Statement of Good Practice

Unauthorised trading frameworks

Transparency Draft

FMSB invites comments on this Statement of Good Practice by 15th September 2025. Please address any comments or enquiries to secretariat@fmsb.com.

Introduction

Financial Markets Standards Board

Financial Markets Standards Board ("FMSB") was established in 2015 in accordance with the recommendations of the UK Fair and Effective Markets Review with a mandate to help raise standards and effectiveness in wholesale financial markets. FMSB has developed a body of Standards ("Standards") and Statements of Good Practice ("SoGPs") over time, prioritising those areas where FMSB member firms ("Member Firms") observed a lack of clarity in market processes, the standards of behaviour expected of market participants, a lack of understanding of the issues relevant to a product or transaction type, or evidence of conduct resulting in unsatisfactory outcomes for customers, counterparties or the markets.

Applicability of FMSB Statements of Good Practice (SoGP)

SoGPs are issued by FMSB from time to time. SoGPs do not form part of FMSB Standards, and they are not subject to FMSB's adherence framework. Rather, they reflect FMSB's view, in discussion with its Members, of what constitutes good or best practice in the areas covered by the SoGPs in question. Member Firms are expected, and other firms are invited, to consider their own practices in light of the relevant SoGP and make any changes to such practices that they deem to be appropriate. Failing to do so will not, however, create any presumption or implication that a firm has failed to meet its regulatory or other obligations.

Full details of the Member Firms are available at https://fmsb.com/. SoGPs will be shared with non-member firms and their affiliates, who are encouraged to consider them. Information on SoGPs will be made available to users of the wholesale markets (e.g., corporates and end investors) so that they may be made aware of their existence and FMSB's expectation of market conduct. FMSB will, as part of its normal course of business, periodically review the applicability of its published SoGPs to ensure they remain relevant and up to date for market conditions.

Relationship with law and regulation

FMSB Standards and SoGPs do not impose legal or regulatory obligations on Member Firms, nor do they take the place of regulation. In the event of any inconsistency, applicable law, rules, and regulation will prevail. In developing Standards and SoGPs, certain regulators may have commented on their drafting, alongside Member Firms and other bodies, such that the Standards and SoGPs, once finalised and published, are intended to represent an authoritative statement of global good practices and processes. However, they are not normally endorsed by regulators. Where they are endorsed by a regulator, that will be made clear on the face of the Standard or SoGP in question.

Relationship with other codes

Other Codes already exist in relation to certain markets, such as the FX Global Code, while others are in the process of being produced. Some overlap exists between the work of FMSB and such other bodies and FMSB will seek to ensure it adopts a consistent approach in cases of overlap wherever possible and will seek to avoid issuing a Standard or SoGP where the subject matter is already covered adequately by existing regulation, or a Code issued by another body. It may draw attention to Member Firms of an existing code and request that Member Firms act in a manner consistent with it once appropriate steps have been taken to confirm its applicability.

I. Explanation

1. Purpose

1.1. The purpose of this SoGP is to support firms in their efforts to prevent or mitigate the risk of unauthorised trading activity in wholesale markets.

2. Scope and applicability

2.1. This SoGP focuses on unauthorised trading frameworks (as defined in Section II, paragraph 2). It is applicable to all types of trading. It does not catalogue the many variations of unauthorised trading, nor delve into the detail of such topics as end-to-end controls, risk, algo-driven trading or market abuse.

2.2. Application of the Good Practice Statements should be informed by the nature, scale and complexity of the trading business undertaken and the systems and controls planned or in place to mitigate associated risks. Each firm should consider its own practices in light of this SoGP and the extent to which any changes might be appropriate.

II. Context

1. Industry background

Financial services strive to keep pace with evolving global needs. Innovation is driven by those emerging needs and often enabled by advances in technology. Innovation and change can also give rise to new risks.

One constant has been the intention of firms to operate within agreed business models and avoid transaction and other activity that falls outside approved boundaries. Industry has invested heavily in the design and implementation of risk management frameworks to ensure that activities are conducted within authorised boundaries. This includes avoidance of incidents of unauthorised trading which are a potential source of significant financial loss and reputational damage at industry as well as firm level.

Comprehensive industry guidance or published expectations on unauthorised trading remains limited. Cross-jurisdictional regulatory engagement has often been bilateral, with detailed feedback provided to individual firms rather than via industry-wide publications. Baseline standards for unauthorised trading frameworks have not advanced consistently across markets or jurisdictions.

The financial services industry is actively reassessing its approach, including:

- the completeness of unauthorised trading frameworks,
- clarity of related roles and responsibilities across the organisation,
- effectiveness of the control infrastructure, and
- the capacity to respond proportionately and comprehensively to emerging risks or incidents.

Despite significant efforts, there is a continuing risk that novel or existing vulnerabilities could allow unauthorised trading to occur or remain undetected.

The Good Practice Statements provided here seek to help establish practical foundations and more consistent expectations among firms and regulators regarding the frameworks needed to effectively contain unauthorised trading.

2. Key concepts

Certain terms related to unauthorised trading lack consistent definitions across the industry. This section promotes a common understanding of key terms noting that firms may adjust these definitions as needed to align with their own frameworks, taxonomies, or applicable regulatory requirements.

Term	
Authorised Trading	**Definition** Trading which falls within the agreed perimeters of approved business activities, regulatory permissions, trading mandates and defined risk limits (e.g. credit, market, liquidity, other) as well as any other factors specifically prescribed by the firm. **Commentary** Authorisations are typically set at multiple levels within a firm, e.g. at the firm, business, desk and individual levels. They may also be specific to legal entities given regulatory requirements and internal risk appetites across jurisdictions.
Unauthorised trading	**Definition** Trading activity which falls outside the perimeter of authorised trading including the deliberate, and in some cases fraudulent, manipulation of trading books and records. **Commentary** There is a broad spectrum of unauthorised activity or events that can range from intentional to accidental and vary in scale from a malicious and severe impact on clients or the firm, to minor mistakes perhaps more adequately captured as operational risk events. In this document, unauthorised trading includes: • trading activity that is intended to misrepresent risk and/or financial returns or manipulate the trading books and records of the firm, including fraudulent activities. • trading that, while in line with relevant firm definitions and perimeters, fails to adhere to approved authorisations.
Preventative unauthorised trading controls	**Definition** Controls that seek to systematically block initiation, progress or completion of an adverse unauthorised trading risk event (e.g. loss, error or egregious behaviour) pre-trade or at point of trade. **Commentary** • The design of a preventative control should specifically address one or more targeted outcomes that it seeks to mitigate, such as unauthorised trades, intentional fraud and/or limit breaches. • There should be detective controls / monitoring associated with preventative controls to verify coverage of scope and accuracy of blocks in the event of a preventative control failure.
Detective unauthorised trading controls	**Definition** Controls that seek to identify whether an unauthorised trading risk event has occurred or is in prospect upon trade completion and reporting, with the objective of limiting or reversing the impact of the event as quickly and effectively as possible and preventing future or additive events.

Term	
	Commentary Detective controls reflect post-trade, intra-day, end-of-day, T+1 and beyond controls (i.e. reconciliations, exceptions monitoring, risk reporting or other trade analytics) that identify a trade or series of trades as unauthorised.
Pre-trade	**Definition** The period of time and activities that take place prior to trade execution (e.g. client prospecting, ideation, initiation, pricing discussions). **Commentary** The multiple steps involved in trade preparation should include obtaining any required advance authorisations (e.g. onboarding, limits).
Point-of-trade	**Definition** Activities that take place directly at the point of trade execution. **Commentary** This primarily refers to inputting transactions into an execution system that connects to external markets or counterparties and initiates a trade.
Post-trade	**Definition** The period of time and activities that take place once a trade has been executed. **Commentary** This reflects the point at which a trade is normally visible to the counterparty and to other third parties of a public market trade (noting that false trades or the suppression of trade confirmations can occur).
Hard block	**Definition** A hard block is a systematic control which prevents an action from being undertaken. **Commentary** In some cases, a hard block can be released following escalation and approval by more senior management in accordance with the firm's pre-agreed authorities.
Soft block	**Definition** A soft block interrupts a process, which can then be resumed by the originating actor, enabling the process to move forward toward completion. **Commentary** A soft block often takes the form of an automated warning message to the originator which requires acknowledgement to enable proceeding. Escalation within the originator's business unit may be required but this would still not elevate a soft block to becoming a control.

III. Good Practice Statements

Governance

Good practice statement 1: Framework

Firms should establish and maintain a clear framework that outlines the parameters of authorised trading, sets out robust governance and supervision arrangements and promotes consistent adherence.

Commentary

1.1. A clear framework for authorised trading is essential for the risk management of business activities, ensuring ongoing compliance with laws, rules and regulations, internal policies, defined risk appetites, and, in extreme cases, mitigating the risk of egregious fraudulent trading that could significantly impact a single firm or broader market participants.

1.2. The authorised trading framework should comprise components which collectively seek to mitigate the risk or impact of unauthorised trading. Examples of key components include policies, procedures, defined roles and responsibilities, controls across the transaction lifecycle, management information and reporting, and consequence management processes.

1.3. The framework should provide practical context as to how controls around trading fit together and how each of the support functions are integrated into oversight.

1.4. The framework should align with other pertinent frameworks in place within the firm for governance, risk management, and end-to-end controls.

1.5. The framework should be reviewed periodically to ensure that it is up-to-date and fit for the purpose of achieving defined target outcomes.

Good practice statement 2: Authorisation perimeter

Firms should ensure that the boundaries of authorised activities are clearly defined and understood by relevant business units and control functions. These boundaries should take into account regulatory restrictions, the firm's risk appetite, and internal mandates at various levels, including firm-wide, specific business units, desks, and individual roles.

Commentary

2.1. A clear and traceable audit trail should underpin the process by which trading activity is authorised and the perimeter established.

Trading that does not fall within the perimeter of authorisation is, by definition, unauthorised.

2.2. Firms should have a clear view of any legal or regulatory restrictions that apply to trading activity across their operating jurisdictions, in alignment with their licenses, permissions and regulatory expectations of the legal entities through which they operate.

2.3. Firms should establish and maintain a set of clear and readily identifiable authorisations that establish constraints around the ability to conduct trading activity. This should include consideration of appropriate trade channels, existing products, variations, and/or new products, client type, geographic location or legal entity, trading venue, trading channel, trading capacity and such other restrictions the firm might apply.

2.4. Firms should consider the level of granularity at which authorisations and internal mandates are set to mitigate the risk of authorisations that are misaligned with business strategy and the skills, experience and capabilities of individuals conducting such trading activities. This includes evaluating the appropriateness and detail of the taxonomies utilised to define authorisations, together with the level at which authorisations are granted (e.g. business unit, desk or individual).

2.5. A robust process should be in place to effectively approve, maintain, review and challenge the perimeter of authorised trading activity on an ongoing basis. To meet the expectations of local accountability regimes and local regulatory expectations, firms should consider where local as well as non-local changes to authorisations are required (e.g. the senior management of an impacted booking entity).

Good practice statement 3: Accountability

Firms should assign and document accountable owner(s) and function(s) responsible for the design, implementation, and effectiveness of unauthorised trading controls as well as governance and monitoring mechanisms, ensuring alignment with the broader risk management framework of the firm.

Commentary

3.1. Ultimate accountability for the unauthorised trading framework sits with the heads of the trading businesses. This should be clearly set out in organisational documentation, together with any delegated responsibilities.

3.2. Control functions within both the 1st and 2nd lines should have specific accountability for designing and executing the controls that collectively contribute to mitigating the risk of unauthorised trading.

3.3. The 2nd line should establish effective independent monitoring and review and challenge processes to ensure the unauthorised trading framework remains fit-for-purpose on an ongoing basis.

3.4. Firms should consider how they periodically obtain independent assurance with respect to the effectiveness of the unauthorised trading framework, including through periodic audit reviews and testing.

Good practice statement 4: Roles and responsibilities

Firms should clearly document roles and responsibilities across all components of the unauthorised trading framework. This includes delineating the duties of business units and control functions across the front-to-back lifecycle of a transaction to promote common understanding of how each function's activities and controls contribute to the prevention and detection of unauthorised trading.

Commentary

4.1. Firms should establish both general and job-specific roles and responsibilities for desk heads, trading staff and other roles related to unauthorised trading activity including organisational units and staff across all three lines. Role-specific responsibilities may vary according to the desks, markets, products, other factors and the risks that may arise.

4.2. Firms should ensure that relevant staff and their supervisors are aware of and trained for their roles and responsibilities related to unauthorised trading and the expectations placed upon them. This may be evidenced by requiring formal acknowledgement by staff of their roles and responsibilities. For 2nd line functions, this includes ensuring there is sufficient understanding, skill and authority to engage effectively with the 1st line should concerns arise.

4.3. Roles and responsibilities should be supported by checks and balances including systematically applied segregation of duties, ensuring those responsible for committing, executing and risk managing trading activities cannot also perform or adversely influence critical activities further down the trade lifecycle (e.g. confirmations, reconciliations, payments or settlements). In particular, firms should consider how these responsibilities are appropriately enforced for joiners and movers across business areas and control functions, including through systems access entitlements (see Good Practice Statement 7).

Good practice statement 5: Risk culture, conduct and behaviour

In order to embed a culture of effective supervision and risk management related to unauthorised trading across the organisation, firms should deploy and promulgate appropriate leadership communication, training, measurement and monitoring tools.

Commentary

5.1. Firms should ensure staff are informed and adequately trained on the authorisation parameters governing trading activity and adherence is reinforced by appropriate communications (tone from the top) and support from management.

5.2. Firms should promote the importance of embedding a practice of voicing observations and concerns to support the early identification of potential unauthorised trading activity and ensure that staff feel comfortable in doing so.

5.3. Firms should encourage traders and desk supervisors to promptly self-identify or report significant adverse changes in exposures including unrealised or unexpected losses. This may permit management to address problems at an early stage and preclude potentially greater harm to the firm and/or its clients or customers.

5.4. Firms should ensure there are tools or platforms made available to staff to anonymously or discreetly raise or identify issues (of any nature) to a firm's management without fear of reprisal.

5.5. Firms should deploy comprehensive training programmes focused on the prevention and identification of unauthorised trading, applicable control environments, escalation processes, supervisory expectations and consequences of engaging in or aiding unauthorised trading. Training should be reinforced regularly and, where appropriate, tailored to specific roles or functions (e.g. front office vs. middle office roles).

5.6. Firms should be mindful of the attendant risks arising from factors such as business models and products deployed as well as the design of compensation and incentives, financial or otherwise, on the potential behaviour of staff.

5.7. Managers and supervisors should be alert to the behaviour of staff (e.g. instances of strong resistance before agreeing to adherence), especially when it seems different and out of character or reflecting persistent non-alignment with policy, process and cultural expectations which could reinforce normalising such behaviour. The risks of adverse behaviour under pressure can be assessed at the point of recruitment and at various career development stages (e.g. transfers or promotions) as well as day-to-day.

Good practice statement 6: Consequences

Firms should ensure the unauthorised trading framework outlines the consequences that apply to instances of unauthorised trading reflecting the severity of the actual or potential impact.

Commentary

6.1. Consequences for unauthorised trading activity should be commensurate with the seriousness of the event, its nature, its actual or potential impact internally and externally and other factors.

6.2. Consequences may range from retraining individuals, a reduction in mandate or risk limits, formal disciplinary proceedings, including those that impact performance ratings and compensation (e.g. bonus adjustments), and such other factors as specified by the firm. Significant and egregious instances of unauthorised trading may lead to dismissal.

6.3. Consequences arising from unauthorised trading should be consistently applied across the firm, irrespective of whether these are regulatory breaches or result in profits or losses.

6.4. The board and senior management, as appropriate, should have a periodic overview of how consequences are considered and applied to ensure they are appropriate, fair and consistent.

Controls and monitoring

Good practice statement 7: Pre-trade and point-of-trade controls

Firms should employ a range of pre-trade and point-of-trade control mechanisms to mitigate unauthorised trading scenarios, including limiting the breadth of book and systems access, and utilising blocks or notifications prior to trade execution.

Commentary

7.1. Firms should establish a risk-based methodology for determining where pre-trade and/or point-of-trade controls related to unauthorised trading are required across the transaction lifecycle, ensuring controls are implemented as close as possible to when and where the risk can best be addressed.

7.2. Firms should employ active trading supervision by sufficiently senior and experienced individuals capable of directly challenging trading activity or P&L attribution. This form of pre-trade oversight may result in supervisory intervention that enables undesired activity to be stopped and is an important component of the overall framework.

7.3. Where there is a risk of breaches of authorised or permitted activities, firms should assess whether pre or point-of-trade controls are necessary to prevent such. Controls should be implemented on a proportionate basis, taking into account the nature and materiality of the risk.

Such controls may include:

- Individual entitlements for system access and authorisations, including book and systems access, with consideration given to potentially problematic access combinations (e.g. self-escalation)
- Products and services provided
- Venues or platforms where transactions are executed
- Legal entities where transactions are booked
- Counterparties faced
- Size, price or value of transaction
- Magnitude of risk posed by the transaction
- Official sanction prohibitions

7.4. Firms should ensure there is alignment between regulatory restrictions, licenses, internal authorisations and the controls that enforce adherence, including client onboarding, book access, systems access, pre-trade check mechanisms and point-of-trade notifications or blocks.

7.5. Firms should have processes and controls to ensure those responsible for a given trade are accurately captured and recorded on each trade. The accurate recording of responsible trader(s) is critical for effective post-trade monitoring, addressed in GPS 8 and 9.

7.6. Firms should consider the role of automated and systematic solutions that deploy controls designed to prevent the execution of unauthorised trades.

7.7. Where there is sufficiently low ambiguity over the unauthorised nature of a potential trade, or where the consequences of such a scenario would be significant, firms should consider whether fully preventative measures, including systematic restrictions or hard blocks, are required.

7.8. Where human judgment is required or there are subtleties to the circumstances through which a trade could be viewed as authorised or unauthorised, firms should consider whether point-of-trade alerts or notifications (i.e. soft blocks) would be an effective risk mitigant across the range of trading channels (e.g. including phone trades).

7.9. Where soft blocks are used, firms should monitor their effectiveness. Persistent overrides or overuse of soft blocks can limit their usefulness and could indicate a need to review relevant policies, processes, business drivers, market conditions, data inputs or controls.

7.10. Hard and soft blocks should be reviewed periodically to ensure that they continue to effectively mitigate the relevant risk. For example, signalling or impediment triggers should be suitably calibrated to market activity and pertinent thresholds, or other metrics, and trade parameters (price movement, volume, basket size).

7.11. Firms should periodically review entitlements for system access to ensure that, on a risk basis, they remain appropriate. Firms should consider how independent control functions can be utilised to verify ongoing appropriateness. Certain role changes may warrant full reassessments of system access as a risk management step (e.g. onboarding and off-boarding staff that move between particular functions).

Good practice statement 8: Post-trade controls

Firms should employ a range of controls post-execution that may identify and/or signal potential unauthorised trading.

Commentary

8.1. Post-trade controls should work collectively with pre-trade and point-of-trade controls to detect unauthorised trading. These controls are detective in nature occurring intra-day, end-of-day, T+1 or at a later time. Where practicable, optimal control methods and frequency should be adopted, for example automated rather than manual, intra-day rather than end-of-day. Post-trade controls can be complemented by later stage trend analysis, as described in GPS 9.

8.2. Firms should employ a holistic suite of controls designed to detect operational or unintentional errors, such as trading outside of authorised perimeters or mandates as well as scenarios involving deliberate manipulation or falsification of books and records to illegitimately influence risk and profit and loss.

Such control topics may include, but not be limited to:

- Book and relevant account opening processes and monitoring
- Monitoring of concentrated, large or unusual positions and exposures, e.g. volumes, risk, gains, losses or fees
- Cancelled and amended trades
- Reconciliation and confirmations
- Off-market rates or other elements
- Late and unconfirmed trades
- Extended / unsettled trades
- Unallocated or failed trades
- Margin / collateral e.g. disputes
- Suspense and wash accounts monitoring
- Internal intercompany transaction monitoring
- Actual breaches and near breaches of risk limits
- Trader mandate violations
- New product approval processes
- Income and balance sheet substantiation
- Independent price testing results
- Potentially suspicious behaviours e.g. out of hours, unusual off-premises trading, mandatory vacation avoidance)
- Unauthorised trade bookings, including the use of unregulated entities

8.3. Across products, geographies, and legal entities, controls should be implemented in a manner proportionate to the risk.

Good practice statement 9: Unauthorised trading analytics

Firms should monitor financial and non-financial controls and indicators across the front-to-back trade lifecycle that may identify and/or signal potential unauthorised trading. Consideration should be given to how these indicators may interrelate or aggregate in unauthorised trading scenarios. Risk-based analysis and trend analysis should be employed to highlight linkages between signals and/or potential outliers that warrant further investigation.

Commentary **9.1.** Firms should establish minimum standards for the production of unauthorised trading indicators and metrics, including the quality and granularity of data sets, the frequency of production and timeliness of review.

9.2. In order to identify outlier patterns of behaviour, as well as transactional trends, unauthorised trading analytics should consider metrics at an individual trader level, where practicable, associated with multiple preventative and detective controls operating across the 1st and 2nd lines.

9.3. Firms should enable the aggregation of control metrics undertaken by different functions (e.g. Front Office, Compliance, Risk, Product Control, Middle Office) to build widely scoped unauthorised trading analytics that enable contextualised and risk-based judgements, rather than limiting oversight via review of distinct alerts / control metrics in isolation.

9.4. Firms should enable and support a coordinated, collegial approach to multi-indicator controls across functions to enhance understanding in a manner that is more effective than a siloed approach, increasing the likelihood of identifying patterns of unauthorised trading rather than one-off breaches. This is important for the detection of intentional unauthorised trading, i.e. the fraudulent or deliberate manipulation or falsification of books and records.

9.5. Firms should consider how unauthorised trading analytics can be aggregated and visualised to enable effective consumption and review by those control functions accountable for deep-dive monitoring and assessments alongside Front Office supervisors.

Good practice statement 10: Unauthorised trading controls testing and review

Firms should conduct regular testing of unauthorised trading controls to verify their ongoing effectiveness.

Commentary

10.1. Firms should conduct dedicated periodic reviews and risk-prioritised testing of the design and effectiveness of controls for unauthorised trading in reducing or eliminating targeted behaviour or events.

10.2. Testing should be conducted with consideration of both trading parameters that are representative of normal, day-to-day trading as well as unusual trades or trading circumstances that are more likely to cause a control failure.

10.3. Periodic testing results should be recorded and reflected in management reporting at the appropriate level where corrective action can be discussed and initiated if needed.

10.4. Relative to the nature, scale and complexity of the business, firms may, on a risk basis, wish to consider using their own scenarios and simulating unauthorised trading activities to test how their systems and controls work in prevention or detection.

10.5. Firms should ensure the results of control testing activities demonstrably feeds back to the design and operation of their unauthorised trading controls and monitoring.

Good practice statement 11: Horizon scanning, scenarios and stress-tests

Firms should, on an ongoing basis, and proportionate to their size and complexity, identify and assess the potential unauthorised trading scenarios that may occur, informed by recent or historic industry events, internal events and the relative strengths and weaknesses of the control environment.

Commentary

11.1. Firms should conduct periodic reviews of market developments as well as internal events with the objective of identifying potential new forms of unauthorised trading as well as their preparedness for such events.

11.2. Reviews should include "what if" scenarios which are deemed worthy of attention followed by gap analyses against existing policy, procedures, controls and action plans / playbooks.

11.3. Firms should consider additions to their suite of financial and non-financial controls to address potential new unauthorised trading risks arising from horizon scanning and related efforts.

Intervention and Reporting

Good practice statement 12: Escalation

Firms should be prepared to deal with a potential or actual unauthorised trading event expeditiously by ensuring that escalation channels and procedures are in place, including the requirements for rapid engagement with senior management and, where needed, other functions such as risk, compliance, legal, and human resources.

Commentary

12.1. Firms should have documented procedures for the escalation and resolution of actual or suspected unauthorised trading or weaknesses in policy, process, controls or behaviours that could give rise to such adverse events.

12.2. Firms should ensure that staff and supervisors are aware of the escalation process, including any nuances for escalations that may need to be made across organisational divisions or locations.

12.3. For high-risk concerns that warrant the immediate attention of senior management, firms should ensure procedures and channels are designed to achieve timely escalation.

12.4. Responses should include coordinated activity across the three lines and senior management, proportionate to the significance or materiality of the event.

12.5. Firms should have arrangements for supervisees to escalate concerns outside of their supervisory chain of command, such as directly to human resources or via an anonymous 'Speak Up' channel.

Good practice statement 13: Management information

Firms should establish periodic management reporting on the unauthorised trading framework, tailored to the needs of relevant stakeholders including supervisors, control functions, business leadership and executive management or board committees. Such reporting should incorporate a regular process for validating data quality.

Commentary

13.1. Firms should continuously enhance data quality, both upstream and downstream, to ensure that unauthorised trading controls are operating effectively and management information (MI) reports can be relied upon.

13.2. Firms should regularly provide management with digestible, action-oriented information on the controls used to detect or prevent unauthorised trading. This reporting should reflect the accountabilities, roles and responsibilities of the recipients.

13.3. Identified or potential unauthorised trading activity should feed back into policy and process updates as well as staff training ideally conducted on risk-adjusted timetable.

13.4. Firms should identify who the intended audience for the MI as well as who is best placed to review it. The MI should be carefully curated to align with the audience, purpose and target outcomes. Board level reporting should be meaningful for oversight purposes without being burdensome.

13.5. Firms should consider how the ongoing effectiveness and quality of MI is continually reviewed and improved.