12 October 2010

Level of application: All institutions

Guidelines on the management of operational risks in market-related activities

1. Introduction

1. In accordance with Article 22 of Directive 2006/48/EC (CRD), *"home Member States shall require that every credit institution have robust governance arrangements which include a clear organisational structure with well defined transparent and consistent lines of responsibility, effective processes to identify and manage, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative and accounting procedures. These arrangements, processes and mechanisms shall be comprehensive and proportionate to the nature, scale and complexity of the credit institution's activities".*

2. As with any type of business, appropriate governance mechanisms and internal control systems are crucial for managing risks, preventing the occurrence of operational risk events in the context of market-related activities and for mitigating their impact on the institution. Market-related operational risk events are often associated with rogue trading, unauthorized or leverage operations, complex instruments, new products, model risks and the rapid increase in the number of operations. Some institutions have focused their attention on market risk and have not recognised sufficiently the importance of appropriate operational risk management.

3. Past and recent cases show that when institutions do not adhere to basic principles of sound internal governance, the severity of operational risk events in market-related activities can be very high, jeopardising the institution's earnings, the existence of the particular business area, or even the existence of the whole institution.

4. Against this backdrop, the high level principles on Internal Governance set out in Section 2 of the "Guidelines on the Application of the Supervisory Review and Evaluation Process (SREP) under Pillar 2" (CEBS paper issued in January 2006), the "High-level Principles for Risk Management" (CEBS

paper issued in February 2010) and the "High-level Principles for Remuneration Policies" (CEBS paper issued in April 2009)[1], are the primary reference tools institutions should consider at a general level for risk management and risk control, including the prevention and mitigation of operational risks in market-related activities.

5. The objective of this paper is to complement this framework of high-level guidelines with more specific principles and implementation measures for the identification, assessment, control and monitoring of operational risks in market-related activities.

6. In particular, this paper aims to highlight supervisory expectations relating to specific arrangements, procedures, mechanisms and systems in trading areas that could prevent or mitigate operational risk events. The subject is addressed from three different angles, described in the following sections - Governance mechanisms (Section 2), Internal controls (Section 3) and Reporting systems (Section 4).

7. People, processes, systems and external events are drivers of operational risks. Management efforts and actions aimed at preventing or mitigating operational risks in market-related activities are directed to these drivers, while these drivers are, at the same time, used to manage market risk positions. Due to this interconnectivity, some principles could be understood as also being directed to market risk or even credit risk management.

8. However, the focus of the paper is limited to the management of operational risks in market-related activities and is not intended to cover the management of the other types of risk that usually characterise this kind of business[2]. The Guidelines on the Scope of Operational Risk and Operational Risk Loss (CEBS paper published in September 2009, labelled as the "Compendium"[3]), which contain detailed guidelines on the boundaries between operational risk and market risk, may help to clarify the subject of operational risk in market-related activities, including the

---

[1] The Guidelines on Supervisory Review Process (GL03), the High Level Principles for Risk Management and the High Level Principles on Remuneration Policies can be downloaded at: http://www.c-ebs.org/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx, http://www.c-ebs.org/documents/Publications/Standards---Guidelines/2010/Risk-management/HighLevelprinciplesonriskmanagement.aspx and http://www.c-ebs.org/getdoc/34beb2e0-bdff-4b8e-979a-5115a482a7ba/High-level-principles-for-remuneration-policies.aspx

[2] For instance, core principles of market risk management require firms to set appropriate limits on their net positions and to strictly monitor, utilise and comply with these limits. The internal governance elements and needs that stem from these principles (e.g. the definition of appropriate risk monitoring and risk control systems) fall outside the scope of this document.

[3] The guideline is published within the "Compendium" under the following link: http://www.c-ebs.org/getdoc/0448297d-3f85-4f7d-9fa6-c6ba5f80895a/CEBS-2009_161_rev1_Compendium.aspx

scope of operational risk losses[4] and hence better position the scope of this document.

9. More generally, institutions need to manage all the risks appropriately. As a result, the management of operational risks is sometimes undertaken by staff in the business units, while the accountability for the implementation of an appropriate operational risk management framework is located in the management body or in the control and support functions (see paragraph 12 below), in particular, in the independent operational risk management function.

10. While these guidelines are relevant to all institutions, the principle of proportionality should be taken into account in their application[5]. Accordingly, the level of sophistication of governance mechanisms, internal controls and reporting systems for the management of operational risks in market-related activities should be commensurate with the complexity and magnitude of these activities within the individual institution.

11. CEBS expects its members to implement the guidelines on the management of operational risks in market-related activities by 30 June 2011. CEBS is aware that their implementation will encompass not only the amendment of national guidelines, but also supervisory processes.

2. Governance mechanisms

Principle 1. The management body[6] should be aware of the operational risks, actual or potential, affecting market-related activities. It should develop and maintain an organisational structure, internal controls and a reporting system suitable for the identification, assessment, control and monitoring of operational risks in market-related activities.

12. Consistent with paragraph 602 of CEBS's GL10, the management body may, where appropriate, establish specific Committees and delegate to

[4] With reference to the interaction between operational risk and the other Pillar 1 risk types, for AMA institutions the CRD deals with the boundaries between operational risk and credit and market risks with different treatments for the two types of boundaries. While credit-related operational risk losses are excluded from the operational risk capital requirement (as long as they continue to be treated as credit risk for the purpose of calculating minimum regulatory capital), operational risk/market risk boundary events are included in the scope of operational risk for regulatory capital calculation.

[5] According to the principle of proportionality, guidelines for institutions and supervisors are to be applied in a proportionate manner to reflect the nature, scale and complexity of the activities of the institutions (see CEBS Guidelines on the Application of the Supervisory Review Process under Pillar 2).

[6] The term 'management body', which represents the top management level of an institution, is used in this document to embrace different structures, such as unitary and dual boards (see also the above mentioned GL03 paper)

them certain aspects of the framework for the management of operational risks in market-related activities. These Committees should have:

- the material and human resources necessary to carry out the required tasks. In particular, members of the "control and support functions" (see paragraph 13 below) should be pivotal to these Committees - either due to the number of their representatives or due to their roles in the committee - so as to be able to effectively challenge the activities undertaken by the front office;

- widely drawn scope to allow them to consider all the issues that are pertinent to ensuring the effectiveness of the management of operational risks in market-related activities. This scope should extend to examining the institution's policies relating to recruiting, assignments, ethics codes and compensation – including bonuses;

- access to the output of reporting and internal control systems, including any alerts transmitted to supervisory authorities; and

- responsibility for supporting the management body in its decisions on identifying, assessing, controlling and monitoring operational risk.

13. The organizational structure should provide for adequate segregation of duties between the front office and the functions in charge of supporting, verifying and monitoring transactions (e.g. operations, settlements, legal, finance, risk control, compliance and internal and external audit, hereafter called "control and support functions"). Institutions should consider whether an appropriate physical segregation of the functions would enhance the implementation of rules regarding the segregation of duties (e.g. front office staff should not have physical access to back office IT systems, printers and documentation in the absence of back office staff). Duties should be allocated appropriately to control and support functions and individuals. It should be ensured that, in handling business transactions, activities that provide scope for conflicts of interest are carried out by different persons.

14. Institutions should carefully consider how the control and support functions are organised in relation to the areas they monitor and verify. If the control and support functions are fragmented between several units, this should be counterbalanced appropriately to ensure that controls are effective, transparent and cover all the significant activities. Institutions should consider that:

- the integration or co-operation of control and support functions, in particular including finance and risk control, may increase the level of surveillance and control of the trading activities and help to create a holistic view of such activities;

- control and support functions aligned with business lines may lead to the emergence of questionable practices (e.g. in the confirmation process and margining areas) that might be better challenged if entrusted to a wider unit. However, institutions need to assign and formalise the responsibilities for the latter in a way that ensures that

gaps in the control framework are avoided. Appropriate checks (e.g. by internal audit) should be performed to ensure that the different control and support functions cover all significant activities and that efficient processes have been implemented; and

- the sound organisation of key post-trade processes, notably in the back office and accounting areas, is crucial for implementing appropriate controls.

Principle 2. The management body should promote, particularly in the front office, a culture designed to mitigate operational risks in market-related activities.

15. High professional standards and a sound risk culture should be promoted particularly in the front office in a way that supports professional and responsible behaviour. This should include, but is not limited to, developing and implementing appropriate policies and procedures setting standards (often in the form of a "code of conduct") for relations between traders[7] and their counterparts, and training procedures.

16. Appropriate policies and procedures relating to leave requirements and staff movements should be developed, implemented and regularly monitored. In particular:

    - a policy establishing a minimum absence requirement of at least two consecutive weeks' leave for traders (via a vacation, "desk holiday" or other absence from the office or trading, including a prohibition on using mobile devices to access trading systems) represents sound practice, so that traders are physically unable to mark or value their own books, this responsibility being carried out by a different person during those periods; and

    - if staff change job positions between front, middle and back offices or IT this should be properly tracked. The potential risks stemming from a change in positions, especially if occurring within the same activity or product line, should be counterbalanced by appropriate control procedures.

Principle 3. Senior management[8] should ensure that they, and the staff in the control and support functions, have the appropriate

[7] The term "trader" also refers to other staff involved in front office market-related activities such as "structurers" or "dealers".

[8] According to paragraph 413 of the Guidelines on Validation (http://www.c-ebs.org/getdoc/5b3ff026-4232-4644-b593-d652fa6ed1ec/GL10.aspx) the management body represents the top management level of an institution, and senior management (which is not defined in the CRD) should be understood to represent the level of management below the management body.

understanding, skill, authority and incentive to provide an effective challenge to traders' activities.

17. Senior management need to acquire, maintain and deepen their knowledge and skills to fulfil their responsibilities. This includes having a good understanding of the potential and actual operational risks within market-related activities, including operational risk exposures in the front office, in the settlement processes and in new products and processes.

18. To support the effective implementation of control processes and procedures, staff in control and support functions should be appropriately qualified. This includes appropriate recruiting policies and measures to retain qualified staff in control functions, as well as providing appropriate training.

19. Consideration should be given to the possibility of introducing incentive mechanisms at the level of the control and support functions to reward the sound conduct of those functions. Staff members engaged in control functions are independent from the business units they oversee and should therefore be compensated in accordance with the achievement of objectives linked to their functions, independent of the performance of the business areas they control.

Principle 4. Operational risk should be taken into account in setting objectives for, and in the assessment of, an individual's or business unit's performance in market-related activities.

20. Institutions should find the appropriate balance between the profitability drivers and operational risk culture or risk tolerance at the different levels of the hierarchy, starting from the front office.

21. For example, institutions may set objectives for business managers and traders or business units in terms of a maximum acceptable level of operational risk and/or take into account the level of operational risk in the attribution of their variable remuneration. This could be done by considering the observed level of operational risk losses or by setting operational risk limits on the basis of key risk indicators, scorecards, alert levels, etc. The objectives and limits should be in line with the risk strategy and the overall risk appetite.

Principle 5. Proactive behaviour against actions which are considered as fraud[9] or suspicious activities in market-related activities should be a key element of internal controls and reporting systems.

[9] For the scope of these guidelines "fraud" encompasses internal and external fraud as defined in Dir 2006/48/EC, Annex X, Part V. This includes losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or

22. Institutions should analyse possible sources of fraud and define anti-fraud measures, taking into account the fraud exposure resulting from their market-related activities. Depending on the size and type of exposures to fraud within the market-related activities, some measures may be part of the daily control processes within the market area, while others may be performed on a less frequent but, in any case, regular basis.

23. The following examples of detection and prevention of fraud and suspicious, activity, while referring to market-related activities, could be valid and applicable to any business of an institution:

- use of scenarios to increase understanding of how fraud might occur at various levels within the organisation and of the institution's ability to detect and manage internal and external fraudulent activities;
- regular fraud incident review and analysis, for example, by the use of a lessons-learnt process for analysing fraud events (e.g. password violations, other IT security issues, limit breaches) and implementing measures to reduce the probability of re-occurrence;
- a framework enabling the testing of fraudulent intrusions in the firm's infrastructure including inappropriate usage of passwords, user profiles and production of fictitious documents or booking of fictitious positions;
- a specific programme for identifying the risk of fraud and developing a mapping of risks of fraud which can be a part of the integrated framework of risk management that is coherent with the risk assessment used for operational risk;
- measures to increase the staff's fraud awareness;
- appropriate definition of access rights and an infrastructure providing appropriate protection from undue interference of the data used for post-trading processes (for instance via physical or logical separation of the infrastructure used for trading and post-trading processes) and
- setting of triggers for reviewing operational risk exposures, including integrated and effective alert/warning systems allowing management to identify and respond to any fraudulent or suspicious activity in a timely manner. In particular sensitive processes, businesses and product lines should be covered.

24. Escalation processes should be in place to inform the appropriate level of management about incidents which exceed pre-determined risk tolerance levels or have certain characteristics, including those due to actual fraud or suspicious activity.

---

company policy, excluding diversity/discrimination events, which involves at least one internal party (internal fraud) and losses due to acts of a type intended to defraud, misappropriate property or circumvent the law by a third party (external fraud).

25. The supervisory authority should be notified of cases of fraud or suspicious activity exceeding a given threshold or having certain characteristics (making use, for example, of ad hoc templates required by the supervisory authority or adopting COREP templates where they have been introduced).

3. Internal controls

Principle 6. Traders should initiate transactions only when these are compliant with their set terms of reference. Minimum standards for the initiation and conclusion of transactions should be followed.

26. The existence of appropriate terms of reference describing the activity of each trader or group of traders is an essential prerequisite for the sound management of market-related operations. It gives to each of the parties involved - traders, managers at all levels and control and support functions - the means of verifying that the nature, volumes and overall size of the transactions dealt with by each trader or group of traders are within the limits and strategy defined by the institution's management.

27. One objective of an authorized trading framework for the front office should be to formalize rules for traders enabling them to ensure they operate within a clear framework. Examples of deliverables could include lists of permitted products, market risk limits and specific responsibilities (e.g. oversight guidelines for desk heads). An appropriate process of escalation and challenge should be in place to investigate any breach of permitted activities or limits.

28. Trades which are not in line with market conditions (e.g. deals concluded with roll-overs of historical rates) should, in general, be limited in number and nominal value and adhere to internal rules governing the type, scale and structure of the trades, and the characteristics of, and communication to, the counterparts. The deviation from market conditions should be clearly visible from the documentation and reported to the relevant control and support functions and, if necessary, to senior management.

29. The terms of reference and minimum standards for the initiation and execution of trades should be subject to strict monitoring by the control functions. In particular, immediately after the conclusion of the trades, the relevant data and documentation should be passed to the control and support functions to allow for their proper verification, confirmation, settlement and reconciliation.

30. Traders' conversations relating to transactions should be voice recorded and the recordings retained for an appropriate period.

Principle 7. Documentation requirements for trading activities should be properly defined. Legal uncertainties should be minimised so that the contracts are enforceable as far as possible.

31. Institutions should determine their document requirements in advance of trading. In particular, if a counterparty requires special arrangements – such as third party payments or prime brokerage services – those arrangements should be agreed upon and documented in advance of trading as far as feasible.

32. Where a master agreement is used with a counterparty it should, whenever possible, contain legally enforceable provisions for "closeout" netting and settlement netting.

Principle 8. As a general rule transactions should be initiated and concluded in the trading room and during trading hours.

33. Trading outside the business premises (for instance by using mobile devices) should only be permitted within the scope of internal rules that specify, in particular, the authorised individuals, the scope of permitted trading and the recording of trades. Those rules should consider the operational risks which stem from trading outside the business premises. The trades should be identified and reported as soon as possible for review by the relevant control functions.

34. Trades concluded after the cut-off time for settlement (late trades) should be marked as such and included in that day's positions (including subsequent settlement) if they result in substantial changes. The transaction data and documentation relating to late trades should be reported immediately to the relevant control functions.

Principle 9. All relevant positions, cash flows and calculations associated with a transaction (for example trading book positions, profits and losses and contingent cash flows) should be clearly recorded in the institution's IT systems with a documented audit trail.

35. Audit trails are crucial for the institution's post-trade controls which should be regularly performed by the control and support functions (e.g. operational risk managers, risk control, finance, internal or external auditors) and the reconciliation of operations. Also, the accounting for transactions and cash flows requires strict monitoring and internal controls.

36. The audit trail should allow for the tracing of cash flows both downstream and upstream at a sufficiently granular level (e.g. traders, books, products and portfolios).

37. Ideally, the audit trail should start with the trader who initiated the transaction and go all the way to the counterparty which received or paid for the transaction. However, an automated front-to-end audit trail (corresponding to a readily available "push button" audit trail) may not be required as long as the audit trail sufficiently documents the input and change of data regarding transactions (including settlement), positions, valuations and other relevant issues, and ensures the complete audit trail

(including the responsible manager or traders) can be produced either on demand or within an acceptable period of time.

Principle 10. Institutions should ensure that they have an appropriate framework of controls over the relationships between traders and their market counterparts.

38. Institutions should define and implement appropriate controls and procedures from the opening of the relationship to the daily follow-up and monitoring of traders and associated counterparts, as well as for internal trades[10], dormant portfolios (i.e. portfolios that are no longer monitored by the front office) and dummy counterparts (that are pending allocation).

39. The relationship and connection between professional clients or eligible counterparties and front office staff should also be considered. Institutions should monitor these relationships (including compliance with standards and a "code of conduct" (as mentioned in paragraph 15) e.g. monitoring ex-gratia payments, any other significant payments made or received outside the scope of the contractual arrangement) and how operational risk events are treated by the front office. In particular, the fact that the relationship is managed by the front office may mean that institutions do not react with the necessary scrutiny and diligence to alerts coming, for instance, from the middle or back offices of their counterparties. Pricing issues, legal issues, trade and settlement queries as well as error and claims management should be directed to and carried out by the control and support functions or by dedicated business staff independent from the trading function under the oversight of the control functions.

Principle 11. Confirmation, settlement and reconciliation processes should be appropriately designed and properly executed.

40. Confirmation, settlement and reconciliation processes should be defined to prevent gaps and points of weakness and to help identify and resolve breaks. The appropriateness of these processes should be regularly assessed.

41. The control and support functions should remain accountable for the confirmation, settlement and reconciliation processes. In performing the pertinent activities of control, these functions may require additional information from the front office (e.g. for clarifying issues and for obtaining additional data or information).

42. Institutions should have a rigorous and reliable process for confirming the terms and conditions of transactions with external counterparts in a timely

[10] Internal trades refer both to trades between legal entities belonging to the same group (inter-company trades) or between books/desks of the same legal entity.

manner and with unambiguous meaning[11], so as to avoid the accumulation of unreconciled transactions which represent a major source of risk. This can include automatic reconciliation systems, if they provide the same level of confidence.

43. In cases where the completion of full documentation and confirmation processes is pending, the use of affirmation processes should be considered to prevent operational risks, in particular fraud risks, by demonstrating the existence of the transaction (e.g. additional telephone affirmations between the control and support functions of the institutions involved in the trade). Unaffirmed and unconfirmed deals should be reported appropriately.

44. As a general principle, the confirmations should be exchanged with counterparties' relevant control and/or support functions and matched for all market transactions, including those that will be netted and those conducted through third-party advices, such as Reuter's logs, EBS trade tickets and voice broker advices. Exemptions from this principle should be possible only in exceptional cases (e.g. with certain counterparties or for specific transactions) which should, in any case, be clearly set out, fully documented, reported and properly assessed by the control functions.

45. Appropriate processes and procedures for the settlement of transactions should be defined and implemented to mitigate effectively the operational risks inherent in such activities. Institutions may consider the following elements, amongst others, that serve this purpose:

    - the authorization of inputs by the back office;
    - payment/settlements carried out against independent documents;
    - reconciliation between front office and back office systems; and
    - reconciliation procedures independent of the processing functions.

46. Controls should include daily reconciliations of positions and known cash flows across own systems (front office, risk, settlement and general ledgers) and with external parties. These reconciliations should include all events attached to the transactions including amendments, cancellations, exercises, resets and expiries.

47. Internal trades (see footnote 10) should be subject to conditions and controls, creating the same level of confidence as those in place for trades with external counterparts. In particular, when not subject to margining or physical settlements, both sides of the trades should be reconciled daily on their key attributes.

48. For over-the-counter transactions (OTC) in particular close attention should be paid to the following points:

---

[11] This can be achieved, for instance, by resorting to standard confirmation formats or electronic confirmation matching.

- the use of contracts that are as standardised as possible, for example using model contracts developed by industry associations;

- the availability of a specific process, internal to each institution, which would trigger the intervention of the appropriate unit outside the front office if clauses of a contract deviate from the clauses of the model contract or if unamended model contracts are used for bespoke transactions;

- an appropriately staffed function to verify that the contracts conform to the originally negotiated terms and that those conditions are drawn up and signed. Any change, cancellation or reaction by the counterpart should give rise to a suitable review process. This particularly concerns novations that involve the intervention of third parties who were not parties to the original contract;

- the secure retention of documentation (e.g. by the use of a trade repository capable of preserving a copy of each contract for the purpose of establishing authenticity in the event of litigation);

- frequent review of the number and duration of failed, amended and cancelled transactions, and the establishment of a process to ensure that transactions are confirmed within an appropriate timeframe. Specific consideration should be given to certain unconfirmed OTC trades which contain characteristics that pose greater risks (such as OTC trades with no near term cash flow with a counterparty with whom there are no collateral arrangements in place);

- reporting of an exhaustive list of transactions where the settlement failed, adapted to the activities of the institution, with warning systems alerting the relevant control and support functions of the people directly involved in the transactions; and

- reporting to the appropriate control function of any anomalies and operational risk events discovered within OTC trades, either originated within the institution or stemming from external parties/outsourcers.

Principle 12. Institutions should ensure that their margining processes are working properly and that any changes are reconciled with the relevant positions on their books.

49. Large positions require large margin or collateral calls. Therefore, institutions should reconcile margin and collateral calls to help ensure that the margin calls are correct and that the positions on the book are accurate. Institutions should implement appropriate controls, including alert procedures, to ensure that collateral and collateralised counterparty risks are followed up appropriately. When an anomaly is identified, institutions should be able to trace the issue back to the transaction and the trader.

50. As far as possible, institutions should have in place real-time credit systems able to calculate credit lines and usage information as trades are initiated.

Institutions need to be able to aggregate exposures globally across all trading desks and to accurately reflect the effect of netted transactions.

51. In the derivatives trading environment, substantial changes in positions are usually executed through either listed products or collateralised OTC contracts. Any significant inconsistency between the amounts and/or the direction of OTC mark-to-market and collateral calls can, therefore, be a sign of inappropriate trading book management or maintenance. A close co-ordination between the control function (responsible for P&L and independent price verification) and the collateral management function is necessary.

Principle 13. Sources of operational risks in market-related activities should be properly identified and monitored with the appropriate level of scrutiny, intensity and timeliness.

52. Institutions should understand which aspects lead to the P&L generated in the trading area. The P&L should be plausible in the context of the trading mandate and market developments. Major implausibilities discovered within the P&L should be further analysed to see if they are caused by operational risk events. In particular monitoring of anomalies such as cancellations, amendments, late or off-market trades should be integrated into the daily and monthly P&L examination processes. Substantial trade amendments should be formally reported to the market and/or credit risk control functions. P&L attribution is a key control for understanding the risk in a trading operation, especially where more complex products or basis risks are traded. Moreover, institutions should ensure that any large positions in the P&L, and large P&L amounts, are adequately analysed from day one, including those which have been cancelled or amended.

53. Unusual and remarkable transactions, anomalies in confirmation and reconciliation processes, errors in recording, processing and settling transactions, along with cancellations, amendments, late trades and off-market rates should be monitored with sufficient granularity by the relevant control and support functions and reported to the appropriate levels in the hierarchy. The monitoring procedures and their effectiveness should be reviewed periodically.

54. The use of technical accounts (e.g. suspense accounts) should be analysed and understood by middle and back offices and challenged when used inappropriately by the front office. Any suspicious activity across these accounts should be escalated to, and acted on, by senior management.

55. Furthermore, institutions should review sensitive accounts (e.g. pending accounts) and implement appropriate controls to ensure that they are followed up appropriately. Institutions should determine the appropriate frequency of monitoring for market-related activities, depending on the object of the monitoring (e.g. traders or group of traders, books, products, portfolios and processes) and their risk profile.

56. In order for controls to have a deterrent effect and to allow for remedial action to be taken early, monitoring should in all cases be performed with the frequency necessary to detect inappropriate activity or anomalous behaviour as soon as possible. Introducing only monthly controls on trading books (e.g. funding cost allocation, internal and intercompany trade reconciliations, suspense accounts control and reporting) may lead to an undue delay in the detection of anomalies.

Principle 14. The nominal value of transactions/positions should be kept under strict control for monitoring operational and counterparty risks through the definition of pertinent limits and/or participation in initiatives for the novation of contracts.

57. The traditional market risk controls of the net transactions/positions (e.g. limits on net amounts set at traders, books, products and portfolios levels) should be supplemented with controls over the nominal values of the transactions/positions where needed, since net figures do not necessarily identify the operational risks or counterparty risks underlying those transactions/positions. Such controls could encompass alert procedures, the surveillance of high volume trades or unusual trading activities, and controls based on volumes or limits. Exemptions from this principle are possible only in exceptional cases, which should, in any case, be clearly set out, fully documented and properly assessed by the control functions.

58. Regardless of the nature of the trade (i.e. internal or external), limits on the cumulative nominal values of the transactions/positions at the required level of granularity (e.g. traders, books, products and portfolios) should be appropriately set, updated in a timely manner and periodically reviewed. The control and support functions should monitor the front office's compliance with limits.

59. In some jurisdictions, participation in schemes for the novation or "tear-up" of contracts may be useful in reducing the notional position and the operational and counterparty risk exposures of the institution without significantly changing its market risk position.

Principle 15. Information systems in the trading area should be appropriately designed, implemented and maintained so as to ensure a high level of protection in market-related activities[12].

60. Generally, access to information technology resources should be controlled by a procedure that has been formally endorsed by senior management. This procedure should include periodic reviews of access requirements, and should itself be updated as often as necessary to keep up with advances in

[12] The management of operational risk in the context of IT systems is an area that could be part of the future work of CEBS.

the information systems technology used by the institution. Compliance with these rules should ensure that assigned functions match authorised access and should also prevent access to information systems for fraudulent purposes.

61. The level of security of these systems should be regularly tested and monitored in order to prevent non-authorized access.

4. Internal reporting system[13]

Principle 16. The operational risk reporting system for market-related activities should be designed to generate appropriate warnings and should alert management when suspicious operations or material incidents are detected.

62. Operational risk management systems should set criteria, indicators and thresholds enabling the identification of material incidents detected by internal control procedures. These elements should be adapted to the activity of the institution and should cover potential losses even when they have not yet materialized. Material incidents should be reported to senior management without delay. A prerequisite for this is that institutions keep track of significant operational risk losses in market-related activities and analyse those losses with regard to possible interconnections (i.e. losses based on one loss event or root cause).

63. Whistle-blowing and alert-monitoring may help to detect abnormal trading patterns and to assist in the investigation of incidents detected by the internal control system. These should also include escalation of warnings and concerns expressed by exchanges, brokers, clearers and custodians and procedures ensuring that all questions from external entities are thoroughly investigated.

Principle 17. Institutions should ensure the quality and consistency of their internal reports and that they are appropriate to the needs of the recipients for which they are intended.

64. Different levels of management and/or control have information needs that vary in both content and frequency. Business units should produce documents to meet their own management and control needs and for reporting to other units. These documents can be standardised or they can respond to specific needs which evolve over time. Information provided needs to be sufficient to serve the intended purpose.

65. Institutions should ensure there is sufficient quality and adequate explanation in the internal reports sent to the different levels of the

[13] This Section, while drafted for market-related activities, is generally valid and applicable to any other business area of a firm.

hierarchy to make them a key element of a robust internal control system. For example, the reports aiming to detect operational risks in market-related activities should be produced under the responsibility of the control functions. If the report is produced outside the control functions, they should specify the format and content and have appropriate controls in place to ensure that reporting requirements are complied with. In addition, these reports should make use, to the maximum extent possible, of alternative inputs and sources adopted by the front office for initiating and concluding trades.

66. It is essential that the information circulating between different departments is well structured, particularly in complex organizations, in order to avoid delays or alterations in the communication of crucial information caused by the filtering role played by intermediate layers.

67. Reports should be understandable and should contain well articulated and relevant calls for corrective actions to be implemented at all levels of the organization. The implementation of corrective actions should be tracked appropriately. The latter, as well as the effectiveness of the reporting framework should be within the scope of internal audits.