Turquoise

Technical Description

Turquoise Risk Controls

Version 1.3

26 February 2021

1 Revision History

History of changes		
11/09/2020	1.0	Initial version.
28/09/2020	1.1	Second version, includes the addition of Turquoise Europe.
25/01/2021	1.2	Section 3 and 4 introductions updated to add clarity that some ELC are managed by Turquoise. Sections 4.6, 4.6.1, 4.6.2 updated to reflect the migration of SFTP to MFT for uploading of Restricted Instruments Lists.
26/02/2021	1.2	This version of the document has been updated to reflect brand changes for London Stock Exchange Group (LSEG), Turquoise® and Turquoise Europe™. Front page – Introduces Turquoise as 'An LSEG Business'. Section 2.0 updated to reflect the document relates to Turquoise® and Turquoise Europe™. Various sections updated to reflect use of the Turquoise brand and its trade marks.

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
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 Turquoise Risk Controls for trading users
TGHE	Turquoise Global Holdings Europe B.V. (*TGHE or Turquoise Europe*™ and together with TGHL, Turquoise®) is an investment firm authorised and regulated by the Autoriteit Financiële Markten (AFM) of the Netherlands. TGHE is a wholly-owned subsidiary of TGHL.
TGHL	Turquoise Global Holdings Limited[1] (*TGHL or Turquoise*®) is an investment firm authorised and regulated by the Financial Conduct Authority of the United Kingdom. Initially founded in 2006 by a consortium of nine investment banks, TGHL has been majority owned by London Stock Exchange Group (LSEG) in partnership with the user community since 2010.
TRC	Turquoise Risk Controls

[1] © 2021. Turquoise® and Turquoise Plato™ are trademarks of Turquoise Global Holdings Limited.

3 Introduction

Turquoise optional Turquoise Risk Controls (TRC) are designed to manage risk for trading users of TGHL and TGHE.

TRC are managed by Turquoise or 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 of TGHL or TGHE. Member Firms who are not their own Risk Controller can request a read only version of the Risk Monitoring Portal should they require.

TRC 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 TRC, Drop Copy Gateway and the Risk Monitoring Portal.

Sponsored Access trading services are not supported for GCMs.

4 Turquoise Risk Controls

TRC are optional and are managed by Turquoise or 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).

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

All Orders submitted via a Risk Monitored User will pass through the Turquoise Risk 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 Turquoise, 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 **Turquoise Lit Order Books™** and trading.

For more information on Reference Price Collars, please see Section 7.6 in the Turquoise Trading Service Description.

4.2 Maximum Order Value

The Maximum Order Value limit prevents Orders with uncommonly large values from entering the **Turquoise Lit™**, **Turquoise Plato Lit Auctions™** and **Turquoise Plato™** Order Books.

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 of TGHL or TGHE will be validated against the Maximum Order Value set for the Risk Monitored Member of TGHL or TGHE. 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 (cancel/replace) request is greater than the Maximum Order Value set for the user, the request will be rejected.

If no Maximum Order Value is set, then no TRC Maximum Order Value validation is carried out on Orders submitted by that Risk Monitored Member. However, there is a Turquoise system-wide Maximum Order Value, which is implemented in addition to the TRC validation, which supersedes this check:

- if no valid TRC Maximum Order Value is in place, the Turquoise Maximum Order Value will be adhered to.

- if the TRC Maximum Order Value > Turquoise Maximum Order Value, the Turquoise Maximum Order Value will be the valid limit.

The Turquoise Maximum Order Values can be found in Section 8.3 of the Turquoise Trading Service Description.

The Maximum Order Value check equally applies to Block Indications, submitted to **Turquoise Plato Block Discovery™**.

Maximum Order Values can be set by Market Operations (MOPS):

- market.operations@tradeturquoise.com
- +44 (0)20 7382 7676

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 Maximum Order Quantity check equally applies to Block Indications, submitted to **Turquoise Plato Block Discovery™.**

The Maximum Order Quantity levels can be requested from the contact the Technical Account Management Team:

- londontam@lseg.com
- +44 (0)20 7797 3939

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 or Block Indication which would result in the Current Gross Consideration exceeding the configured Maximum Gross Consideration, the Order or Block Indication will be rejected.

Current Gross Consideration (exposure) is defined as the sum of all Trades and value of all open Orders and open Block Indications:

Current Gross Consideration	**=**	**Consideration of all Trades during the day** **+** **Value of all currently Open Orders and Open Block Indications**

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 or Block Indication 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 or Block Indication 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 or Block Indication, 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. For more information on the Member Portal and how to register to gain access, please click the following link here.

Alternatively, please contact the Membership Team:

- membership@lseg.com
- +44 (0) 20 7797 1900

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.

Turquoise applies a threshold to all Users (whether Risk Monitored or not), and Risk Controllers can request a more conservative threshold for Risk Monitored Users.

4.6 Restricted Instrument Lists (RIL)

Restricted Instrument Lists (RIL) allow the Risk Controller to restrict Orders and Block Indications 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 or Block Indication in a restricted instrument, it will be rejected.

Lists are created (following notification from the Risk Controller) by Turquoise Market Operations team (MOPS).

Restricted Instruments on each list are maintained by the Risk Controller by uploading a .csv file:

- By the Risk Controller by uploading a .csv file:
  - via SFTP/FTP (refer to TQ102 - Connectivity Guide),
  - or via the Risk Monitoring Portal.

In situations where access to SFTP or the Risk Controls Portal is not possible, Turquoise's Market Operations (MOPS) team can assist;

- Risk Controller must submit a request to the Turquoise 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 Turquoise MOPS, Turquoise will cancel any open Orders and open Block Indications of the Risk Monitored User in the restricted instrument. Until Turquoise MOPS cancels all open Orders and Block Indications, a Risk Monitored User will continue to be able to amend any open Orders and open Block Indications on restricted instruments.

4.6.1 Updating a Restricted Instrument List (RIL) via SFTP/FTP

Risk Controllers that would like to update their restricted lists using a .csv file would need to apply for a managed SFTP account. This can be requested via the Technical Account Management Team (londontam@lseg.com).

Once the SFTP account has been set up and the Restricted Instrument List shell(s) have been created, Risk Controllers can upload (intraday) .csv files to add or remove Instruments from a particular Restricted List. Any intraday uploads to the Restricted Instrument list will be made active within 5 minutes.

Please note that when a new list is uploaded onto the SFTP site, existing unexecuted Orders and Block Indications on added instruments will not be automatically deleted. Risk Monitored Users will continue to be able to amend and/or cancel any remaining open Orders and Block Indications on the newly Restricted Instruments.

The SFTP server will be available for file processing from 06:00 to 17:30 (UK Time) during trading days. An authentication error will occur if an attempt to log on to the SFTP server is made outside these hours. Any files submitted outside of these hours will receive no acknowledgement response and any files inside portal gateway folder will be deleted when Turquoise restarts.

The SFTP repository will have the following directories:

Directories	Description
Outgoing	This is where users can see what happened to every file (with a correct name and valid size) that they asked Turquoise to process
Incoming	The is where users can upload Restricted list .csv files.

The uploaded.csv file must adopt the following characteristics:

- The file must have the following naming convention:
    - The Restricted List name will be provided by Turquoise and must be used in the file name submitted within the file itself.
    - The file must have the following naming convention and be unique for a given business day. [RestrictedListName]_[YYYYMMDDHHMMSS].csv
- The file must not exceed a size of 200KB.
- The file should contain a list of all the instruments that the Risk Monitored User cannot trade, with a maximum limit of 100 instruments.
- The Instrument ID must be used to identify the restricted instruments.
- The .csv file should be comma delimited. The first row of the file must use the following format:

    <[RistrictedListName]>, <Instrument ID A>, <Instrument ID B>

If a file is uploaded and does not meet initial required validation on the file name, the file will be transferred to /Outgoing prefixed with INVALIDNAME_

The initial validation is the filename must be prefixed matching part of the username.

Please note that:

- In case an erroneous Instrument ID is indicated, the file will be entirely rejected.
- Files with a date different from the current date in their filename will not be processed.
- To add an instrument, you would add it to the list of instruments previously submitted.

- To remove an instrument, you would delete it from the list of instruments previously submitted.
- It is not possible to update more than one Restricted List with a single file upload.
- Up to 10 attempts can be made to update each Restricted List per day.
- Uploading a file with no underscores present in the filenames will result in failure.

Upon **successful** processing of an incoming file, the Risk Controller will receive:

- A response file with the same name of the uploaded file and an ".ok" file extension into the "Outgoing" directory.
- The successfully processed file stored in the "Incoming" directory.

Upon **partially** successful processing of a file, the Risk Controller will receive:

- A response file with the same name of the uploaded file and an ".ok" file extension to the "Outgoing" directory. This file will contain the list of instruments which were successfully processed and a warning message "One or more entry uploads have failed".
- A response file with the same name of the uploaded file and an ".err" file extension to the "Outgoing" directory. The file will contain a list of instruments which were unsuccessful, along with the reasons for failure.
- The successfully processed file stored in the "Incoming" directory.

Upon **unsuccessful** processing of a file, the Risk Controller will either:

- Be provided no results (i.e. not provide an error file) in case –
    - the file has been named with an incorrect Restricted List name prefix.
    - the file exceeds the maximum permitted size.
    - On the second error where a firm has already exceeded their 10 attempts i.e. on the 12th attempt.
- Be provided a file with the same name of the uploaded file and an ".err" file extension to the "Outgoing" directory. Where a filename is not unique, a timestamp will be added to the ".err" extension to make it unique
    - e.g. XYZ_ABCTRADING_RL16_20180124060004.err_201812111503
    - The file will contain the original contents provided on line 1 and an error code and description on line 2. The error code provided will be the first error detected

Note: Response files sent to the "Outgoing" directory and Restricted List.csv files uploaded in the "Incoming" directory will be stored for 7 days.

The following table summarizes the errors that can be provided.

Error Code	Scenario Description	Reason for error
0001	The File cannot be processed (due to incorrect file format or corrupt file)	File cannot be processed
0002	Incorrect or non-existing Restricted Instrument List	Restricted instrument List Shell/group not found

Error Code	Scenario Description	Reason for error
0003	Invalid Instrument / Instrument does not exist	Instrument(s) not found
0004	A Restricted Instrument List update failed due to Exchange Manager having terminated or the file update failed because Exchange Manager was in the process of failing over	System Unavailable
0005	File contains Instruments which are already added through an Expression	File contains expression based Instrument(s)
0006	The file name is the same as the previously uploaded file or The file name's timestamp is older than that of the previously processed file with the same Instrument Group	Outdated file
0007	The file's content is same as the previously uploaded file for the same Instrument Group	No update from previous file
0008	An Instrument Group update is rejected by Exchange due to EOD process not being completed	Update rejected by System
0009	Upload (N+1)th file when Max_RIL_Updates = N	The maximum number of Restricted List updates has been exceeded for 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
0011	Instrument Group specified in the file does not match the Instrument Group specified in the file name	The Instrument Group Name in the File Name, does not match the Instrument Group Name within the file
0012	Duplicate file is uploaded before the gateway processes the initial file	The file is a duplicate
0013	System error is encountered while processing	File cannot be processed due to system error

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 Turquoise MOPS, and such Risk Monitoring User has been enabled with the appropriate privilege by Turquoise 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 and Block Indications in the affected instruments will not be automatically deleted and firms should arrange for existing Orders and Block Indications to be deleted themselves. Until such open Orders and Block Indications are deleted, a Risk Monitored User will continue to be able to amend any open Orders and open Block Indications 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.
System unavailable	The file upload request has been in a "Processing" state for longer than 30 seconds.	n/a

Status	Description	Remarks
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 the day. No further updates will be accepted or .err files provided	0009, Max instrument group updates exceeded, InstGrp_20111103035100
0010	Max Instruments per group Exceeded	The maximum number of Instruments within the file have been exceeded	0010, Max instruments per group exceeded

Error Code	Description	Reason for error	Example entry on .err file and 'Remarks' column
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 of TGHL or TGHE 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 Turquoise Risk Controls. Alternatively, they can also be set up without Turquoise Risk Controls being configured.

For further information on the FIX Drop Copy Gateway, see TQ203 Drop Copy Gateway (FIX 5.0), available in the Turquoise Document Library.

a) Cancel on Disconnect

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

All Risk Monitored User's Orders and Block Indications will be deleted from the **Turquoise Lit™**, **Turquoise Plato Lit Auctions™**, and **Turquoise Plato™** Order Books and **Turquoise Plato Block Discovery™**, and all new Orders / Block Indications, and Order / Block Indication amendments rejected, 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 Order Books 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 and Block Indications will be deleted from Order Books 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 and Block Indications 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 TQ203 Drop Copy Gateway (FIX 5.0), available in the Turquoise Document Library.

4.9 Rejecting Un-priced and Pegged Orders

All Orders and Block Indications entered without a limit price (e.g. Market Orders) and all pegged Orders and Block Indications (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 TRC nominal validation limits (Maximum Order Value and Maximum Gross Consideration) are specified in a base currency for the Risk Monitored User. All Orders and Block Indications 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 Turquoise via a daily file upload.

For more information on exchange rates, please contact Turquoise MOPS.

4.11 Turquoise Risk Controls Parameters Summary

As described above, TRC 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 Turquoise.

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.

TRC 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.

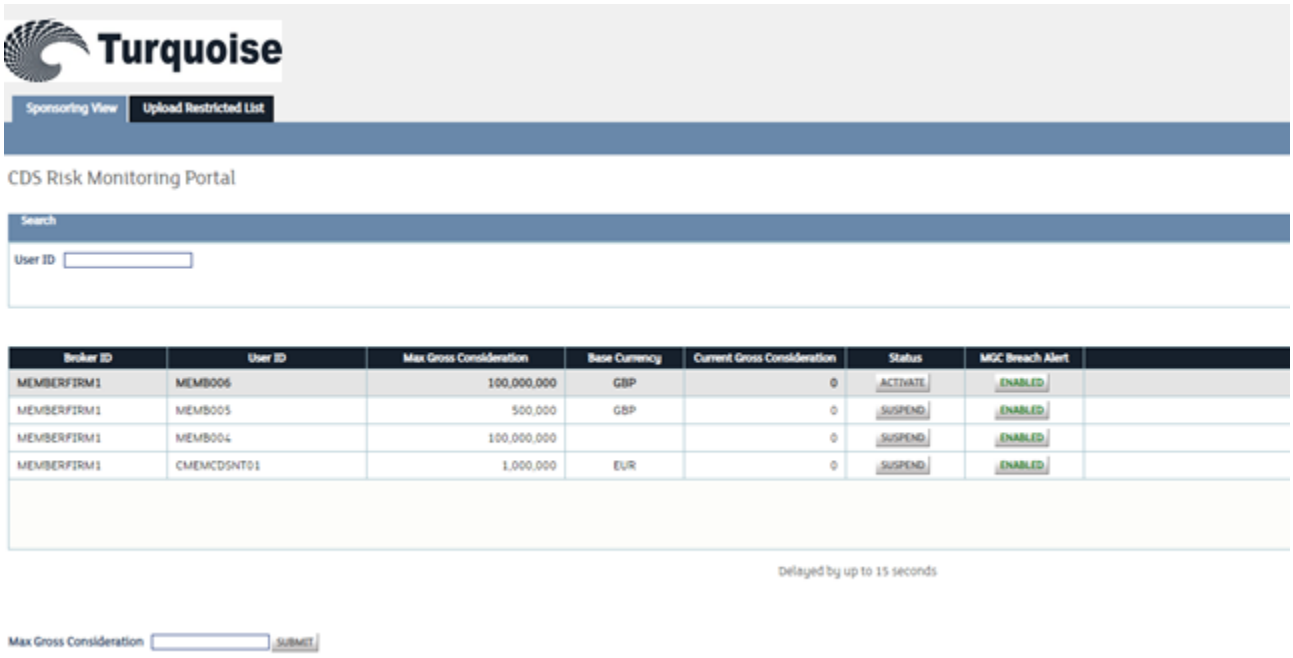
The Risk Monitoring Portal is available from 03:00 to 18:15 (UK time).

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 TRC information for the Trading Sessions you are monitoring:

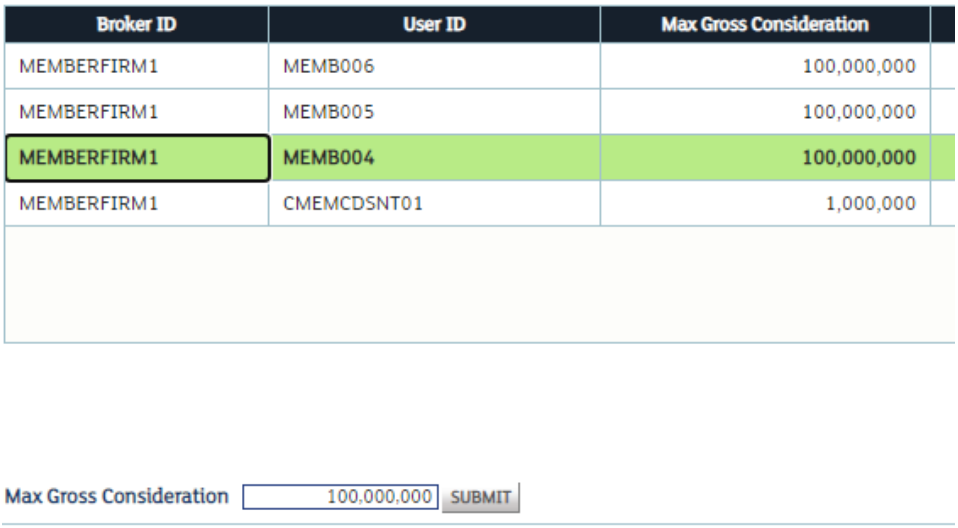
- List of Monitored Users
- Maximum Gross Consideration (MGC) set per User ID
- Current Global Gross Consideration
- Status – Suspend or Activate users
- MGC Breach Alert – Enable/Disable notifications of MGC is breeched.
- Alerts – Email notifications sent when MGC utilisation percentages are breached 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’.

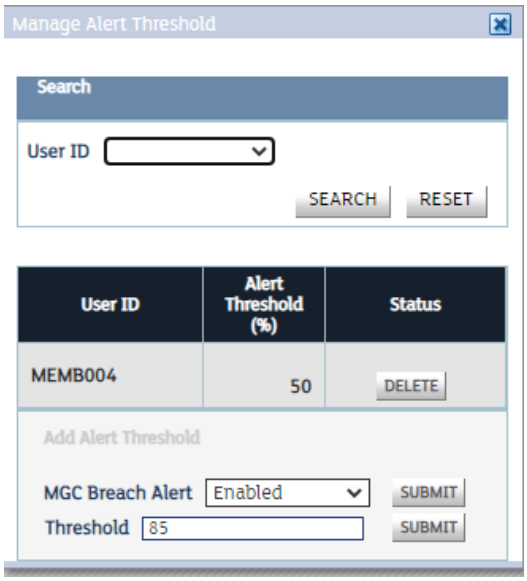
d) Setting Maximum Gross Consideration Breach Alert Levels

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 Turquoise Risk Controls with Risk Monitoring Portal access?

6.1 Risk Controller and Member Firm access

Member Firms of TGHL and TGHE can grant access to the Risk Monitoring Portal by submitting a Turquoise Risk 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 Turquoise Risk 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 Turquoise's Market Operations (MOPS) team.

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 TRC enablement.

An optional Daily Life Cycle (DLC) test is conducted with the Risk Controller 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 of TGHL or TGHE have with Turquoise. For further information on the daily life cycle please email market access.

Disclaimer

This service description is being distributed by Turquoise Global Holdings Limited only to, and is directed only at (a) persons who have professional experience in matters relating to investments who fall within Article 19(1) of the FSMA 2000 (Financial Promotion) Order 2005 and (b) persons to whom it may otherwise lawfully be communicated (together “relevant persons”). Any investment or investment activity to which this document relates is available only to and will be engaged in only with, relevant persons. Any person who is not a relevant person should not act or rely on this service description or any of its contents.

Turquoise Global Holdings Limited is an authorised investment firm by the Financial Conduct Authority.

Turquoise Global Holdings Europe B.V. is an investment firm authorised and regulated by the Autoriteit Financiële Markten (AFM) of the Netherlands.

Contact Details

Turquoise Global Holdings Limited
10 Paternoster Square
London EC4M 7LS
E: sales@tradeturquoise.com
T: +44 20 7382 7600

Turquoise