 1999** **Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008** **Sanctions and Asset-Freezing (Jersey) Law 2019** **Terrorism (Jersey) Law 2002**
Code of Practice (conduct and prudential)	**Code of Practice for Alternative Investment Funds** **Code of Practice for Certified Funds** **Code of Practice for Deposit Taking Business** **Code of Practice for Fund Services Business** **Code of Practice for General Insurance Mediation Business** **Code of Practice for Insurance Business** **Code of Practice for Investment Business** **Code of Practice for Money Services Business** **Code of Practice for Trust Company Business**
Code of Practice (financial crime)	**Code of Practice set out in the AML/CFT/CPF Handbook**

3.5 You may also be required to include overseas financial service business requirements if relevant to your firm. For firms with branches or holding companies in other jurisdictions, your

CMP may need to extend to the relevant obligations in those other jurisdictions as failure to comply with them could have regulatory consequences for the Jersey business.

3.6 Your CMP may also extend beyond the financial services and countering financial crime legislation to include areas such as:

3.6.1 data protection laws

3.6.2 revenue laws and regulations

3.6.3 relevant industry standards applicable to your business

3.6.4 registry laws and regulations

3.6.5 certain contractual obligations which could impact your risk assessment

3.7 The CMP should be tailored to your business. We understand that you may prioritise resources of the compliance function to ensure that appropriate focus aligns with the risks associated with your business and your legal obligations.

Good practice	Poor practice
The CMP maps all applicable legal and regulatory requirements, with an approved document detailing each mapped requirement.	Reliance on group-level CMP procedures lacking detail on Jersey-specific regulatory requirements.
Use of a subscription service for timely notification of changes to the relevant legal and regulatory requirements.	
Technology compliance solutions are updated regularly to reflect changes in relevant regulations and standards to ensure alignment.	

Step 2: Identify control environment

3.8 Once the relevant legislative and regulatory requirements have been established, the controls needed to manage the risk of non-compliance should be identified or reviewed for effectiveness.

3.9 Controls comprise policies, procedures, and activities. They may also include:

3.9.1 oversight by business control units

3.9.2 internal audit

3.9.3 technology-enabled mechanisms such as:

- automated exception reporting
- data validation tools

3.9.4 ongoing training for staff to build an effective compliance culture.

3.10 When establishing or reviewing the controls you have in place, any gaps identified should be remediated. Where technology is used as a control or to support a control function, you should ensure appropriate validation, audit trails, and contingency procedures are in place.

Good practice:
Where gaps in the control environment are identified, timely actions are instigated to remedy the position in a way that ensures the control mitigates the risk.
Using regulatory technology to automate certain monitoring activities which enhance efficiency and accuracy of results.

Step 3: Undertake assessment of risks relating to non-compliance

3.11 Once the controls have been identified, you can assess the compliance risks in relation to the relevant legislative and regulatory requirements. This assessment should consider both the potential impact and the likelihood of non-compliance. It should also evaluate the inherent risk, before controls are applied and the residual risk, after the controls are implemented in your business.

3.12 The risk assessment enables the identification of key controls. Certain key controls which significantly reduce the risk of non-compliance tend to be subject to oversight by:

3.12.1 business control units

3.12.2 internal audit

3.12.3 automated monitoring systems

3.13 The risk assessment should cover all risks (e.g. operational, regulatory and financial crime).

3.14 As part of your CMP, you can use different methods to assess your firm's risk profile. These methods should be proportionate to your business model and aligned with applicable regulatory requirements and financial crime prevention obligations (e.g., AML/CFT/CPF frameworks and principle 3.3 of the codes of conduct). Some firms adopt multiple types of risk assessments to address different organisational functions and categories of risk. Below are examples relevant to compliance monitoring:

Jersey Financial Services Commission

Types of risk assessment in compliance monitoring

Type	Purpose	Regulatory context
Enterprise-wide risk assessment (EWRA)	Provides a comprehensive view of inherent and residual risks across the firm.	Required under AML/CFT/CPF regulations to identify and mitigate financial crime risks at an organisational level.
Functional or departmental risk assessment	Evaluates risks within specific functions (e.g., Compliance, Operations, Client onboarding).	Supports targeted monitoring where higher-risk activities occur.
Product or service risk assessment	Assesses financial crime risks linked to products, services, or delivery channels.	Required under AML/CFT/CPF frameworks when introducing new products or reviewing existing ones.
Customer risk assessment	Determines the risk level of individual customers or customer segments.	Integral to Customer Due Diligence (CDD) and ongoing monitoring obligations.
Thematic or issue-based risk assessment	Focuses on emerging risks or specific regulatory themes.	Often triggered by regulatory updates or supervisory findings.
Technology and cyber risk assessment	Evaluates risks related to IT systems and data integrity.	Relevant where technology underpins compliance processes (e.g., eKYC).
Project or change risk assessment	Assesses compliance risks during organisational changes or major projects.	Supports maintaining adherence to regulatory standards during transitions.

Examples of good and poor practices in risk assessments

Good practice	Poor practice
The risk assessment considers a range of information sources, including relevant revenue, complaints, breaches, operational incidents, JFSC publications (such as public statements, on-site examination feedback, and guidance notes), previous compliance monitoring results, audit reports, and concerns raised by senior management.	The risk assessment relies excessively on "negative assurance," such as assuming compliance with legislative and regulatory requirements solely on the basis that there are no recorded breaches
The risk assessment is updated at the time of a trigger event (e.g. a change to regulation) as well as being reviewed periodically (e.g. annually).	The risk assessment assumes that having controls in place is enough, without reviewing the effectiveness of those controls, or testing the level of compliance
The risk assessment uses a structured form of rating, such as a red, amber green (RAG) scale or numerical scoring system, to support prioritisation and transparency.	

Step 4: Design and approve compliance monitoring plan

3.15 The CMP should reflect the results of the risk assessment. It should focus on those legislative and regulatory requirements where the residual risk (i.e. after controls have been applied) is highest.

3.16 The CMP should detail the following:

3.16.1 legislative and regulatory requirements

3.16.2 the controls to be tested

3.16.3 any other restrictions to the scope (e.g. a focus on a particular business line, department, or team)

3.16.4 a timetable for completion

3.16.5 The content of a CMP will differ between firms, reflecting a risk-based approach tailored to the nature, scale, and complexity of each business. While variation across sectors and firm sizes is expected, every firm must maintain a CMP that is proportionate to its specific circumstances and risks.

3.16.6 Where a firm is part of a group, we recognise the efficiencies of shared resources and controls. However, it is critical that the CMP explicitly addresses Jersey-specific risks and regulatory obligations. This means:

3.16.6.1 Documenting how group frameworks and testing plans have been adapted for Jersey

3.16.6.2 Ensuring the local board reviews and approves the adapted CMP, and

3.16.6.3 Maintaining clear evidence that the CMP meets Jersey's legal and regulatory requirements, including any enhancements made to reflect Jersey's risk profile

3.16.7 Failure to tailor the CMP to Jersey-specific risks will not meet regulatory expectations, even where group standards are otherwise robust.

3.17 The CMP should be reviewed on a regular basis by the compliance function, escalating material changes to the board and/or senior management as deemed appropriate. This ensures the board and/or senior management has an appropriate level of oversight of the CMP.

Good practice	Poor practice
The CMP includes areas where testing has previously identified weaknesses, to test the effectiveness of previous remedial action taken.	The CMP is not periodically reviewed or approved by the board and/or senior management, and it operates as a fixed schedule of tests that are repeated on a routine basis without considering operational changes or evolving compliance risks.
The CMP is reviewed and approved by the board and/or senior management on an annual basis and reviewed by the compliance function on a quarterly basis, with any significant changes reported to the board and/or senior management.	

The output of the risk assessment directly influences the compliance monitoring plan, ensuring a risk-based approach to testing and appropriate use of resource.	Over reliance is placed on group CMP meaning testing does not address relevant Jersey-specific risks.
Policies and procedures relating to the CMP include provisions relating to periodically assessing the effectiveness of the testing methodologies used.	Poor documentation relating to the CMP such as a failure to set out how the CMP was developed, approved and delivered.
Where the CMP identifies weaknesses in the control environment, consideration is given to whether the issues identified are systemic or whether they may also be prevalent in other parts of the business.	The CMP is not periodically considered nor approved by the board and/or senior management.

Step 5: Undertake Testing

There is no prescribed approach to testing. However, testing should produce robust, evidence-based findings that can be used to report on your compliance.

Good practice	Poor practice
Testing plans are clearly documented and detail the objective and scope of the testing, the work to be undertaken, the proposed timescales and are shared with relevant individuals in the business.	Over-reliance is placed on unverified verbal statements from staff as to how they comply with systems and controls, including policies and procedures.
A variety of testing approaches are used, such as interviewing individuals, reviewing customer files (holistically or in part), analysing data, stress testing technology, reviewing corporate documents, and listening to recorded conversations.	Inadequate or no working papers produced to evidence the testing undertaken or support findings.
Where appropriate, sample testing is used and the findings are extrapolated, for example, testing an agreed percentage of high/medium/low customer files.	Testing not done at all, to an adequate standard, or in line with the CMP.
	Inconsistent treatment of CMP findings due to a lack of documented guidelines or methodology, leading to varied assessments of findings across tests.
	Misalignment between the CMP and the actual testing undertaken by firms without a clearly documented rationale for the variance.

Step 6: Report

3.18 The results of the testing should be shared with relevant individuals in the business for feedback, and appropriate remedial actions should be agreed (see below). These results should then be presented to the board. The escalation process should be clearly defined and proportionate to the severity of the issue – including where urgent escalation to the board is appropriate.

3.19 The compliance function's written report to the board should include compliance monitoring as a standing agenda item. It should provide details of the CMP and the testing completed during the reporting period as well as:

3.19.1 relevant findings

3.19.2 corresponding remedial actions

3.19.3 progress with outstanding remediation since the previous report

3.20 Rating and prioritising findings supports effective board oversight by encouraging discussion, scrutiny and challenge on the findings as well as evidencing informed decision-making.

3.21 If there are instances of non-compliance with relevant laws or regulations, you should consider the obligations and consequences outlined in sector-specific codes of practice and legislation. Upon discovery, we encourage you to engage openly and cooperatively with the JFSC. Where necessary or mandated it is expected that you would report any breaches.

Good practice	Poor practice
A summary of testing, findings, and remedial action is documented in compliance monitoring reports, and extracts are included in the compliance function's report to the board.	Insufficient evidence of board oversight of the content and results of testing under the CMP in internal communications and records (including board minutes).
The compliance function's report to the board includes progress against the approved CMP.	No report is provided to the board on compliance monitoring activities.
Ratings are assigned to individual findings and to the overall compliance monitoring report to support prioritisation and oversight.	The board fails to support or follow up on the completion of remedial actions resulting from testing.
Comprehensive records of testing are maintained in support of test results.	Failing to record breaches identified in the testing in the breaches register.
The board and/or senior management provides regular input or feedback in relation to the structure and content of reports presented to them, particularly regarding the level of detail, the way in which the results are presented, and input into how resultant actions are to be prioritised from the CMP.	

Step 7: Remediate

3.22 Where testing identifies gaps, weaknesses or non-compliance, steps should be taken to address the findings in a timely and proportionate manner. The nature and urgency of the remedial action should reflect the severity and potential impact of the issue.

3.23 Responsibility for the remedial action should be clearly allocated to appropriate individuals, and the compliance function should have oversight of its completion. Progress should be monitored against specified timelines, and delays or failures to implement agreed actions should be escalated as appropriate.

3.23.1 The board and/ or senior management should seek regular updates to ensure effective compliance and remediation is achieved.

3.24 To ensure sustainability, firms should assess the long-term effectiveness of remedial actions through follow-up testing and consider whether the issue indicates a broader or systemic weakness. Remediation activity should be documented and tracked to support transparency and accountability.

Good practice	Poor practice
Where an issue is identified, the wider implications are considered with the purpose of identifying any systemic weaknesses or trends that should be addressed.	An ambiguous statement is provided by the business in response to findings, and no remedial action is agreed or implemented.
Remedial action is agreed between the compliance function and relevant individuals within the business.	Remedial actions resulting from CMP tests are not adequately prioritised or addressed due to a lack of clear follow-up and oversight.
Any breaches of regulatory requirements or controls are recorded centrally and monitored for recurrence.	Board and/or senior management do not: › make effective decisions considering remedial action › provide regular oversight › require regular updates on improved compliance and remediation
Remedial actions are revisited periodically to assess whether they are fully embedded and sustainable in practice.	

4 Benefits of compliance monitoring

4.1 The benefits for firms of having a robust and risk-based approach to compliance monitoring include:

4.1.1 an enhanced risk management framework that supports early identification and mitigation of compliance risks

4.1.2 the ability to demonstrate the board's oversight of the effectiveness of controls implemented to manage compliance risk

4.1.3 proactive identification of control weaknesses, incidents, and breaches of relevant legislative and regulatory requirements

4.1.4 the ability to target business improvements that reduce the risk of legal or regulatory sanctions, material financial loss, or reputational damage

4.1.5 access to reliable data to inform the completion of annual declarations required under regulatory requirements relevant to the business

4.2 We encourage you to report identified breaches to us in a timely manner. Doing so reflects positively on your governance and enables you to demonstrate the remedial action taken or planned to address the issue. Concealing a breach which was known to you, but which had not been disclosed to us, during a routine supervisory visit or onsite examination could increase the potential seriousness of the examination outcome.

5 The use of regulatory technology in compliance

5.1 We understand the benefit regulatory technology can bring when delivering an effective and efficient CMP. The following guidance provides you with some support when considering the use of technology in compliance:

5.1.1 the regulatory technology implementation guide

5.1.2 the financial crime and regulatory technology guide

5.2 Regulatory technology can modernise and strengthen compliance monitoring by introducing greater efficiency, accuracy, and responsiveness. When used effectively, it can significantly reduce the administrative burden on compliance teams and enhance an organisation's ability to meet regulatory obligations.

5.3 However, technology should complement, not replace, human judgement. While automation and data-driven insights are valuable, you should be able to demonstrate how you are maintaining human oversight on any identified gaps, deficiencies or regulatory breaches. This is critical to ensure ethical consideration and strategic decision-making regarding the design, implementation and reporting of your CMP.

5.4 Any use of technology within the business must comply with both internal and external compliance legal and regulatory requirements. This includes Jersey-specific obligations and, where relevant, international laws and standards. Firms should ensure that technology solutions are implemented and operated in a way that supports compliance, data protection, operational resilience and financial crime prevention.

5.5 Technology governance should include clear accountability, board oversight for material changes, and documented risk assessments. Controls must address data privacy, cybersecurity, and third-party risk, with appropriate contractual safeguards and audit rights. Systems should provide reliable audit trails, support statutory record-keeping, and maintain resilience through tested business continuity and disaster recovery plans.

5.6 Where group-level technology frameworks are adopted, it is critical that they are tailored to Jersey-specific risks and regulatory expectations. This includes documenting local adaptations, securing local board approval, and retaining evidence that the solution meets Jersey requirements. Failure to do so will not meet regulatory expectations, even where group standards are robust.

6 Conclusion

6.1 The JFSC does not expect every firm to undertake compliance monitoring in the same way. Compliance monitoring should be proportionate and risk-based, reflecting the nature, size, and complexity of your business. However, the JFSC does expect the board and/or senior

management to understand and demonstrate the importance of compliance monitoring and explain the prioritisation set out in the CMP to comply with the relevant requirements set out in legislation and codes of practice.

6.2 The CMP should be clearly documented, regularly reviewed, and supported by appropriate records that evidence the design, execution, and oversight of the testing undertaken.

6.3 Should you have any questions please contact your supervisor.

Jersey Financial Services Commission

Appendix A: Scenarios of compliance monitoring practices

This appendix presents example scenarios that illustrate both effective and ineffective use of a CMP, along with the consequences of each. These examples can support training efforts and help build a deeper understanding of how a well-implemented CMP can reduce risk. They also highlight the potential impact of errors or missed actions. Using real-world contexts for these scenarios can improve engagement and reinforce the importance of strong compliance planning.

Entity A – Strengthening compliance through good compliance monitoring practices

Entity A, a mid-sized regulated business, upgraded its compliance monitoring to meet evolving regulatory standards and internal governance needs.

The process began with Entity A updating its business risk assessment (BRA), clearly mapping legal and regulatory obligations (e.g., AML/CFT/CPF, governance, data protection). This helped business units understand their compliance duties and identify control gaps—such as outdated onboarding procedures and weaknesses in its oversight of certain outsourced activities. Corrective actions were assigned to the business units and tracked via monthly compliance meetings.

To improve risk awareness, a risk matrix was added to the BRA, highlighting high-risk areas identified from the onboarding and outsourcing review. These insights informed a risk-based CMP, prioritising specific issues with onboarding and a more targeted approach to reviewing its outsourcing arrangements. The CMP was reviewed and approved by the compliance committee and the board.

Entity A then implemented a structured testing approach, covering planning, investigation, reporting, and follow-up. For example, a recent outsourcing test involved document reviews, staff interviews, and system walkthroughs. Findings were rated (Effective, Partially Effective, Not Effective), with recommendations presented to the board. Remedial actions were assigned to business owners, and progress was reported quarterly.

Entity A's enhanced CMP led to stronger internal controls, better regulatory compliance, and reduced risk exposure. By aligning risk assessments with legal obligations, prioritizing high-risk areas, and implementing structured testing and oversight, the firm improved accountability and resilience across its operations.

Entity B – Inadequate compliance monitoring practices undermining effective risk management

Entity B, encountered significant challenges with its compliance monitoring due to a series of poor practices. Rather than conducting its own Business Risk Assessment (BRA), Entity B relied on the BRA of a group company. The BRA relied on by Entity B was a generic version provided by its parent company. However, the business model and regulated services provided by Entity B differed from that of the group company. The BRA failed to identify key operational and compliance risks relevant to its business, such as deficiencies in client onboarding and weak oversight of outsourced IT services. Compounding the issue, the board of Entity B did not actively

review or question the content of the BRA, which led to limited visibility and inadequate oversight of compliance risks.

This misalignment in the BRA affected the CMP design because it was based on inaccurate and incomplete data. For example, the CMP did not include testing for adequate records relating to personal account dealing when looking at conflicts of interest. This oversight could be directly attributed to the BRA having been conducted against a different licence type to the one held by Entity B. As a result, some compliance tests were poorly scoped and missed critical areas. Remedial actions identified during testing were assessed against an incomplete picture of the risk position and therefore findings were inadequately prioritized and tracked. This led to some issues remaining unresolved for a significant period of time, exposing Entity B to potential regulatory breaches.

Entity B was left exposed to regulatory breaches and operational vulnerabilities, undermining its overall risk management. Due to poor CMP practices that included inadequate risk assessments, failures in board oversight and unresolved control gaps.

Entity C – Bouncing back from a poor risk assessment

During its annual compliance monitoring cycle, Entity C realises it has overlooked the step of assessing risks related to non-compliance. This discovery occurs just before testing begins. Recognizing the potential impact, the compliance team pauses the process and undertakes an up to date risk assessment, uncovering new regulatory obligations and operational vulnerabilities.

The CMP is revised to reflect the updated risk profile, and the scope of testing is adjusted to include previously unaddressed high-risk areas. Reporting is enhanced to incorporate insights from the new assessment, and remediation efforts are redirected to address the newly identified gaps.

By proactively correcting the oversight, the firm avoids regulatory breaches, strengthens its control environment, and demonstrates a commitment to continuous improvement. This approach reinforces the integrity of the compliance monitoring cycle and supports a culture of accountability and responsiveness.

Entity D – Reporting and its impact on governance and compliance culture

Entity D completes its compliance monitoring cycle, but the reporting produced is vague, lacks detail, and fails to highlight key risks and unresolved issues. The report presented to the board and senior management focuses on areas of strong performance while omitting findings from high-risk areas that were either inadequately tested or not remediated from testing in an earlier period.

As a result, the board and senior management make strategic decisions under the assumption that the firm's compliance position is sound. Months later, a regulatory inspection reveals significant breaches that had not been escalated. The board is caught off guard, and senior management faces scrutiny for governance failures and lack of oversight.

This incident prompts a reassessment of Entity D's compliance culture. The board takes steps to reinforce its commitment to transparency and accountability by mandating clearer, risk-focused reporting and ensuring that compliance findings are presented with sufficient context and candour. They also introduce regular board-level reviews of compliance risks and establish direct lines of communication with the compliance function to ensure that emerging issues are surfaced and attended to early.

By actively engaging in the compliance process and setting expectations for integrity in reporting, the board helps restore trust and embeds a culture where compliance is seen as a shared responsibility across all levels of the organisation.