Managing challenges in automated trading services

Regulatory updates and control framework

August 2015
KPMG China
Managing challenges in Automated Trading Services

With the growing dependence on information systems and evolving regulatory requirements, automated trading services (“ATS”) operators are facing heightened technological and operational challenges. Management should be aware of the compliance requirements and appropriately manage these challenges in order to realise the potential competitive advantages which can be gained through technology adoption.

**Automated trading services**

- Internet trading platforms
- Algorithmic trading systems (“Algos”)
- Alternative liquidity pools (“ALPs” or dark pools)
- Smart Order Routers
- Market Making pricing engines
- High-frequency trading systems

**More specific regulatory requirements**

Regulators worldwide are strengthening their focus on electronic trading systems and service providers.

**Hong Kong regulatory updates timeline**

- **1 Jan 2014**
  - Securities and Futures Commission (SFC) launches new requirements under the SFC Code of Conduct to regulate electronic trading.

- **2 Sept 2014**
  - During a supervisory briefing, the SFC emphasises that electronic trading controls will be one of the three future inspection focuses.

- **27 Feb 2015**
  - SFC proposes strengthening the regulation of ATS and ALPs.

- **15 May 2015**
  - SFC releases consultation conclusions on proposals to enhance the regulation of ALPs.

- **2016 onwards**
  - More on-site inspections of electronic trading controls?
  - More specific guidelines and further strengthening of electronic trading control requirements?
Managing challenges in Automated Trading Services

Electronic trading control framework

Based on the SFC’s requirements regarding electronic trading, we have put together a control framework, summarising key controls (order handling and execution trade life cycle) generally applicable to ATS operating in Hong Kong.

- Management structure
- Roles and responsibilities
- Supervision and escalation protocols
- System development life cycle
- Client onboarding governance
- Data encryption
- Network segregation
- Data leakage prevention
- Intrusion prevention
- Capacity management
- Contingency arrangement
- Data backup
- Pre-trade
- Intraday (e.g. key limits, market risk)
- Post-trade
- Monitoring and reporting

Transaction and data controls
- System architecture and design
- Master data governance
- Information barriers
- Cross-system identity and access management

Governance

Cybersecurity

Reliability

Business controls

Are you ready to meet the regulatory requirements?

Electronic trading control compliance checklist

☑ Revisit governance and supervision structure to ensure sufficient management involvement
☑ Ensure latest compliance requirements are fulfilled prior to roll-out of new ATS initiatives
☑ Ensure sufficient records to evidence testing and internal controls requirements
☑ Establish clear classification of “qualified investor” (for ALP)
☑ Reassess adequacy of current staff training programme
☑ Review current technological and operational controls, and identify compliance gaps (refer to pages 3-9 of this publication for suggested control framework)
☑ Develop an ATS compliance road map
☑ Conduct regular compliance monitoring/assessment

© 2015 KPMG, a Hong Kong partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
Taking a closer look

- **Governance structures** with clear lines of accountability, delegated authorities, and standardised policies and procedures for managing business and operational risks.

- **Periodic risk assessment and control effectiveness evaluation** to manage potential risks and control deficiencies.

- **Client onboarding governance** that includes know your customer (KYC), client communication, investor education, proper documentation and disclosure.

- **New electronic business/activities committee** that involves senior management and risk approvals prior to ATS operation.

- **Proper training and user awareness programmes** for both the business and operation teams.

- **Effective reporting mechanism** with well-established escalation protocols.

- **System development life cycle (SDLC)** that defines system testing requirements and includes segregation of testing and production environment.

- **Vendor management** process to ensure third-party service providers comply with internal policies.
Taking a closer look (continued)

- **System architecture and design** to enable effective control over access to transactions and data
- **Master data governance** to ensure comprehensive and consistent implementation and interpretation of client/trade master data
- **Identity and access management** framework for ATS, and relevant ecosystem applications to enforce appropriate privilege rights and prevent conflict of interest (**segregation of duties**)
  - Regular **review on systems logs** to detect abnormal user activities
  - **Up-to-date system access control list** with accurate information on authorised traders
  - **Privileged account management** procedures to avoid abuse of super-user accounts
- Regular and **user-friendly centralised entitlement review process** with input from key supervisors, and the risk and compliance departments (where relevant)
Business controls

- **Design, development and testing of algorithms** in a dynamic environment, and documentation for new Algos and key changes to existing Algos and/or trading strategies
- **Standardised procedures and approvals** for system testing, reviews, modifications, upgrades or rectifications of systems
- **Regular reviews** of electronic trading Algos and trading strategies
- Implementation of **automated controls** to identify temporary trade constraints/exchange limitations and suspension of such unqualified trades breaching **predetermined criteria**
- **Pre-trade controls**, that include validation controls such as Fat Finger Limits, quantity limits, price collars, and execution and message throttles
- **Real-time controls**, key limits monitoring and reporting; key limits may include market risk and/or regulatory-specific limits
- **Activity monitor on the crossing systems** for suspicious orders or activities to safeguard efficiency and integrity
- **Kill switch/emergency shutdown** protocol
- **Post-trade controls** including transaction monitoring and alert triggers
- **Regular review to ensure the accuracy of key data feeds** (e.g. real-time updates)
- **Operational procedures** documented in case of key incidents such as loss of exchange connectivity
Reliability

- **Capacity management and stress testing** that includes data latency monitoring, transaction throttling and rate limits, performance bottlenecks and exception reports
- **Alert mechanism** to monitor system performance (e.g. system capacity, network bandwidth)
- **System contingency arrangement** that includes suitable backup facility, and valid and legitimate alternative arrangements for order execution
- **Secure system data backup** to ensure data availability and prevent unauthorised access to ATS data
- **Performance of business impact analysis (BIA)** to define appropriate incident response time frame and measures accordingly
- **Proper communication protocols** to promptly notify clients and regulators regarding any incidents (e.g. a system outage)
- **Due diligence** on third-party provided trading systems or algorithms to ensure compliance with regulatory requirements
Cybersecurity

- Comprehensive audit logs and incident reports
- System architecture security that includes network segregation and data encryption
- Operational security controls to detect unauthorised intrusion, security breaches and attacks
- Regular application layer denial of service (DoS) attack assessments, with gaps promptly addressed
- Attack mitigation measures to protect ATS from external malicious attacks
- Periodic penetration testing to detect any potential loopholes in the systems so that remedial action can be taken promptly
- System hardening and patch management to standardise ATS security requirements and enforce regular security configuration review
- Data leakage detection and prevention mechanisms that include transaction data identification and internal data flow behavioural analysis
- Encryption to safeguard the data in storage and in transit
SFC Consultation Conclusions
Concerning the Regulation of ALPs

“The SFC seeks to impose a uniform set of requirements set out in the ‘Code of Conduct for Persons Licensed by or Registered with the SFC’ which all ALP operators and licensed/registered persons who route orders to ALPs will be obligated to comply with.”

Key updates from the May 2015 SFC Consultation Conclusions

Highlights
- **Individual investors** will not be allowed to use ALPs [29]*
- **Client facilitation orders** will be treated as proprietary [55]
- **No mandatory opt-in** requirement [58]

ALP operator governance and order origination requirements
- ALP operators obliged to ensure all orders, including those placed by group companies, originate from qualified investors [38]
- Fund manager considered user of ALPs; no “look through” to underlying fund investors [40]

Client onboarding
- **Professional investor** (PI, defined via section 3(b) of Professional Investor Rules) cannot use ALPs [29]
- **Corporations and partnerships** may be able to use ALPs if they meet threshold tests (portfolio > HKD 8 million or total assets > HKD 40 million) [30]
- Focus on trading risk and not investment risk – no suitability requirement to ALP regime [33-34]

User communications
- Comprehensive and accurate ALP Guidelines must be provided to users of ALP
- Opt-out procedures only (given user restriction imposed and consistent with other major jurisdiction) [64]
- Contingency measures and emergency communication plan with clients remain critical [67]
- ALP operator should establish a written contingency plan to cope with emergencies and disruptions [S8.17]

Record-keeping
- Information on authorised traders to include **client details of individual traders for each trading instruction** [74]
- Keep trading documentation **not less than seven years**; keep comprehensive documentation of ALP **not less than two years after the ALP ceases to operate** [S8.20-22]

Implementation time frame and way forward
- New provision of Code of Conduct will be effective from 1 December 2015.

* [#] represents the paragraph reference numbers from the SFC Consultation Conclusions Concerning the Regulation of ALPs.
**Governance**

- Robust managerial/supervisory controls designed to manage electronic trading business, conduct and operational risks.
- Qualified investor definition and client account coding – PI as defined under section 3(b) of PI Rules do not meet the definition of qualified investors.
- Client communication including investor education and disclosure of guidelines. Disclosure materials to include:
  - Trading and operational matters
  - User restrictions, user priority, order routing, order aggregation and execution methodology
  - Internal controls and potential risk associated with ALP use.

**Transaction and data controls, Reliability**

- Set up information walls to prevent misuse of customer information and conflict of interest.
- Activity-level logs of ALP transaction details including those reported to regulatory bodies; access to ALP including type of/time of information accessed.
- Order tagging focusing on client agency vs client facilitation order, high capacity (“HC”) clients (certain clients may opt out of crossing against HC), inter-entity orders, etc.
- Governance of master data, from creation to regular maintenance and update, focusing on the accuracy of account codes (client vs firm), investor types/order tags, and opt-out indicators.

**Cybersecurity, Business controls**

- Order execution logics are reviewed and approved to ensure order priority is assigned according to origin of order.
- Sufficient monitoring tools to demonstrate adherence to industry standards (e.g. fiduciary duty to clients).
- Dynamic pre-trade, intraday and post-trade validation controls to ensure adherence to internal risk tolerances and/or external regulatory limits.

---

**Reference to recent regulatory fines due to ineffective ALP controls**

4. European bank – ongoing lawsuit, since 2014
5. US bank – USD 0.8 million (2014)
### Independent Compliance Assessment
- Provides an output of a **list of gaps, with recommended improvement suggestions**
- Examples: SDLC, Technology and Operational Risk Management Assessment and Transaction Controls Code Assessment
- **Enables ATS operators to focus internal resources on addressing any key gaps**

### Cyber Security Assessment
- Assesses the security maturity of the ATS cybersecurity exposure
- Provides a detailed report of findings and model maturity assessment, with strategic recommendations and an actionable road map
- **Enables ATS operators to take progressive steps to close any key gaps**

### Remediation Support
- Provides professional remediation support to address the identified gaps in an efficient and cost-effective manner
- **Enables ATS operators to quickly and effectively close gaps and achieve compliance**

### Control Design & Implementation
- Provides control design assistance, policy and procedure enhancement, key control implementation assistance, and staff training
- **Enables ATS operators to quickly and easily enhance their ATS/ALP governance model**

### Contact us

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Jenkins</td>
<td>Partner, Financial Services</td>
<td>+852 2143 8570</td>
<td><a href="mailto:tom.jenkins@kpmg.com">tom.jenkins@kpmg.com</a></td>
</tr>
<tr>
<td>Henry Shek</td>
<td>Partner, Management Consulting</td>
<td>+852 2143 8799</td>
<td><a href="mailto:henry.shek@kpmg.com">henry.shek@kpmg.com</a></td>
</tr>
<tr>
<td>Jia Ning Song</td>
<td>Director, Risk Consulting</td>
<td>+852 2978 8101</td>
<td><a href="mailto:jianing.n.song@kpmg.com">jianing.n.song@kpmg.com</a></td>
</tr>
<tr>
<td>Alvin Li</td>
<td>Senior Manager, Management Consulting</td>
<td>+852 2978 8233</td>
<td><a href="mailto:alvin.li@kpmg.com">alvin.li@kpmg.com</a></td>
</tr>
<tr>
<td>Vicki Fan</td>
<td>Director, Front Office Supervision Lead</td>
<td>+852 2847 5057</td>
<td><a href="mailto:vicki.fan@kpmg.com">vicki.fan@kpmg.com</a></td>
</tr>
<tr>
<td>Paul McSheaffrey</td>
<td>Partner, Risk Consulting</td>
<td>+852 2978 8236</td>
<td><a href="mailto:paul.mcsheaffrey@kpmg.com">paul.mcsheaffrey@kpmg.com</a></td>
</tr>
</tbody>
</table>
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2015 KPMG, a Hong Kong partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in Hong Kong. The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.

Publication number: HK-MC15-0003       Publication date: August 2015