ACH Clearing Rules
Guidance Note No. 13

KEY TOPICS

1. Risk Management Framework document
2. Key Risks and Internal Systems Statement

ACH Clearing Rules

1. 4.4
2. 4.5

Guidance Note History

Issued:
14 February 2006

Previously:
15 December 2004

Risk Management Framework Document and Key Risks and Internal Systems Statement

Purpose

The purpose of this Guidance Note is to provide Direct and General Participants with a recommended Risk Management Framework document and issue a revised Attestation by Directors / Responsible Executives – Key Risks and Internal Systems Statement.

Risk Management Framework

In March 1999, guidance on a recommended Risk Management Framework was provided to all Participants as part of the Capital Liquidity Handbook. This Framework has now been revised to provide an up to date discussion of risk management issues, including Corporate Governance.

ASX has prepared the Risk Management Framework to heighten the awareness of Participants of the need for adequate risk management and the principles and concepts associated with risk management.

The paper describes a Participant's potential sources of risk, the corresponding risk management methods, and the risk management responsibilities within the Participant's organisation.

All Direct and General Participants should undertake a comprehensive review of their current risk management framework against the principles outlined in that paper to ensure they are able to maintain a standard of operation commensurate with the requirements of a Direct and General Participant to enable the Directors / Responsible Executives to be in a position to sign the key risks and internal systems statement (see below) on an annual basis.

Key Risks and Internal Systems Statement

Existing Participants

All Direct and General Participants would be familiar with the existing Key Risks and Internal Systems Statement requiring lodgement at the time the annual audited financial returns are due. To date this statement has focussed on the systems and procedures in place to maintain compliance with the capital requirements.

The revised Key Risks and Internal Systems Statement continues to require sign off in relation to the capital requirements but additionally now requires acknowledgement that systems and procedures appropriate for the nature and extent of the trading activities undertaken exist, are operating effectively and the Participant is complying with the rules.

Commencing with all financial year-ends beginning after 1 January 2005, the revised Key Risks and Internal Systems Statement will be required to be lodged by all existing Direct and General Participants at the time their annual audited financial returns are due.

The Key Risks and Internal Systems Statement is provided at ACH Clearing Rule Procedures, Annexure 4.4.3-2.

New Participants

Commencing immediately, all new Direct and General Participants will be required to lodge revised Key Risks and Internal Systems Statement as part of their application.

Qualification

ACH has published this note to promote commercial certainty, and assist Direct and General Participants. Nothing in this note necessarily binds ACH in the application of the Rules in a particular case. In issuing this note ACH is not providing legal advice and Direct and General Participants should obtain their own advice from a qualified processional person in respect of their obligations ACH may replace this Guidance Note at any time. Readers should contact ACH to ensure they have the latest version.

RISK MANAGEMENT FRAMEWORK

ASX

AUSTRALIAN STOCK EXCHANGE

ASX DISCLAIMER

The Risk Management Framework document has been prepared to heighten the awareness of Participants of the need for adequate risk management and the principles and concepts associated with risk management.

Whilst ASX has taken every care in the preparation of this document and believes it to be accurate and reliable at the date of publication, no warranty is given or implied as to its accuracy or completeness. In issuing this document, ASX is not providing legal advice and Participants should obtain their own advice from a qualified professional person in respect of their individual situations and obligations. However, ASX, its subsidiaries and their employees do not make any representations or warranties regarding the accuracy, reliability or completeness of the document and will not be liable for any loss arising from or in connection with use of, or reliance on, any of the document.

© 2004 Copyright in the document vests in Australian Stock Exchange Limited.

1. INTRODUCTION

a) WHY IS RISK MANAGEMENT IMPORTANT?

> "The collapse of Barings was significant not just from the perspective of the customers of Barings itself, but also for the broader impact which it had on attitudes within the financial services community and among the regulators. Barings was a bank which was supervised by the Bank of England, one of the most highly respected bank supervisors in the world, and which the day before its collapse had apparently been well capitalised and profitable. Indeed, the chairman of Barings, Peter Baring, had recently told Brian Quinn, the director of the Bank of England responsible for banking supervision, that "it is not actually terribly difficult to make money in the securities business". Yet Barings had seen its capital wiped out in a few days by a lack of control over one employee in a relatively small office on the other side of the world.
>
> *What Barings showed in the clearest terms was that the real issue was not derivatives in general, or over-the-counter derivatives in particular. The real issue was about the quality of management and control required in modern international financial markets*."[1]

The above quote precisely identifies the importance of risk management. An analysis of all the spectacular losses suffered by organisations around the globe over the last two decades, which on the surface may have arisen from adverse movements in the markets in which positions were held were in fact the result of a break down in, or total lack of an effective risk management and control environment within the organisations concerned.

b) CORPORATE GOVERNANCE

The most important and critical component of the risk management framework is the structured and disciplined oversight of the overall operations of the organisation. This includes oversight at both the board level and at the management level.

The board is at the centre of corporate governance, and it has the ultimate responsibility for the organisation's sound and prudent management. It is the board's responsibility to review and approve business strategies and policies, to determine the organisation's risk tolerance, approve the risk management strategy, and to ensure that management applies effective risk controls. Delegating authority to board committees or to management does not relieve the board from its responsibilities[2].

---

[1] Goldman, Sachs & Co, SBC Warburg Dillon Read (1998). *The Practice of Risk Management*", Euromoney Publications, p.25.

[2] See also: APRA (2004). *Corporate Governance: A Prudential Perspective*, Speech by John Laker, APRA Chairman.

The ASX Corporate Governance Council has issued a document "Principles of Good Corporate Governance and Best Practice Recommendations" which is available at www.asx.com.au. Included in this document are ten essential corporate governance principles and these are restated below:

A company should:

1. Lay solid foundations for management and oversight
2. Structure the board to add value
3. Promote ethical and responsible decision-making
4. Safeguard integrity in financial reporting
5. Make timely and balanced disclosure
6. Respect the rights of shareholders
7. Recognise and manage risk
8. Encourage enhanced performance
9. Remunerate fairly and responsibly
10. Recognise the legitimate interests of stakeholders

Participants are encouraged to visit the website noted above, review the corporate governance document and consider the detailed guidelines provided in it for each of these ten principles.

The remainder of this paper outlines ASX expectations of best practice in relation to risk management of activities in the Markets, and the Clearing and Settlement facilities conducted by ASX.

c) RISK MANAGEMENT

Risk management is a term that is often used to mean different things. In this paper, risk management refers to the policies, controls, procedures and systems that are necessary for any organisation, no matter how large or small, to be able to effectively manage, monitor and control their exposure to risk. Combined, the policies, controls, procedures and systems form the Risk Management Framework.

> "The implementation of strong and effective risk management and controls within securities firms promotes stability throughout the entire financial system. Specifically, internal risk management controls provide four important functions:
>
> - to protect the firm against market, credit, liquidity, operational, and legal risks;
> - to protect the financial industry from systemic risk;
> - to protect the firm's customers from large financial losses; and
> - to protect the firm and its franchise from suffering adversely from reputation risk.

> Sound and effective risk management and controls promote both securities firm and industry stability which, in turn, inspires confidence in the investing public and counterparties. Securities firms have economic and commercial incentives to employ strong risk management internal control systems. Without such controls, a firm is vulnerable to risk."[3]

2. PURPOSE OF THIS PAPER

Over the past two decades, there have been many studies completed and reports commissioned into the area of financial markets risk management by regulatory bodies around the world such as the Bank of International Settlement's Basle Committee on Banking Supervision and the International Organization of Securities Commissions. Individually, those studies and reports have resulted in the definition of principles and concepts, in the identification of controls and systems that, in aggregate, define a "world's best practice" risk management framework. This paper attempts to draw into one document, those key risk management principles, concepts and controls, to provide Participants with a comprehensive outline of what is considered a "world's best practice" risk management framework.

It is not expected that all Participants will need to establish and implement a risk management framework within their organisations that addresses all of the principles and concepts, or that integrates all of the controls, to the extent implied by the discussion in this document. A robust risk management framework is one that adequately addresses the risks to which an organisation is exposed and is therefore dependent on the size and range of activities that an organisation is involved in. That is, the risk management framework of a particular organisation may be adequate even though it is relatively "weak" in some areas, or possibly does not address some aspects of risk that is documented in this paper, simply because the characteristics of the organisation does not warrant it.

In practice, the size and location of the risk management function will correlate to the size and range of activities of the organisation. In a large firm, there may exist an independent risk management unit, "middle office", or compliance unit. However, in a small firm, the risk management function might be the responsibility of, for example, the financial controller or company secretary, or some other person who is sufficiently removed from the trading area.

ASX has prepared this paper to heighten the awareness of Participants of the need for adequate risk management and the principles and concepts associated with risk management. Some Participants, such as specialist clearing organisations that clear for other execution-only Participants, will need to pay closer attention to the risk management framework given the unique risks that they are exposed to. ASX may require such organisations to demonstrate that their risk management framework is adequate in relation to the size and extent of their business activities prior to being authorised as a General Participant (i.e. third party clearer).

[3] IOSCO (1998). *Risk Management and Control Guidance for Securities Firms and Their Supervisors*, p.4.

All Participants are encouraged to undertake a comprehensive review of their current risk management framework against the principles outlined in this paper to ensure they are able to maintain a standard of operation commensurate with the requirements of a market and/or clearing Participant.

3. STRUCTURE OF THIS PAPER

The sections following the Introduction, the Purpose, and the Structure of this Paper are:

4. SOURCES OF RISK

Lists and defines the risks that an organisation operating in the financial markets can be exposed to.

5. RISK MANAGEMENT RESPONSIBILITIES

States the organisation's areas responsible for risk management, and details the responsibilities for each.

6. RISK MANAGEMENT METHODS

Details the methods for managing risk.

7. RISK MANAGEMENT MATRIX

Combines Sections 4, 5, and 6 in a matrix that maps the responsibilities and methods to the risk areas involved.

It is important to note that this paper seeks to define and describe a comprehensive, albeit generic, risk management framework for organisations that are involved in the markets, and the clearing and settlement facilities operated by ASX. As discussed earlier, the extent to which it applies to a specific organisation will depend on the size and sophistication of the organisation, and the range of activities in which it is involved.

4. SOURCES OF RISK

a) OPERATIONAL RISK

Operational[4] risk is the risk that improper operation of trade processing or management systems will result in financial loss. Operational risk encompasses the risk of loss due to the breakdown in controls within the firm including, but not limited to, unidentified limit excesses, unauthorized trading, fraud in trading or in back office functions including inadequate books and records and a lack of basic internal

[4] "Operation" is the processing, settlement, reporting, and overall management of a transaction from order receipt, deal execution until **final** settlement.

accounting controls, inexperienced personnel, and unstable and easily accessed computer systems[5].

b) MARKET RISK

Market risk is the risk of financial loss arising from an adverse movement in the market rates and prices used to value the financial instruments that are held by an organisation as an investment or as part of proprietary trading positions.

c) CREDIT RISK (INCLUDES COUNTERPARTY AND SETTLEMENT RISK)

Credit risk can be defined as the risk of loss arising from the failure of a counterparty to perform its obligations under a contract. It has three main components.

1. Credit exposure: credit exposure relates to the amount of loss in the event of counterparty default or failure to settle a trade. It is possible to identify a current and future component[6].
2. Probability of default: the probability that the counterparty will fail to perform a contractual obligation. This will reflect the current creditworthiness of the counterparty and its prospective creditworthiness over the lifetime of any transaction.
3. Recovery rate: the proportion of the market value of a position that is expected to be recovered if the counterparty defaults[7].

d) LIQUIDITY RISK

Liquidity risk can be defined as the risk to a firm's ability to meet commitments in a timely and cost effective manner while maintaining assets. Liquidity risk can also mean the inability to pursue profitable business opportunities and continue as a viable business due to a lack of access to sufficient cost-effective resources. The liquidity risk management practices of well-managed firms contain specific definitions that incorporate both core and broader components into their approach to liquidity risk management[8].

e) DOCUMENTATION / LEGAL RISK

Documentation and legal risk is the risk of financial loss due to:

1. unenforceable legal documents;
2. erroneous or incomplete documentation; and

[5] IOSCO (1998). *Risk Management and Control Guidance for Securities Firms and Their Supervisors*, p.5.

[6] Current credit exposure (e.g. in a derivatives transaction) is usually interpreted as the replacement value of the contract in the event of default; potential future exposure is an estimate of the replacement cost of the transaction if a counterparty defaults at some future time during the life of the transaction.

[7] IOSCO (2000). *The Management of Credit Risks by Securities Firms and Recommendations to Firms and Regulators*, p.1.

[8] IOSCO (2002). *Sound Practices for the Management of Liquidity Risk at Securities Firms*, p.3.

3. legal actions against the organisation.

f) REPUTATION RISK

Reputation risk is the risk of financial loss arising from the perception of the organisation in the market place changing adversely. It specifically relates to the opinions and attitudes of external parties.

g) REGULATORY RISK

Regulatory risk is the risk of financial loss resulting directly from the failure of the organisation to meet the rules and statutory requirements of the market in which it operates relating to the operation of the business.

h) SYSTEMIC RISK

Systemic risk[9] refers to:

1. the scenario that a disruption at a firm, in a market segment, or to a settlement system could cause a "domino effect" throughout the financial markets toppling one financial institution after another, or
2. a "crisis of confidence" among investors, creating illiquid conditions in the marketplace. Systemic risk encompasses the risk that failure in one firm or one segment of the market would trigger failure in segments of, or throughout, the entire financial markets[10].

5. RISK MANAGEMENT RESPONSIBILITIES

a) BOARD AND MANAGEMENT OVERSIGHT

1. The most important and critical component of the risk management framework is the structured and disciplined oversight of the overall operations of the organisation. This includes oversight at both the board level and at the management level.
2. The board and management should participate together in frequent and active discussions on the risk management framework and include in those discussions, where appropriate, staff from the various risk management and operational divisions, regarding procedures for measuring and managing risk.
3. The basis for a successful risk management framework should be provided and include at a minimum:
    a) the board and management should ensure that they understand, and that the whole organisation understands, derivatives and other financial

[9] Systemic risk is listed here for completeness. Please note, that it will not be discussed further in this paper: Systemic risk refers to a financial markets crisis risk, while this paper focuses on the risk management of individual companies.

[10] IOSCO (1998). *Risk Management and Control Guidance for Securities Firms and Their Supervisors*, p.7.

instruments and how the use of them contributes to the organisation's overall risk profile;

b) the board and management should promote a widely shared control and risk management culture within the organisation;

c) the board should ensure that management has in place sufficient resources and adequately skilled and qualified staff to manage and control risks;

d) the board should ensure that management has widely distributed the organisation's manual of policies and procedures within the organisation, that it is readily accessible by staff, and that staff are continually kept abreast of changes in policy and procedures;

e) the board should ensure that management has structured compensation policies in such a way as to be sufficiently independent of the performance of trading activities, thereby avoiding the potential incentive for excessive risk taking that can occur if, for example, remuneration is substantially tied to the profitability of the trading unit;

4. The scope of the organisation's risk management should be defined and guidance provided; at a minimum:

a) the board should approve the business activities and products that the organisation has the capacity and authority to be involved in;

b) the board should quantify the organisation's risk appetite in terms of the organisation's capital by approving global overall limits for the risk categories that its business activities expose it to (for example, market risk if it take principal positions, counterparty and credit risk if it is responsible for settling with clients and counterparties);

c) the board should ensure that management has in place a system of limits which:

i) is consistent with the organisation's overall risk measurement approach;

ii) is integrated to the fullest extent possible with the organisation's overall group wide global limits;

iii) is consistent with the effectiveness of the organisation's overall risk management process and with the adequacy of its capital position;

iv) establishes boundaries for risk taking;

v) permits management to control exposures, initiate discussions concerning opportunities and risks, and to monitor actual risk-taking against predetermined tolerances; and

vi) defines escalation / reporting / approval procedures for managing limit breaches;

vii) accurately reflects current or expected market conditions;

5. Risk management systems should be implemented; at a minimum:

a) the board should approve and oversee the implementation of all significant systems and policies relating to the management of risks throughout the organisation;

b) management should establish and implement a system for identifying, assessing, monitoring, and managing risk throughout the organisation. This system will include the organisation's internal compliance and control systems.

   In establishing appropriate procedures management can take into account AS/NZS4360 – Risk management within the Internal Audit Process, The Institute of Internal Auditors Australia and Standards Australia, 2002. Further reference can be found at www.standards.com.au and www.iia.org.au[11];

c) the board should ensure that the systems provide regular reports, and that it receives regular reports, on the profitability and risk profile of the organisation. For those organisations that have implemented proprietary risk assessment models, these reports should include information concerning:

   i) the accuracy and effectiveness of those models (for example, through back-testing); and

   ii) the impact on the risk profile of possible events or circumstances (for example, through stress testing) such as a breakdown in key measurement assumptions (such as correlations, volatility etc);

6. The board and management should ensure that there are clear delineations of lines of responsibility for:

   a) managing risk;

   b) implementing adequate systems for measuring risk;

   c) establishing appropriately structured limits on risk taking;

   d) establishing effective internal controls; and

   e) establishing a comprehensive risk-reporting process;

7. The effectiveness of the risk management systems should be reviewed at least annually and at a minimum:

   a) the board should ensure that systems, once established, are effectively operating, as designed, on a continuous basis;

   b) the board should re-evaluate risk management policies, systems, and the risk tolerance regularly. The frequency with which these are re-evaluated depends on the size of the organisation, the range of activities it is involved in, and the rate of change within the organisation;

   c) management should continuously re-evaluate the organisation's activities and ensure that where those activities have changed significantly (for

[11] ASX Corporate Governance Council (2003). *Principles of Good Corporate Governance and Best Practice Recommendations*, p.44.

example, in terms of the risk profile of the activity), the changes are approved by the board or its delegate;

8. Regarding the organisation's financial reporting - the chief executive officer (or equivalent) and the chief financial officer (or equivalent) should state to the board in writing that:

    a) the capital returns are founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the board;

    b) the company's risk management and internal compliance and control system is operating efficiently and effectively in all material respects.

b) INDEPENDENT RISK MANAGEMENT FUNCTION

1. The independent risk management function is a specialist unit that is independent of the trading and operational units;

2. The reporting lines of that unit should also be independent of the trading and operation units. In practice, however, the size and location of the risk management function will correlate to the size and range of activities of the organisation. While segregation of duties is always an issue in risk management, some overlap may be unavoidable based simply on size of firm. However, that overlap should never involve trading and risk management[12];

3. The personnel staffing the risk management unit should have the appropriate qualifications and experience to completely understand the risks associated with all of the organisation's activities. Accordingly, the compensation policies for these individuals should be adequate to attract and retain personnel with such skills and background;

4. The risk management unit should:

    a) prepare submissions to the board, or its delegate, for the approval of risk limits;

    b) draft policies concerning the management of risk for board approval;

    c) specify risk methodologies for the risk measurement systems;

[12] It is important here to draw a distinction between the risk management performed by traders and the risk management policies, procedures, controls and systems of the organisation's risk management framework. Traders take positions in financial instruments and are responsible for managing the risk (generally limited to market risk although some traders are also responsible for managing positions that involve the trading of credit or issuer risk) in those positions. They do this by monitoring the positions closely and hedging the positions according to their own (or managements) strategy. On the other hand, risk management in the context of the risk management framework, as discussed earlier, refers to the policies, controls, procedures and systems that are necessary for any organisation, no matter how large or small, to be able to effectively manage, monitor and control their exposure to the sources of risk detailed in Section 4. Combined, the policies, controls, procedures and systems form the risk management framework.

d) implement and maintain the risk measurement systems and keep them up to date with respect to products, limits and any assumptions used in the running of models;

e) re-evaluate the risk measurement methodologies and models at least annually (and more often if necessary) to ensure they keep up to date with changes in the market and with innovations in risk management and measurement techniques;

f) review limit structures and compare limits to actual exposures. Consideration of whether or not existing measures of exposure and limits are appropriate in view of the organisation's past performance (assessed through back testing) and capital position should be part of this review;

g) collect and authorise daily revaluation rates and prices, and ensure all open positions are independently and accurately marked to market;

h) provide input on all risk issues;

i) provide input on identifying and measuring the risk in new business activities and products;

j) monitor and report utilisation against limits. Reporting should be performed daily. Reporting should, as far as possible, be automated and integrated with the other support systems used within the organisation to minimise the risk of errors;

k) monitor the level of settlement fines (e.g. fail fees) relating to clients (who fail to complete a contract);

l) monitor abnormal levels of cancellations (of executed trades) and re-bookings (transfer of an executed trade from one client's account to another) relating to each Market Participant with whom the organisation has a Clearing Agreement; and

m) maintain the organisation's transaction documentation function. This includes:

    i) keeping pro-forma agreements up to date. Note: Where for commercial reasons, a pro-forma agreement is modified, management and Legal Counsel should be involved in, and approve, the modification. Modifications should be documented and a process for tracking them established;

    ii) issuing agreements to clients for signing;

    iii) maintaining a system to keep track of documentation; and

    iv) ensuring agreements are in place prior to transaction execution;

5. Generally, a separate independent unit is responsible for the credit area, however, as discussed earlier, this largely depends on the size of the organisation[13]. This unit should:

   a) analyse the credit risk of individual clients and counterparties;

   b) prepare submissions to the board, or its delegate, for the approval of lending, market, product and tenor limits. The basis of the recommendations contained in the submissions are explicitly tied to the credit analysis performed in (a) above;

   c) monitor and report credit risk utilisation against limit;

   d) draft policies concerning the management of credit risk for board approval;

   e) approve limit excesses intra day prior to deal execution within delegation;

   f) establish policies and procedures concerning the acceptance and administration of collateral arrangements, including collateral agreements; and

   g) establish policies and procedures concerning close-out netting, including the execution of close-out netting master agreements.

6. RISK MANAGEMENT METHODS

In this section, a range of risk management methods is recommended. Many of these methods are applicable to all sources of risk (see section 7, Risk Management Matrix, for more detail). In addition, the subsections c) and d) deal with risk measurement and management methods specifically related to market, credit, liquidity, and legal and regulatory risk.

a) COMPREHENSIVE POLICY AND PROCEDURES MANUAL[14]

1. Regarding oversight – the policy should, at a minimum, include:

   a) the respective accountabilities of the board, audit committee (or other appropriate board committee), management, and the internal audit function;

   b) the identification of those within the organisation that have the delegated authority to approve:

      i) changes to procedures;

[13] It is important to note however, that even in the smallest firm, the assessment, limiting and monitoring of credit and counterparty risk is mandatory. Who performs this in the organisation is dependent on the size of the firm (although it should never be anyone who is also responsible for trading).

[14] Referred to as 'the policy' in this paper. See also: ASX Corporate Governance Council (2003). *Principles of Good Corporate Governance and Best Practice Recommendations*, p.43.

ii) changes to risk measurement methodology;

iii) changes to risk limits;

iv) allocation of limits; and

v) limit excesses;

2. Regarding risk profile – the policy should, at a minimum, include:

a) the business activities that the board has approved the organisation's involvement in, and the corresponding material risks facing the organisation. Material risks can be financial and non-financial;

b) the instruments and products that the board has approved trading in, and the corresponding material risks facing the organisation. Material risks can be financial and non-financial;

3. Regarding risk management – the policy should, at a minimum, include:

a) methodologies for measuring risk;

b) the accounting policies that define and establish criteria for the recording of the firms assets and liabilities, revenues and expenses;

c) the identification of those areas that require segregation of duties and the reasons for functions to be segregated from other functions. For functions that should be segregated but are not due to the size of the organisation, the policy should document the additional controls that are in place to mitigate the additional exposure to the organisation arising from the lack of segregation;

d) communication of the escalation procedures and associated benchmarks for extraordinary events such as (not limited to):

i) exceeding a trading limit (i.e. Market Risk Limit), including any disciplinary action;

ii) exceeding a counterparty / credit / settlement limit including any disciplinary action;

iii) failure of a counterparty to settle; and

iv) material inadequacies and breakdowns in controls;

e) regarding new product processes or new business activities – the policies and procedures should:

i) give guidance on what constitutes a new business activity or product for the organisation (this could include for example a new market), and assess whether a new product fits within the existing risk framework of the business;

ii) document the approval process and the delegated authorities;

iii) set out the way in which the new business activity or product, in which the organisation may have no previous experience, is to be introduced so as to limit any potential losses arising as a result of that inexperience. In addition, it should provide for adequate and appropriate testing of controls, procedures and systems prior to the introduction of the new product or activity or, if this is not practical, as soon after its introduction as possible;

iv) identify the minimum information that should be addressed in the business plan for the new business activity or product and which should generally include:

a) a description of the relevant financial products, markets and business strategies;

b) the resources required to establish sound and effective risk management systems and to attract and retain professionals with specific expertise in the proposed business activity;

c) an analysis of the reasonableness of the proposed activities in relation to the organisation's overall financial condition and capital levels;

d) an analysis of the risks that may arise from the activity;

e) the procedures that the organisation will use to measure, monitor and control those risks;

f) the relevant accounting guidelines and accounting treatment of the transactions arising from the activities;

g) the relevant tax treatment of transactions arising from the activities;

h) an analysis of any legal restrictions and whether the activities are permissible; and

i) the disaster recovery plan procedures that will be established with respect to the proposed business activities;

f) specifically regarding the responsibility towards clients – the policy should include:

i) dispute resolution procedures that would be activated in the event of a dispute with any clients, or in the case of General Participants, with any Market Participants with whom the organisation has a Clearing Agreement;

ii) procedures relating to the protection of client assets;

iii) procedures regarding access to client cash management accounts;

iv) procedures regarding the issuing of statements/records to clients in respect of their trading activities;

v) procedures for ensuring that all clients' open positions are correct;

vi) procedures for communicating with Market Participants about their clients' derivatives positions;

g) specifically regarding credit risk – the policy should include:

   i) procedures regarding the establishment of trading/settlement limits for each client or, if applicable, for each Market Participant;

   ii) procedures for opening accounts for clients;

   iii) policies and procedures for dealing with the breach of an agreed limit by a client or, if applicable, by a Market Participant;

   iv) procedures for consolidating client risk across all products traded for a client to which the organisation is exposed (including, if applicable, transactions for that client executed by multiple Market Participants);

   v) policies and procedures concerning credit reduction techniques implemented to manage, control and limit the exposure to the default of a client;

   vi) arrangements for streamlining client payments that facilitate achievement of timely settlement;

   vii) procedures dealing with the potential for a client credit limit to be exceeded intra day;

   viii) for participants authorised to clear Options Market Transactions and/or Futures Market Transactions, policies and procedures for dealing with the collection of margin payments from clients and for ensuring adequate cover is in place;

   ix) procedures for monitoring exposure to client derivatives positions;

   x) procedures regarding margin lending facilities and how margin liabilities are covered; and

   xi) policies and procedures dealing with requests for increases to predetermined limits and tolerances to particular counterparties/clients, reporting of performance against predetermined limits and tolerances, and breaches of predetermined limits and tolerances;

h) the Disaster Recovery Plan ("DRP"), which should:

   i) document the frequency and nature of testing the plan;

   ii) identify the key features / components of the plan;

   iii) identify broad categories of events and the associated responses. This is particularly important with respect to the analysis of stress tests (refer below) and the identification of significant errors or defaults. The response to such events should include a qualitative analysis of the actions management might take under particular scenarios and contingency plans outlining the operating procedures and lines of communication, both formal and informal, should the hypothetical event become a reality;

iv) identify officers of the organisation with special delegated authority; and

v) define levels of "normal" activities and services that are necessary to the operation in the event of the DRP being used;

vi) Business Continuity Plan arrangements must be communicated to all staff;

i) the organisation's Code of Conduct by which it expects its staff to conduct themselves;

4. Regarding control – the policy should, at a minimum, include:

a) procedures for ensuring that all transaction documentation (agreements and confirmations etc) is executed on a timely basis and by those officers in the organisation that have the appropriate delegation and authority. Procedures and policy concerning the non-signing of confirmations and agreements should be put in place to manage the exposure;

b) the identification of the transaction cycle (trade execution, confirmation, accounting, risk measurement, limit monitoring and settlement). The components of the cycle should be automated as much as possible to limit operational risk; and

c) the specification of daily reconciliations that must be completed, including:

i) trust accounts;

ii) general bank accounts;

iii) client suspense accounts;

iv) house accounts;

v) all general ledger and subsidiary ledger suspense and holding accounts; and

vi) settlement and accumulation accounts (entrepot);

5. Regarding assessment of effectiveness – the policy should include the means of analysing the effectiveness of its risk management and internal compliance and control system and of the effectiveness of their implementation.

This assessment will generally be undertaken by the internal audit function, but an alternative mechanism may be employed to achieve the same outcome depending on the company's size and complexity and the types of risk encountered.

A company, particularly a substantial company, is encouraged to have an internal audit function[15].

[15] ASX Corporate Governance Council (2003). *Principles of Good Corporate Governance and Best Practice Recommendations*, p.44.

b) AUDIT FUNCTION

1. The audit function (internal or external) should audit and test the risk management process and internal controls on a periodic basis, with the frequency of the review based itself on a careful assessment of risk;

2. The depth and frequency of audits should be increased if:

    a) weaknesses and significant issues are discovered;

    b) significant changes have been made to:

        i) business activities;

        ii) product lines;

        iii) risk modelling methodologies;

        iv) the risk oversight process;

        v) internal controls; or

        vi) the overall risk profile of the organisation;

3. The audit should evaluate the independence and overall effectiveness of the organisation's risk management function, in terms of:

    a) the effectiveness of internal controls relevant to measuring, reporting and limiting risk;

    b) compliance with risk limits and the reliability and timeliness of information reported to the organisation's management and board;

4. Regarding the internal audit function[16]:

    a) guidance on the internal audit function is found in the Technical Information and Guidance section on the homepage of the Institute of Internal Auditors at www.iia.org.au;

    b) the audit committee should recommend to the board the appointment and dismissal of any chief internal audit executive;

    c) the internal audit function should be independent of the external auditor;

    d) the internal audit function should report to management and should have all necessary access to management and the right to seek information and explanations;

    e) the audit committee should oversee the scope of the internal audit and should have access to the internal audit function without the presence of management. In order to enhance the objectivity and performance of the internal audit function, companies should consider a second reporting line from the internal audit function to the board or relevant committee.

[16] ASX Corporate Governance Council (2003). *Principles of Good Corporate Governance and Best Practice Recommendations*, p.44.

c) *RISK MEASUREMENT – CONCERNING MARKET, CREDIT, LIQUIDITY RISK*

1. The organisation should implement approved, accurate and comprehensive methodologies for measuring[17] all relevant sources of risk on an organisation-wide basis;

2. The organisation must mark-to-market its positions at least daily using rates and prices that have been sourced independently of the trading and operational units. Where this is not possible, procedures need to be established to ensure the integrity of the market data being used to value the organisations positions;

3. The sophistication of the risk measurement methodologies used to measure risks is positively correlated to the size of the organisation, the range of business activities that it is involved in, and the markets in which it operates. For example, the risk measurement methodologies for a small firm whose business activities are limited to agency business and some small proprietary investments in equities are likely to be the same as the methodologies required for the calculation of regulatory capital[18]. On the other hand, a large firm that is involved in all markets, structures deals for clients and has a significant proprietary trading operation is likely to implement a risk measurement system that uses proprietary risk models that assess risk far more accurately than that of the regulatory capital requirements. Such firms use their own internal models for day to day monitoring of positions while at the same time ensuring that they satisfy the regulatory capital liquidity requirements;

4. The calculation of the risks should be automated and integrated into the day-to-day management of the organisation and provide an assessment of the organisation's exposure to the various risk categories on a consolidated basis;

5. The organisation should analyse and assess stress scenarios that could potentially have a significant and permanent adverse impact on the organisation. Such stress scenarios calculate the financial loss to the organisation from an event and can be calculated regardless of the risk measurement methodology used in the organisation. Examples of stress scenarios include:

   a) a breakdown in the assumptions used in the "normal" modelling and measurement of risk (for example, correlations and volatility) in a sophisticated proprietary model;

   b) the repeat of significant historic events (e.g. the 1998 Russian and emerging market debt crisis, the 1997/8 Asian meltdown, 1987 stock market crash, Paul Keating's 1986 "Banana Republic" speech, the Gulf War etc) (this could be assessed regardless of methodology used);

---

[17] It should be noted that techniques and methodologies for the measurement of market, credit, and liquidity risk are currently well researched and documented. Quantifying risk in the other categories is more problematic. For example, if the firm has a large legal case pending and substantial damages may be awarded against it, the quantification of legal risk could be the value of the firm as the damages may bankrupt the organisation.

[18] Regulatory capital is the capital requirements of ASX.

c) an assessment of the state the market would have to be in for the organisation to lose all of its capital; and

d) an assessment of the financial loss caused by financial stress in a particular demographic that represents a major component of the organisations client base;

6. Position and Value-at-Risk (VaR) limits and measurement methodologies should be established for accurate and timely measurement, monitoring, and reporting of exposures on principal positions;

7. The risk measurement methodologies should be tested by comparing the results of the measurement process with realised behaviour (i.e. back testing).

i) Risk Measurement – Specifically concerning Credit Risk

1. The quantification of credit risk should be the sum of the positive mark to market of the exposure to an individual counterparty plus a measure of the potential exposure based on an assessment of the potential future market value of the position up until settlement;

2. The assessment of future exposure can be based on sophisticated modelling techniques or simple "add-ons" (depending on the sophistication and size of the organisation), both of which should be based on underlying assumptions concerning the volatility of prices and rates that determine the value of the underlying positions;

3. The use of master netting agreements and collateralisation can reduce the counterparty risk as long as the agreements and recourse provisions are legally enforceable in all relevant jurisdictions, and the organisation should demonstrate that it has undertaken the appropriate due diligence to ascertain that certainty;

4. The organisation must establish counterparty credit limits with each counterparty with which it conducts business and ensure that it has the appropriate systems and procedures in place to accurately and on a timely basis measure, monitor, and report on utilisation against those limits and to have policies, procedures and delegations for approving and / or dealing with breaches of those limits;

5. The limits should be based on an assessment of the creditworthiness of the counterparty and expressed in terms of credit risk limits (i.e. face value lending limits), counterparty risk limits (i.e. replacement value), product limits, and tenor limits and these should be reassessed continually throughout the relationship with the counterparty.

ii) Risk Measurement – Specifically concerning Liquidity Risk

1. The organisation should establish limits for liquidity risk (gap limits, maturity mismatch limits);

2. In assessing controls for liquidity risk, the organisation should factor in the possibility that it could lose access to one or more markets, either because of concerns about the organisation's own creditworthiness, the creditworthiness of a major counterparty, or because of generally stressful market conditions;

3. The organisation's liquidity plan should reflect the organisations ability to turn to alternate sources of funding, or to provide sufficient collateral or other credit enhancements in order to continue trading under a broad range of scenarios;

4. The organisation should ensure that daily cash and portfolio reconciliations are completed so that it has accurate and timely information concerning its settlement obligations.

d) Management of Legal, Reputation, and Regulatory Risk

1. Legal risk should be limited and managed through policies developed by the organisation's legal counsel. There should be, at a minimum, guidelines and processes in place to ensure the enforceability of counterparty agreements;

2. Before contracting with counterparties, the organisation should reasonably satisfy itself that the counterparty has the legal capacity, and necessary regulatory authority, to engage in those transactions;

3. Before contracting with the counterparty, the organisation should ensure that the counterparty has the power and authority to enter into the transaction and that the counterparty's obligations arising from them are enforceable;

4. The organisation should ensure that its rights with respect to any margin or collateral received from a counterparty are enforceable and exercisable;

5. The organisation should ensure that its netting agreements are adequately documented and that they have been properly executed;

6. The organisation must ensure that it is familiar with all regulatory requirements;

7. The organisation should ensure that all relevant staff in the organisation are aware of, and comply with, their responsibilities with respect to the applicable regulations that govern the organisation and that they are suitable skilled and experienced to comply with those requirements.

7. RISK MANAGEMENT MATRIX

Function / Control	Operations	Market	Credit	Liquidity	Legal	Reputation	Regulatory
RISK MANAGEMENT RESPONSIBILITIES – BOARD AND MANAGEMENT OVERSIGHT							
Disciplined oversight;	✓	✓	✓	✓	✓	✓	✓
Frequent discussions between board, management, and staff;	✓	✓	✓	✓	✓	✓	✓
Basis for successful risk management framework should be provided:							
a) board and management understand risk profile;	✓	✓	✓	✓	✓	✓	✓
b) board and management promote a risk culture;	✓	✓	✓	✓	✓	✓	✓
c) management ensures sufficient resources and skilled and qualified staff;	✓	✓	✓	✓	✓	✓	✓
d) management ensures the policy and procedures manual is current and widely;	✓	✓	✓	✓	✓	✓	✓
e) management ensures that compensation policies avoid incentives for excessive risk taking;	✓	✓	✓	✓	✓	✓	✓
Scope of the organisation's risk management should be defined:							
a) board approves business activities and products;	✓	✓	✓	✓	✓	✓	✓
b) board quantifies risk appetite		✓	✓	✓			
c) management ensures that the system of limits:							
i) is consistent with overall risk measurement approach;		✓	✓	✓			
ii) is integrated to the fullest extent possible;		✓	✓	✓			
iii) is consistent with the overall risk management process;		✓	✓	✓			
iv) establishes boundaries for risk taking;		✓	✓	✓			
v) permits management to control exposures;		✓	✓	✓			

vi) defines escalation / reporting / approval procedures.		✓	✓	✓			
Risk management systems should be implemented:							
a) board approves and oversees implementation of systems;	✓	✓	✓	✓	✓	✓	✓
b) management establishes and implements system for managing risk;	✓	✓	✓	✓	✓	✓	✓
c) board ensures that systems provide regular reports concerning:							
i) effectiveness of models;		✓	✓	✓			
ii) risk impact of possible events;	✓	✓	✓	✓	✓	✓	✓
Board and management ensure delineation of responsibilities for:							
a) managing risk;	✓	✓	✓	✓	✓	✓	✓
b) implementing systems;	✓	✓	✓	✓	✓	✓	✓
c) establishing limits;	✓	✓	✓	✓	✓	✓	✓
d) establishing internal controls;	✓	✓	✓	✓	✓	✓	✓
c) establishing risk reporting process;	✓	✓	✓	✓	✓	✓	✓
Effectiveness of risk management systems should be reviewed at least annually:							
a) board ensures that systems are operating;	✓	✓	✓	✓	✓	✓	✓
b) board re-evaluates policies and risk tolerance.	✓	✓	✓	✓	✓	✓	✓
c) management re-evaluates the organisation's activities;	✓	✓	✓	✓	✓	✓	✓
Regarding financial reporting, CEO and CFO should state in writing that:							
a) capital returns are founded on sound risk management system;	✓	✓	✓	✓	✓	✓	✓
b) risk management and internal compliance and control system is operating effectively;	✓	✓	✓	✓	✓	✓	✓

RISK MANAGEMENT RESPONSIBILITIES – INDEPENDENT RISK MANAGEMENT FUNCTION							
Specialist unit independent of trading;	✓	✓	✓	✓	✓	✓	✓
The reporting lines should be independent;	✓	✓	✓	✓	✓	✓	✓
The personnel should have the appropriate qualifications and experience;	✓	✓	✓	✓	✓	✓	✓
The risk monitoring unit should:							
a) prepare submissions to the board;	✓	✓	✓	✓	✓	✓	✓
b) draft policies;	✓	✓	✓	✓	✓	✓	✓
c) specify risk methodologies;	✓	✓	✓	✓	✓	✓	✓
d) maintain risk measurement systems;		✓	✓	✓			
e) re-evaluate risk measurement methodologies;		✓	✓	✓			
f) review limit structures;		✓	✓	✓			
g) collect and authorise daily revaluation rates / prices;		✓	✓	✓			
h) provide input on all risk issues;	✓	✓	✓	✓	✓	✓	✓
i) provide input on defining the risk in new products;	✓	✓	✓	✓	✓	✓	✓
j) monitor and report utilisation against limits;		✓	✓	✓			
k) monitor the level of settlement fines (e.g. fail fees) relating to clients			✓				
l) monitor abnormal levels of cancellations relating to Market Participants			✓				
m) maintain the transaction documentation, this includes:							
i) keeping pro-forma agreements up to date;			✓		✓	✓	✓
ii) issuing agreements to clients for signing;			✓		✓	✓	✓
iii) maintaining system to track documentation;			✓		✓	✓	✓
iv) ensuring agreements are in place.			✓		✓	✓	✓

The credit risk area should:							
a) analyse the credit risk of individual counterparties;			✓				
b) prepare submissions to the board on limits;			✓				
c) monitor and reporting utilisation against limit;			✓				
d) draft policies on management of credit risk;			✓				
e) approve limit excesses intra day ;			✓				
f) establish policies/procedures concerning collateral arrangements;			✓		✓		
g) establish policies/procedures concerning close-out netting			✓		✓		
RISK MANAGEMENT METHODS – POLICY AND PROCEDURES MANUAL							
Regarding oversight the policy should include:							
a) accountabilities of board, audit committee, management and the internal audit function;	✓	✓	✓	✓	✓	✓	✓
b) identification of delegated authority to approve:							
i) changes to procedures;	✓	✓	✓	✓	✓	✓	✓
ii) changes to risk methodology;	✓	✓	✓	✓	✓	✓	✓
iii) changes to risk limits;		✓	✓	✓			
iv) allocation of limits;		✓	✓	✓			
v) limit excesses;		✓	✓	✓			
Regarding risk profile the policy should include:							
a) board-approved business activities;	✓	✓	✓	✓	✓	✓	✓
b) board-approved instruments and products;	✓	✓	✓	✓	✓	✓	✓
Regarding risk management the policy should include:							
a) methodologies for measuring risk;		✓	✓	✓			
b) accounting policies;		✓	✓	✓			

c) segregation of duties;	✓	✓	✓	✓	✓	✓	✓
d) escalation procedures for:							
i) exceeding a trading limit ;		✓	✓	✓			
ii) exceeding a counterparty limit;		✓	✓	✓			
iii) failure of a counterparty to settle; and			✓				
iv) material control problems;	✓	✓	✓	✓	✓	✓	✓
e) regarding new product processes the policies and procedures should:							
i) define a new product;	✓	✓	✓	✓	✓	✓	✓
ii) document the approval process;	✓	✓	✓	✓	✓	✓	✓
iii) specify the introduction-process of a new product;	✓	✓	✓	✓	✓	✓	✓
iv) the business plan for a new product should:							
a) describe relevant financial products, markets, strategies;	✓	✓	✓	✓	✓	✓	✓
b) state the required resources;	✓	✓	✓	✓	✓	✓	✓
c) analyse the reasonableness of the proposal;	✓	✓	✓	✓	✓	✓	✓
d) analyse the risks;	✓	✓	✓	✓	✓	✓	✓
e) detail procedures to measure / monitor / control risks;	✓	✓	✓	✓	✓	✓	✓
f) detail accounting treatment;		✓	✓	✓			
g) detail tax treatment;							✓
h) analyse legal restrictions;					✓		
i) identify DRP procedures;	✓	✓	✓	✓	✓	✓	✓
f) specifically regarding clients the policy should include:							
i) dispute resolution procedures;	✓		✓		✓		
ii) procedures protecting clients;	✓		✓				

iii) client cash account access procedures;	✓		✓				
iv) procedures for issuing records to clients;	✓		✓				
v) client position controls ;	✓		✓				
vi) communication procedures;	✓		✓				
g) specifically regarding Credit Risk, the policy should include:							
i) establishment of trading limits;			✓				
ii) procedures for opening client accounts;			✓				
iii) procedures for dealing with limit breaches;			✓				
iv) procedures for consolidating client risk;			✓				
v) procedures re credit reduction;			✓				
vi) streamlining arrangements;			✓				
vii) procedures for dealing with intra-day limit breaches;			✓				
viii) procedures re margin payments;			✓				
ix) procedures for monitoring derivatives exposure;			✓				
x) procedures for margin lending facilities;			✓				
xi) procedures for limit increases;			✓				
h) Disaster Recovery Plan, which should include:							
i) frequency and nature of testing the plan;	✓	✓	✓	✓	✓	✓	✓
ii) identify the key features / components of the plan;	✓	✓	✓	✓	✓	✓	✓
iii) identify categories of events and responses;	✓	✓	✓	✓	✓	✓	✓
iv) identify officers with special authority; and	✓	✓	✓	✓	✓	✓	✓
v) define levels of “normal” activities/services required;	✓	✓	✓	✓	✓	✓	✓
i) **Code of Conduct;**	✓	✓	✓	✓	✓	✓	✓

Regarding control the policy should include:							
a) procedures for ensuring all documentation is properly executed;	✓	✓	✓	✓	✓	✓	✓
b) identification of transaction cycle;	✓	✓	✓	✓	✓	✓	✓
c) daily reconciliations of:							
i) trust accounts;		✓	✓	✓			
ii) general bank accounts ;		✓	✓	✓			
iii) client suspense accounts;		✓	✓	✓			
iv) house accounts;		✓	✓	✓			
v) all suspense and holding accounts;		✓	✓	✓			
vi) settlement and accumulation accounts;		✓	✓	✓			
Regarding assessment of effectiveness the policy should include:							
a) means of analysing effectiveness of risk management (internal audit);	✓	✓	✓	✓	✓	✓	✓
RISK MANAGEMENT METHODS – AUDIT FUNCTION							
The audit function should audit and test risk management process;	✓	✓	✓	✓	✓	✓	✓
Depth and frequency of audits should increase if:							
a) weaknesses and significant issues are discovered;	✓	✓	✓	✓	✓	✓	✓
b) significant changes have been made to:							
i) business activities;	✓	✓	✓	✓	✓	✓	✓
ii) product lines;	✓	✓	✓	✓	✓	✓	✓
iii) risk modelling methodologies;	✓	✓	✓	✓	✓	✓	✓
iv) the risk oversight process;	✓	✓	✓	✓	✓	✓	✓
v) internal controls; or	✓	✓	✓	✓	✓	✓	✓
vi) the overall risk profile;	✓	✓	✓	✓	✓	✓	✓

Audit should evaluate independence/effectiveness of risk management function:							
a) in measuring, reporting and limiting risk;	✓	✓	✓	✓	✓	✓	✓
b) compliance with limits / reliability of reports;	✓	✓	✓	✓	✓	✓	✓
Regarding internal audit function:							
a) for additional guidance see www.iia.org.au;	✓	✓	✓	✓	✓	✓	✓
b) audit committee should recommend to board appointment / dismissal of chief internal audit executive;	✓	✓	✓	✓	✓	✓	✓
c) internal audit should be independent;	✓	✓	✓	✓	✓	✓	✓
d) it should report to management;	✓	✓	✓	✓	✓	✓	✓
e) audit committee should oversee scope of internal audit.	✓	✓	✓	✓	✓	✓	✓
RISK MANAGEMENT METHODS – RISK MEASUREMENT – MARKET, CREDIT, LIQUIDITY RISK							
The organisation should implement risk measurement methodologies;		✓	✓	✓			
Mark-to-market daily;		✓	✓	✓			
Take into account size of organisation;		✓	✓	✓			
Automate calculations;		✓	✓	✓			
Analyse and stress test:							
a) a breakdown in model assumptions;		✓	✓	✓			
b) the repeat of historic events;		✓	✓	✓			
c) market state for loss of all capital;		✓	✓	✓			
d) effects of financial stress in particular demographic;		✓	✓	✓			
Establish position and VaR limits;		✓	✓	✓			
Back test.		✓	✓	✓			

RISK MANAGEMENT METHODS – RISK MEASUREMENT – SPECIFICALLY CREDIT RISK							
Quantify counterparty risk;			✓				
Assess future exposure;			✓				
Use master netting agreements;			✓				
Establish counterparty credit limits;			✓				
Assess creditworthiness of counterparty;			✓				
RISK MANAGEMENT METHODS – RISK MEASUREMENT SPECIFICALLY LIQUIDITY RISK							
Establish liquidity limits;				✓			
Assess controls;				✓			
Assess sources of alternative funding;				✓			
Ensure accurate information.				✓			
RISK MANAGEMENT METHODS – MANAGEMENT OF LEGAL, REPUTATION AND REGULATORY RISK							
These risks should be limited through:							
Legal counsel policies;					✓	✓	✓
Ensuring counterparty's legal capacity;					✓	✓	✓
Ensuring counterparty's power and authority to enter transaction;					✓	✓	✓
Ensuring rights are exercisable;					✓	✓	✓
Documenting netting agreements;					✓	✓	✓
Familiarity with regulatory requirements;					✓	✓	✓
Ensuring staff awareness.					✓	✓	✓