Financial Industry Regulatory Authority

2017 FINRA Annual Conference

Washington, DC | May 16 – 18, 2017

Supervision of Trading Desk Operations
Tuesday, May 16
3:00 p.m. – 4:00 p.m.

FINRA staff and industry practitioners discuss supervision of the trading desk and internal controls firms should have in place for monitoring trading activity, maintaining information barrier policies and procedures, reviewing electronic communications and conducting regular employee training, among other important topics.

Moderator:
Mark Frankenberg
Director
FINRA Member Regulation, Office of Risk Oversight and Operational Regulation

Panelists:
Cheryl Geremia
Global Head of Operational Risk
Morgan Stanley

Julius Leiman-Carbia
Chief Compliance Officer
MUFG Securities Americas Inc.

Lisa Rizzi-Grieco
Fixed Income Compliance Officer
KGS Alpha Capital Markets LLC

Supervision of Trading Desk Operations Panelist Bios:

Moderator:

Mark Frankenberg is Director of Funding and Liquidity with FINRA's Risk Oversight and Operational Regulation (ROOR). He has been with FINRA since 2010. Prior to coming to FINRA, he worked at the several large member firms including EF Hutton, Prudential Securities and Citigroup. In addition he has experience in Operational Risk at Lava Trading and Sungard.

Panelists:

Cheryl Geremia is Global Head of Operational Risk for Morgan Stanley. She joined Morgan Stanley in 2008 as Managing Director, Global Head of Operations Risk & Control. She subsequently took on responsibility for Enterprise Operational Risk & Control which was integrated into the Operational Risk Department in early 2013 to form a single unit led by Ms. Geremia. Additionally, she is Co-Chair of the Firm's Recovery and Resolution Planning program. Prior to joining Morgan Stanley, Ms. Geremia was at Deutsche Bank from 1996 to 2008. During her last two years at Deutsche Bank, she was Managing Director and Global Head of the Bank's Reconciliation Utility. She also served as the Chief Operations Officer for Deutsche Bank Securities Inc. from 2003 - 2008. Ms. Geremia graduated with a Bachelor of Science degree in Accounting from City University of New York and earned a Masters in Finance from St. John's University. She is a Certified Public Accountant and a Registered Finance & Operations Principal. Ms. Geremia is a Member of the Board of the Women's Bond Club, serving as Treasurer and Finance Committee Chair.

Julius Leiman-Carbia has more than 25 years of experience in leadership roles, mostly with Compliance departments within large global financial services organizations with multiple lines of business. Most recently, Mr. Leiman-Carbia served as Chief Compliance Officer for MUFG Americas. As CCO, he was responsible for directing and implementing Compliance programs on behalf of MUFG Union Bank and the US Branches of BTMU in the US, Latin America and Canada. Prior to that, Mr. Leiman-Carbia served in various leadership roles at J.P. Morgan Chase, BP Energy, Citigroup Global Markets, J.P. Morgan Securities, and Goldman Sachs. Mr. Leiman-Carbia has almost nine years of experience as a regulator serving two different stints at the SEC. Mr. Leiman-Carbia holds a law degree from the University of Pennsylvania Law School and a B.S.F.S. from Georgetown University – School of Foreign Service.

Lisa Rizzi-Grieco joined KGS-Alpha Capital Markets LLC in 2014 and is currently responsible for the surveillance program as well as trade floor regulatory compliance. Previously she served as an SVP Fixed Income Product Compliance at Jefferies LLC, primarily advising the Securitized Product Sales and Trading Desk. Prior to that, she served as a Director of Fixed Income Compliance at Nomura Securities. Ms. Rizzi-Grieco also worked for Commerzbank and RBC Dominion Securities where she held a various compliance roles. She earned her B.A. specializing in Economics from the University of Toronto.

Supervision of Trading Desk Operations

FINRA

Panelists

- **Moderator**
  - Mark Frankenberg, Director, FINRA Member Regulation, Office of Risk Oversight and Operational Regulation
- **Panelists**
  - Cheryl Geremia, Global Head of Operational Risk, Morgan Stanley
  - Julius Leiman-Carbia, Chief Compliance Officer, MUFG Securities Americas Inc.
  - Lisa Rizzi-Grieco, Fixed Income Compliance Officer, KGS Alpha Capital Markets LLC

Morgan Stanley

Supervision of Trading Desk Operations: Operational Risk Considerations

2017 FINRA Annual Conference

May 16, 2017

Agenda

Firm's Risk Appetite Framework

The Firm's Risk Appetite Framework informs the Operational Risk Tolerance Program

Firm Risk Appetite Statement

Morgan Stanley's Risk Appetite defines the types of risk that the Firm is **willing to accept in pursuit of its strategic objectives and business plan**, taking into account the interest of clients and customers and the fiduciary duty to shareholders, as well as capital and other regulatory requirements. This Risk Appetite shall be embedded in Morgan Stanley's Risk Management Culture and linked to its short-term and long-term strategic, capital and financial plans, as well as compensation programs

Operational Risk Tolerance Statement

The Firm's Operational Risk tolerance is for a level of risk that is expected to be less than the **benefits obtained from executing the business strategy and not to pose a material risk to the Firm's capital adequacy, reputation, regulatory standing**, or ability to **execute its strategy**

Operational Risk Tolerance Program

The Firm's operational risk tolerance is monitored by Operational Risk Department against **quantitative or qualitative factors** relating to the Top Operational Risks ("TOR")

Framework

Risk Level Standards

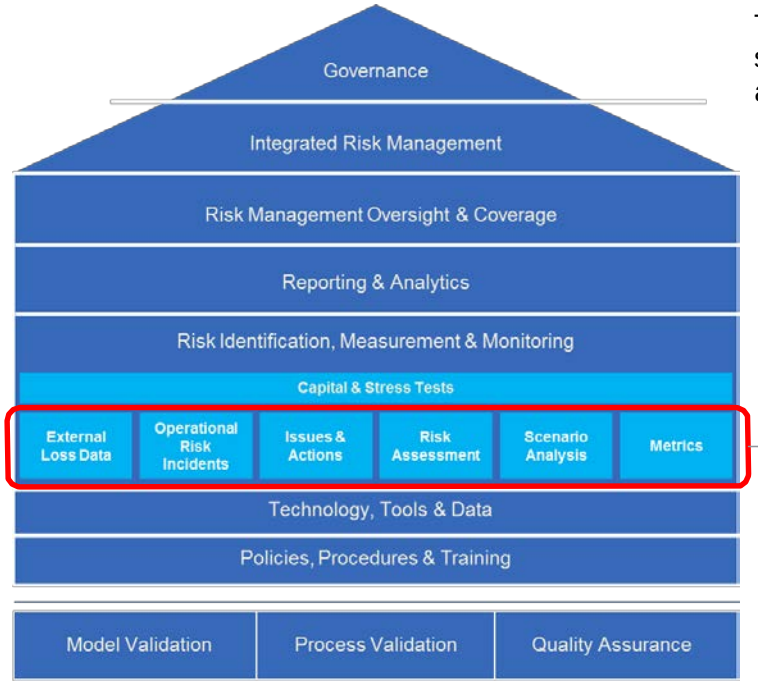
Top Operational Risks

Risk Management: Three Lines of Defense

Overview of 3 Lines of Defense Model (Operational Risk & Compliance)

Risk Identification, Measurement and Monitoring

Key Controls, Metrics and New Product Approval are central techniques to monitor operational risk



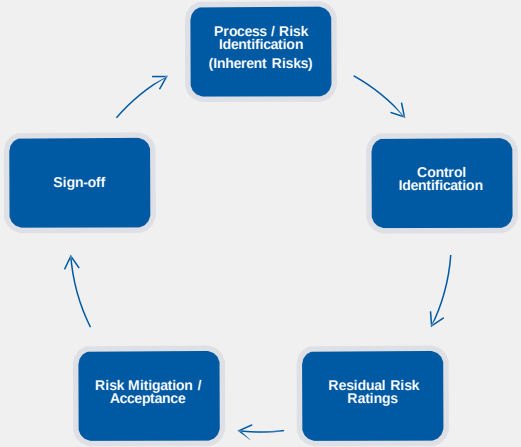
The Operational Risk Framework includes strategic techniques to identify, measure and monitor operational risk:

- Key Controls
- Metrics
- New Product Approval
- Incidents
- Scenario Analysis
- Risk Assessments

Risk Identification, Measurement and Monitoring

Risk and Control Self Assessment ("RCSA")

- The Firm's annual RCSA provides a systematic means to **identify the operational risks and related control weaknesses** that can result in heightened risk exposures
- RCSA serves as the Firm's **inventory of key operational risks** and their risk levels as assessed using Firm-wide Risk Level Standards
- Through RCSAs, Business Areas and Support Functions:



Operational Risk Incidents ("ORIs")

- An Operational Risk Incident ("ORI") is the financial or non-financial impact to the Firm that results from an operational risk event
- Historical ORI data is essential to risk management and is a key input to the **operational risk capital model**
- The reporting of ORIs enhances the **risk culture** and **supports improvements of the control environment.** ORI analysis helps to identify lessons learned and allows the Firm to conduct remedial action to prevent reoccurrence
- Business Units and Support Functions must capture ORIs in the Firm's central incident data repository

Risk Identification, Measurement and Monitoring

Scenario Analysis

- The Firm assesses the risk of low frequency, high severity events through Scenario Analysis
- Scenario Analysis is a systematic process of obtaining expert opinions to derive reasoned assessments of the likelihood and loss impact of plausible, high-severity operational risk events (e.g., 1 in 100 years)
- Operational Risk organizes and facilitates Scenario Analysis workshops which are attended by subject matter experts from the Business Units, Risk Management and Support Functions
- Operational Risk determines the areas and risk event categories that should be covered during these workshops by considering internal and external operational risk events, RCSA ratings, Issues and Actions
- These assessments are inputs into the **operational risk capital model**, Firm-wide Comprehensive Capital Analysis and Review ("CCAR") and to the **Risk Tolerance Framework**

Risk Remediation (Issues and Actions)

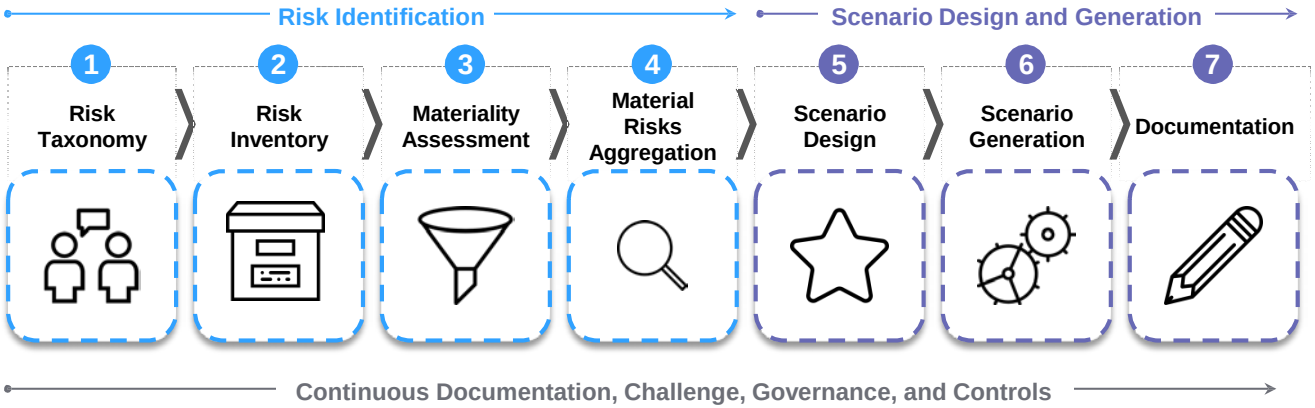
- Business Units and Support Functions are responsible for developing and implementing action plans where needed to remediate operational risk issues identified through ORIs, Scenario Analysis, RCSA etc.
  - ***Issue:*** *Deficiency in the Firm's control environment, that requires an enhancement*
  - ***Action Plan:*** *Composed of one or more actions that remediate an issue (i.e., mitigate the risk to an accepted level)*
- High and Critical risk Issues and related Actions are recorded and tracked in the Firm's centralized database
- Issue owners and Action implementers must use the database to track progress against target dates

Stressing the Risk

Scenario Analysis is a key component in the quantification of Operational Risk

Scenario Workshop Estimates are leveraged to:

- Inform the selection of the Firm's Top Operational Risks
- Assess the materiality of risk segments
- Determine key scenario factors and stress the Firm's material risks



Financial Industry Regulatory Authority

2017 FINRA Annual Conference

Washington, DC | May 16 – 18, 2017

Supervision of Trading Desk Operations
Tuesday, May 16
3:00 p.m. – 4:00 p.m.

Resources

FINRA Notices

- FINRA *Regulatory Notice 15-09: Equity Trading Initiatives: Supervision and Control Practices for Algorithmic Trading Strategies Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies* (March 2015)

  www.finra.org/sites/default/files/notice_doc_file_ref/Notice_Regulatory_15-09.pdf

Additional Resources

- Bank for International Settlements, Basel Committee on Banking Supervision: Principles for the Sound Management of Operational Risk (June 2011)

  www.bis.org/publ/bcbs195.pdf

- U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations National Examination Risk Alert: Strengthening Practices for Preventing and Detecting Unauthorized Trading and Similar Activities (February 2012)

  www.sec.gov/about/offices/ocie/riskalert-unauthorizedtrading.pdf

Regulatory Notice 15-09

Equity Trading Initiatives: Supervision and Control Practices for Algorithmic Trading Strategies

Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies

Executive Summary

As algorithmic trading strategies, including high frequency trading (HFT) strategies (hereinafter referred to collectively as "algorithmic strategies"), have grown to compose a substantial portion of activity on U.S. securities markets, the potential for these strategies to adversely impact market and firm stability has likewise grown. Although a reasonable supervision and control program may not foresee every potential failure or prevent every undesirable consequence, in an effort to reduce the future occurrence of such potential issues, FINRA is providing guidance on effective supervision and control practices for member firms and market participants that use algorithmic strategies. These effective practices are focused on five general areas: General Risk Assessment and Response; Software/Code Development and Implementation; Software Testing and System Validation; Trading Systems; and Compliance.

Questions concerning this *Notice* should be directed to:

- Susan Tibbs, Vice President, Quality of Markets, Market Regulation, at (240) 386-5082 or *susan.tibbs@finra.org*;
- Sherilyn Belcher, Director, Market Regulation, at (240) 386-5614 or *sheri.belcher@finra.org*; or
- Brant K. Brown, Associate General Counsel, Office of General Counsel, at (202) 728-6927 or *brant.brown@finra.org*.

March 2015

Notice Type
- Guidance

Suggested Routing
- Compliance
- Internal Audit
- Legal
- Operations
- Risk
- Senior Management
- Systems
- Technology
- Trading
- Training

Key Topics
- Algorithmic Trading Strategies
- High Frequency Trading
- Self-Trades
- Supervision
- Systems-Related Issues
- Trading Practices

Referenced Rules & Notices
- FINRA Rule 2010
- FINRA Rule 3110
- FINRA Rule 5210
- FINRA Rule 6140
- NTM 98-96
- NTM 89-34
- Regulatory Notice 14-10
- SEC Regulation NMS
- SEC Regulation SCI
- SEC Regulation SHO
- SEA Rule 15c3-5 (Market Access Rule)

Background & Discussion

This *Notice* is one of seven FINRA initiatives relating to equity market structure and automated trading activities, including HFT.[1] These initiatives are designed to increase the scope of trading information FINRA receives, provide more transparency into trading activities to market participants and investors, and require firms engaged in electronic trading and their employees to be trained, educated and accountable for their role in equity trading.

As algorithmic strategies have grown to account for a substantial portion of activity on U.S. securities markets, the potential for such strategies to adversely impact market and firm stability has likewise grown. FINRA member firms that engage in algorithmic strategies are already subject to a number of existing SEC and FINRA rules governing their trading activities, including those listed below, as well as FINRA Rule 3110 (Supervision).[2] Thus, many existing requirements address the risks of, and impose obligations on, trading activity conducted by algorithmic strategies.

FINRA has long noted that, in addition to specific requirements imposed on trading activity, firms have a fundamental obligation generally to supervise their trading activity to ensure that the activity does not violate any applicable FINRA rule, provision of the federal securities laws or any rule thereunder.[3] This would include, for example, ensuring that the firm's trading activity that uses algorithmic strategies complies with applicable rules and regulations, including:

- **FINRA Rule 5210 (Publication of Transactions and Quotations):** Rule 5210 provides that "no member shall publish or circulate, or cause to be published or circulated, any ...communication of any kind which purports to report any transaction as a purchase or sale of any security unless such member believes that such transaction was a bona fide purchase or sale of such security; or which purports to quote the bid price or asked price for any security, unless such member believes that such quotation represents a bona fide bid for, or offer of, such security." This rule prohibits activities such as fictitious quoting, spoofing and layering of quotes. In addition, Supplementary Material .02 to Rule 5210 requires firms to adopt policies and procedures regarding "self-trades," which are defined as "transactions in a security resulting from the unintentional interaction of orders originating from the same firm that involve no change in the beneficial ownership of the security."[4] Under Rule 5210 and Supplementary Material .02, firms must have policies and procedures in place that are reasonably designed to review their trading activity for, and prevent, a pattern or practice of self-trades resulting from orders originating from a single algorithm or trading desk or from related algorithms or trading desks. Self-trades resulting from orders that originate from unrelated algorithms or separate and distinct trading strategies within the same firm are generally considered to be bona fide transactions.

- **FINRA Rule 6140 (Other Trading Practices):** Rule 6140 contains several provisions that were adopted to ensure the promptness, accuracy and completeness of last sale information and to prevent that information from being publicly trade reported in a fraudulent or manipulative manner. For example, Rule 6140(a) prohibits a firm from executing purchases of NMS stocks at successively higher prices (or sales at successively lower prices) for the purpose of creating or inducing a false, misleading or artificial appearance of activity in such security; unduly or improperly influencing the market price for such security; or establishing a price that does not reflect the true state of the market for such security.
- **FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade):** Rule 2010 requires firms, in the conduct of their business, to observe high standards of commercial honor and just and equitable principles of trade. These general requirements extend to any trading activity engaged in by the firm.
- **SEC's Market Access Rule (Securities Exchange Act Rule 15c3-5):** SEA Rule 15c3-5 requires brokers and dealers with market access,[5] or that provide customers with market access, to establish, document and maintain a system of risk management controls and supervisory procedures that are reasonably designed to manage the financial and regulatory risks related to market access.[6] A firm with market access is also required to establish, document and maintain a system for regularly reviewing the effectiveness of the risk management controls and supervisory procedures and for promptly addressing any issues.
- **SEC Regulation NMS:** Regulation NMS includes multiple provisions regarding the national market system that affect a firm's trading activity.[7] For example, Rule 611, the Order Protection Rule, requires trading centers (*e.g.*, national securities exchanges, ATSs, exchange and OTC market makers, and brokers or dealers that execute orders internally by trading as principal or crossing orders as agent) to establish, maintain and enforce written policies and procedures reasonably designed to prevent the execution of trades at prices inferior to protected quotations displayed by other trading centers, or, if relying on one of Rule 611's applicable exceptions, that are reasonably designed to assure compliance with the exception.[8] Trading centers must surveil regularly to ascertain the effectiveness of their policies and procedures and take prompt action to remedy deficiencies. In addition, Rule 610, the Access Rule, includes provisions designed to prevent locked or crossed markets.[9]
- **SEC Regulation SHO:** Regulation SHO establishes a set of requirements regarding a firm's ability to sell securities short.[10] For example, Rule 201(b)(1) requires that trading centers establish, maintain and enforce written policies and procedures reasonably designed to prevent the execution or display of a short sale order in a covered security that has declined 10 percent or more from the prior day's closing price at a price that is less than or equal to the current national best bid.[11] This prohibition remains in effect for the remainder of that trading day and the following trading day when a national best bid is calculated and disseminated on a continuing basis by a plan processor pursuant to an effective national market system plan.

With the occurrence of a number of market-impacting events related to technology issues in the past several years, the SEC, FINRA, other U.S. and foreign regulators, academics and commentators have focused on the issues of whether the current regulatory framework provides sufficient protection against the occurrence of technology failures by market participants, particularly where the failures can have a systemic impact on our highly automated and interconnected markets, and whether additional steps are necessary to mitigate the risks of the reoccurrence of such events in the future.[12] Most recently, the SEC adopted Regulation SCI with the stated intent of strengthening the technological infrastructure of key market participants. Although, as adopted, Regulation SCI applies primarily to self-regulatory organizations and alternative trading systems (ATSs) and not to broker-dealer algorithmic trading activity, the SEC stated that it could in the future seek comment on whether to expand the scope of Regulation SCI to include broker-dealer operations as well.[13] The guidance in this *Notice* regarding firms' responsibilities for their algorithmic strategies is consistent with the SEC's fundamental approach in Regulation SCI of requiring that comprehensive policies and procedures be in place for certain technological systems and mandating the testing and review of those systems.

FINRA staff has conducted a number of examinations and investigations over the past several years that were prompted by the detection of systems-related issues at firms engaged in algorithmic strategies, and several of these investigations have resulted in settlements of formal actions. Among other things, these actions have noted that some firms lack appropriate supervisory controls and procedures related to the creation, modification, usage and testing of trading algorithms for such activity as wash sales and excessive levels of message traffic. As a result of these reviews and working with member firms engaged in algorithmic strategies, FINRA has developed the following list of suggested effective practices for such firms. These effective practices are focused on five main areas: General Risk Assessment and Response; Software/Code Development and Implementation; Software Testing and System Validation; Trading Systems; and Compliance.

As an initial matter, firms must have appropriate policies and procedures in place to review and test any trading algorithms they use, including development, deployment and post-implementation monitoring of algorithmic strategies. Although a reasonable supervision and control program will not foresee every potential failure or prevent every undesirable consequence, this *Notice* provides a list of effective supervision and control practices for firms that use algorithmic strategies that are based largely on FINRA staff's examination and investigative work related to algorithmic strategies. FINRA believes that firms' implementation of the suggested effective practices may help to reduce the future occurrence of unintended systems issues by firms engaging in algorithmic strategies; however, the list below is not intended to be an exhaustive list of steps firms should consider in conducting such activities. The suggested effective practices are largely drawn from discrete issues FINRA staff identified in connection with specific investigations and examinations. A firm's implementation of these effective practices in and of themselves

would not necessarily suffice to satisfy its supervisory and other obligations that may arise under FINRA rules, the rules of other self-regulatory organizations, and SEC rules and regulations. In this regard, the effective practices below complement, rather than supplant, obligations firms have under existing or future rules and regulations, including those noted above.

Suggested Effective Practices for Firms Engaging in Algorithmic Strategies

I. General Risk Assessment and Response

As noted above, as the use of algorithmic strategies has increased, the potential of such strategies to adversely impact market and firm stability has likewise grown. When assessing the risk the use of algorithmic strategies creates, firms should undertake a holistic review of their trading activity and consider implementing a cross-disciplinary committee to assess and react to the evolving risks associated with algorithmic strategies.[14] These committees are most effective when they include representation from areas outside of trading, such as those engaged in support and control types of functions within the firm.

II. Software/Code Development and Implementation

A firm's supervisory efforts should be focused on every stage in the process of developing algorithmic strategies and not be limited to reviewing trading activity by algorithmic strategies only after they have been put into production. Consequently, firms should also focus efforts on the development of algorithmic strategies and on how those strategies are tested and implemented. Firms should consider, for example:

- implementing a development and change management process that tracks the development of new trading code or material changes to existing code. An effective process should include a review of test results and a set of approval protocols that are appropriate given the scope of the code or any change(s) to the code.[15]
- monitoring activity to assure that algorithm development and change procedures are followed.
- employing redundant or multiple system validations before introducing new or materially changed code into production.
- archiving code versions in a retrievable manner for a period of time that is reasonable in view of the firm's size and the complexity of its algorithmic trading program.
- maintaining, at a minimum, a basic summary description of algorithmic strategies that enables supervisory, compliance and regulatory staff to understand the intended function of an algorithm without the need to resort, as an initial matter, to direct code review.
- providing mechanisms by which the firm may quickly disable the algorithm or supporting platform with a minimal number of steps.

- when implementing controls, account where necessary for the particular type or location of hardware as well as an algorithm's destination trading center. For example, if the hardware is co-located with a specific trading center or the code is targeted toward an individual trading center, or specific order types offered only through an individual trading center, it may call for different controls than code or hardware that can be used for multiple trading centers.
- where feasible, deploying new algorithmic strategies in a pilot phase of limited size, increasing only as results are confirmed.
- when deploying new code, maintaining heightened scrutiny of the impacted trading account, including real-time monitoring of the subject algorithmic strategy.

III. Software Testing and System Validation

Testing of algorithmic strategies prior to being put into production is an essential component of effective policies and procedures. When developing their policies and procedures around testing and system validations, firms should consider:

- conducting testing to confirm that core code components operate as intended and do not produce unintended consequences. To the extent practicable, firms should consider the profile of the subject security, market and the existence of adverse or fast market conditions.
- establishing a quality assurance process such that testing is performed independently of code development.
- implementing and periodically evaluating test controls to confirm their adequacy and reliability.
- implementing data integrity, accuracy and workflow validation testing processes.
- maintaining a record of testing protocols and results, as well as the remediation of identified significant code defects.
- conducting any significant testing in a development environment that is segregated from production.

IV. Trading Systems

A firm's supervisory obligations continue after any algorithmic strategy is put into production. Consequently, firms should develop their policies and procedures to include review of trading activity after an algorithmic strategy is in place or has been changed. Firms should consider:

- implementing controls, monitors, alerts and reconciliation processes that enable the firm to quickly identify whether an algorithm is experiencing unintended results that may indicate a failure at the firm or in the market.

- periodically evaluating the firm's controls and associated policies and procedures to assure that they remain adequate to manage access and changes to the firm's infrastructure including, but not limited to, the hardware, connectivity, and algorithms.
- implementing a protocol to track and record significant system problems.
- documenting and periodically reviewing parameter settings for the firm's risk controls, and making any parameter changes deemed appropriate.
- implementing checks on downstream market impacts.[16]
- making system capacity scalable to the extent a firm anticipates growth and peak levels of market activity such as messaging volume.
- implementing security measures to limit code access and control system entitlements.
- placing appropriate controls and limitations on a trader's ability to overwrite or otherwise evade system controls.
- implementing controls to manage outbound message volume via threshold parameters.

V. Compliance

Ensuring that there is effective communication between compliance staff and the staff responsible for algorithmic strategy development is a key element of effective policies and procedures. To that end, firms should consider:

- developing compliance monitoring tools that are broad enough in scope to include activity that may result from the interaction of multiple algorithms (*e.g.*, wash sales, self-trades, manipulation).
- providing for adequate communication between supervisory and compliance staff related to the function and control of algorithms such that the firm meets its regulatory obligations.
- implementing periodic training for supervisory and compliance staff related to the firm's policies and procedures regarding algorithmic strategies.
- conducting periodic evaluations of compliance tools and updating those tools as appropriate.
- conducting periodic reviews of the adequacy of staffing levels and expertise for responding to regulatory inquiries and conducting surveillance of the firm's activities to monitor for compliance with applicable self-regulatory organization rules and federal securities laws.
- implementing controls, monitoring tools and alerts to address the operation and financial risks of algorithmic strategies and aggregate firm activity, and periodically evaluating the supervisory framework in light of current market conditions.

Endnotes

1. *See* FINRA's September 19, 2014, News Release "*FINRA Board Approves Series of Equity Trading and Fixed Income Rulemaking Items*."

2. Effective December 1, 2014, NASD Rule 3010 was moved into the Consolidated FINRA Rulebook as FINRA Rule 3110. *See* *Regulatory Notice 14-10* (March 2014).

3. *See, e.g.*, *Notice to Members 98-96* (December 1998) (outlining minimum standards that the written supervisory procedures and supervisory systems of firms engaged in market-making activities must meet); *Notice to Members 89-34* (April 1989) (noting that a firm's "supervisory system must cover all aspects of the firm's investment banking and securities business, including back office; corporate financing; trading activity;" and other types of activity).

4. For a full discussion of Supplementary Material .02, *see* *Regulatory Notice 14-28* (June 2014). Wash sales (*i.e.*, trading involving no change in beneficial ownership that is intended to produce the false appearance of trading) continue to be strictly prohibited under both the federal securities laws and FINRA rules. *See, e.g.*, 15 U.S.C. 78i(a)(1); FINRA Rule 6140(b).

5. The term "market access" is defined as access to trading in securities (i) on an exchange or alternative trading system (ATS) as a result of being a member or subscriber of the exchange or ATS or (ii) on an ATS provided by a broker-dealer operator of an ATS to a non-broker-dealer. The term includes not only sponsored access and direct market access, but also includes access to trading for proprietary accounts or more traditional agency trading activities. *See* 17 CFR 240.15c3-5(a)(1).

6. *See* 17 CFR 240.15c3-5.

7. *See* 17 CFR 242.600 et seq.

8. *See* 17 CFR 242.611.

9. *See* 17 CFR 242.610.

10. *See* 17 CFR 242.200 et seq.

11. *See* 17 CFR 242.201(b)(1). The prior day's closing price is determined as of the end of the prior day's regular trading hours on the security's listing market. *See* 17 CFR 242.201(b)(3).

12. Among the many efforts in this regard are the following. The SEC hosted a roundtable entitled Technology and Trading Roundtable: Promoting Stability in Today's Markets in October 2012, and, in November 2014, the SEC adopted Regulation Systems Compliance and Integrity (Regulation SCI). *See* Securities Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72252 (December 5, 2014). A transcript of the SEC roundtable is available at *http://www.sec.gov/news/otherwebcasts/2012/ttr100212-transcript.pdf*. In September 2013, the CFTC approved for publication *Concept Release on Risk Controls and System Safeguards for Automated Trading Environments* setting forth a series of proposed risk controls for participants in the futures markets. *See* Commodity Futures Trading Commission Release, 78 FR 56542 (September 12, 2013). The CFTC reopened the comment period for this CFTC Concept Release on January 21, 2014, through February 14, 2014. *See* Commodity Futures Trading Commission Release, 79 FR 4104 (January 24, 2014). The Federal Reserve Bank of Chicago conducted a survey of how HFT firms control risks. *See* Carol Clark and Rajeev Ranjan, *How Do Proprietary Trading Firms Control the Risks of High Speed Trading?* March 2012. A working group has written a proposal for the adoption of an ISO 9000-like standard for firms engaged in HFT. *See* Ben Van Vliet et al.,

The Rationale for HFT 9000: An ISO 9000-style Quality Management System for High Frequency Trading, August 2012. In October 2012, the Foresight Programme of the UK Government Office for Science released its final report relating to potential measures to be taken as a consequence of the growth of computerized trading in the financial markets. *See* Government Office for Science, London, Foresight: *The Future of Computer Trading in Financial Markets* (2012). The European Securities Markets Association (ESMA) issued guidelines for entities engaged in automated trading. *See* ESMA, *Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms, and competent authorities*, December 2011. In November 2010, the FIA Principal Traders Group issued a series of recommendations for risk controls over electronic trading. *See* FIA Principal Traders Group, *Recommendations for Risk Controls for Trading Firms*, November 2010.

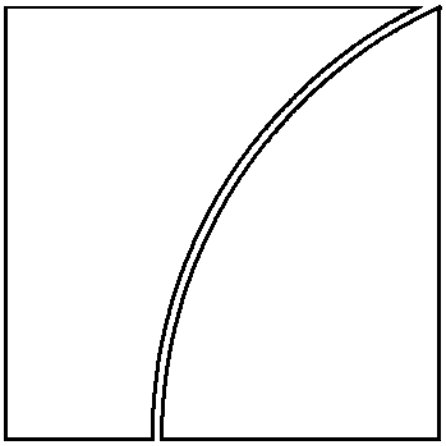
13. *See* Securities Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72252 (December 5, 2014).

14. Although cross-disciplinary committees may help firms with their compliance efforts regarding algorithmic strategies, committees should not take the place of oversight of these strategies by appropriately registered personnel of the firm.

15. While the application of these effective practice suggestions may vary greatly across firms, it is generally appropriate to give greater focus to material code portions and system functions.

16. While not an exhaustive list, particular consideration should be given to monitoring for activity such as messaging volume, order looping, and matched or wash trades.

Basel Committee
on Banking Supervision



Principles for the Sound Management of Operational Risk

June 2011

BANK FOR INTERNATIONAL SETTLEMENTS

Copies of publications are available from:

Bank for International Settlements
Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org

Fax: +41 61 280 9100 and +41 61 280 8100

This publication is available on the BIS website (www.bis.org).

ISBN 92-9131-857-4 (print)
ISBN 92-9197-857-4 (online)

Members of the SIG Operational Risk Subgroup

Chairman: Mitsutoshi Adachi, Bank of Japan

Australian Prudential Regulation Authority	Michael Booth
National Bank of Belgium	Jos Meuleman
Banco Central do Brasil, Brazil	Wagner Almeida
Office of the Superintendent of Financial Institutions, Canada	James Dennison Aina Liepins
China Banking Regulatory Commission	Meng Luo
Banque de France	Jean-Luc Quémard
Deutsche Bundesbank, Germany	Marcus Haas
Federal Financial Supervisory Authority (BaFin), Germany	Frank Corleis
Reserve Bank of India	Rajinder Kumar
Bank of Italy	Marco Moscadelli
Bank of Japan	Madoka Miyamura
Financial Services Agency, Japan	Tsuyoshi Nagafuji
Surveillance Commission for the Financial Sector, Luxembourg	Didier Bergamo
Netherlands Bank	Claudia Zapp
Polish Financial Supervision Authority	Grazyna Szwajkowska
Central Bank of the Russian Federation	Irina Yakimova
South African Reserve Bank	Jan van Zyl
Bank of Spain	María Ángeles Nieto
Finansinspektionen, Sweden	Agnieszka Arshamian
Swiss Financial Market Supervisory Authority	Paul Harpes
Financial Services Authority, United Kingdom	Andrew Sheen Khim Murphy
Federal Deposit Insurance Corporation, United States	Alfred Seivold
Federal Reserve Board, United States	Adrienne Townes Haden Kenneth G. Fulton
Federal Reserve Bank of Boston, United States	Patrick de Fontnouvelle
Federal Reserve Bank of New York, United States	Ronald Stroz
Office of the Comptroller of the Currency, United States	Carolyn DuChene Maurice Harris
Office of Thrift Supervision, United States	Eric Hirschhorn
Financial Stability Institute	Amarendra Mohan
Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements	Andrew Willis

Contents

Principles for the Sound Management of Operational Risk and the Role of Supervision

Preface

1. In the *Sound Practices for the Management and Supervision of Operational Risk* (Sound Practices), published in February 2003, the Basel Committee on Banking Supervision (Committee) articulated a framework of principles for the industry and supervisors. Subsequently, in the 2006 *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version* (commonly referred to as "Basel II"), the Committee anticipated that industry sound practice would continue to evolve.[1] Since then, banks and supervisors have expanded their knowledge and experience in implementing operational risk management frameworks (Framework). Loss data collection exercises, quantitative impact studies, and range of practice reviews covering governance, data and modelling issues have also contributed to industry and supervisory knowledge and the emergence of sound industry practice.

2. In response to these changes, the Committee has determined that the 2003 Sound Practices paper should be updated to reflect the enhanced sound operational risk management practices now in use by the industry. This document – *Principles for the Sound Management of Operational Risk and the Role of Supervision* – incorporates the evolution of sound practice and details eleven principles of sound operational risk management covering (1) governance, (2) risk management environment and (3) the role of disclosure. By publishing an updated paper, the Committee enhances the 2003 sound practices framework with specific principles for the management of operational risk that are consistent with sound industry practice. These principles have been developed through the ongoing exchange of ideas between supervisors and industry since 2003. *Principles for the Sound Management of Operational Risk and the Role of Supervision* replaces the 2003 Sound Practices and becomes the document that is referenced in paragraph 651 of Basel II.

3. *A Framework for Internal Control Systems in Banking Organisations* (Basel Committee, September 1998) underpins the Committee's current work in the field of operational risk. *The Core Principles for Effective Banking Supervision* (Basel Committee, October 2006) and the *Core Principles Methodology* (Committee, October 2006), both for supervisors, and the principles identified by the Committee in the second pillar (supervisory review process) of Basel II are also important reference tools that banks should consider when designing operational risk policies, processes and risk management systems.

4. Supervisors will continue to encourage banks "to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices".[2] Consequently, while this paper articulates principles from emerging sound industry practice, supervisors expect banks to

---

[1] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006.

[2] BCBS (2006), paragraph 646.

continuously improve their approaches to operational risk management. In addition, this paper addresses key elements of a bank's Framework. These elements should not be viewed in isolation but should be integrated components of the overall framework for managing operational risk across the enterprise.

5. The Committee believes that the principles outlined in this paper establish sound practices relevant to all banks. The Committee intends that when implementing these principles, a bank will take account of the nature, size, complexity and risk profile of its activities.

Role of Supervisors

6. Supervisors conduct, directly or indirectly, regular independent evaluations of a bank's policies, processes and systems related to operational risk as part of the assessment of the Framework. Supervisors ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank**.**

7. Supervisory evaluations of operational risk include all the areas described in the principles for the management of operational risk. Supervisors also seek to ensure that, where banks are part of a financial group, there are processes and procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In performing this assessment, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary.[3] Some supervisors may choose to use external auditors in these assessment processes.[4]

8. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors use the tools most suited to the particular circumstances of the bank and its operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms directly with banks and external auditors (eg internal bank management reports on operational risk could be made routinely available to supervisors).

9. Supervisors continue to take an active role in encouraging ongoing internal development efforts by monitoring and evaluating a bank's recent improvements and plans for prospective developments. These efforts can then be compared with those of other banks to provide the bank with useful feedback on the status of its own work. Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process.

---

[3] Refer to the Committee's papers *High-level principles for the cross-border implementation of the New Accord*, August 2003, and *Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA)*, November 2007.

[4] For further discussion, see the Committee's paper *The relationship between banking supervisors and bank's external auditors*, January 2002.

Principles for the management of operational risk

10. Operational risk[5] is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme. As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems. The Committee, through the publication of this paper, desires to promote and enhance the effectiveness of operational risk management throughout the banking system.

11. Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each.

12. Sound internal governance forms the foundation of an effective operational risk management Framework. Although internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk operational risk management challenges may differ from those in other risk areas.

13. The Committee is seeing sound operational risk governance practices adopted in an increasing number of banks. Common industry practice for sound operational risk governance often relies on three lines of defence – (i) business line management, (ii) an independent corporate operational risk management function and (iii) an independent review.[6] Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary. In all cases, however, a bank's operational risk

---

[5] Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

[6] As discussed in the Committee's paper *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches*, June 2011, independent review includes the following components:

Verification of the Framework is done on a periodic basis and is typically conducted by the bank's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall Framework, consistent with policies approved by the board of directors, and also test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies.

Validation ensures that the quantification systems used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

governance function should be fully integrated into the bank's overall risk management governance structure.

14. In the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

15. A functionally independent corporate operational risk function (CORF)[7] is typically the second line of defence, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

16. The third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

17. If operational risk governance utilises the three lines of defence model, the structure and activities of the three lines often varies, depending on the bank's portfolio of products, activities, processes and systems; the bank's size; and its risk management approach. A strong risk culture and good communication among the three lines of defence are important characteristics of good operational risk governance.

18. Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively.[8] Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as the third line of defence.

19. Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the Framework meets organisational needs and supervisory expectations. For example, while internal audit

---

[7] In many jurisdictions, the independent corporate operational risk function is known as the corporate operational risk management function.

[8] The Committee's paper, *Internal Audit in Banks and the Supervisor's Relationship with Auditors,* August 2001, describes the role of internal and external audit.

should not be setting specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

20. Because operational risk management is evolving and the business environment is constantly changing, management should ensure that the Framework's policies, processes and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers' concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings.

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management[9] should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture[10] exists throughout the whole organisation.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Governance[11]

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement[12] for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

---

[9] This paper refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

[10] Internal operational risk culture is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management.

[11] See also the Committee's *Principles for enhancing corporate governance*, October 2010.

Senior Management

Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

Risk Management Environment

Identification and Assessment

Principle 6: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Monitoring and Reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Control and Mitigation

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Business Resiliency and Continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

---

[12] "Risk appetite" is a high level determination of how much risk a firm is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance. "Risk tolerance" is a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept. In this document the terms are used synonymously.

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

21. Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

22. The board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.[13]

23. Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organisation. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

24. The fundamental premise of sound risk management is that the board of directors and bank management understand the nature and complexity of the risks inherent in the portfolio of bank products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems.

25. A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation

[13] See also: the Committee's *Report on the range of methodologies for the risk and performance alignment of remuneration,* May 2011*;* the Financial Stability Forum's *Principles for sound compensation practices*, April 2009; and the Financial Stability Board's *FSB principles for sound compensation practices – implementation standards*, September 2009.

including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

26. The Framework should be comprehensively and appropriately documented in board of directors approved policies and should include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework.

27. Framework documentation should clearly:

(a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

(b) describe the risk assessment tools and how they are used;

(c) describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

(d) describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(e) establish risk reporting and Management Information Systems (MIS);

(f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives[14];

(g) provide for appropriate independent review and assessment of operational risk; and

(h) require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

Governance

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

28. The board of directors should:

(a) establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control

[14] An inconsistent taxonomy of operational risk terms may increase the likelihood of failing to identify and categorise risks, or allocate responsibility for the assessment, monitoring, control and mitigation of risks,

environments that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise;

(b) provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management;

(c) regularly review the Framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (eg changing business volumes);

(d) ensure that the bank's Framework is subject to effective independent review by audit or other appropriately trained parties; and

(e) ensure that as best practice evolves management is availing themselves of these advances.[15]

29. Strong internal controls are a critical aspect of operational risk management, and the board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.

30. When approving and reviewing the risk appetite and tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors should approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.

31. The board of directors should regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches. The board should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

Senior Management

Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the

---

[15] See the Committee's 2006 *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version;* paragraph 718(xci).

organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

32. Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three lines of defence approach is operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.

33. Senior management should translate the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

34. Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

35. The managers of the CORF should be of sufficient stature within the bank to perform their duties effectively, ideally evidenced by title commensurate with other risk management functions such as credit, market and liquidity risk.

36. Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.

37. A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

(a) Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee;

(b) Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include

independent non-executive board members, which is a requirement in some jurisdictions; and

(c) Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

Risk Management Environment

Identification and Assessment

Principle 6: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

38. Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors[16] and external factors.[17] Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.

39. Examples of tools that may be used for identifying and assessing operational risk include:

(a) Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors.

(b) Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic.[18] Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

(c) External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures;

---

[16] For example, the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover.

[17] For example, changes in the broader environment and the industry and advances in technology.

[18] Mapping internal loss data, particularly in larger banks, to the Level 1 business lines and loss event types defined in Annexes 8 and 9 of the 2006 Basel II document can facilitate comparison with external loss data.

(d) Risk Assessments: In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

(e) Business Process Mapping: Business process mappings identify the key steps in business processes, activities and organisational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action;

(f) Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

(g) Scenario Analysis: Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;

(h) Measurement: Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

(i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

40. The bank should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

41. In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations. A bank should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

42. A bank should have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process should consider:

(a) inherent risks in the new product, service, or activity;

(b) changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;

(c) the necessary controls, risk management processes, and risk mitigation strategies;

(d) the residual risk;

(e) changes to relevant risk thresholds or limits; and

(f) the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

Monitoring and Reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

43. Banks are encouraged to continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.

44. Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The results of monitoring activities should be included in regular management and board reports, as should assessments of the Framework performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.

45. Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:

(a) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;

(b) details of recent significant internal operational risk events and losses; and

(c) relevant external events and any potential impact on the bank and operational risk capital.

46. Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

Control and Mitigation

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

47. Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.[19]

48. Control processes and procedures should include a system for ensuring compliance with policies. Examples of principle elements of a policy compliance assessment include:

(a) top-level reviews of progress towards stated objectives;

(b) verifying compliance with management controls;

(c) review of the treatment and resolution of instances of non-compliance;

(d) evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management; and

(e) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

49. An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and be subject to careful independent monitoring and review.

[19] The Committee's paper *Framework for Internal Control Systems in Banking Organisations*, September 1998, discusses internal controls in greater detail.

50. In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:

(a) clearly established authorities and/or processes for approval;

(b) close monitoring of adherence to assigned risk thresholds or limits;

(c) safeguards for access to, and use of, bank assets and records;

(d) appropriate staffing level and training to maintain expertise;

(e) ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;[20]

(f) regular verification and reconciliation of transactions and accounts; and

(g) a vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

51. Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.

52. The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.[21] Sound technology risk management uses the same precepts as operational risk management and includes:

(a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;

(b) policies and procedures that facilitate identification and assessment of risk;

(c) establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;

(d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and

(e) monitoring processes that test for compliance with policy thresholds or limits.

53. Management should ensure the bank has a sound technology infrastructure[22] that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated

---

[20] For example, where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach.

[21] Refer also to the Committee's July 1989 paper *Risks in Computer and Telecommunication System*, and its May 2001 paper *Risk Management Principles for Electronic Banking*.

[22] Technology infrastructure refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.

and comprehensive risk management. Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.

54. Outsourcing[23] is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

(a) procedures for determining whether and how activities can be outsourced;

(b) processes for conducting due diligence in the selection of potential service providers;

(c) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;

(d) programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;

(e) establishment of an effective control environment at the bank and the service provider;

(f) development of viable contingency plans; and

(g) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

55. In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme. While the specific insurance or risk transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.[24]

56. Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having

---

[23] Refer also to the Joint Forum's February 2005 paper *Outsourcing in Financial Services*.

[24] See also the Committee's paper, *Recognising the risk-mitigating impact of insurance in operational risk modelling,* October 2010.

mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (eg counterparty risk).

Business Resiliency and Continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.[25]

57. Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

58. Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes. A bank should identify critical business operations,[26] key internal and external dependencies,[27] and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.

59. A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

---

[25] The Committee's paper, *High-level principles for business continuity,* August 2006, discusses sound continuity principles in greater detail.

[26] A bank's business operations include the facilities, people and processes for delivering products and services or performing core activities, as well as technology systems and data.

[27] External dependencies include utilities, vendors and third-party service providers.

Role of Disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

60. A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice.

61. A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

62. A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.[28]

63. A bank should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.[29]

---

[28] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006, paragraph 810.

[29] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, Section V (Operational Risk), paragraph 646, Basel, June 2006, paragraph 821.

Appendix

Reference material

A Framework for Internal Control Systems in Banking Organisations (BCBS, September 1998)

Internal audit in banks and the supervisor's relationship with auditors (BCBS, August 2001)

The relationship between banking supervisors and bank's external auditors (BCBS, January 2002)

Core Principles for Effective Banking Supervision (BCBS, October 2006)

Core Principles Methodology (BCBS, October 2006)

High-Level Principles for Business Continuity (BCBS, August 2006)

Outsourcing in financial services (Joint Forum, February 2005)

Risk Management Principles for Electronic Banking (BCBS, May 2001)

Risks in Computer and Telecommunication Systems (BCBS, July 1989)

Principles for Enhancing Corporate Governance (BCBS, October 2010)

Recognising the risk-mitigating impact of insurance in operational risk modelling (BCBS, October 2010)

High-level principles for the cross-border implementation of the New Accord (BCBS, August 2003)

Principles for home-host supervisory cooperation and allocation mechanisms in the context of Advanced Measurement Approaches (AMA) (BCBS, November 2007)

National Examination Risk Alert

By the Office of Compliance Inspections and Examinations[1]

Volume II, Issue 2 **February 27, 2012**

Key Takeaways:

This Risk Alert encourages firms to review their controls designed to prevent unauthorized trading and other unauthorized activities.

Unauthorized activities may include a range of activities. Thus, controls should address: potential unauthorized trading for the firm's own account or for a customer or client account; position mismarking; exceeding trading limits; personal trading activities of associated persons or other employees; and creation and maintenance of inaccurate or altered records.

Strengthening Practices for Preventing and Detecting Unauthorized Trading and Similar Activities

Introduction

Unauthorized trading or other unauthorized activities are not a new problem. Such activities may cause firms and investors to incur losses, and subject firms to legal, regulatory and reputational risks. While broker-dealers and investment advisers are subject to different regulatory requirements, their risk exposures can be similar.[2] In this Alert, we use the term "unauthorized trading" to refer broadly to a range of activities, including:

- "rogue" or other unauthorized trading or trade execution in customer or client or proprietary accounts;
- exceeding firm limits on position exposures, risk tolerances and losses;
- intentional mismarking of positions; and
- creating records of nonexistent (or sham) transactions.

The staff recommends that in any review of business practices and internal controls, firms should seek to identify any circumstances that might permit an individual (or group of

---

[1] The Securities and Exchange Commission ("SEC"), as a matter of policy, disclaims responsibility for any publication or statement by any of its employees. The views expressed herein are those of the staff of the Office of Compliance Inspections and Examinations, in coordination with other SEC staff, including in the Division of Trading and Markets, and do not necessarily reflect the views of the Commission or the other staff members of the SEC. *This document was prepared by the SEC staff and is not legal advice.*

[2] With regard to broker-dealers, see FINRA Regulatory Notice 08-18 dated April 2008 (the "FINRA Notice") that addressed risks and set forth a non-exclusive set of practices designed to prevent or mitigate the risk of unauthorized trading. With regard to registered investment advisers, *see* Compliance Programs of Investment Companies and Investment Advisers, Advisers Act Release No. 2204 (December 17, 2003), 68 F.R. 74714 (Dec. 23, 2004).

individuals) to engage in or conceal unauthorized transactions. Such individuals may include traders, trader assistants, portfolio managers, brokers, investment advisers, order placement personnel or trading desks, (collectively, "traders"), as well as mid-or back-office, risk management and other personnel.

One critical element in mitigating the risks posed by unauthorized trading is to have independent and mutually reinforcing controls. Toward this end, firms may want to consider actively engaging such control functions as operational risk, audit, legal and compliance to work closely with management in performing an independent identification of risks and practices that could permit unauthorized trading. A fresh review of reports of past unauthorized trading incidents suffered by the industry may be illustrative in this effort. It may also be appropriate to review and/or test internal controls on a regular basis as well as assessing their adequacy to prevent unauthorized trading in light of internal business changes and current market conditions, among other factors.

Upon identifying any potential weaknesses that could enable unauthorized trading, firms should consider working closely with the above-mentioned control functions to develop enhanced controls and processes to address such weaknesses. Management and non-management employees should be appropriately trained to identify unauthorized activity. Firms also should carefully consider how best to facilitate proper and immediate escalation of any detected activity without fear of retaliation.

Some Insights

Highlighted below are some insights from the Commission's National Examination Program that may help firms identify risks and strengthen their practices for preventing and detecting unauthorized trading. This Alert is not intended as a comprehensive summary of all supervisory and compliance matters pertaining to unauthorized trading; rather, it discusses certain measures that may assist firms in complying with their supervisory and compliance obligations. Firms are encouraged to consider the practices described below in assessing their own procedures and implementing improvements that will best protect the firm and its clients. Firms are cautioned that these factors and suggestions are not exhaustive, and they constitute neither a safe harbor nor a "checklist." Other practices besides those highlighted here may be appropriate as alternatives

or supplements to such practices. The adequacy of compliance or supervisory controls can be determined only with reference to the profile of the specific firm and the specific facts and circumstances. [3]

- **Front Office Supervision:** The firm's supervisory structure, both on the trading desk and across the firm, is its most important control. Strong and effective business line supervision at all levels is essential both to promote an overall culture of compliance and to detect and prevent unauthorized trading. Below are some elements that can be considered when a firm assesses its supervision systems.

  - *Define independent and clear reporting lines*. This should include making provision for mutually reinforcing checks and balances, so that more than one person and chain of control are responsible for monitoring the integrity of a business activity.

  - *Knowledge of Complex Securities/Trading Strategies:* In order to provide effective front office supervision, it is important for those within the chain of management and supervision to have an appropriate understanding of the complex products and trading strategies employed by the firm's traders.

  - *Discussions with Direct and Indirect Reports:* Beyond systems-based trading reviews, direct and indirect supervisors (as appropriate) should engage in discussions with traders, portfolio managers and others and review their trading portfolios or account positions on a holistic basis, focusing on any positions that seem atypical or anomalous given the trading strategy or client mandate. Additional discussions and scrutiny may be required with traders responsible for larger trading books or portfolios, or with lesser experienced traders.

  - *Structuring of incentives.* Consider how well compensation packages and other incentives for traders and their supervisors are aligned with responsible risk-taking.

  - *Disaggregation of functions*. Discourage aggregating functions in one trader or desk (e.g., trade execution, booking, clearance, etc.)

  - *Management "Open-Door" Policy:* Firms may want to instruct traders that, if any position begins to lose value in an unanticipated way, the best course of action is to promptly raise the matter with management. An affirmative "open-door" policy that encourages early reporting of unrealized or unexpected losses may permit

[3] The functions performed by traders vary among businesses and among firms. Traders typically may perform trade execution functions while other aspects of the lifecycle of the transaction, such as booking, clearing and settling a trade, are handled by other personnel or departments. However, there may be situations where traders have some role in such other functions. The practicality of some of the practices described below may depend in part on the specific role performed by a given set of traders, as well as by factors such as their compensation structure, the manner in which trades are cleared and settled, etc.

management to identify and address problems before they manifest themselves in greater harm to the firm and/or its clients or customers.

- *Trading and Booking Systems Reviews:* In addition to discouraging aggregation of trading and post-trade functions (as discussed above), only certain individuals should be granted access to these systems (including for the prevention of insider trading and other violations of securities laws and rules). It is therefore appropriate for supervisors (either directly, through a control function, or more formally through their audit department) to periodically review which traders and other persons have access to particular trading books to determine that their access conforms to their business needs. In particular, the supervisor may want these reviews to focus on ensuring that employees' "legacy" access is removed so that only the appropriate personnel have the ability to book trades into particular portfolios.

- *Potential Additional Controls and Scrutiny:* Supervisors, legal/compliance and operational risk personnel may find it prudent to assess the need for specific additional controls or heightened scrutiny. Some of these controls may lend themselves to daily monitoring.

    - By way of example, some additional controls or heightened scrutiny that could be monitored on a daily or intra-day basis may focus on:

        - trade breaks, unfilled bids and offers, paper tickets and changes in venues where trades are executed;
        - changes in trading patterns;
        - concentrated risks;
        - audit trails;
        - unusual or high volume of error account activity (*e.g.*, cancel/corrects);
        - aged inventory monitoring;
        - manual trade adjustments;
        - unexplained or uncorrelated profitability to a specific book or investment mandate, profile or risk tolerance for a particular trader or client;
        - instances where trades are inappropriately reported to the tape but not cleared, and vice versa; and
        - concentrations of profitable or unprofitable trades, or patterns of trades and offsetting trades, with the same counterparty.

    - Other controls or areas for heightened scrutiny that may also be considered for monitoring on a regular basis include

        - frequency of risk limit breaches;
        - frequent requests for trade limit increases for the same counterparty;
        - reasons for and patterns in remote access to trading accounts;
        - robustness and integrity of controls for trade capture, confirmation and validation; and
        - incentives created by compensation arrangements or promotion criteria.

- Where anomalies are identified that suggest the need for additional analysis and investigation, steps that firms may wish to consider include

    - review of personal and family investments and trading accounts, to the extent that the firm requires that these be available to it for surveillance;
    - review of changes in lifestyle that may evidence an unexplainable increase in wealth; and
    - collection and review of email, phone logs and other communications such as text messages or social networking activities, to the extent that the firm requires these to be available for surveillance.

- **Transfer of Personnel into Trading Positions:** Firms may from time to time offer a trading desk position to personnel from other areas in the firm. Providing employees new opportunities in different areas of the firm may be positive in many respects. At the same time, personnel from areas such as operations, finance or risk control groups that move into trading desk positions may take with them awareness of any idiosyncratic process "workarounds" or procedural weaknesses that could be exploited to hide unauthorized activity. Firms may wish to take this into account in assessing internal controls and securities safeguards on systems, as well as in supervisors being alert to any "red flag" indicators of possible unauthorized trading. In all events, firms are encouraged to determine that all systems access permitted as part of an employee's prior position is terminated prior to any trading by such a transferred individual employee. Some firms terminate all system entitlements, other than payroll-related entitlements, for employees who transfer functions. By treating such employees as a "new hire" with respect to system entitlements, firms have greater assurance that such employees no longer have inappropriate access to mid-or back-office systems. Also, on a periodic basis, supervisors may want to engage a control function or the firm's audit department to verify that unneeded system access has been properly terminated.

- **Extended Settlements/"Rolling" of Positions:** Both extended settlement trades and apparent client or firm positions that are rolled over many times can be cause for potential concern. Firms may wish to consider carefully the development of special supervisory reviews, exception reports or other tools to review transactions that feature extended settlements or "rolls" of positions, based on frequency, length of settlement extensions or extensions that are inconsistent with normal or standard conventions applicable to the particular trading instruments. In some cases, it may be appropriate to contact the client/counterparty to ensure that such person knows the trades as well. As a particularly strong control and a parallel safeguard to its order management system, some firms require a verbal independent confirmation by a designated mid- or back-office person of each extended settlement trade, within minutes of the order being created.

- **Trade Confirmations:** Broker-dealers of course are required to give or send confirmations of securities transactions to their customers.[4] However, inter-company

[4] Securities Exchange Act Rule 10b-10.

transactions where confirmations may not be present and certain delays in obtaining client signatures or authorizations (if any are required) may merit additional scrutiny (*e.g.*, for confirmations of many securities-based derivative transactions) to ensure that such absence or delay is not hiding unauthorized trading. Similarly, the street-side "comparison" process should also be reviewed to ensure that it is not being used to facilitate or hide unauthorized trading. Management may want to consider providing training to middle and operations personnel to emphasize the need to receive timely signed confirmation acknowledgements and when to escalate backlogs.

- **Mandatory Vacations:** Policies requiring mandatory vacations without remote access to trading accounts have been adopted by many firms, requiring traders and perhaps certain other personnel to be out of the office for a period of time (*e.g.*, 10 consecutive business days), without any out-of-office access to the firm. This policy, however, may not necessarily *on its own* bring any unauthorized trading to light, especially if fictitious trades have been booked to the firm. For firms that adopt such mandatory vacation policies, supervisors may consider how best to assign the management of the trader's portfolio(s) to another trader during the trader's absence. For example, it may be prudent to assign the book to another supervisor or to a "peer" trader, as opposed to a less-experienced trader. Similarly, a supervisor may want to do a special review of an absent trader's portfolio(s) during expiration to detect any unusual activity. More generally, firms may wish to consider limiting or eliminating the type of remote trade-book access (e.g., electronic, phone) that traders have while away from the office.

- **Independent Trading Reviews:** Firms should consider actively engaging their audit department and/or control functions such as their compliance department and their financial, credit and operational risk units to periodically check trading strategy, business performance and risk profile.[5] Independent valuation, and validation, of trading positions including any hedging transactions, is an important control. Also, with respect to "strategies," it is important to validate whether traders are actually following a prescribed strategy and whether the performance risk of each strategy is appropriate for the firm's risk profile.

- **Silo Systems:** An additional risk area faced by many firms is that transaction information may exist in multiple automated or other recordkeeping systems. These situations could exist due to: (1) legacy acquisitions; (2) the use of multiple trading platforms; and (3) the use of various security types. The existence of multiple systems may make it difficult to observe, manage, identify and report on transactions seamlessly across a firm. Firms may, as appropriate, work to align disparate systems either through robust reporting, data migration or middleware products to ensure "full picture" monitoring.

- **Control Testing:** Finally, it may be appropriate to periodically test the controls designed to identify unauthorized trading activities. Tests may need to be conducted and reviewed

[5] Risk profile includes market, credit, liquidity, trading supervision and operational risk including review of operational incidents, if any.

by supervisors, or their designees, and, if appropriate, those independent of the businesses with knowledge and experience in both trading various securities and the systems used to support various trading desks.

- **"Tone From the Top":** Past unauthorized trading incidents and regulatory guidance[6] underscore the need for a firm's culture of compliance to be one that is articulated and followed by top-level senior management and one that emphasizes honesty, integrity, accountability and responsible risk-taking, as well as the need for rigorous supervisory and compliance control systems that emphasize quick and proper escalation without fear of retaliation. Financial firms operate in an environment focused on performance but must also create a culture where personnel can acknowledge that the firm's reputation and financial well-being is a shared responsibility. Traders should report unexpected and unusual losses early in order to prevent such losses from becoming worse, and potentially becoming disastrous. Non-trading personnel should be trained to be sensitive to suspicious activities and encouraged to quickly escalate any activity that seems unusual or inconsistent with compliance, financial and operational controls. Management should not tolerate any activity designed to discourage employees from quickly escalating concerns, such as bullying or inappropriately relying on seniority to impede openness.

Conclusion

The risks posed by unauthorized trading are a permanent concern to financial institutions and regulators. The staff hopes that the observations shared above will be helpful to firms in strengthening their compliance and supervisory controls regarding unauthorized trading.

The staff also welcomes comments and suggestions about how the Commission's examination program can better fulfill its mission to promote compliance, prevent fraud, monitor risk, and inform SEC policy.

If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify us at http://www.sec.gov/complaint/info_tipscomplaint.shtml.

[6] FINRA has emphasized the importance of not ignoring unauthorized trading merely because it proved to be profitable, as well as the importance of a "tone at the top" from senior management that establishes a strong corporate culture of compliance. FINRA Notice, *supra* note 2, at 1, 6.