ets connect
UK

ETS Connect UK Contributor FIX Rules of Engagement DRAFT

21 January 2026
Version 0.1

Contents

CTP FIX Contributor Rules of Engagement

1. Document control

This document defines the Rules of Engagement ("RoE") applicable to all Contributors submitting data to the UK Bond Consolidated Tape ("CTP").

This is a controlled document and subject to formal versioning. Updates may be issued periodically to reflect regulatory change, operational experience, or enhancements to the CTP service.

Normative language:
- MUST – mandatory requirement
- SHOULD – strong recommendation
- MAY – optional capability

In the event of conflict, contractual and regulatory obligations take precedence.

2. Purpose and regulatory context

The purpose of this document is to define the behavioural, operational, and technical obligations of Contributors connecting to and submitting data into the CTP.

This RoE supports market integrity, operational resilience, and compliance with the FCA Concession Agreement.

3. Scope and document structure

This RoE governs contributor onboarding, certification, FIX session behaviour, data quality, incident handling and service management processes.

It does not define message schemas, connectivity specifics, or commercial terms, which are covered by separate controlled documents.

https://ets-connect.co.uk/access/contributor-connectivity/

4. Contributor eligibility and obligations

Only approved entities may act as Contributors.

Contributors must comply with this RoE on an ongoing basis and notify the CTP of material changes.

5. Environments and access

Separate environments are provided for certification and production.

Production must not be used for testing. Configuration parity between environments is mandatory.

The following table specifies the system environments made available to FIX Contributors and formally defines their respective purposes, usage constraints, and operational scope.

Environment	Intended Function
UAT (User Acceptance Testing)	The UAT environment is provided exclusively for pre-production activities, including FIX protocol integration testing, message schema validation, functional verification, and mandatory certification. Contributors shall use this environment to validate session behaviour, business workflows, error handling, and recovery scenarios The CTP shall lead the testing process and the Contributor shall provide all assistance that is reasonably requested by the CTP (including providing real or dummy data (at the Contributor's election) for test purposes).
PROD (Production)	The Production environment is designated solely for live operational FIX connectivity and the exchange of production-grade messages. It supports real-time data flows and is governed by strict security, availability, monitoring, and compliance controls. Access to the Production environment is restricted to FIX Contributors that have successfully completed certification, satisfied all onboarding requirements, and received explicit authorisation to proceed to production.

6. Connectivity and transport requirements

This section defines the mandatory technical and security requirements governing FIX connectivity between Contributors and the CTP FIX Contributor Gateway.

6.1. Transport Protocol and Session Establishment

Inbound FIX contributions MUST be transmitted over persistent, TCP-based FIX tag=value sessions in accordance with the applicable FIX specification and this Rules of Engagement. FIX sessions must be established using approved endpoints and session identifiers assigned during onboarding, and Contributors must not transmit application-level messages until the FIX Logon sequence has completed successfully.

6.2. Connection Management, Retry, and Backoff Behaviour

Contributors MUST implement an exponential reconnect backoff strategy with randomised jitter for all FIX session reconnection attempts. The initial retry delay shall be no less than five (5) seconds, doubling on each subsequent failure up to a maximum retry interval of three hundred (300) seconds. Reconnect attempts at fixed short intervals, parallel reconnect attempts for the same FIX session, or aggressive retry loops are strictly prohibited. Backoff behaviour must be applied consistently regardless of disconnect cause, including network or transport-level failures, receipt of Logout (35=5) messages, or Logon rejects. Contributors must investigate and remediate the underlying cause of repeated disconnects before continuing automated reconnection attempts.

6.3. Transport Security and Mutual TLS (mTLS)

All FIX connectivity between the Contributor and the CTP FIX Contributor Gateway MUST be secured using mutual Transport Layer Security (mTLS). Both parties must present and validate X.509 certificates during TLS session establishment, and FIX sessions must not be established unless the mTLS handshake completes successfully using TLS version 1.2 or higher.

6.4. Certificate Issuance, Validity, and Renewal

All client certificates shall be issued and signed by CTP, or by a Certificate Authority operating under CTP's control, following submission of a Certificate Signing Request (CSR) by the Contributor through the official CTP onboarding process. Issued certificates shall have a maximum validity period of 12 months, consistent with industry security best practices. Contributors must initiate certificate renewal no later than thirty (30) calendar days prior to certificate expiry to ensure continuity of service.

6.5. Environment Isolation and Trust Anchor Segregation

Trust anchors, certificate authorities, and certificate chains used for non-production environments (including UAT) are logically and cryptographically isolated from those used for the Production environment. Certificates issued for one environment must not be reused, trusted, or accepted in another environment. Separate certificates and trust chains are required per environment.

6.6. Private Key Protection and Certificate Usage

Certificates must be used exclusively by the approved Contributor system and must not be shared across multiple legal entities, environments, or unrelated applications. Contributors are responsible for the secure generation, storage, and protection of private keys, as well as timely certificate renewal or rotation in accordance with CTP-defined timelines. Any expired, revoked, compromised, or otherwise invalid certificate may result in connection refusal or administrative Logout, and Contributors must promptly notify CTP of any suspected private key compromise or unauthorised certificate use.

6.7. Monitoring, Enforcement, and Remedial Actions

CTP may monitor connectivity behaviour, TLS handshakes, certificate usage, and reconnection patterns for compliance with this section. Non-compliant behaviour may result in throttling, administrative Logout, temporary suspension of connectivity, or mandatory remediation prior to reconnection.

6.8. Authentication and contributor identification

Each Contributor shall be issued with unique authentication credentials (e.g., username and password) and FIX session identifiers (including SenderCompID and any additional credentials required at Logon) that are used to authenticate and uniquely identify the Contributor and the specific FIX session. All identifiers and credentials must be used strictly as allocated, must not be shared across systems, users, or third parties, and must be protected against unauthorised access in accordance with the Contributor’s internal security policies and industry best practices. Credentials must be securely stored, transmitted only within encrypted transport channels where applicable, and rotated or replaced when compromise is suspected. Any misuse, loss, or suspected compromise of credentials must be reported to CTP immediately, and CTP reserves the right to suspend or revoke access where credential integrity cannot be assured..

7. FIX session rules

Contributors must operate FIX sessions in full compliance with FIX Trading Community session-layer standards, including proper use of Logon, Heartbeat, TestRequest, ResendRequest, Sequence Reset, and Logout messages. Sessions must maintain continuous message sequencing across reconnects, apply negotiated Heartbeat intervals, and perform liveness checks using TestRequest when inactivity thresholds are exceeded. Graceful session termination via Logout is required where possible and forced disconnects must occur when liveness or sequence integrity cannot be maintained. All recovery and reconnect activity must follow the retry and backoff policy defined in this RoE, and parallel or aggressive session re-establishment attempts are prohibited.

8. Sequence numbers, recovery and replay

Contributors are responsible for the correct and continuous management of FIX message sequence numbers (MsgSeqNum, Tag 34) for each FIX session and must preserve sequence integrity across disconnects and reconnects. Contributors must support standard FIX recovery mechanisms, including the detection of sequence gaps, issuance and processing of ResendRequest (MsgType=2), and proper handling of replayed messages and SequenceReset messages (including Gap Fill). Application messages must be processed in strict sequence order. Sequence number resets must not be performed unless explicitly agreed with CTP or during formally coordinated session resets. Failure to correctly manage sequence numbers, recovery, and replay behaviour may result in session termination or suspension of connectivity

9. Message submission rules

Only supported MsgTypes may be submitted.

Mandatory fields, enumerations, and logical ordering must be respected.

The following table specifies the supported message types both inbound and outbound.

FIX Message Type	MsgType (Tag 35)	Definition and Intended Use
Logon	A	Used to establish a FIX session between the Contributor and the CTP FIX Gateway. The Logon exchange authenticates the Contributor, negotiates session parameters (e.g. HeartBtInt), and synchronises sequence numbers. Contributors **MUST** successfully complete the Logon process before sending any application-level messages.
Logout	5	Used to terminate a FIX session in an orderly manner or to signal an administrative or error condition. Upon receipt of a Logout, the receiving party **MUST** immediately cease message transmission and close the session in accordance with FIX session rules.
Heartbeat	0	Used to maintain session liveness in the absence of application messages and to respond to TestRequest messages. Heartbeats **MUST** be exchanged at the negotiated heartbeat interval.
TestRequest	1	Used to verify session liveness when expected Heartbeat or application messages are not received within the negotiated interval. Upon receipt, the counterparty **MUST** respond with a Heartbeat containing the corresponding TestReqID.
ResendRequest	2	Used to request retransmission of messages when a sequence gap is detected. The receiving party **MUST** respond by retransmitting the requested messages, subject to standard FIX resend and gap-fill rules. Contributors

		MUST support ResendRequest handling as part of session recovery.
SequenceReset	4	Used to reset or adjust message sequence numbers, typically as a Gap Fill (GapFillFlag=Y) during resend processing. SequenceReset messages **MUST** be processed strictly in accordance with FIX session rules to maintain sequence integrity. Unauthorised or inappropriate sequence resets are prohibited.
MarketDataIncrementalRefresh	X	Used by Contributors to publish incremental bond market data updates to CTP, including additions, changes, and deletions relative to the previously published state. Messages **MUST** be sent and processed strictly in sequence to ensure data consistency and correct downstream consolidation.
MarketDataAck	EQ	Used to acknowledge the processing status of market data messages, including rejection or issue notification (flagged with DQ issue), where acknowledgment workflows are enabled under the defined market data processing model.

10. Data quality and validation expectations

Contributors retain full responsibility for the accuracy, completeness, consistency, and timeliness of all data submitted to the CTP. The CTP performs validation and quality controls in support of consolidation and publication but does not assume responsibility for the correctness of contributor data.

Contributors MUST ensure that submissions:

- reflect the underlying executed transaction accurately,

- are submitted as soon as technically possible following execution,
- contain all mandatory fields populated correctly and are internally consistent across related fields (e.g. price, size, identifiers, timestamps).

10.1. Timeliness

Contributors are expected to submit data **without undue delay** and in accordance with applicable regulatory reporting requirements. Systematic late submission, repeated correction of stale data, or batching behaviour that materially delays publication may be treated as a data quality issue.

10.2. Amendments and Cancellations

Contributors **MUST** ensure that amendments and cancellations:

- correctly reference the original transaction,
- are submitted only where genuinely required,
- and reflect a clear and auditable lifecycle of the transaction.

High volumes of amendments or cancellations may be monitored as an indicator of upstream control weakness.

10.3. Persistent Data Quality Issues

Where persistent or systemic data quality issues are identified, the CTP may:

- require enhanced monitoring or reporting,
- mandate remediation actions,
- require partial or full re-certification,
- or apply enforcement measures in accordance with this RoE.

11. Rejects, errors, notifications and remediation

Session-level and application-level rejects may be issued.

Contributors must investigate, remediate, and prevent recurrence.

The following table specifies the session and application-level reject Message Types:

Message Type	MsgType (35)	Level	Definition and Intended Use
Reject	3	Session	Used to indicate a protocol-level or session-layer validation failure, such as missing mandatory tags, invalid tag formats, incorrect tag ordering, or other FIX structural violations. Reject messages relate to session integrity rather than business processing. Upon receipt of a Reject, Contributors **MUST** evaluate and remediate protocol defects before continuing normal message flow. Persistent session-level errors **MAY** result in administrative Logout.
MarketDataAck	EQ	Application	Used to acknowledge receipt and processing outcome of market data messages submitted by Contributors. The acknowledgment may indicate acceptance with error (with DQ issue) or rejection in accordance with the defined market data workflow. This message type is used for operational transparency and downstream reconciliation and does not replace FIX session-level recovery mechanisms. The following describes the 2 types of MarketDataAck response that will be received by a Contributor: 1. Rejected – ReportStatus=2, RejectText=<Code and Error message describing the error>

			2. Accepted with DQ Issue – ReportStatus=3, NoLinesOfText=<Number of DQ criteria that failed>, Text=<Repeating text of error code and error message describing the failure>

12. Message correction and governance

The correction of previously submitted data is permitted **only where necessary to rectify a genuine error** and must be performed in a controlled, auditable manner.

Contributors **MUST NOT** use correction mechanisms to:

- mask upstream system defects,
- re-sequence transactions for convenience,
- or retrospectively alter economic outcomes.

12.1. Exceptional Circumstances

Corrections are expected to be **exceptional** and may include, for example:

- incorrect price or quantity,
- incorrect instrument or identifier,
- erroneous trade classification.

Corrections relating solely to internal reconciliation convenience are not permitted.

12.2. Correction Mechanism

All corrections **MUST** follow the technical mechanisms defined in the CTP FIX specification, using the appropriate amend or cancel semantics. Direct overwrite or resubmission without linkage to the original record is prohibited.

12.3. Operational Coordination

For material or widespread corrections, Contributors **MUST** notify the CTP in advance where practicable and cooperate on timing, sequencing, and communication. The CTP may impose conditions or constraints on correction activity to protect market integrity and service stability.

12.4. Auditability

Contributors **MUST** retain sufficient records to demonstrate:

- the root cause of the error,
- the rationale for correction,
- and the linkage between original and corrected records.

13. Operational resilience requirements

Contributors are expected to operate contribution services with a level of resilience proportionate to their role in supporting the CTP.

This includes the ability to:

- tolerate transient infrastructure failures,
- recover cleanly from disconnection,
- and resume contribution without data loss or duplication.

Guidance on infrastructure connectivity requirements can be found here;

Contributor Connectivity | ETS Connect – UK

13.1. Behaviour During Disruption

During CTP incidents, degraded modes, or recovery events, Contributors **MUST**:

- follow instructions issued by the CTP,
- refrain from uncoordinated recovery actions,
- and avoid behaviour that could exacerbate instability (e.g. reconnect storms, uncontrolled replays).

CTP instructions issued during an incident **take precedence** over standard operating behaviour.

13.2. Recovery and Resumption

Following disruption, Contributors **MUST**:

- re-establish FIX sessions in accordance with session rules,
- correctly recover message sequence state,
- and ensure continuity and integrity of data submission.

Where instructed by the CTP, Contributors may be required to pause, throttle, or sequence resubmission activity.

13.3. Testing and Preparedness

Contributors are expected to periodically validate their ability to restart, recover, and reconnect in accordance with this RoE. Participation in coordinated readiness or resilience exercises, where requested, forms part of ongoing operational readiness.

14. Time synchronisation requirements

Accurate and consistent time synchronisation is critical to the integrity of the consolidated tape. Contributors are responsible for ensuring that all timestamps submitted to the CTP accurately reflect the timing of the underlying transaction events.

Contributors **MUST** synchronise all systems involved in data generation and submission to a recognised, authoritative time source and ensure that timestamps are applied consistently across their contribution stack.

14.1. Clock Synchronisation

Contributors **MUST**:

- synchronise system clocks using a reliable time synchronisation mechanism (e.g. NTP or equivalent),
- ensure continuous time synchronisation during operational hours,
- and monitor clock offset and drift on an ongoing basis.

The use of unsynchronised local system clocks is prohibited.

14.2. Timestamp Accuracy and Tolerance

All timestamps submitted to the CTP **MUST**:

- be correctly formatted in accordance with the FIX specification (UTCTimestamp data type i.e. YYYYMMDD-HH:MM:SS.ssssss),
- fall within the permitted tolerance window defined by the CTP,
- and be internally consistent across related fields (e.g. execution time, sending time).

Submissions with timestamps that are materially in the future, materially in the past, or inconsistent with observed system time may be rejected or flagged for investigation.

14.3. Clock Drift and Failure Handling

Contributors **MUST** detect and remediate clock drift or synchronisation failures promptly.

Where a time synchronisation issue is identified, Contributors are expected to:

- suspend or correct affected submissions where necessary,
- notify the CTP if data integrity may be impacted,
- and take appropriate corrective action before resuming normal operation.

Persistent or unremediated clock drift may be treated as a data quality issue.

14.4. Testing and Evidence

As part of certification and ongoing operation, Contributors **MUST** be able to demonstrate:

- correct time synchronisation configuration,
- monitoring of clock offset and drift,
- and appropriate handling of time-related errors.

Evidence may be requested by the CTP during certification, incident investigation, or supervisory review.

15. Certification test scenarios

Mandatory certification scenarios are defined in Appendix B and include session, recovery, data quality, idempotency, and resilience tests.

16. Change management and re-certification

Material changes must be notified in advance and may require re-certification.

Unauthorised changes may result in suspension.

17. Monitoring, reporting and evidence

Contributors must monitor contribution flows and retain logs and metrics.

Evidence must be supplied upon reasonable request.

18. Incident management and escalation

Contributors must promptly notify incidents impacting contribution and cooperate fully in resolution and review.

19. Enforcement and sanctions

The CTP applies a graduated enforcement model including warnings, throttling, suspension, and decertification.

20. Confidentiality and data handling

CTP endpoints and data must be used only for authorised purposes and protected against unauthorised disclosure.

21. Appendix A – CTP FIX Contributor Certification Checklist

(Contributor-facing, one-page checklist)

1. Legal & Governance (Pre-Requisite)

- ☐ Contributor Agreement executed
- ☐ Named operational contacts agreed
- ☐ Incident notification contact agreed
- ☐ Change management contact agreed
- ☐ Contributor registered in CTP onboarding register (CTP use only)

2. Identity & Access

- ☐ SenderCompID allocated and confirmed
- ☐ TargetCompID confirmed
- ☐ SubID usage agreed (if applicable)
- ☐ IP ranges allowlisted
- ☐ TLS certificates installed (if applicable)

3. FIX Session Compliance

- ☐ Valid Logon sequence
- ☐ Heartbeat interval honoured
- ☐ TestRequest handled correctly
- ☐ Graceful Logout supported
- ☐ No unexpected disconnects

4. Sequencing & Recovery

- ☐ MsgSeqNum strictly increasing
- ☐ Gap detection functions correctly
- ☐ ResendRequest handled correctly
- ☐ Clean session restart and recovery

5. Message & Schema Compliance

- ☐ Only supported MsgTypes submitted
- ☐ Mandatory tags always populated
- ☐ Enumerated values conform to specification
- ☐ Repeating groups correctly formed
- ☐ Unknown/unsupported tags handled per RoE

6. Timestamp & Clock Discipline

- ☐ SendingTime correctly formatted
- ☐ Timestamp precision meets requirements
- ☐ Clock skew within tolerance
- ☐ Future timestamps correctly rejected

7. Data Quality Obligations

- ☐ Unique trade identifiers enforced
- ☐ Amendments handled correctly
- ☐ Cancellations handled correctly
- ☐ No logically invalid values submitted
- ☐ Contributor accepts responsibility for data correctness

8. Idempotency & Retry Behaviour

- ☐ Safe retry logic implemented
- ☐ Duplicate identifiers correctly handled
- ☐ Out-of-order retries do not corrupt state

9. Rate Limiting & Flow Control

- ☐ Sustained message rate within limits
- ☐ Burst behaviour controlled
- ☐ Backoff applied when throttled
- ☐ No aggressive reconnect behaviour

10. Resilience & Incident Behaviour

- ☐ Client restart tested
- ☐ Network interruption tested
- ☐ Contributor responds appropriately to CTP incidents
- ☐ Logs and evidence can be supplied on request

Certification Outcome:

☐ Pass ☐ Conditional Pass ☐ Fail

CTP Sign-off: ____________________ Date: ____________________

22. Appendix B – CTP FIX Contributor Certification Test Matrix

Inbound FIX (tag=value)

1. Pre-Certification Preconditions

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
P-01	Legal	Contributor agreement executed	M	Agreement in force	Signed contract
P-02	Identity	SenderCompID/SubID allocated	M	IDs registered	ID register
P-03	Network	IP allowlisting complete	M	TCP connect succeeds	Firewall logs
P-04	Security	TLS handshake (if applicable)	M	Handshake succeeds	TLS logs

2. FIX Session Establishment

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
S-01	Logon	Valid Logon message	M	Session established. Logon received.	FIX logs
S-02	Auth	Invalid credentials rejected	M	Logout + disconnect	Reject msg
S-03	Heartbeat	Heartbeat interval honoured	M	No missed beats. No TestRequest received or sent.	Metrics
S-04	TestRequest	Responds correctly	M	Heartbeat returned	Transcript
S-05	Logout	Graceful Logout	M	Clean close	Transcript

3. Sequence Numbers & Recovery

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
R-01	Sequencing	Monotonic MsgSeqNum	M	No gaps. No ResendRequest sent or received.	Logs
R-02	Recovery	Gap detection	C	ResendRequest issued	Logs
R-03	Replay	Correct replay behaviour	C	Expected messages only	Logs
R-04	Reset	ResetSeqNumFlag usage	C	Per RoE	Logs

4. Message Submission & Schema

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
M-01	MsgTypes	*Supported MsgTypes only	M	Unsupported rejected	Rejects
M-02	Required	*Mandatory tags present	M	No missing tags	Validation report
M-03	Enums	*Valid enum values	M	Invalid rejected	Rejects
M-04	Groups	*Repeating groups valid	M	Parsed correctly	Logs
M-05	Unknown	*Unknown tags	M	Rejected	Logs

* Contributors can use the sample FIX message defined in Appendix E

5. Time Synchronisation

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
T-01	Format	SendingTime format	M	Parsed OK	Logs
T-02	Skew	Clock skew tolerance	C	Within limits	Monitoring
T-03	Future	Future timestamps	C	Rejected	Rejects

6. Data Quality & Validation

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
D-01	Uniqueness	*Unique trade IDs	M	No duplicates	Audit
D-02	Amend	*Amend lifecycle	M	Correct state	Logs
D-03	Cancel	*Cancel lifecycle	M	Correct state	Logs
D-04	Logic	*Logical validity	M	Rejected if invalid	Rejects (MarketDataAck)
D-05	Outlier	*Outlier detection	M	DQ flagged	Notification (MarketDataAck)
D-06	Consistency	*Cross-field consistency	C	Rules satisfied	QA report

* Contributors can use the sample FIX message defined in Appendix E

7. Rate Limiting & Flow Control

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
F-01	Rate	Sustained rate	C	Within limits	Metrics
F-02	Burst	Burst over limit	C	Throttle applied	Throttle logs
F-03	Backoff	Client backoff	C	Rate reduces	Metrics
F-04	Abuse	Sustained abuse	C	Disconnect	Session logs

8. Resilience & Restart

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
O-01	Restart	Client restart	M	State recovered	Logs
O-02	Network	Mid-flow disconnect	C	Successful recovery	Logs
O-03	CTP	CTP restart	M	No data loss	Audit
O-04	Degraded	Degraded mode	C	Adapts	Metrics

9. Incident Behaviour

ID	Test Area	Description	Requirement	Pass Criteria	Evidence
E-01	Errors	Error storm handling	M	Remediates	Incident record
E-02	Notify	Incident notification	M	Timely notice	Email/ticket
E-03	Evidence	Evidence provision	M	Logs supplied	Evidence pack

23. Appendix C – Material Change & Re-Certification Policy

This appendix defines what constitutes a material change for a certified FIX contributor and when re-certification is required.

Change Type	Examples	Re-Certification Required
FIX Engine	Engine change or major upgrade	Yes
FIX Version	FIX version or service pack change	Yes
FIX Data Dictionary	FIX Data Dictionary Updates	Yes
Message Logic	Mapping or lifecycle logic change	Yes
Identifier Usage	SenderCompID / SubID changes	Yes
Clock Source	Time sync mechanism change	Yes
Network	New IP ranges or routing	Yes
Resilience Design	Failover or restart logic change	Yes
Volume Profile	Sustained volume increase	Conditional
Infrastructure	OS or hardware changes only	No (Notify)
Bug Fix	No behavioural change	No (Notify)

Unnotified material changes may result in throttling, suspension, or decertification.

24. Appendix D – Service Management Information

(Contributor operational readiness)

This appendix defines the core service management capabilities Contributors are expected to maintain on an ongoing basis to support stable and resilient contribution to the CTP.

1. Service Ownership & Governance

Clear accountability for the contributor FIX service, including named business, technical, and operational owners with defined escalation paths.

2. Availability & Support Model

Defined support arrangements aligned to CTP operating hours, including contact coverage and response expectations.

3. Incident Management

Documented processes for incident detection, classification, notification, resolution, and post-incident review.

4. Monitoring & Alerting

Active monitoring of FIX connectivity, message flow, sequencing, error rates, and time synchronisation.

5. Change Management

Formal control of changes affecting FIX contribution, including assessment of material changes and notification to the CTP.

6. Release & Deployment Controls

Controlled release practices ensuring separation of testing and production, with approval and rollback mechanisms.

7. Resilience & Recovery

Documented and tested restart, recovery, and failover procedures for contributor-side systems.

8. Security & Certificate Management

Ongoing management of mTLS certificates, credentials, and access controls, including rotation and revocation.

9. Logging, Audit & Evidence

Retention of sufficient logs and audit trails to support incident investigation and supervisory review.

10. Capacity & Performance Management

Assessment and management of message volumes, peak load behaviour, and adherence to rate limits.

11. Training & Awareness

Appropriate training for staff involved in FIX contribution, including incident and change handling.

12. Periodic Review & Attestation

Periodic internal review of contribution arrangements and ability to attest compliance to the CTP on request

25. Appendix E - Example FIX messages

Test	FIX Message	FIX Response	Expectation
Baseline	35=X|1031=MDMSG-BASE-0001|268=1|279=0|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000001|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C		This is a minimal valid 35=X input trade with required enums and the required repeating groups.
M-01	35=D|1031=MDMSG-M01-0001|268=1|279=0|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP	8=FIXT.1.1|9=120|35=3|34=2|49=MTE|52=20260116-12:05:12.236623|56=E2E_CONTRIBUTOR_1|45=3|58=Invalid MsgType, field=35|371=35|372=D|373=11|10=150|	CTP rejects because Input from Contributors is

<table>
<tr><td></td><td></td><td></td><td>defined as MarketDataIncrementalRefresh MsgType = X.</td></tr>
<tr><td><b>M-02</b></td><td>35=X|1031=MDMSG-M02-0001|268=1|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000002|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td>8=FIXT.1.1|9=126|35=3|34=5|49=MTE|52=20260116-10:07:47.766544|56=E2E_CONTRIBUTOR_1|45=5|58=Required tag missing, field=279|371=279|372=X|373=1|10=001|</td><td>Rejected due to missing mandatory tag (279).</td></tr>
<tr><td><b>M-03</b></td><td>35=X|1031=MDMSG-M03-0001|268=1|279=9|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000003|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td>8=FIXT.1.1|9=152|35=3|34=4|49=MTE|52=20260116-12:05:12.257379|56=E2E_CONTRIBUTOR_1|45=5|58=Value is incorrect (out of range) for this tag, field=279|371=279|372=X|373=5|10=189|</td><td>Rejected for invalid enum value (279=9)</td></tr>
<tr><td><b>M-04</b></td><td>35=X|1031=MDMSG-M04-0001|268=1|279=0|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000004|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C</td><td>8=FIXT.1.1|9=153|35=3|34=5|49=MTE|52=20260116-12:05:12.268587|56=E2E_CONTRIBUTOR_1|45=6|58=Incorrect NumInGroup count for repeating group, field=768|371=768|372=X|373=16|10=044|</td><td>Rejected or parse error because group instances do not match</td></tr>
</table>

			declared counts.
M-05	35=X|1031=MDMSG-M05-0001|268=1|279=0|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000005|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C|9999=SHOULD_REJECT	8=FIXT.1.1|9=145|35=3|34=6|49=MTE|52=20260116-12:05:12.279148|56=E2E_CONTRIBUTOR_1|45=7|58=Tag not defined for this message type, field=9999|371=9999|372=X|373=2|10=124|	Rejected due to unknown/unexpected tag (9999)
D-01	35=X|1031=MDMSG-DQ-0001|268=1|279=0|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000001|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C		This is a valid 35=X message with the required fields and expected combination of fields.
D-02	35=X|1031=MDMSG-DQ-0001|268=1|279=1|269=2|270=193.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000001|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C		This is a valid 35=X message with MDUpdateAction set to 1 (AMND).
D-03	35=X|1031=MDMSG-DQ-0001|268=1|279=2|269=2|270=193		This is a valid 35=X

<table>
<tr><td></td><td>.64|423=3|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000001|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td></td><td>message with MDUpdateAction set to 2 (CANC).</td></tr>
<tr><td><b>D-04</b></td><td>35=X|1031=MDMSG-D04-0001|268=1|279=0|269=2|270=193.64|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000005|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td>35=EQ|3110=MDMSG-D04-0001|3113=2|1328=Rejected: business validation failed - MDEntryPx(270) present but PriceType(423) is missing; when 270 is reported, 423 must be provided.</td><td>Rejected due to missing PriceType tag 423. When Price is reported, PriceType should NOT be missing.</td></tr>
<tr><td><b>D-05</b></td><td>35=X|1031=MDMSG-D05-0001|268=1|279=0|269=2|270=193.64|423=9|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000005|1906=5|768=2|769=20260107-08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td>35=EQ|3110=MDMSG-D05-0001|3113=3|33=1|58=Accepted with errors: business validation warning - MDEntryPx(270)=193.64 exceeds the threshold value of 25 when PriceType(423)=9 (YIELD).</td><td>Flagged with DQ issue. Yield exceeds expected threshold.</td></tr>
<tr><td><b>D-06</b></td><td>35=X|1031=MDMSG-D06-0001|268=1|279=0|269=2|270=99.64|423=9|55=[N/A]|48=GB00BMBL1G81|22=4|30=XLON|15=GBP|1907=1|1903=TVTIC-000005|1906=5|768=2|769=20260107-</td><td></td><td>Valid 35=X message and field combination.</td></tr>
</table>

<table>
<tr><td></td><td>08:00:00.100000|770=1|771=C|769=20260107-08:00:00.300000|770=11|771=C</td><td></td><td></td></tr>
</table>

26. Appendix F - Industry Production Readiness Period

In advance of initial operational launch, the CTP intends to conduct a time-limited industry production readiness period, designed to support collective preparedness across Contributors and, where appropriate, a representative subset of Users. This period is intended to validate end-to-end operational readiness, including failure handling, recovery behaviour, notification processes, and coordination between the CTP and market participants.

During the production readiness period, the CTP may coordinate a small number of planned, non-disruptive resilience and communications exercises, focused on severe but plausible scenarios such as temporary service degradation, contribution interruption, or controlled failover. Participation by Contributors is expected, with the emphasis on observation, coordination, and learning rather than enforcement. Outcomes will be used to inform final operational procedures, communications playbooks, and readiness for live operation, and are not intended to be punitive.

The scope, scenarios, and participation model for the industry production readiness period will be informed and shaped through the CTP Consultative Committee. Over the coming months, the Committee will be invited to advise on the focus areas for readiness testing, taking into account market feedback, implementation timelines, and proportionality. This approach is intended to ensure that readiness activities are targeted, practical, and aligned with the needs of both Contributors and Users, while remaining consistent with the CTP’s regulatory and operational objectives.