RESTRICTED LIST SINGLE SOURCE REQUIREMENTS

**COMPLIANCE**

Published as March 18, 2020

|  |
| --- |
| Contents  [1 overview 2](#_Toc36544767)  [2 BUSINESS VALUE 2](#_Toc36544768)  [3 SCOPE 3](#_Toc36544769)  [4 current state process 3](#_Toc36544770)  [5 future state process 6](#_Toc36544771)  [6 functional requirements 7](#_Toc36544772)  [7 non-functional requirements 10](#_Toc36544773)  [8 approval 13](#_Toc36544774)  [appendix 1 – user table mock-up 14](#_Toc36544775)  [APPENDIX 2 – USER TABLE SPECIFICATIONS 15](#_Toc36544776)  [APPENDIX 3 – RESTRICTION TYPES AND RULES 16](#_Toc36544777) |

1. overview

Compliance is responsible for managing and monitoring controls around restricted issuers and securities. The key component of these controls is a reliable, accurate and complete list of active restrictions; a single source of the truth available to all authorized downstream systems and users.

Currently BCI maintains three restricted lists in three different systems, all with different nomenclature to refer to the restricted issuer, and all based on human-entered issuer names with no supporting data validation.

Compliance is seeking to improve the controls, efficacy and efficiencies of the restricted list maintenance by implementing a single source of the restricted list with embedded data validation, end dating, the ability to add and store commentary, enhanced permission management, and a detailed audit trail.

1. BUSINESS VALUE

Implementing a single source restricted list with built in data validation at this time positions Compliance well for upcoming audits, automation and efficiencies.

This initiative will significantly improve controls around the access and maintenance of the restricted list by closing several control gaps and preparing for subsequent planned initiatives to automate Compliance processes. These control risks and mitigating measures are detailed in the Current State and Future State process flow sections of this document.

This initiative also allows Compliance to capture operational efficiencies by centralizing all restricted issuers, irrespective of the restriction reason, in a single place and augmenting the restricted list with critical information such as start and end dates, whether the restriction should apply to the named issuer, or the issuer and its subsidiaries, the name(s) of persons who alerted to the need for the restriction. It enables an automated method of end dating applicable restrictions (e.g. standstill agreements, insider blackout periods) with pre-defined end dates, and with automated periodic emails to persons who originally alerted the need for the restriction. This will prompt people to notify Compliance when restrictions can be removed for assessment and timely end dating, keeping the restricted list a manageable length.

A centralized single restricted list is the foundational component enabling planned Compliance efforts to automate a post trade monitoring of potential restricted issuers, and an automated employee pre-clearance process.

It further establishes a trusted copy restricted list to support pre-trade compliance checks in the current and future OMS enabling an automated identification of all tickers associated with the restricted issuer, and automatically applying pre-trade restrictions.

Preliminary research and discussions with IT and EDM indicate this initiative requires limited effort and is a viable solution which will deliver significant value.

1. SCOPE

These requirements focus on the design, development and delivery of a single source restricted list with embedded data validation and a monthly automated email reminder to Portfolio Managers who raised the need for a restriction to confirm whether restrictions should still be active.

Any integration with downstream pre and post trade monitoring processes is out of scope of these requirements and will be addressed, in priority, in subsequent requirement documents.

The following process sections in this document depict the current and future state processes is end-to-end and therefore refer to additional future initiatives to integrate the single source restricted list with pre and post trade systems and processes. These processes extend beyond the single source restricted list simply to illustrate how this initiative sets Compliance up for future improved controls, automation and efficiencies.

Section 6 Requirements only address the Single Source Restricted List and Automated Email reminders.

1. current state process

The current state restricted list process is manual and inefficient. It involves multiple entries to implement the restriction for pre and post-trade monitoring across multiple systems. The following chart illustrates the current state process accompanied by the step-by-step description.





* 1. **Process Flow Description**

1. a. Once the decision to add a corporate or wall restriction has been made, Legal looks up the issuer name on the Bloomberg terminal to source the issuer name. (Legal may have completed this step during their determination whether to apply a restriction.) Move to step 2.
2. b. Once Compliance becomes aware of a required ESG or Sanction restriction, Compliance looks up the issuer on the Bloomberg terminal to source the issuer name. Move to step 7.
3. Legal manually adds the restricted issuer to their Access Database based on the issuer name provided by Bloomberg OR the name provided in any relevant documentation. The issuer name has no embedded data validation to protect against typos or inaccuracies.
4. Legal prepares a Wall or Corporate Restriction Memo and emails the memo to the applicable parties and the Compliance shared email.
5. Compliance monitors the shared email for Wall or Corporate Restriction notifications (additions, and removals).
6. Compliance reviews the issuer name to be added to the restricted list and determines a condensed “root” version of the issuer and adds this to the SCD restricted list Excel. E.g. If the restricted issuer in the Corporate Restriction Memo is Enbridge Pipelines Inc, Compliance might add \*Enbridge\* to the SCD restricted list. Move to step 13.
7. Compliance looks up the restricted issuer on Bloomberg and identifies the primary security tickers associated with the Issuer Sedol (in some cases, Legal provides the ticker).
8. Compliance manually adds the ticker(s) to the XIP restricted list. Note, this is not an exhaustive list of all tickers associated with the issuer.
9. XIP applies pre-trade checks against the tickers in the restricted list.
10. XIP stops trades in restricted tickers. Compliance may override these restricted trades on a case-by-case basis.
11. From time to time, BCI employees emails the shared Compliance email with requests for personal trades. These emails may include a ticker, a security name, or an issuer name.
12. Compliance manually looks the employee requested name up against the Legal Access Database restricted list.
13. Compliance determines whether there is a match in the request name and the restricted list based on the information available. If yes, Compliance declines the employee request.
14. Compliance manually verifies the SCD list of restricted issuers aligns with the Legal Access Database. Note, Compliance is unable to do a full reconciliation since the issuer names differ, and Legal maintains a subset of all restrictions.
15. Compliance saves the daily SCD restricted securities Excel spreadsheet to the public S:\TRANSFER folder.
16. Compliance runs the SCD Excel macro on the shared Bloomberg terminal which automatically applies fuzzy logic to compare the restricted “root” issuers to Bloomberg issuers to SCD transactions with similar issuer names. This process produces a high number of false positives. Compliance saves the results on S:\Compliance and deletes the file from S:\TRANSFER
17. Legal approves the addition of read, write users to the Legal Access Database.
18. Compliance and Trade Management can approve read, write access to XIP compliance rules.

The current state process has several material risks that impede Compliance’s ability to implement strong pre and post trade controls. These risks are:

* Multiple restricted lists reside in multiple systems; Legal Access database (the master list), XIP and SCD. Different restriction types are recorded in each list. The three lists cannot be fully reconciled to ensure the lists are aligned.
* The restricted issuers are captured differently in each list and rely on human data entry and interpretation. There is no reliable and consistent reference, such as an LEI or other standard issuer reference ID between the lists.
* Updates to the disparate databases are made at different times. Additions and deletions to the master list are communicated through the issuance of corporate restriction and wall emails. Emails may be missed, or erroneously deleted resulting in missing names from the XIP and SCD lists. There may also be a significant delay in the additions or deletions to each list resulting in potential trading in a security already restricted.
* Different people are responsible for the different lists. Legal adds names to the Legal Access database, Compliance adds a “root” version of the name to SCD list, and Compliance adds the ticker of securities associated with the name to the XIP list.
* Legal and/or Compliance manually researches the ticker of securities associate with the Issuer to add to the XIP list. The list of tickers is not exhaustive exposing traders to potentially trading a restricted security.
* Securities are not related to issuers using a primary key or any data validation. Securities may erroneously be related to the wrong issuer. Corporate actions due to name changes, CUSIPs, M&A activity cannot be applied to the restricted issuer or securities with may lead to a misalignment or omission of restrictions.
* The SCD restricted list is managed and maintained in a password-protected Excel spreadsheet which may result in accidentally deleted restrictions or characters of restricted issuers which may lead missed transactions in the post-trade monitoring.
* The end-to-end process is un-auditable.

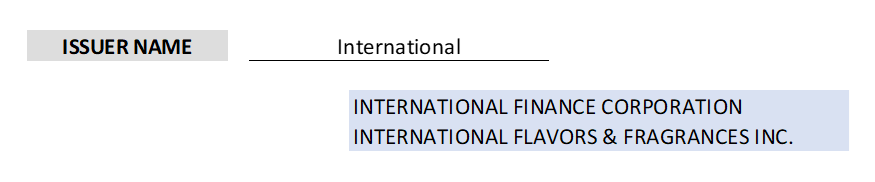
1. future state process





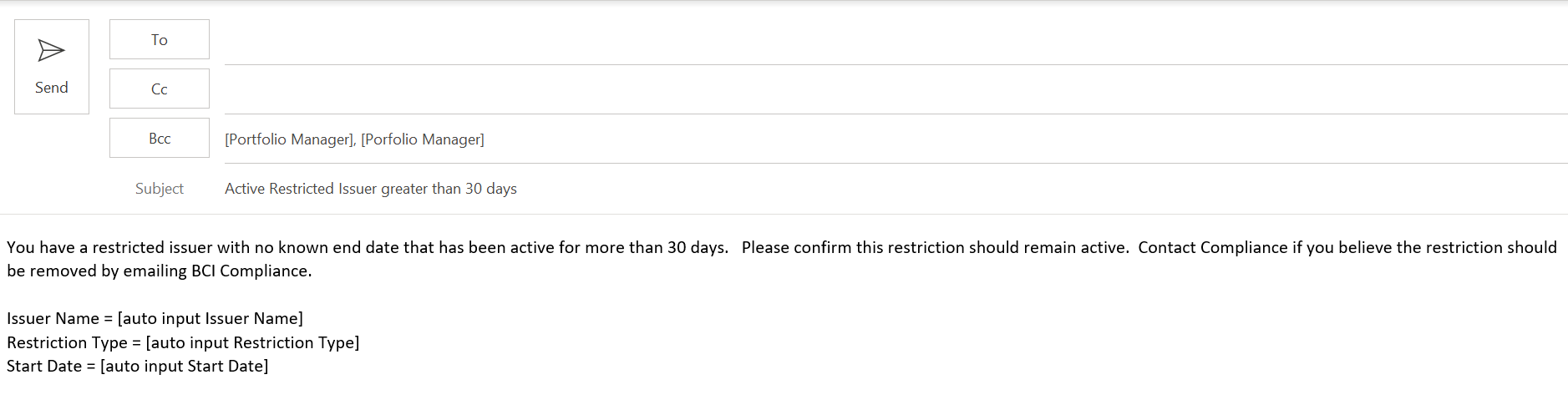
* 1. **Process Flow Description**

1. Compliance adds ALL restrictions to the single source restricted list.
2. Compliance selects the restricted issuer from an automated drop-down based on search-as-you-type suggestions from the data base of over 6million issuers.
3. The system automatically looks up and stores the primary key associated with the issuer. The use of a primary key ensures all processes relying on the restricted list consistently and accurately refer to the restricted issuer, irrespective of corporate actions. It also allows the system to automatically cascade the restriction to subsidiaries and securities issued by the restricted issuer.
4. Compliance manually adds the restriction type, based on a pre-defined drop-down list, the end date (if known), the Portfolio Manager name(s) who raised the need for a restriction, and the names of any persons deemed to be behind the wall (if applicable). Compliance can also add comments.
5. The system automatically pushes the new, removed or amended restriction to the down stream system consumers in real time.
6. The system automatically identifies all publicly traded tickers associate with the restricted issuer and stores in the OMS pre-trade compliance rules.
7. The OMS automatically updates its pre-trade restriction rules with a timestamp which matches the restricted list to within a second. This allows pre-trade rules to be applied exactly when restrictions are added (or removed exactly when restrictions are removed).
8. The OMS automatically applies pre-trade rules according to the restriction type. E.g. Sanctions = hard stop, Issuer Concentration = Soft stop etc. Refer to Appendix 3 for a list of potential restriction types and resulting rules.
9. Employees submit a personal pre-trade request. Employees select the desired security from a drop-down list of tickers.
10. The system automatically checks the employee’s requested ticker against the restricted list.
11. If the security is associated with a restricted issuer, the system automatically declines the employee requests.
12. On a T+1 basis, the restricted securities monitoring report automatically pull the prior day’s transactions.
13. The report automatically references the single source of the restricted list and compares transactions to the restricted issuers, start and end dates.
14. The report automatically identifies any transactions in restricted securities based on the restricted list issuer’s primary key.
15. Compliance controls all read and write access to the restricted list by approving user and system requests for access.
16. Data base can generate reports listing all users and system who have access to the restricted list on an ad hoc basis for Compliance to verify access controls.
17. Compliance reconciles the access report to the list of approved persons and systems, in production and non-production environments.
18. Database automatically logs all user and system interactions, including a full history of changes to restrictions.
19. Compliance can request audit logs on demand to support investigations or control verification.
20. functional requirements
    1. **Restricted List “Single Source”**
21. Create a user-friendly tool for Compliance to add restrictions in a single source.
    1. Allow compliance users to add a restriction to the restricted list by selecting an issuer from a drop-down list generated by a ‘search-as-you-type’ function. The system should suggest issuer names from the database based on the value the user types into the Issuer field. E.g.



* 1. Compliance may only select the Issuer from the values offered by the system.
  2. If the issuer name is not in the drop-down list (and therefore not in the database) Compliance must contact Data Operations to request the creation of the Issuer. This scenario only occurs in some cases where the issuer is a private company.
  3. When Compliance selects an issuer, the system must automatically populate the corresponding EDM Party ID to be used as the primary key.
  4. Allow Compliance to assign a restriction type by selecting from a pre-defined list of values.
     1. MNPI Wall
     2. MNPI Corporate
     3. Standstill Agreement
     4. Insider Blackout
     5. Sanctioned Issuer
     6. Issuer Concentration
     7. ESG
  5. Allow Compliance to indicate any portfolios that are excluded from the restriction by selecting one or many model portfolios from a drop down list.
     1. Where the excluded portfolios field is left blank, the system must apply the restriction to all portfolios.
  6. Allow Compliance to indicate whether the restriction should be inherited by subsidiaries of the restricted issuer.
     1. Where the user indicates N, the restriction is not inherited by issuers marked as a child of the restricted issuer
     2. Where the user indicates Y, the restriction is automatically inherited by issuers marked as a child of the restricted issuer
  7. Allow Compliance to select a start date either, by a calendar or by the user typing in the date.
     1. If the user does not enter a start date, automatically apply the current date.
  8. Allow Compliance to select an end date, either by a calendar or by the user typing in the date.
     1. Users may opt to leave the end date null
  9. Display all dates in the UI as MMM DD YY.
  10. Allow Compliance to select the names of Portfolio Managers to track who reported/requested the restriction.
      1. Users must be able to enter none, one or many names
      2. The names must be tied to the BCI single source of employee emails
  11. Allow Compliance to select the names of employees deemed to be “Insiders”.
      1. Users must be able to enter one or many names
      2. The names must be tied to the BCI single source of employees

1. Allow Compliance users to edit exiting restrictions.
   1. Compliance must be able to edit certain fields of an existing restriction:
      1. Restriction Type
      2. Excluded Portfolio(s)
      3. End Date
      4. Portfolio Manager
      5. Insiders
      6. Comments
   2. Compliance must **not** be able to edit:
      1. Restricted Issuer
      2. Issuer Identifier
      3. Start Date
      4. Created By
      5. Created Date
      6. Updated By
      7. Update Date
2. Compliance must not be able to delete records. If a restriction is no longer valid, Compliance must end date the restriction.
3. The Restricted List Single Source must be available to approved consumers (people and systems) to support pre and post trade monitoring and controls.
   1. **Automated Emails**
4. Compliance requires the solution to generate automated monthly email reminders to the Portfolio Managers associated with active restrictions older than 30 days.
   1. Active restrictions are where current date is ≥ the Start Date and < the End date, or where the end date is null
   2. Older than 30 days is where current date is at least 30 days greater than the start date
5. On the last business day of each month, the system should automatically generate an email as follows:



1. The system should send the email from ‘BCI Compliance’ to the portfolio managers associated with the restriction.
   1. Addressees should be blind copied.
2. non-functional requirements

**Availability**

1. Compliance requires access to the solution 24/7 99% of the time.
2. Scheduled maintenance should be planned outside of BCI trading hours (Monday to Friday 05:00 PT to 17:00 PT.
   1. Compliance requires 48-hour advance notice of any scheduled maintenance
   2. Notifications should be emailed to DL Compliance
   3. Notifications should include:
      1. Date and time of scheduled maintenance
      2. Estimated duration of outage
      3. Reason for scheduled maintenance
      4. Overview of impact
      5. IT contact person
3. Compliance requires notification of unscheduled maintenance as soon as the required maintenance is determined.
   1. Notifications should be emailed to DL Compliance
   2. Notifications should include:
      1. Date and time of unscheduled maintenance
      2. Estimated duration of outage
      3. Reason for unscheduled maintenance
      4. IT contact person
      5. Date and time of next update

**Auditability**

1. Compliance requires the ability to request ad hoc reports on systems and users who have read or write permissions against the restricted list.
2. Compliance requires the ability to request ad hoc restricted list audit trails including:
   1. Additions
   2. Edits
      1. Prior value
      2. New value
      3. Username of the editor
      4. Time stamp of the edits
3. FUTURE REQUIREMENT Compliance requires the ability to request ad hoc restricted list system audit trail including:
   1. Date and time stamp of push to downstream systems
   2. Status of push
      1. Success and number of records
      2. Partial success, including records incomplete
      3. Failure and error code

**Data Migration**

1. Compliance requires the current lists of active restrictions from the Legal Access Database, and XIP to be migrated to the new restricted list as a precondition of go live.
2. Compliance may need the support of IT and EDM to identify the correct issuers during the data migration effort.
3. The integrity of any start dates of existing restrictions must be migrated to the new restricted list.
4. The created by field should display SYSTEM for all restrictions migrated to the new solution.

**Data Retention**

1. Restricted records should never be deleted.
2. All active and inactive (end dated) restrictions must be retained indefinitely (until BCI defines a data retention policy).
3. Restrictions with end dates > 7 years in the past may be archived.

**Extendibility**

1. Compliance requires the ability to add new restricted type values as required post go-live.
2. Compliance requires the ability to retire (disable, not remove) field as required post go-live.
   1. Retired fields do not need to be backwards enabled (i.e. only applies on a go forward basis)
3. Compliance requires the ability to add new fields as required post go-live.
   1. Added fields do not need to be backwards enabled (i.e. only applies on a go forward basis)

**Integration**

1. The restricted list should integrate with BCI’s single source for Issuers (Parties), Issuer (Party) Relationships, Issuer-Security relationships, and employee email names and addresses.
2. The restricted list solution must be available for integration with downstream applications where the downstream applications are able to consume external data including:
   1. Order Management Systems (XIP, Bloomberg, Super Derivatives, FLS etc.) to support pre-trade compliance
   2. Execution Management Systems (Triton, Bloomberg etc.) to support pre-trade compliance
   3. T+1 Compliance monitoring tools (SCD, & future automated solution) to support post-trade compliance
   4. Employee pre-trade clearance systems and tools

**Performance**

1. Users must be able to add new restrictions with no human discernible lag.
2. Users must be able to edit existing restrictions with no human discernible lag.
3. Issuer drop-down lists should appear and dynamically change with the user’s typing in under 1 second.
4. Employee name drop-down lists should appear and dynamically change with the user’s typing in under 1 second.
5. All other drop-down should appear with no human discernible lag.
6. FUTURE REQUIREMENT New or changed restricted list records must be able to be pushed near-time to downstream future consumers.

**Permissions**

1. Compliance must approve all requests for read or write access to the restricted list, for both human and system users.
2. Upon go live the following personnel should have read and write access to the restricted list in production:
   1. Daniel Speirs
   2. Julia Liu
   3. Chris Baxter
   4. Larry Nguyen
   5. Grace Wan
   6. Krista Robinson
   7. Megan Scholz
3. Only Compliance approved IT and EDM support personnel may have read access to the restricted list in non-production environments post go-live.

**Support**

1. Compliance may require the creation of a new issuer (in the case of private issuers) in MEDM to support the restricted list. Compliance requires the support of Data Operations to create new issuers.
   1. Requests should be addressed within 4 business hours.
2. Compliance may require IT support for the maintenance of stability of the restricted list single source copy.
   1. Compliance must be able to submit support requests through service now.
   2. FUTURE REQUIREMENT (once the restricted list is integrated with downstream consumers) Support requests must be addressed on a high priority basis as delays in the correct application of restrictions to pre trade controls may result in regulatory breaches and/or legal violations.
3. approval

These requirements have been reviewed and approved by:

| **Name** | **Role** | **Date** |
| --- | --- | --- |
| Patricia Bood | Executive Business Sponsor |  |
| Daniel Speirs | Business Sponsor |  |
| Chris Baxter | Business Owner |  |
| Chris Allen | Stakeholder |  |
| Sumit Dhall | BSE |  |
| Bhagyasri Velpula | Development Lead |  |

appendix 1 – user table mock-up

The following mock-up is for illustrative purposes only and does not reflect actual restrictions.



APPENDIX 2 – USER TABLE SPECIFICATIONS



APPENDIX 3 – RESTRICTION TYPES AND RULES

The following table provides an example of how Compliance can configure the rules, or outcomes, associated with each distinct restriction type. The table as depicted may not reflect current procedures.

Maintaining a list of rules associated with restriction types provides Compliance with the flexibility to amend the rules if policies or procedures change.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **RESTRICTION**  **TYPE** | **INDEX**  **EXEMPT** | **POOL**  **TRADING** | **BCI**  **TRADING** | **PERSONAL TRADING** |
| MNPI Wall | N/A | Hard Stop if behind the wall | No impact | Prohibited if behind the wall |
| MNPI Corporate | Yes | Hard Stop | Hard Stop | Prohibited |
| Standstill Agreement | No | Hard Stop | Hard Stop | No restriction |
| Insider Blackout | No | Hard Stop if insider | Soft Stop | Prohibited if insider |
| Sanctioned Issuer | No | Hard Stop | Hard Stop | No restriction |
| Issuer Concentration | No | Soft Stop | Soft Stop | No restriction |
| ESG | Yes | Hard Stop | Hard Stop | No restriction |

Hard Stops = Can only be overridden by Compliance

Soft Stops = Can be overridden by trader