London Stock Exchange

Technical Description

Exchange Level Controls

Version 1.0

25 August 2020

London Stock Exchange Group

1 Revision History

History of changes		
25/08/2020	1.0	Initial version.

2 Glossary

Term	Definition
ADT	Average Daily Turnover
CGC	Current Gross Consideration – on-going sum of open exposure, Orders and executed Trades per user per day
ELC	Exchange Level Controls
FTP	File Transfer Protocol
GCM	General Clearing Member
ICM	Individual Clearing Member
MGC	Maximum Gross Consideration – maximum allowed sum of open exposure, Orders and executed Trades per user per day
MOV	Maximum Order Value
RIL	Restricted Instrument List
Risk Controller	A user who manages Exchange Level Controls for trading users

3 Introduction

London Stock Exchange optional Exchange Level Controls (ELC) are designed to manage risk for trading users.

ELC are managed via the Risk Monitoring Portal, which allows the Risk Controller to set and manage limits at the user level (single connection)

The Risk Controller can be a General Clearing Member (GCM) or Member Firm. Member Firms who are not their own Risk Controller can request a read only version of the Risk Monitoring Portal should they require.

ELC consist of real-time gateway level validations. Alerts can be sent when configured limits are breached. Users can also monitor risk exposure in real time via the Risk Monitoring Portal, where a kill switch is also available, in addition to being available via the FIX Drop Copy Gateway.

The objective of this document is to provide an overview of the ELC, Drop Copy Gateway and the Risk Monitoring Portal.

Sponsored Access trading services are not supported for GCMs.

4 Exchange Level Controls

ELC are optional and are managed via the Risk Monitoring Portal, which allows the Risk Controller to set and manage limits at the user level (single connection i.e. FIX Comp ID and/or Native User ID).

Exchange Level Controls (order validation checks), are applied to all Orders submitted by Risk Controller, in order to restrict and prevent trading beyond certain limits.

All Orders submitted via a Risk Monitored User will pass through the Exchange Level Controls before reaching the Order Book. This validation is specific to Orders from Risk Monitored Users and is in addition to the standard checks in place on London Stock Exchange, which are implemented and enforced for all Participants.

4.1 Reference Price Collars

Reference Price Collars prevent Orders with an overly aggressive limit price from entering the Order Book and trading.

London Stock Exchange currently operates a one-way band limit depending on whether the incoming priced Member Firm Order is a buy or a sell. The ruling limit is set at Trading Parameter level and is defined as a percentage offset, computed against the reference price of the last traded price or the previous day's closing price when the stock has not yet generated an Order book trade that day.

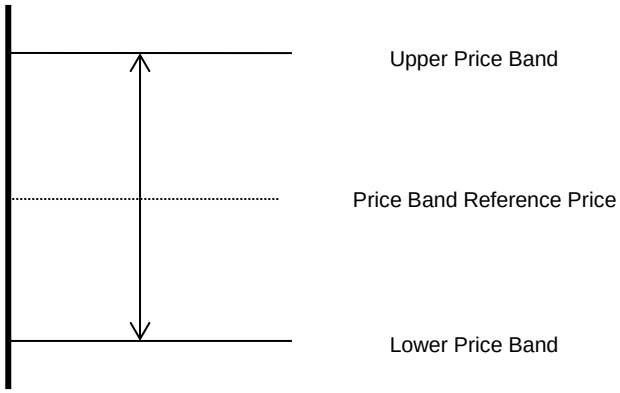
The following Orders will be **rejected** on entry:

— Buy Orders with a limit price equal to or greater than the upper price band limit (reference price + price band offset)

— Sell Orders with a limit price equal to or less than the lower price band limit (reference price – price band offset)

— All un-priced Orders.

Reference Price Collars are in addition to the standard London Stock Exchange dynamic and static circuit breakers, which Member Firm Orders cannot invoke.



During Regular Trading, to prevent a circuit breaker being invoked, the Reference Price Collar is set 1 basis point less than the ruling ***Dynamic Price Monitoring %*** for that instrument. To give more flexibility during auction call phases the ruling Reference Price Collar is doubled from that in place for Regular Trading. The ***Dynamic Price Monitoring %*** can be found for each trading sector on the 3rd tab of ***Millennium Exchange and TRADEcho Business Parameters***.

4.2 Maximum Order Value

The Maximum Order Value limit prevents Orders with uncommonly large values from entering the Order Book(s).

The limit is set per Risk Monitored User, in a base currency. A currency conversion rate is applied to the traded currency of the Order to give the value in the correct base currency. For more information, please refer to section 4.10 Currency Conversion.

All Orders entered by the Risk Monitored Member will be validated against the Maximum Order Value set for the Risk Monitored Member. If the Order value (price x Order size) is greater than the Maximum Order Value, the Order will be rejected.

The same logic will also be applied for Order amendments. If the new Order value (new price x new Order size) in the Order amend request is greater than the Maximum Order Value set for the user, the request will be rejected.

4.3 Maximum Order Quantity

The Maximum Order Quantity limit prevents orders with an uncommonly large order quantity from entering the Order Book(s).

The limit is set at the individual instrument level and is applicable to all Users (specified as a number of shares).

The current limit is set for a maximum of 5,000,000 shares per instrument and per Order.

4.4 Maximum Gross Consideration

The Maximum Gross Consideration limit prevents Risk Monitored Users from trading beyond a financial limit set by the Risk Controller. If a Risk Monitored User attempts to submit an Order which would result in the Current Gross Consideration exceeding the configured Maximum Gross Consideration, the Order will be rejected.

Current Gross Consideration (exposure) is defined as the sum of all Trades and value of all open Orders. i.e.

Current Gross Consideration = **Consideration of all Trades during day + Value of all open Orders**

The value is configured per Risk Monitored User for a trading day, in a base currency for the Risk Monitored User. FX conversion will be carried out based on the trading currency of the instrument. For more information, please refer to section 4.10 Currency Conversion.

The value is calculated as a cumulative value, i.e. A buy or sell Order will be added to the overall Gross consideration and no netting of buy and sell positions will take place.

> *For example, a buy Order in Vodafone of 500 shares at 100p followed by a sell Order of 500 shares at 100p, will increase the overall Current Gross Consideration by 100,000p (compared with a net exposure position in Vodafone of 0).*

All Risk Control Members must set a Maximum Gross Consideration limit for each of their Risk Monitored Users (and can be set at an individual Risk Monitored User level). If this is not defined (i.e. set to 0), the Risk Monitored User will not be able to trade as no limit is applied. This value can be either increased or decreased intra-day via the Risk Monitoring Portal.

4.4.1 Maximum Gross Consideration Alerting via Risk Monitoring Portal and email

Risk Controllers are able to receive advance warnings to alert them about their Risk Monitored User's Order and trading activity in relation to their Max Gross Consideration limit via the Risk Monitoring Portal and via email (to an email group) when their Risk Monitored Users breach set limits.

Alerts are sent when a limit is breached for a Risk Monitored User and when a Risk Monitored User's Order is rejected due to an attempt to breach their Max Gross Consideration limit.

e.g. When 50%, 75%, 90% and 100% of the Risk Monitored User's Max Gross Consideration is breached.

For Example:

A Risk Monitored User has a Max Gross Consideration of 100,000 Euros. An alert has been set up to warn the Risk Controller (via the Risk Monitoring Portal and email) when the Risk Monitored User's Order and Trade Consideration breaches 75% of their Max Gross Consideration limit.

i.e. When the Risk Monitored User's Current Gross Consideration exceeds 75,000 Euros.

Where multiple limits are breached by a single Order, only the alert for the highest limit will be sent. An alert will only be sent once during any given day, unless the Risk Monitored User's Max Gross Consideration is updated

Risk Controllers can request to receive alerts via the Member Portal.

Once set up, Risk Controllers will be able to maintain their alert limits for their Risk Monitored Users via the Risk Monitoring Portal.

4.5 Maximum Message Rate

Risk Controllers will be required to apportion a maximum message rate limit in order to prevent Risk Monitored Users from entering an overly large number of messages. The limit will be set as a maximum number of messages per second per Risk Monitored Users and will be allocated from the total limit allowed for the Risk Controllers allocation.

4.6 Restricted Instrument Lists (RIL)

Restricted Instrument Lists (RIL) allow the Risk Controller to restrict Orders entered by a Risk Monitored user to a limited set of instruments, in the form of a negative permission list(s) (set for an individual Risk Monitored User), i.e. the RIL is the list of instruments the Risk Monitored User **cannot** trade. If a Risk Monitored User attempts to submit an Order in a restricted instrument, it will be rejected.

Lists are created (following notification from the Risk Controller) by London Stock Exchange's Market Operations team (MOPS). The restricted instruments on each list are then maintained either:

- By MOPS;
  - Risk Controller must submit a request to the Exchange's MOPS for changes to the RIL of Risk Monitored Users. Please refer to Section 6.1 for further information.
  - Where an instrument becomes restricted intraday by MOPS, the Exchange will cancel any open Orders of the Risk Monitored User in the restricted instrument. Until the Exchange cancels all open Orders, a Risk Monitored User will continue to be able to amend any open Orders on restricted instruments.
- Or by the Sponsoring Firm by uploading a .csv file
  - via SFTP (via data.lseg.com),
  - or via the Risk Monitoring Portal.

4.6.1 Updating a Restricted Instrument List (RIL) via SFTP

Sponsoring Firms that would like to update their restricted lists themselves (intra or inter-day) using a .csv file can apply for an LSE managed SFTP/FTP account.

Once the SFTP/FTP account has been set up and the Restricted List shell has been created and assigned to the Sponsored User (or Users) by the Exchange's MOPS, Sponsoring Firms can upload .csv files to add or remove Instruments from a particular Restricted List.

Please note that when a new list is uploaded, into the SFTP/FTP via this automated process, existing Orders in the affected instruments will not be automatically deleted and firms should arrange for existing Orders to be deleted. Until such open Orders are deleted, a Sponsored User will continue to be able to amend any open Orders on restricted instruments.

The SFTP/FTP server should be available 24 hours a day, 365 days a year for file submission, but will only process files between 06:00 and 18:00 (UK time) on trading days. Files can be submitted outside of this time window.

The SFTP/FTP will have the following directories:

Directories	Description
Outgoing (default home directory folder after login)	This is where users can upload updated Restricted List .csv files
Audit	This is where users can see what happened to every file (with a correct name and valid size) that they have asked the Exchange to process
Current	This is where users can see the most recent list successfully processed
Incoming/Inbox	Reserved for future use
Archive	Reserved for future use

The .csv file uploaded, must adopt the following characteristics:

- The Restricted List name will be provided by the Exchange's MOPS team and must be used in the file name submitted and within the file itself.
- The file must have the following naming convention and be unique for a given business day:
  - [RestrictedListName]_[YYYYMMDDHHMMSS].csv
    - e.g. [XXXX][YYY]SP_20111130142535.csv
      - X represents the Sponsoring Firm (Member Firm)
      - Y represents the Sponsored User OR Group of Sponsored Users
      - SP = Sponsored Access Production/ ST = Sponsored Access Test
  - The timestamp used must be unique and should be current.
- The file must not exceed a size of 200KB.
- The file should contain a list of all the instruments that the Sponsoring Firm would like to restrict on a given Restricted List. If an erroneous instrument ID is included in a file that is uploaded the entire file will be rejected.

  For example:

  - To add an instrument, you would add it to the list of instruments previously submitted.
  - To remove an instrument, you would delete if from the list of instruments previously submitted.
- All Restricted Lists will persist overnight, meaning a file should only be submitted if there is a change required to a given Restricted List. It is expected that each file will result in at least one addition or one removal of an instrument from the specified Restricted List.
- A file should only include updates to a single Restricted List. It is **not** possible to update more than one Restricted List with a single file.
- Each Restricted List can contain up to 100 instruments.
- The csv file should be comma delimited. The first row of the file should contain the following format:
  - <Restricted List Name>,<Instrument A>,<Instrument B>,…
  - The Instrument ID should be used to identify the instrument(s) to be restricted.

— Up to 10 attempts (with files that are not out of date) can be made to update each Restricted List per day.

Upon **successful** processing of a file, we will deliver:

— A file with the same name with a .ok file extension (replacing .csv) to the “Audit” directory;

AND

— If a file for the same Restricted List exists in the “Current” directory, it will be updated with the new Restricted List.

The content of the file in “Audit” and “Current” directories will contain the original contents provided on line 1 which have been successfully loaded.

Upon ***partially successful*** processing of a file, we will deliver:

— A file with the same name with a .ok file extension (replacing .csv) to the “Audit” directory. The file will contain the list of instruments which were successful and a warning message “One or more entry uploads have failed.”

AND

— If a file for the same Restricted List exists in the “Current” directory, it will be updated with the new Restricted List.

The content of the file in “Audit” and “Current” directories will contain a list of successfully loaded restricted instruments on line 1.

— A file with the same name with a .err file extension to the “Audit” directory. The file will contain a list of instruments which were unsuccessful, along with the reasons for failure.

Upon **unsuccessful** processing of a file, we will either:

— Do nothing (i.e. **not** provide an error file) where:
  — The file has been named with an incorrect Restricted List name prefix
  — A file exceeds the permitted size
  — On the second error where a firm has already exceeded their 10 attempts. i.e. on the 12th attempt.
— Deliver a file with the same name with a .err file extension (replacing .csv) to the “Audit” directory. Where a filename is not unique a timestamp will be added to the .err extension to make it unique

  e.g. FirmName_RL1_20111130142535.err_20111130142540.

  — The file will contain the original contents provided on line 1 and error codes and descriptions on line 2 onwards. Each error line of the “.err” file will contain the error code, relevant description, the instrument group and the list of instruments which got rejected under the particular error code. Where multiple entries are rejected under the same error code, they will be stated on the same line.

Please note: Instrument Group and Symbol will only be stamped if applicable to the error.

The following table summarises all of the errors that can be provided.

Error Code	Description	Reason for error	Example entry on .err file
1	File cannot be processed	File is not formatted correctly or file is corrupt	0001, File cannot be processed
2	Instrument Group not found	Restricted list does not exist or is incorrect	0002, Instrument group not found, Inst_Grp_x
3	Instrument not found	Instrument provided is invalid	0003, Instrument not found, Inst_Grp_1, Inst_x
4	System unavailable	There was an error processing the file	0004, System unavailable
5	File contains expression based instrument(s)	There is an issue in the way the Restricted List has been set up, as a query has been used. MOPS will need to be contacted to resolve this issue	0005, File contains expression based instrument(s), Inst_Grp_1, Inst_x
6	Out-dated file	File has an out of date timestamp	0006, Out-dated file
7	No update from previous file	File has not changed	0007, No update from previous file
8	Update rejected by system	There was an error in processing the file	0008, Update rejected by System
9	Max Instrument Group updates exceeded	The maximum number of Restricted List updates has been exceeded for the day. No further updates will be accepted or .err files provided	0009, Max instrument group updates exceeded, InstGrp_20111103035100
10	Max Instruments per Group exceeded	The maximum number of Instruments within the file have been exceeded	0010, Max instruments per group exceeded
11	Instrument Group does not match file name	The Instrument Group Name in the File Name, does not match the Instrument Group Name within the file	0011, Instrument group does not match file name
12	Duplicate file	The file is a duplicate	0012, Duplicate file

4.6.2 Updating a Restricted Instrument List via the Risk Monitoring Portal

Risk Controllers can update their Restricted Lists (intra or inter-day) using a .csv file or they can do so via the Risk Monitoring Portal.

For characteristics and format requirements of the .csv file, please refer to the relevant part of Section 4.6.1 Updating a Restricted Instrument List via SFTP.

Once the Restricted List shell has been created via the Member Portal and assigned to the Risk Monitoring User (or Users) by London Stock Exchange MOPS, and such Risk Monitoring User has been enabled with the appropriate privilege by London Stock Exchange MOPS, the Risk Controller can browse and upload a single .csv file every 20 seconds to add or remove Instruments from a particular Restricted List.

Please note that when a new list is uploaded via the Risk Monitoring Portal, existing Orders in the affected instruments will not be automatically deleted and firms should arrange for existing Orders

to be deleted themselves. Until such open Orders are deleted, a Risk Monitored User will continue to be able to amend any open Orders on restricted instruments.

The Risk Monitoring Portal will carry out some basic validations before attempting to upload a file. When validations fail, a pop-up message will be displayed in the Risk Monitoring Portal with one of the following reject messages:

Scenario	Reject Message
File size is too large for the framework to process (in the megabyte range)	The file upload failed.
File name length is more 49 characters	File name is too long.
Invalid file type (Only .csv files are allowed.)	An invalid file type.
File content longer than 4000 characters	File content is too long.
File contains data in multiple lines. File can contain data in only one line.	File contains data in multiple lines
Another file exists with the same file name.	Duplicate file name.

As per Section 4.6.1 Updating a Restricted Instrument List via SFTP, Risk Controllers can expect to receive the same .ok and .err files, as appropriate for the ***successful***, ***partially successful*** and ***unsuccessful*** processing of Restricted Instrument Lists uploaded via the Risk Monitoring Portal, "Remarks" column (see table below).

Once a file has been uploaded, the system will indicate the request is being processed in the Risk Monitoring Portal and have the status of 'Processing'. Once processed, the "Status" of the file uploaded will be updated.

The following table provides a complete set of Risk Monitoring Portal "Status", descriptions and "Remarks" provided:

Status	Description	Remarks
Processing	The file has successfully passed the basic validations and has been uploaded ready for the processing.	n/a
Partially successful	The file has been uploaded and one or more entries have been processed successfully.	For "Partially Successful" processed files, the remark column will state: **"One / or more entry uploads have failed."** By clicking on the download links, users can download the .ok. and .err. files.
Successful	The file upload has been successfully processed.	By clicking on the download links, users can download the .ok. file.

Status	Description	Remarks
System unavailable	The file upload request has been in a "Processing" state for longer than 30 seconds.	n/a
Failed	The file upload has been rejected due to one of the reasons that follows in the Error Code table below.	For "Failed" processed files which generate a single error code, the remark column will state: **"Error Information: <Description>"** For "Failed" processed files which generate multiple error codes, the remark column will state: **"File processing failed due to multiple errors."** By clicking on the download links, users can download the .err. file.

The following table summarises all of the errors that can be provided:

Error Code	Description	Reason for error	Example entry on .err file and 'Remarks' column
0001	File cannot be processed	File is not formatted correctly or file is corrupt	0001, File cannot be processed
0002	Instrument Group not found	Restricted list does not exist or is incorrect	0002, Instrument group not found, Inst_Grp_x
0003	Instrument not found	Instrument provided is invalid	0003, Instrument not found, Inst_Grp_1, Inst_x
0004	System unavailable	There was an error processing the file or the file has taken longer than 30 seconds to process	0004, System unavailable
0005	File contains expression based Instrument(s)	There is an issue in the way the Restricted List has been set up, as a query has been used MOPS will need to be contacted to resolve this issue	0005, File contains expression based instrument(s), Inst_Grp_1, Inst_x
0006	Out-dated file	File has an out of date timestamp	0006, Out-dated file
0007	No update from previous file	File has not changed	0007, No update from previous file
0008	Update Rejected by System	There was an error in processing the file	0008, Update rejected by System
0009	Max Instrument Group Updates Exceeded	The maximum number of Restricted List updates has been exceeded for	0009, Max instrument group updates exceeded, InstGrp_20111103035100

Error Code	Description	Reason for error	Example entry on .err file and 'Remarks' column
		the day. No further updates will be accepted or .err files provided	
0010	Max Instruments per group Exceeded	The maximum number of Instruments within the file have been exceeded	0010, Max instruments per group exceeded
0011	Instrument Group does not match File Name	The Instrument Group Name in the File Name, does not match the Instrument Group Name within the file	0011, Instrument group does not match file name
0012	Duplicate file	The file is a duplicate	0012, Duplicate file
0013	File cannot be processed due to system error	The file cannot be processed due to a system error	0013, File cannot be processed due to system error

4.7 FIX Drop Copy Gateway

Member Firms who are not their own Risk Controller, can consent to provide their GCM a FIX Drop Copy Gateway connection under their own Firm ID or under the GCM's Firm ID, such that they receive all of the relevant Execution Reports from a Member's Native and/or FIX Trading Gateway connection.

FIX Drop Copy Gateways can be set up with Exchange Level Controls. Alternatively, they can also be set up without Exchange Level Controls being configured.

For further information on the FIX Drop Copy Gateway, see MIT 205 Drop Copy Gateway (FIX 5.0), available in the Technical Library.

4.7.1 Cancel on Disconnect

A cancel on disconnect and cancel on logout facility is available.

All Risk Monitored User's Orders will be deleted from the Order Book automatically under the following circumstances:

a) Risk Controller disconnects from the Drop Copy gateway for a longer than a pre-configured time, resulting in the suspension of trading services for all associated Risk Monitored Users (e.g. Submitting Orders).

b) Risk Monitored User disconnects from the Order Book for a longer than agreed pre-configured time.

If this functionality is enabled, Risk Monitoring Firms and Users will need to prove via our test environment that they are able to receive and interpret these messages.

4.8 Kill Switch (Suspension and Reactivation)

A Kill Switch is available to Risk Controllers to “Suspend” a selected Risk Monitoring User. It can be activated manually via the Risk Monitoring Portal or automatically via sending a message via the Drop Copy Gateway.

All Risk Monitoring User’s Orders will be deleted from the Order Book automatically under the following circumstances:

a) Risk Controller activates the Kill Switch for a given Risk Monitoring User from the Risk Monitoring Portal. Note, only possible for Risk Monitored users using the Native protocol

b) Risk Controller activates the Kill Switch for a given Risk Monitoring User via the Drop Copy Gateway. Available for Risk Monitored users using either FIX or Native Protocol.

Risk Monitoring Users can also:

- “Activate” Risk Monitored Users to allow them to resubmit Orders via the Risk Monitoring Portal or via the Drop Copy Gateway.
- See the “Status” of their Risk Monitored Users via the Risk Monitoring Portal or request the “Status” of a Risk Monitored User via the Drop Copy Gateway.

If the Kill Switch functionality is required, Risk Controllers will need to prove via our test environment that they are able to send, receive and interpret Kill Switch messages (suspend, activate, and status) via the Drop Copy Gateway.

For further information on the FIX Drop Copy Gateway, see MIT 205 Drop Copy Gateway (FIX 5.0), available in the Technical Library.

4.9 Rejecting Un-priced and Pegged Orders

All Orders entered without a limit price (e.g. Market Orders) and all pegged Orders (with or without a limit price) entered by Risk Monitored Users will be rejected.

This validation check is system wide for all Risk Monitored Users and is applied as a validation check when Market Orders are submitted to the Order Books.

4.10 Currency Conversion

All ELC nominal validation limits (Maximum Order Value and Maximum Gross Consideration) are specified in a base currency for the Risk Monitored User. All Orders submitted will be converted from the traded currency to the base currency before these limits are applied. The exchange rates for this currency conversion are obtained from a mainstream third-party data provider and maintained by London Stock Exchange via a daily file upload. There will be five base currencies as per the example below:

Trading Currency	Base Currency	Value
SEK	EUR	9.3404
GBP	USD	0.8311
NOK	GBX	0.079809
USD	YEN	1.2767
HKD	GBP	11.567

4.11 Exchange Level Controls Parameters Summary

As described above, ELC limits are set either at an instrument group level (to be applicable to all Risk Monitored Users), or at a Risk Controller specific level, or as checks imposed on Risk Monitored Users at system level by London Stock Exchange.

We have also included more information on the validations that are able to be controlled via the Risk Monitoring Portal. This is summarised below:

	User	Instrument / Instrument Group	System	Amended via Risk Monitoring Portal	Supported by FIX and/or Native Trading Gateways
Price Band Validation		X			NATIVE
Max Order Value	X		X		NATIVE
Max Order Quantity		X	X		NATIVE
Max Gross Consideration	X			X	NATIVE
Max Message Rate	X		X		NATIVE & FIX
Restricted Instrument List	X				NATIVE & FIX
FIX Drop Copy Includes Cancel on Disconnect	X				NATIVE & FIX
Kill Switch (Risk Monitoring Portal)	X			X	NATIVE
Kill Switch (via FIX Drop Copy)	X				NATIVE & FIX
Reject Un-priced Order			X		NATIVE

5 Risk Monitoring Portal

The Risk Monitoring Portal is a secure web-based GUI tool accessed via a secure login (accessible via LSEG infrastructure) which allows Risk Controllers to monitor trading activities and amend limits of their Monitored Users.

ELC features supported in the Risk Monitoring Portal include:

- Amend Max Gross Consideration
- View Current Gross Consideration
- View and Amend Max Gross Consideration Alerts
- Upload Restricted Lists via csv file
- Invoke the Kill Switch

Access to the Risk Monitoring Portal will require the use of LSEG provided RSA soft tokens. These will be provided as part of the enablement process.

The Risk Monitoring Portal is available from 03:00 to 18:15 (UK time).

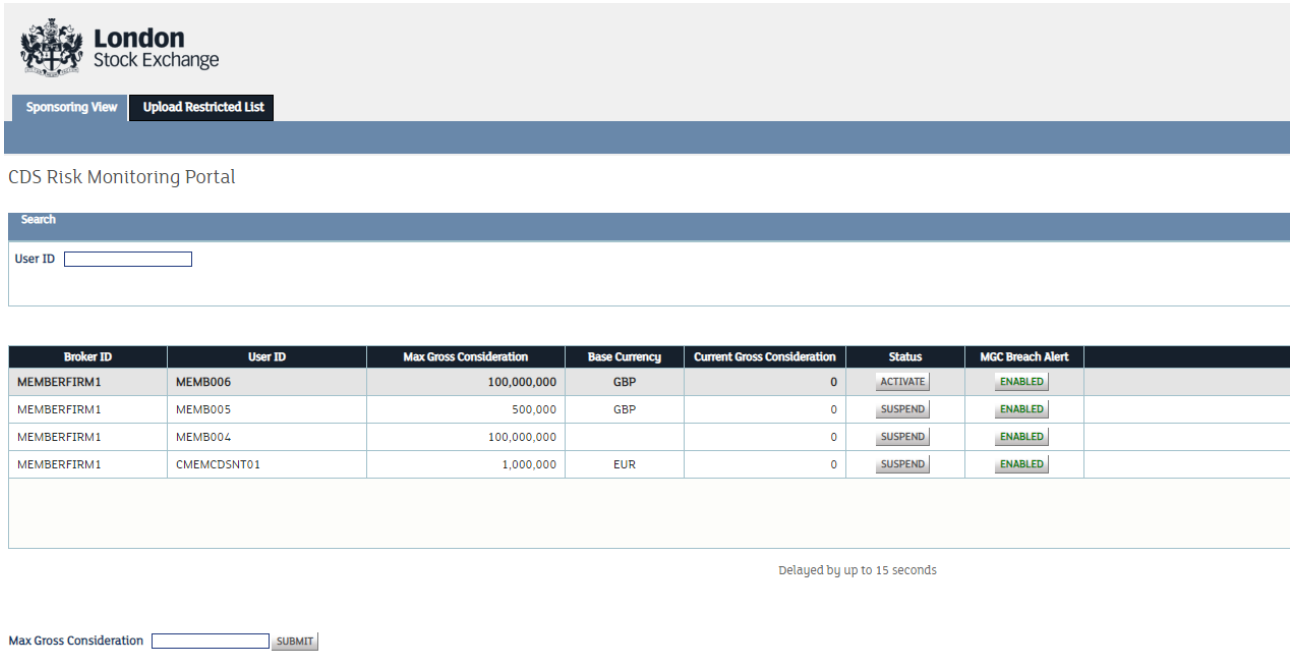
5.1 Risk Controller view

a) Sponsoring View

Once the Risk Controller logs into the Risk Monitoring Portal, the ‘Sponsoring View’ window will be displayed. It will show the summary of ELC information for the Trading Sessions you are monitoring:

- List of Monitored Users
- Maximum Gross Consideration (MGC) set per User ID
- Current Global Gross Consideration
- Status – Suspend or Activate users
- MGC Breach Alert – Enable/Disable notifications of MGC is breeched.

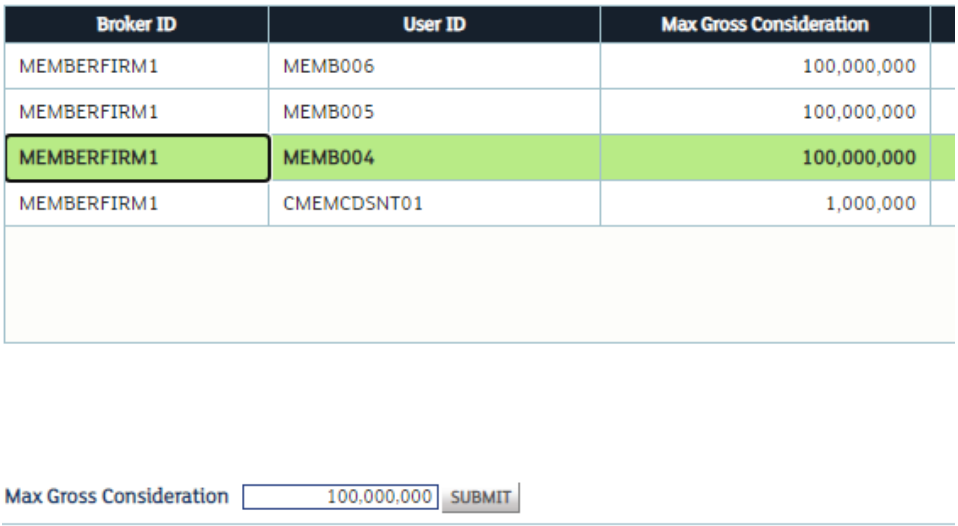
- Alerts – Email notifications sent when MGC utilisation percentages are breached and can be ‘Enabled’ or Disabled’



b) Setting Max Gross Consideration

From the ‘Sponsoring View’ window, Risk Controllers can set Maximum Gross Consideration for each User ID by;

1. Selecting the User ID for MGC limits (Selected row becomes green)
2. Putting a Value in the Max Gross Consideration field
3. ‘Submit’ changes



c) Activate/Suspend a User ID

From the ‘Sponsoring View’ window, the Risk Controller can Suspend or Activate Suspended Users from the ‘Status’ column:

1. Click on ‘Suspend’ button for the User ID you wish to Suspend

2. Confirm the changes.

Note: Suspended User IDs would have ‘Status’ displaying ‘Activate’.

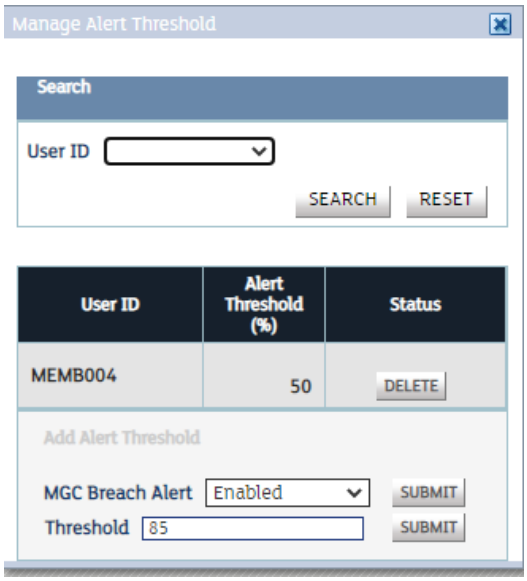
d) Setting Maximum Gross Consideration Breach Alert Levels

From the ‘Sponsoring View’ window, the Risk Controller can choose custom Maximum Gross Consideration (MGC) alert levels. A notification would be seen on the Risk Monitoring Portal if a Risk Monitored user utilises a defined percentage of the MGC. To set MGC Breach alert;

1. Click the ‘Enabled’ button within the ‘MGC Breach Alert’ column that is associated with the User ID you would like to set alerts for.

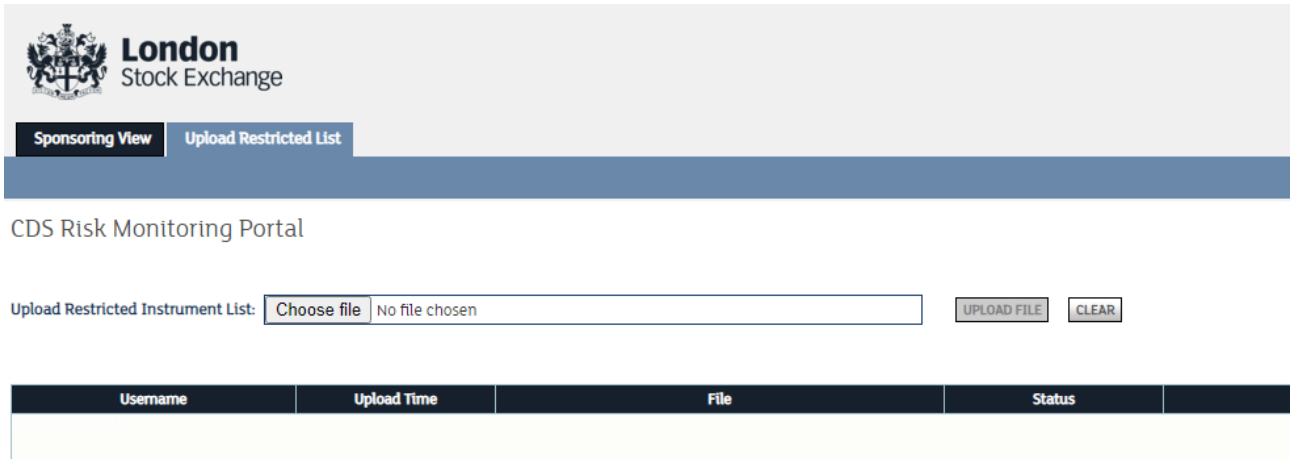
2. The ‘Manage Alert Threshold’ window would appear. Enter a number from 0 to 100 inside the ‘Threshold’ field. The number represents the percentage of the MGC that needs to be utilised by the Risk Monitored User before you receive a notification.

3. Submit changes. Repeat this process if you would like to set additional Alert Threshold percentages.



e) Upload Restricted List

From the ‘Upload Restricted List’, the Risk Controller can upload Restricted Instrument Lists using a .csv.



For characteristics and format requirements of the .csv file, please refer to the relevant part of Section 4.6.1 Updating a Restricted Instrument List via SFTP.

For more information on Uploading Restricted Instrument Lists via the Risk Portal, please refer to section 4.6.2 Updating a Restricted instrument List via Risk Monitoring Portal

6 How to request Exchange Level Controls with Risk Monitoring Portal access?

6.1 Risk Controller and Member Firm access

Member Firms can grant access to the Risk Monitoring Portal by submitting an Exchange Level Controls Consent Form to the Membership Team. Applications can be completed on behalf of a Member Firm where the Risk Controller is the Firm's GCM.

Please contact the Membership Team on +44 (0)20 7797 1900 or membership@lseg.com for the Exchange Level Controls Consent Form.

Once the required paperwork is received by the Membership Team, firms will need to liaise with their dedicated Technical Account Manager or Technical Account Management team londontam@lseg.com or 0207 797 3939 for Risk Monitoring Portal Access, FTP upload (optional) and CDS and Production PTV configurations.

Firms will be expected to complete a Configuration Form provided by the Technical Account Management team to capture these requirements.

6.1.1 Risk Monitoring Portal unavailable

In the event that a Risk Controller cannot access the Risk Monitoring Portal to monitor Firms or adjust limits, the Risk Controller should contact Market Operations and request that they intervene on their behalf. It is also possible to maintain the Restricted Instrument List for validation by contacting London Stock Exchange's Market Operations (MOPS) team.

Intraday change requests can be submitted via email. MOPS will endeavour to make any intraday changes within a reasonable time frame and will confirm when the adjustments have been made.

Market Operations can be contacted on 0207 797 3666 option 1 or by e-mail at msu@lseg.com.

6.2 Customer Testing

Firms can only connect to Production with certified software but there is no additional certification testing required for ELC enablement.

An optional Daily Life Cycle (DLC) test is conducted with the Risk Manager and a member of the CTS Market Access team to test the risk control functionality in the Customer Development Service (CDS) environment prior to production go-live. A DLC test can be booked by contacting the Market Access team marketaccess@lseg.com.

The DLC test will focus on a combination of scenarios including:

- Managing risk limits via the Risk Monitoring Portal

- Managing Breach Alert Limits
- Stop trading via Kill Switch

Access to the CDS environment fall under the existing agreements member firms have with London Stock Exchange. For further information on the daily life cycle please email market access.

Disclaimer

Copyright © January 2020 London Stock Exchange plc.
Registered in England and Wales No. 2075721.

London Stock Exchange plc has used all reasonable efforts to ensure that the information contained in this publication is correct at the time of going to press, but shall not be liable for decisions made in reliance on it.

London Stock Exchange and the coat of arms device are registered Trademarks of London Stock Exchange plc.

London Stock Exchange
10 Paternoster Square
London EC4M 7LS
Telephone: +44 (0)20 7797 1000

www.londonstockexchange.com

London Stock Exchange

10 Paternoster Square, London EC4M 7LS
T: +44 (0)20 7797 1000

London Stock Exchange