Electronic trading

Keeping up with the risk at capital markets firms

January 2018

EY
Building a better
working world

1 | Electronic trading

Contents

3 | Electronic trading

Introduction

Electronic trading is ever increasing: in volumes, in asset classes and in overall importance to market structure. This electronic trend includes the growth of automated trading, algorithmic trading, high-frequency trading and increased routing to all manner of trading platforms, as well as new types of automation, such as the application of artificial intelligence and machine learning to trading logic (collectively in this paper, e-trading).

With increased activity comes increased risk, so it is no surprise that there is growing concern among regulators and risk managers for capital markets firms of all sizes as to whether controls are able to keep pace and effectively manage e-trading risks. Rule-making and regulatory guidance have provided useful standards for control, but the question persists: are controls sufficient for the level of risk?

In analyzing e-trading risks, firms and regulators share the twin goals of preserving market integrity and avoiding catastrophic losses. Unfortunately, given the complexity of e-trading environments and the large order volumes flowing through various components, even small mistakes can have potentially catastrophic impacts – to the market in question and to the firm itself.

Instances of such losses and mini-"flash crashes" have led regulators to be more active in punishing firms that cause market disruption through e-trading errors. Recent fines have grown in size, and regulatory supervisors are actively examining e-trading environments for safety and soundness, including direct involvement by the second line of defense and application of model control standards to the embedded algorithms (algos).

Conduct risks have also extended into e-trading. Firms are expected to prevent or detect misconduct by human or machine, meaning that they must understand what algos are being programmed to do and whether those actions are consistent with applicable regulations, policies and the firm's own disclosures to clients. Two key areas ripe for innovation are surveillance for trader misuse of electronic platforms (starting with layering and spoofing) and oversight of automated trading logic (including the "quants" and IT developers creating and tweaking the code).

Indeed more recent regulation and industry guidance have raised the overall obligation of firms to correctly identify and mitigate all aspects of e-trading risks – from systematic limitations on outgoing orders to accurate disclosure of key functionality to customers and counterparties. It is incumbent on firms to have an end-to-end system of controls for risks that can disrupt markets, harm investors or damage confidence in the markets.[1]

With all this increased focus, boards and senior management at most firms with any degree of e-trading have taken at least initial steps to assess existing risks and controls. Yet the highly specialized, rapidly evolving nature of e-trading presents unique challenges to firms in right-sizing control and oversight processes, and firms are hesitant to stifle innovation and automation given its competitive importance.

To strike this balance, we believe firms need a comprehensive control environment that includes an enterprise-level policy, clear roles across lines of defense, detailed risk assessments, proportionately designed controls of several types, and continuous re-evaluation and testing. This paper discusses each of these key components in more detail, and highlights common challenges unique to e-trading, with suggestions as to how firms can address those challenges. With the right framework, firms joining in the growth of e-trading can be more confident that their controls are keeping up with the risk.

[1] *See page 11 for a discussion of selected regulatory guidance.*

Getting started

Risk identification

The first step is for firms to understand e-trading activities occurring across the enterprise. This may seem obvious, but it can be difficult in practice:

- Who is responsible for collecting information about e-trading (businesses, Technology, others)?
- What is in scope on the continuum from electronically-assisted human trading to fully automated decision-making and execution?
- Are there consistent standards for risk understanding and control, including shared taxonomies and control libraries, to facilitate assessment and reporting?
- How does e-trading aggregate for enterprise risk management and board-level risk tolerance?

To help solve for these challenges, we recommend that firms articulate an enterprise-level e-trading governance framework, starting with a shared definition of e-trading, defined roles and responsibilities, a structure to support the ongoing risk management program, and establishment of a firmwide e-trading policy to set high-level standards.

A key feature of the governance program is to mandate and organize collection of information about e-trading activities, using common definitions and standards for risk identification. Firms following this type of approach have been able to develop asset inventories for the business areas and markets where e-trading (as they have defined it) is already in use, and to impose vetting and approval processes regarding expansions.

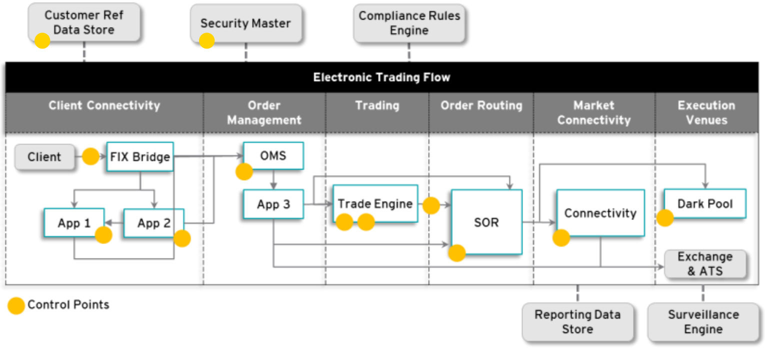
Mapping the flows

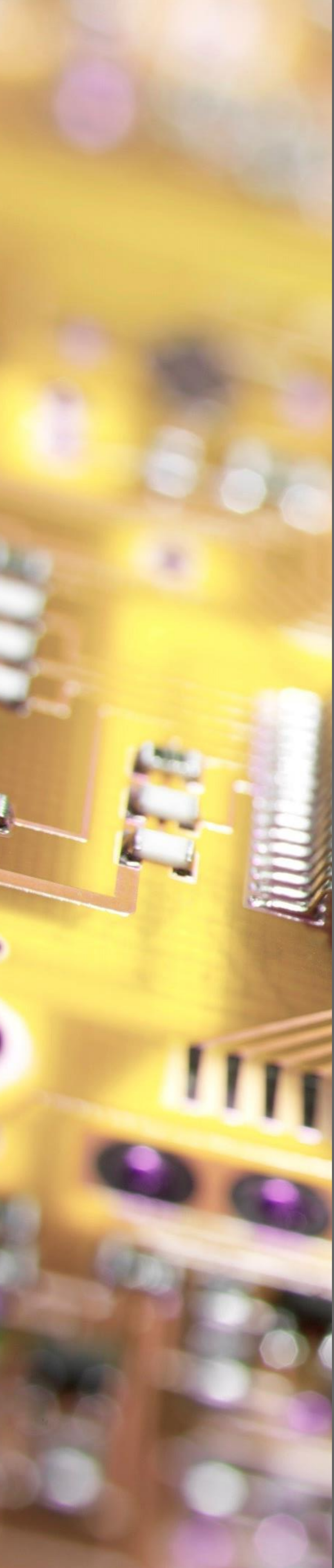
A key consideration for risk identification and the asset inventory is the level of detail that will be required for in-scope activities. E-trading occurs through a series of processes that employ multiple hardware and software components to achieve a specific purpose. Each e-trading process may entail use of multiple algos, each with its own functional purpose, plus other hardware and software components and embedded controls.

As a result, ideal classification and risk identification in the e-trading environment involves mapping each end-to-end process, or “flow,” recognizing that all components and connections in the flow are relevant to evaluating the risks. Creating a detailed mapping of each flow is no small undertaking, but it provides a well-understood, easy-to-reference “place mat” for the flow, highlighting key handoffs between systems, component parts, and all significant inputs/outputs.

Having mapped the end-to-end flows in this fashion, firms can leverage classifications within the policy to identify next steps for different types of activity. For example, critical reference data inputs can be readily identified and checked for legitimacy. Similarly, algos within the flow can be isolated for consideration as potential models (*see page 8*).

Figure 1: Sample e-trading flow

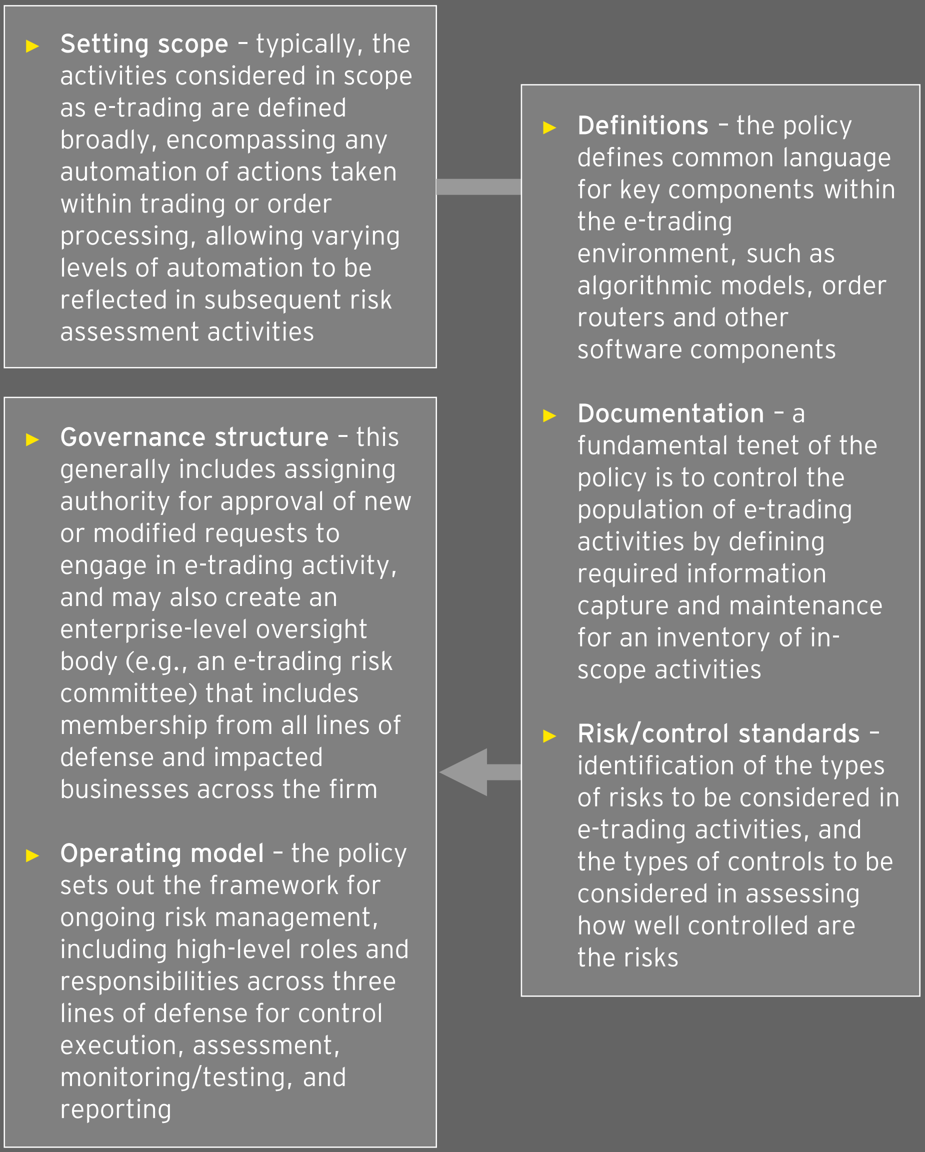




The e-trading policy

Key aspects of the governance framework should be reflected in an enterprise-level e-trading policy, setting the foundation for ongoing oversight and aggregation of e-trading risks.

Figure 2: Key aspects – e-trading policy



- **Setting scope** – typically, the activities considered in scope as e-trading are defined broadly, encompassing any automation of actions taken within trading or order processing, allowing varying levels of automation to be reflected in subsequent risk assessment activities

- **Governance structure** – this generally includes assigning authority for approval of new or modified requests to engage in e-trading activity, and may also create an enterprise-level oversight body (e.g., an e-trading risk committee) that includes membership from all lines of defense and impacted businesses across the firm

- **Operating model** – the policy sets out the framework for ongoing risk management, including high-level roles and responsibilities across three lines of defense for control execution, assessment, monitoring/testing, and reporting

- **Definitions** – the policy defines common language for key components within the e-trading environment, such as algorithmic models, order routers and other software components

- **Documentation** – a fundamental tenet of the policy is to control the population of e-trading activities by defining required information capture and maintenance for an inventory of in-scope activities

- **Risk/control standards** – identification of the types of risks to be considered in e-trading activities, and the types of controls to be considered in assessing how well controlled are the risks

Sizing the risks

Sorting through the details

Having identified in-scope activities, firms next need to assess the level of risk and identify controls related to those activities. To do this for e-trading, firms need to assess processes at a fairly granular level – the level at which e-trading errors occur. This typically requires a "bottom up" review, since existing operational risk assessments tend to be at too high a level to evaluate differential e-trading risks and assess individual controls in operation. This detailed understanding of controls within e-trading flows also becomes important later, as monitoring and testing are employed to develop ongoing oversight.

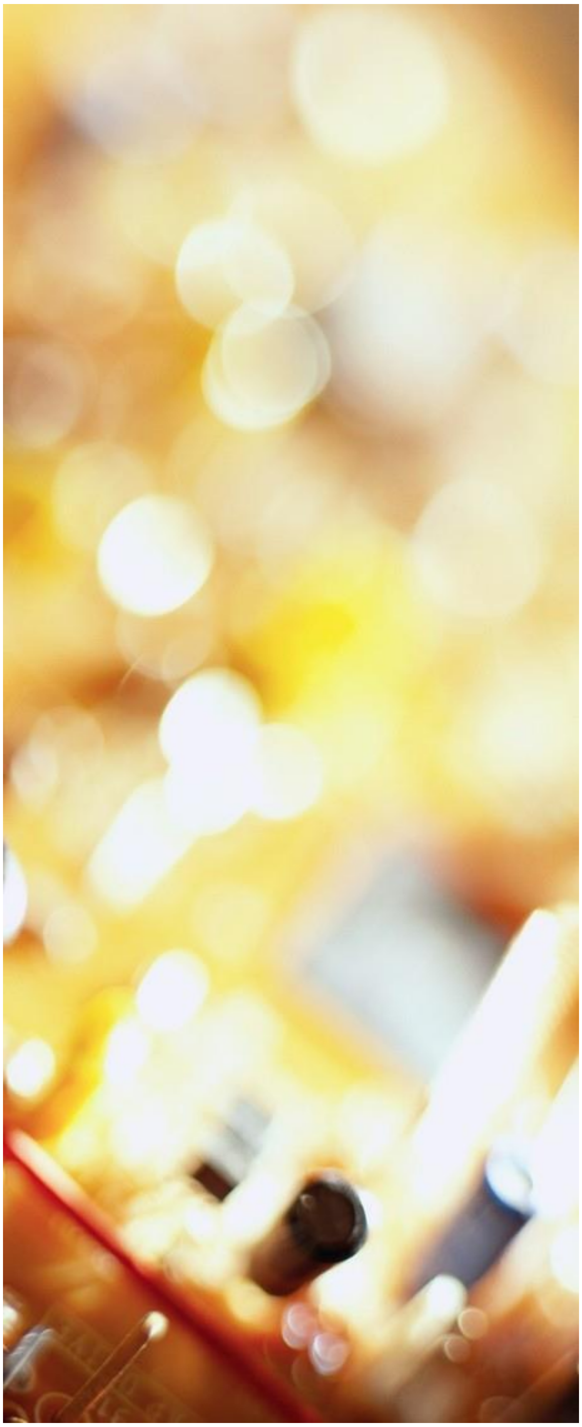
The granular review will cut across many risk and control owners – including the business, Technology, Operations, Model Control and Compliance. Firms should consider overarching controls (such as change management) and those that are specific to individual e-trading flows (those shown on place mats).

Inherent risk is relative

A helpful starting point in evaluating e-trading controls is to establish a common understanding of the varying levels of inherent risk created by different e-trading activities. A simple scoring model can be developed using information collected in the e-trading inventory. For example, starting with the flow's functional significance, it can be scored by its scope (products, regions, business lines), purpose (firm, client, actions taken) and basic functionality (how it achieves the purpose). Additional factors might include:

- Regulation (whether some or all of the functionality has to meet regulatory requirements)
- Complexity (the level of functional complexity and likelihood of errors occurring, absent controls)
- Impact (the use of outputs and consequences of failure, either directly or on downstream processes)

By using a consistent, clear method to determine the relative inherent risk of in-scope activities, firms can gain more comprehensive coverage, but also can prioritize a heightened focus on the riskiest e-trading activities – a key component of "right-sizing" their efforts in this space.



What about models?

Are algorithms models?

After the financial crisis, regulatory supervisors have increasingly focused on models for activities, including risk management, valuation, investment decisions, and assessing capital adequacy. In response to formal supervisory guidance (*see page 11*, describing SR 11–7) and feedback from regulators in various jurisdictions, firms have undertaken broad, multiyear programs to enhance their model risk management (MRM) frameworks, including governance, model definition, model inventory, stature of MRM functions and model control standards across the model life cycle (development, validation and use).

When it comes to e-trading, regulators are expecting MRM functions to identify algorithms within e-trading flows that present model risk and confirm that they are subjected to appropriate model controls. But how can this be accomplished? MRM functions often struggle to integrate model control activities within the context of the overall e-trading flows and the existing controls operated by others, including Technology.

Identification and classification

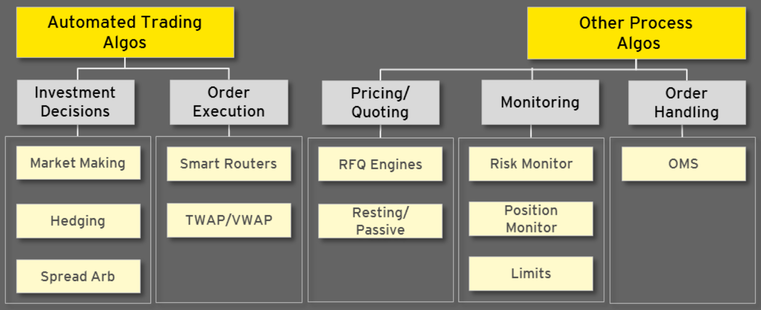
The previously described asset identification process can be used to identify algos operating within each e-trading flow, and those algos can be further classified by function since different uses will present inherently different levels of potential model risk. Once identified, the MRM function can lead a process to capture relevant information about each algo, supporting an assessment of whether it meets the definition of a model (i.e., there is uncertainty in the output from assumptions, and a quantitative method/approach applied vs. a rule-based engine with no uncertainty in the output).

Defining model control activities

Once algos are appropriately classified, MRM functions should confirm that any algo qualified as a model is subject to controls commensurate with its complexity, impact and the level of reliance placed on its outputs. MRM functions likely will need to customize existing model control standards to address the unique nature of e-trading algos (e.g., constant calibration, programmatic parameter updates). MRM can also take into account existing controls surrounding the algos that may partially mitigate model risk (such as relevant input and output checks).

To implement model controls, MRM will need to identify how these activities fit into the overall e-trading control framework, across first and second line of defense functions (e.g., trading, quants, Compliance, Technology, Independent Risk). Focus on model risk will only increase as firms further expand the use of trading algos, including advanced approaches such as machine learning and artificial intelligence (*see page 9*, describing the Financial Stability Board's recent white paper on these topics). We anticipate that the ability to successfully integrate model controls with the broader e-trading control framework will become critical to credibly managing the risks posed by these new capabilities.

Figure 3: Sample e-trading algorithm functional types



Evaluating the controls

Types of controls

Most e-trading is subject to multiple layers of controls that can be categorized broadly into three types, based on the stage (before, during or after trading) within the overall process:

- Pre-trade controls occur primarily in the software development life cycle (SDLC), including turnover management, regression testing, and deployment controls for software and hardware components.
- Trading controls tend to operate on the desk or in infrastructure immediately adjacent to it – these controls will be both preventive and detective in nature, including input and output checks, trader and quant oversight, and layers of limits.
- Post-trade controls provide real-time monitoring and alerting of production incidents as they start to occur, driving responsive actions (automated or manual) while losses can still be mitigated.

Assessing in phases

Typically, we suggest firms approach e-trading control assessment in two key phases. The first is a process review covering key horizontal areas like SDLC, MRM, limit frameworks and incident management. The strength of these control frameworks operates to mitigate risks across e-trading processes.

Second, more focused reviews can be undertaken for the individual e-trading flows, identifying specific potential points of failure in the functional architecture, inbound connections, outbound connections and logic engines (algos). Here, the place mat developed for each flow during asset identification should facilitate the review and allow visualization of embedded controls, assisting in a risk-based prioritization of controls for design and operating effectiveness testing.

SDLC is key

The most fundamental "prevent" controls for e-trading are those in the SDLC. Grouped broadly under **change management** (*see Figure 4*), these controls should include standards for code development, approvals, testing and deployment protocols. Even small tweaks to automated trading or order handling logic can lead to serious issues – whether through unintended impacts to adjoining components in the flow, or by changing customer treatment or trading behavior in a way that violates conduct principles or changes the accuracy of firm disclosures.

Despite the criticality of strong SDLC, many quants and electronic trading managers bemoan the bureaucracy introduced with stronger change management controls, especially when firms include groups outside of the business or Technology into the approval chain (e.g., New Product Committees, Compliance, MRM and Risk). What's more, as a practical matter, the volume and frequency of changes needed in a modern e-trading environment make it impractical to apply an equal standard of review to all changes.

To solve for these challenges, we see leading practice where firms have taken the following steps:

- First, evolving the e-trading architecture to include a degree of "parameterization," which is the ability for predefined variables within the code to be changed on the fly, without a cumbersome process. Built-in limitations on how (or how much) these parameters can change serve to contain the overall risk presented by the real-time changes. In addition, periodic review processes validate that key functionality has not changed, despite the allowance of flexibility in defined areas.
- Second, requiring non-parameter changes to be assigned a risk tier by developers, based upon a defined set of risk triggers that include the potential materiality and impact of the change (e.g., to the flow, Compliance or customer interactions). The resulting risk tier corresponds to the level of pre-vetting required. Periodic look-back reviews are used to validate that risk tiering decisions are being made appropriately.
- Third, recognizing that there will be instances where an expedited process is needed, even for higher risk changes, by creating a process for "emergency turnovers," allowing changes to proceed without aspects of the onerous pre-deployment approval process. These turnovers must be tracked and subjected to post-change challenge as to the legitimacy of invoking the exception, as well as regression testing of the resulting changes.

Designed for failure

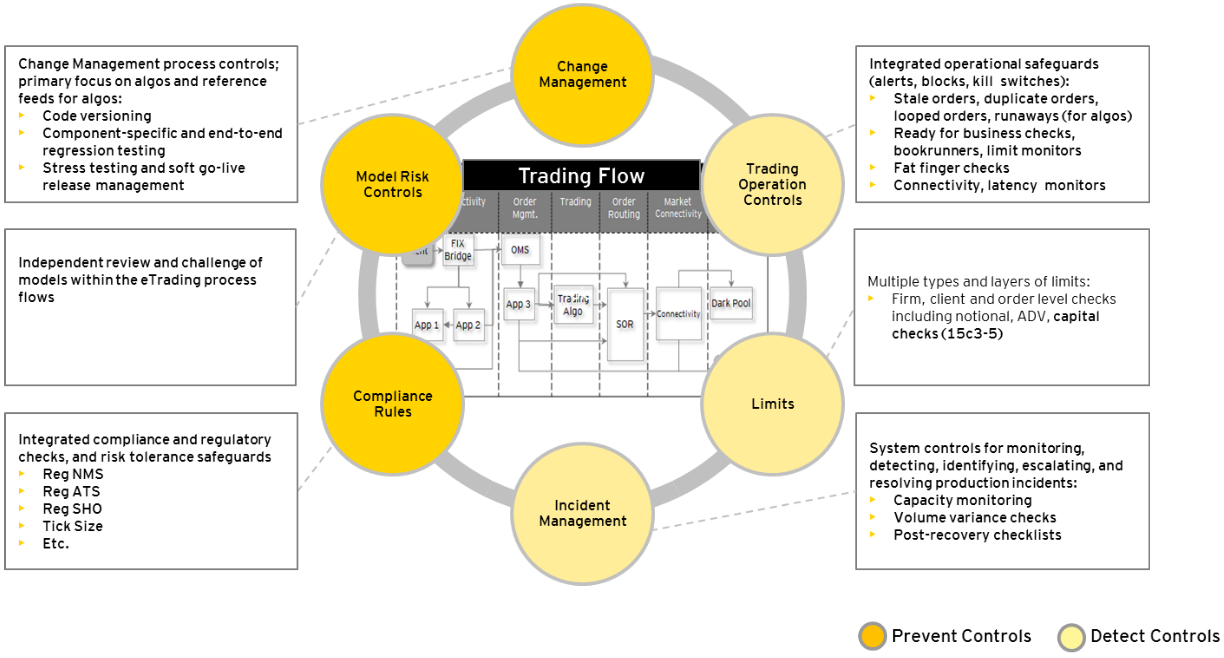
Given the frequency of turnovers and the complexities of the change process, most firm SDLC programs experience regular errors; these occurrences point to an even more important consideration in evaluating controls within an electronic trading flow – the need for intentional redundancy. In other words, firms should have multiple layers of controls, including both those reasonably designed to prevent errors from occurring and those designed to rapidly halt processes when errors nonetheless occur.

Limits as the last clear chance

The ultimate controls designed to operate when other controls have failed are perimeter limits. These coarse-grained limits are set at the outermost edge of the system architecture, designed to halt automated instructions from upstream components when management tolerances in terms of notional size, volume, various risk measures or some combination of factors are exceeded. These limits are required by regulatory directives for systematic avoidance of disruptive impacts to markets or harm to investors (*see page 11*). By design, perimeter limits should be activated only when other limits have failed – more fine-grained limits should be embedded at key action points within the flow, as internal kill switches and "sense checks" to stop processing upon input or output failures or notable calculation mistakes.

As applicable, the embedded and perimeter limit regimes should include sensitivity to credit risk and expected activity levels for customers trading through the firms' infrastructure, and to market risk limit frameworks applicable to the firms' principal flows (market making and hedging). To manage all this, firms should look to establish a limits framework and operating model that operates in real time, including real time management by appropriately segregated first-line personnel and second-line oversight (Market and Credit Risk) of potential intraday risk.

Figure 4: Sample e-trading control types



Change Management process controls; primary focus on algos and reference feeds for algos:
- Code versioning
- Component-specific and end-to-end regression testing
- Stress testing and soft go-live release management

Independent review and challenge of models within the eTrading process flows

Integrated compliance and regulatory checks, and risk tolerance safeguards
- Reg NMS
- Reg ATS
- Reg SHO
- Tick Size
- Etc.

Integrated operational safeguards (alerts, blocks, kill switches):
- Stale orders, duplicate orders, looped orders, runaways (for algos)
- Ready for business checks, bookrunners, limit monitors
- Fat finger checks
- Connectivity, latency monitors

Multiple types and layers of limits:
- Firm, client and order level checks including notional, ADV, capital checks (15c3-5)

System controls for monitoring, detecting, identifying, escalating, and resolving production incidents:
- Capacity monitoring
- Volume variance checks
- Post-recovery checklists

Key regulatory guidance for e-trading

By way of explicit rule-making, prudential supervisory guidance and contributions to published industry standards, regulators globally have articulated expectations for e-trading controls.

Figure 5: E-trading – select guidance

SEC Rule 15c3-5 – Requires firms trading securities directly on an exchange or ATS, or who provide direct market access to others, to have controls reasonably designed to systematically limit their financial exposures, and to ensure orders sent via the access comply with applicable rules. Requires:

- Preventing entry of orders above preset credit or capital limits, or erroneous or duplicative orders above price or size thresholds
- Maintaining control over market access technology (restricting access)
- Regular reviews of controls and supervision

SR 11-7 Letter – OCC defined models broadly and set standards for controlling model risk, considering uncertainty of inputs, complexity of processing, and materiality of outputs.

SEC Reg SCI – US requirement for key market participants (exchanges, ATSs) to strengthen market infrastructure, reducing errors and improving resiliency. Mandates policies and procedures related to capacity, integrity, resiliency, availability and security of key systems. The requirements encompass change management, stress testing, monitoring, cybersecurity, business continuity, disaster recovery and outsourcing.

Market Abuse Regime – EU requirements for firms to reasonably control against key conduct risks, including through automated strategies, and to avoid disruption of markets or unfair use of customer information via e-trading.

Published Standards – expectations for e-trading risk management set out in industry working group papers:

- SSG Algorithmic Trading Briefing Note
- FX Global Code of Conduct
- Treasury Markets Practices Group Automated Trading in Treasury Markets White Paper
- FSB Report on artificial intelligence and machine learning in financial services

In addition, these and other conduct standards detail types of misconduct that firms must prevent, such as front-running and misuse of customer information, that apply equally to the logic of trading algos.

MiFID II – EU rules that seek to mitigate risks of market disruption or unfair advantages from algo trading, including high-speed arbitrage. Mandates separate identification of investment decision-making and execution algos, and storing down specific details about each, along with systematic limits and capacity and resiliency checks.

Testing and monitoring

Staying vigilant

Another uniquely daunting feature of e-trading risk is the number of ever-changing variables involved. In addition to frequent turnovers to the firm's code base, the activities and controls in e-trading rely upon constantly streaming data, multiple connection layers and messaging systems, and external parties such as clients and trading venues. Any of these can be the source of a change to the firm's risk profile, so it is important to engage in continuous monitoring of the trading environment and related controls.

Many types of tests

Checks performed in real time or on a daily basis are essential, and are themselves key forms of control (for example, "heartbeat" monitors, latency monitors, execution quality surveillance). On a less frequent basis, we recommend that firms conduct walk-throughs and targeted tests to specifically confirm the continued operation of key controls (especially key limits, kill switches and alert mechanisms), and to review that the performance of other components continues to be as expected. Another form of leading-practice testing is to carry out simulations. Through a tabletop exercise the firm can challenge key controls and incident response plans through specific scenarios (such as loss of connectivity or an extreme volume spike).

An increasingly important aspect of testing for e-trading involves transparency – firms can be fined for differences between their client disclosures regarding electronic flows and the reality of how trades are processed, orders filled or information shared. Firms are advised to actively design tests of client-impacting functionality (for example, order treatment in dark pool ATSs, or "last look" on principal quotes) to check that marketing materials and disclosures remain accurate through time and after successive changes.

Available metrics

Another source of monitoring is for firms to identify a set of metrics related to the e-trading control environment. Many of these metrics may already be captured by first-line business or Technology groups, but they can be leveraged and reported more broadly as key risk and control indicators. Historical ranges or trends can be used to establish thresholds that, when breached, will indicate a potential need for re-evaluation of a particular component or control.

Indeed, since many controls are designed to catch errors, information about upstream process failures can readily be collected at the point of downstream controls activating. Ongoing analysis and reporting of the causes of errors in various flows should be a core component of the overall e-trading control framework.

Figure 6: Sample e-trading risk metrics

Risk Areas	KRI examples
Change Management	• Number of deployments • Number of emergency turnovers • Number of change management policy breaches • Number of post-deployment roll backs • Number of deployments, turnovers, breaches, etc.
Incidents	• Overall number of technology 'outages' by component • Number of connectivity related technology incidents • Number of component based incidents
Capacity	• Capacity utilization • Number of capacity threshold breaches • Number of capacity adjustments • Number of messages • Number of orders
Latency	• Average latency by flow • Latency threshold breaches
Per order controls limit utilization	• Number of restricted list violations • Maximum open order violations • Number of desk aggregate capital limit violations • Number of emergency limit extensions • Number of customer limit breaches • Number of customer limit extensions
Trade metric trending	• Order to trade ratio • Cancellation rates • Transactions per second / Turnover per second
Trading control trends	• Number of orders cancelled / rejected due to stale order check • Number of orders cancelled / rejected due to duplicate orders • Number of orders cancelled / rejected due to maximum open orders • Number of orders cancelled / rejected due to message volume throttles
Regulatory control violations	• NMS trade through violations • Circuit breaker violations • Reg SHO violations • Sub-penny violations

Lines of defense

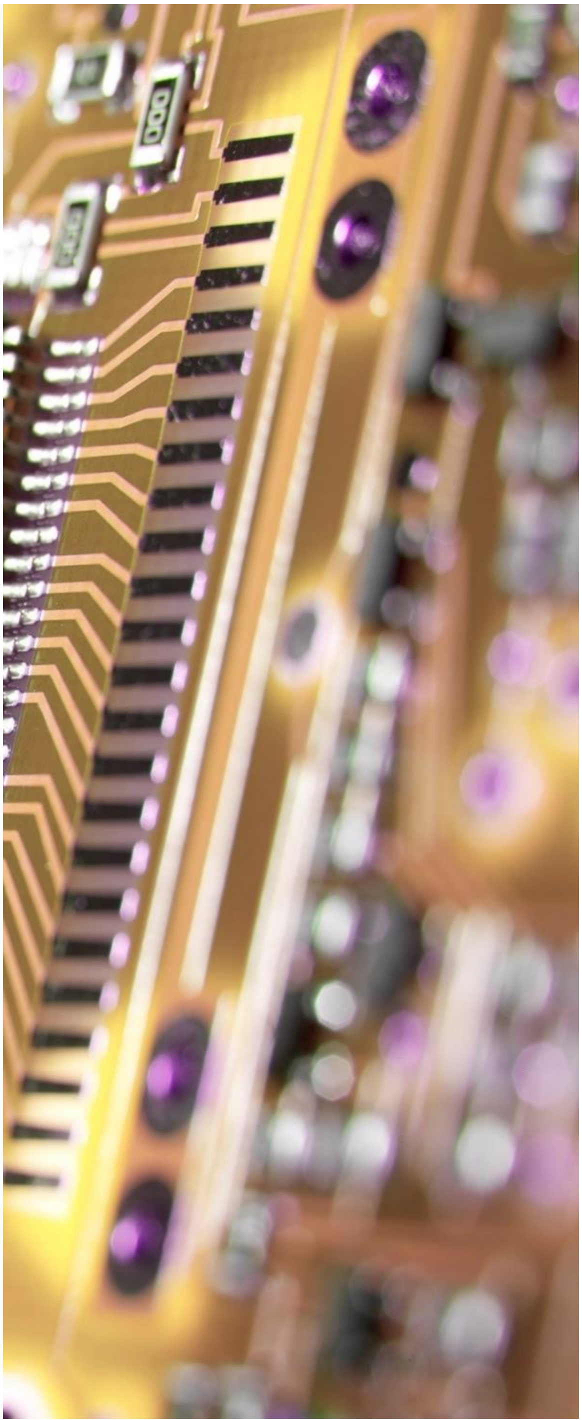
Everyone plays a part

A comprehensive control environment requires robust involvement from all three lines of defense. Yet in the first line, e-trading controls are typically widely distributed, since each flow will involve multiple data providers and technology process owners, in addition to the relevant trading desk. This can lead to confusion or dilution of overall first-line ownership of the firm's e-trading risk. And in the second line, it can be challenging to source sufficiently technical skill sets – especially considering the multiple second-line disciplines that need to be involved for effective oversight (e.g., Compliance, Market, Credit and Operational Risk, and MRM). Similarly, Internal Audit can struggle to gain sufficient understanding of the flows and functionality, and to source the right skill sets to engage in robust review and challenge.

Facing these challenges, many firms have established a dedicated governance committee to take a holistic view and share information across lines of defense. This helps facilitate clear lines of responsibility and raise the awareness of all participants since the committee can include membership from all interested groups, and it plays a role in aggregating and reporting risk and control information to the firm's executive management and board. The committee does not eliminate gaps in specific roles and/or skill sets, but it can help identify the gaps and agree how to address them – whether with third-party assistance or through targeted hiring.

Adding it up

Of course, another challenge for the second and third lines is how to aggregate and measure electronic trading risk. An efficient approach focuses on "rolling up" the information gathered in the detailed place mats and associated control assessments by mapping those risks and controls to higher level risk nodes in the firm's enterprise risk and control taxonomies. This allows reuse of the detailed assessments in the enterprise's risk and control self-assessment (RCSA) program, and should facilitate aggregation of key risk indicators (such as turnover metrics, outages and policy breaches) for ongoing oversight.



Conclusion

Electronic connectivity and automated trading in the capital markets, including use of algos, are not new. However, e-trading has been expanding, not only in the speed and sophistication of the computer models themselves, but also through increased volumes and expansion to new asset classes and markets. The expansion will continue, and innovations such as machine learning are sure to add further complexity in the future.

To compete in increasingly electronic markets, firms must be able to nimbly introduce and support more – and more sophisticated – automation in the trading environment while controlling for the unique risks it presents.

Existing controls and regulatory promulgation of standards are a start. But there are concrete steps that firms can take to help create a comprehensive e-trading control framework, including developing an enterprise-level policy, conducting detailed risk assessments, helping ensure the right types of controls and clear lines of defense, and monitoring/testing. Such a framework will be essential for their e-trading controls to keep up.

How EY can help:

Framework

- Evaluate existing policy coverage and/or design policy framework and definitions to identify and classify activities, including model policies and population of model inventories
- Draft minimum standards and types of controls relevant to electronic trading activities based on regulatory expectation and industry practices
- Map end to end electronic trading processes and apply classification criteria

Assessments and Controls

- Evaluate assessment practices and/or design risk assessment programs for electronic trading activities, including development of inherent risk scoring models
- Assess and/or design SDLC and model risk programs, including risk tiering methodologies
- Identify and document relevant controls; perform control assessments
- Summarize residual risks; develop proposed remediation plans

Testing and Monitoring

- Design assistance for monitoring approaches and incident alerting, response and management
- Develop test plans including targeted reviews, model validation approaches, and embedded coverage based on relevant testing skill sets
- Perform model validation
- Perform tests of specific algorithms and/or electronic trading components, and/or perform ongoing algorithm monitoring (including EY's "Know Your Algo" assessment)

Governance

- Enhance enterprise risk framework and taxonomies to integrate electronic trading risks, including design of governance structures and artifacts (charters, metrics, reporting)
- Define roles and responsibilities across three lines of defense
- Enhance first line controls and operating structure for electronic trading risk management
- Assist with development and optimization of second line testing and validation approaches

Internal Audit Support

- Assist in developing audit plans and scoping for electronic trading risks, including identification of key drivers of risk, types of controls, and potential areas of weakness; assist with enterprise level reporting on audit approaches
- Develop and execute standardized audit program, and/or assist with audit reviews of electronic trading risks and controls, model risks and end to end systems

Contacts

Americas

Mary Lou Peters
212 773 2941
marylou.peters@ey.com

Gagan Agarwala
212 773 2646
gagan.agarwala@ey.com

Andrew Lese
212 773 2070
andrew.lese@ey.com

Sayak Mukherjee
212 773 7677
sayak.mukherjee@ey.com

EMEIA

Mark Selvarajan
44 (0)20 7951 3441
mark.selvarajan@uk.ey.com

Nick Le Fevre
44 (0)79 7661 8977
nlefevre@uk.ey.com

Kieran Mullaley
44 (0)77 7552 4567
kmullaley@uk.ey.com

Asia

David Scott
65 6309 8031
David.scott@sg.ey.com

Sameer Rege
852 2849 9458
sameer.rege@hk.ey.com

Japan

Gary Stanton
81 70 2175 1770
stanton-gry@shinnihon.or.jp

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of EY Global Limited, each of which is a separate legal entity. EY Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Score No. 07226-171Gbl

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com