

Best Practice Recommendations on Market Data Service Levels, Response Times and Communication Procedures

Synopsis	This document outlines Best Practice Recommendations Guidelines endorsed by the FISD and its member committee.
Authors	A consortium of FISD member firms
Version	3.0
Date	11 October 2012
Filename	TBD
Approved	Nick Merritt – SIIA/FISD

1. DOCUMENT HISTORY

Date	Changes	Version
28 th June 2004	First Draft Issued	v0.1 Initial Draft
23 rd July 2004	Incorporates first feedback from Direct recipients	v0.2 Draft
28 th July 2004	Comments added following meeting on the 26 th July 2004	v0.3 Draft
10 th August 2004	Comments added by section leads	v0.4 Draft
23 rd August 2004	Comments addressed and redundancies eliminated.	V0.5 Draft
27 th August 2004	Additional comments from telecom added and ready for group discussion.	V0.6 Draft
9 September 2004	Final revisions as per BPR telecom.	V0.7 Draft
16 February 2005	Revised for Feedback from various Exchanges.	V1.0 Issue
21 August 2007	First Draft for Updated Version	V1.1 Initial Draft
25 October 2007	Second Draft for Updated Version	V1.2 Second Draft
15 November 2007	Third Draft for Updated Version	V1.3 Third Draft
3 December 2007	Final Version for Updated Version	V2.0 Issue
25 July 2009	Updated Version reflecting synchronization of terminology for Version 2.0 and 'FISD Glossary of Terms.'	V2.1 Issue
11 October 2012	Updated Version reflecting changes to Capacity Section 8.3 and Section 10 – Managing Exchange Drive	V3.0 Issue

2. TABLE OF CONTENTS

1. Document History	2
2. Table of Contents and Executive Summary	
3. Best Practice Recommendation on Information Provider Service Levels	8
4. Definitions	10
4.1. Level Playing Field	11
4.2. Major Change	11
4.3. Minor Change	11
4.4. Exceptional Change	11
5. Scheduled Interruptions and change management	13
5.1. Planned Changes	13
5.1.1. Notification Requirements	13
5.1.2. Reminder Communications	13
5.2. Change Management	13
5.2.1. E-Mail Distribution List	13
5.2.2. Web Site Posting	13
5.2.3. Documentation Versioning	13
5.2.4. Source Notification in English	13
5.2.5. Official Communications	13
5.3. Documentation	14
5.3.1. Data feed specification	14
5.3.2. Implementation plan	14
5.3.3. Test schedule and plan	14
5.4. Recipient Testing	14
5.4.1. Testing Availability	14
5.4.2. Test Feed	14
5.4.3. Test Data Format	14
5.4.4. Test Documentation	14
5.4.5. Testing Schedule Changes	14
5.5. Change Implementation	15
5.5.1. Fallback Compatibility	Error! Bookmark not defined.
5.5.2. Implementation Cutover	15
5.5.3. Fallback Schedule	15
5.6. Ongoing Services	16
5.6.1. Two Data Feeds for Production	16
5.6.2. One Data Feed for Disaster Recovery	16
6. Unplanned Interruptions	16
6.1. Initial Notice	17
6.1.1. Immediate Notification	17
6.1.2. Communications Systems or Equipment	17
6.1.3. Dedicated Resource for Communication	17
6.1.4. Notification Procedure	17

6.1.5.	Restoration Projection	17
6.2.	<i>Periodic Follow-up</i>	17
6.2.1.	Notification	17
6.2.2.	Restart Requirements.....	17
6.3.	<i>Service Restoration</i>	18
6.3.1.	Notification	18
6.3.2.	Retransmission of Data	18
6.4.	<i>Problem and Resolution Description</i>	18
6.4.1.	Preliminary Description	18
6.4.2.	Under Investigation.....	18
6.4.3.	Final Description	18
7.	<i>Notification Periods – General Activities</i>	18
7.1.	<i>Annual Schedule</i>	18
7.2.	<i>Market Coverage</i>	18
7.3.	<i>New Listings</i>	18
7.4.	<i>Non Regular Changes</i>	19
8.	<i>System Considerations</i>	19
8.1.	<i>Hours of Service</i>	19
8.1.1.	Core Hours Designation	19
8.2.	<i>Capacity Management</i>	19
8.2.1.	All Service Types	19
8.2.2.	Fully Managed Service	21
8.2.3.	API Based Service	21
8.2.4.	Institution Provided Hardware.....	21
8.3.	<i>System Reliability</i>	21
8.3.1.	All Services	21
8.3.2.	Fully Managed Service	22
8.3.3.	Institution Provided Hardware.....	22
8.4.	<i>Data Quality</i>	22
8.4.1.	Data Accuracy	22
8.4.2.	Corrections	22
8.4.3.	Manual Verification	22
8.4.4.	Numeric Values	23
8.4.5.	Threshold checking	23
8.4.6.	Data Quality Investigations and Root Cause Analysis.....	23
8.5.	<i>Network Latency</i>	23
8.5.1.	Latency Definition	23
8.5.2.	Latency Standards.....	23
8.5.3.	Latency Monitoring and Reporting.....	23
8.6.	<i>Business Continuity and Testing</i>	23
8.6.1.	BCP Communication	23
8.6.2.	BCP Communication with Clients.....	24
8.7.	<i>Data Backup</i>	24
8.7.1.	Record Keeping	24
8.8.	<i>Data Recovery</i>	24
8.8.1.	Contiguous and Sequential Numbers.....	24
8.8.2.	System Communication.....	24
8.8.3.	Data Retransmission	25
9.	<i>Administrative and Policy Changes</i> _ <i>Error! Bookmark not defined.</i>	

9.1.	<i>Changes in Pricing</i>	
9.2.	<i>Changes in Audit Notification</i>	
9.3.	<i>Changes in Billing and Invoicing</i>	24

10. Conclusions and Next Steps _____ *Error! Bookmark not defined.*

<i>Examples of Best Practice</i>	27
--	----

Executive Summary

<i>Subject:</i>	<i>Topic</i>	<i>Synopsis of Recommendation</i>	
<i>Changes</i>			
	<i>Major</i>	<i>At least 120 days notice prior to implementation</i>	
	<i>Minor</i>	<i>At least 60 days notice prior to implementation</i>	
	<i>Exceptional</i>	<i>Significant discussion and interaction necessary (more than 120 days notice is needed)</i>	
<i>Communication</i>	<i>Notification</i>	<i>Annual Calendar of trading days provided no later than Nov 1 of preceding year</i>	
	<i>Distribution</i>	<i>Preferred medium is e-mail</i>	
	<i>Web site</i>	<i>Supporting documentation and schedules posted on Information Provider's website.</i>	
<i>Recipient Testing</i>	<i>Availability</i>	<i>Provided to recipient at least 30 days before minor change and at least 90 days before major change</i>	
<i>Change Implementation</i>	<i>Fallback Capability</i>	<i>All major changes should ensure fallback capability. Minor changes do not warrant a fallback period.</i>	
	<i>Parallel Implementation</i>	<i>Direct recipients should be provided with a "time window" to cutover to new services</i>	
	<i>Implementation Cutover</i>	<i>Data providers should avoid "big bang" implementations</i>	
	<i>"Go/No-go"</i>	<i>"Go/No-Go" announcement should be made at least 2 weeks before announced start date. Any postponement of announced start date should still provide at least two weeks of advance notice for rescheduled start date.</i>	
	<i>Backward Compatibility</i>	<i>Data Providers implementation should facilitate backward compatibility so Vendors can deploy new systems prior to providers implementation.</i>	
<i>Ongoing Services</i>	<i>Dual Feeds</i>	<i>Information Provider should provide a minimum of two copies of any data feed.</i>	
<i>Unplanned Interruptions</i>	<i>Immediate Notification</i>	<i>Notification should be immediate and provide outline of problem and estimated resolution time. Timeliness should trump completeness when forced with such a decision.</i>	
	<i>Status update</i>	<i>Information Provider should provide periodic status updates which include estimate of resolution timeframe.</i>	
	<i>Restoration</i>	<i>Notification should indicate if restoration</i>	

		<i>is full or partial and provide times of when the incident began and when it was resolved.</i>	
	<i>Retransmission</i>	<i>Information Provider should be capable of retransmitting data to fill in gaps when messages are missed.</i>	
	<i>Follow up</i>	<i>Information Provider should provide written explanations of major problems and their resolution and any changes implemented to prevent a recurrence.</i>	
<i>Notification Periods</i>	<i>Market Coverage</i>	<i>Changes (adds/deletions/modifications of issues or instruments) should be provided at least two business days prior to first trading day.</i>	
	<i>New Listings</i>	<i>Provided at least ten business days prior to effective date.</i>	
	<i>Non-Regular Changes</i>	<i>Provided at least 48-72 hours before the effective date.</i>	
<i>System Considerations</i>	<i>Core Hours</i>	<i>Information Provider defines the core hours of continuous service. This includes a safety zone of at least one hour before the start and one hour after the end of data</i>	
	<i>Capacity Management</i>	<i>Average message rates should be calculated and published on a frequent basis. Both bytes/sec and messages/sec are important.</i>	
	<i>Reliability</i>	<i>99.98% uptime is minimum standard</i>	
	<i>Quality</i>	<i>99.9% data accuracy is minimum standard</i>	
	<i>Latency</i>	<i>No more than 200ms latency over 99.98% of trading day</i>	
	<i>Data Backup</i>	<i>All data kept over a period of 30 days</i>	

3. BEST PRACTICE RECOMMENDATION ON INFORMATION PROVIDER SERVICE LEVELS

The global market data industry is dynamic, complex and interrelated. New financial instruments are continually being developed and introduced. The volume of quotes and transactions continue to grow, and there is increasing competition for trading, execution and post-trade processing applications. Real-time market data distribution and efficient trade execution require a high level of consistent and predictable service – all of which are dependent on the close cooperation of many independent organizations and systems.

One of the prerequisites associated with providing exemplary levels of service is adequate notice and open communication between all participants. Market data passes through dozens of different systems and networks on its way to the end user. Failure of these systems, as well as routine enhancements and ongoing adjustments associated with required maintenance, often requires procedural or technical changes that must be carefully designed, developed and tested. For these changes, adequate notification periods provided by Exchanges or other information source providers to direct market data recipients and downstream user firms are essential.

Early assessment of the impact of changes through the various distribution channels is the hallmark of successful service management. In other words, the impact of change (and the lead time required to implement it) will typically vary from Vendor to Vendor and subscriber to subscriber as well as between primary and secondary sources. Thus, a dialogue between an information provider, its direct recipients, subscribers and systems integrators is crucial.

This Best Practice Recommendation (“BPR”) is an initiative sponsored by the Financial Information Services Division (FISD) of the Software & Information Industry Association (SIIA), whose members include leading participants in all segments of the global market data industry, to improve levels of service in the Market Data Industry. The BPR identifies areas of service and communication that should be addressed by all parties involved to achieve improved levels of performance benefiting the whole industry. We have organized the BPR into five core categories including:

- **Scheduled Interruptions and Change Management:** Processes and recommendations for testing, maintenance and new releases including the need for complete release schedules, adequate documentation and reliable test data.
- **Unplanned Interruptions:** Recommendations on notification processes, communications goals, escalation procedures and response targets/timeframes for unplanned service disruptions.
- **Notification Periods for General Activities:** Recommendations on notification periods including communication, timescales, and lead times as defined by FISD for those activities not covered in previous sections.
- **Systems Considerations and Data Recovery:** Recommendations on performance expectations related to capacity management, systems reliability, network latency, business continuity planning, backup data and recovery.
- **Administrative and Policy Changes:** Recommendations for changes in pricing, audit notification and changes in billing and invoicing.

The goal of this document is to create a clear and detailed framework on minimum standards/benchmarks for service level response time and escalation procedures to serve as a non-binding best practice for industry wide reference and adoption. The members of FISD believe that the adoption of the core principles contained herein will benefit the whole financial industry by strengthening the lines of communication between Exchanges, Third Party Information Providers, Direct recipients and End-Users which will in turn greatly reduce delays, misinformation and customer confusion in the event of major interruptions, feed changes or system outages. When adopted by market participants, the FISD will communicate to the financial industry that those participants have met or exceeded the identified requirements.

This document is owned by FISD – both in terms of IP (Intellectual Property) and in terms of future amendment. In order to ensure continued relevance, this document will be reviewed by the Service Level and Communications

Working Group on an annual basis. Substantive changes or modifications to the existing document require approval of FISD Executive Committee.

4. DEFINITIONS

This document was prepared by the Financial Information Services Division (FISD) of the Software & Information Industry Association and various leading market participants in the market data industry in an effort to help the industry identify and implement Best Practices to better plan and control changes affecting market data distribution to ensure sufficient elapsed time for changes to be effected accurately and efficiently. The FISD document "Lead Time Notification: Guidelines and Best Practice Recommendations for Successful Change Management" which can be found via the following URL was used as the basis for this document.

http://www.fisd.net/mdadmin/notfp_leadtime.asp

Term	Definition
Backward Compatibility	Change to data delivery system that allows Vendors and consumers to successfully employ new systems for receipt before data sources initiate new deliveries.
Content	The data and information normally delivered to recipients under the service contract and described in the Information Provider's data feed specification.
Core Hours	Designated hours of service for the data feed during which there will be no anticipated interruptions. Core hours should include one hour before the start and one hour after data broadcast times.
Data Recovery	Ability to identify missing messages and recover the lost information.
Direct recipients	All recipients of the data whether they are Third Party, direct feed recipient or end users.
Fallback Capability	Change to data delivery system that allows data source to utilize a previous version of the product in event of problems with a new implementation.
Fully Managed Service	The source providing, maintaining and remaining responsible for all technology between the point of data collection within the institution itself through to the point of presentation within a direct recipient's data centre.
Hot Cut Implementation	Change to data delivery system or process without a parallel implementation. This implementation is frequently referred to as a "Big Bang Implementation" and typically occurs without any "phase-in" aspect(s).
Information Provider	Any organization that creates and/or disseminates Information that can be redistributed. Examples include, but are not limited to, exchanges, news wires, analysis services and credit rating agencies.
Major Change	See section 4.2 for examples/illustrations.
Minor Change	See section 4.3 for examples/illustrations.
Normal Operations	The hours of operation detailed in the daily message schedule for the Information Provider's data feed.
Parallel Implementation	Simultaneous dual streams of delivery – the legacy and new versions of the product - that allow consumers to determine the timing of the change.
Scheduled interruptions	A planned change to normal service, this covers changes to normal operating schedules and procedures.
Systems considerations	The considerations which need to be provided by the Information Provider when a source implements a technological solution to the problem of distributing data to its recipients. This is needed to ensure the proper

	design, development and management of the solution.
Third Party Providers	Non-Exchange supplier of financial information. (e.g. Broker Feed)
Unplanned interruptions	Any interruption to or degradation of a supplier's service that would cause the loss of messages; stoppage or delay of updates; corruption of message formats or errors in content during normal operations.

4.1. Level Playing Field

If an Information Provider chooses to offer different levels of service to direct recipients, then all direct recipients should be made aware of the existence of these levels of service, and given the opportunity to purchase them. Where multiple direct recipients hold contracts for identical levels of service from a Information Provider, that Information Provider should ensure that those direct recipients receive consistent treatment including, but not limited to, levels of support & communication with the institution, timing and timeliness of data distribution, system reliability, data quality and provision for data backup and recovery.

4.2 Changes

Information Providers should be proactive in early consultation with downstream Vendor and consumer communities before finalizing plans for change.

4.2.1 Major Change

Information Providers should provide data recipients with at least 120 days notice prior to introduction of major changes. The following are examples of major changes. This does not necessarily represent an exhaustive list but should be used as a starting point for identification.

- Changes to technical specifications related to network protocols or application level protocols, feed format, migration to a new feed or data files formats.
- Changes to feed message structures, addition of new messages, or changes to the use and interpretation of existing messages, where these changes must be implemented by the direct recipient to avoid a loss or degradation of service.
- A change to the communications infrastructure required to support an exchange or Information Provider feed. This may include any changes which require provisioning of new communication lines, bandwidth or any network devices (e.g. Routers).
- Addition of, or changes to, multiple fields in one or more message types.
- Addition of new data types (even if within existing data formats).
- Minor changes to symbology (e.g., changes to instruments that do not trade electronically like Nasdaq MFQS)
- Changes to exchange or regulatory display requirements (e.g., mandatory display of certain fields or screen lay-outs)

4.2.2 Minor Change

Information Providers should provide data recipients with at least 60 days notice prior to introduction of minor changes. The following are examples of minor changes. Again, this does not necessarily represent an exhaustive list but should be used as a starting point for identification.

- Addition or change to a single field for a single message.
- Addition of new data items where other data items of the same type exist.
- Changes to the daily or weekly schedules e.g. open and close times, market periods and phases, out of hours trading, availability of instrument and symbol lists.

4.2.3 Exceptional Change

These represent large scale changes which typically require the greatest advance downstream notification (i.e. greater than 120 days). Changes of this magnitude should involve significant discussion and interaction between the parties involved and details should be agreed upon between Information Providers and direct recipients. Data sources should

provide complete details to their customers regarding the planned changes. Data sources should also provide adequate venues and forums for customers to express feedback, concerns and questions, and be open to subsequent amendment to their implementation plans based on feedback. It is critical that data sources work closely with direct recipients to ensure there is broad industry agreement on the feasibility of an Information Provider's targeted implementation date.

Examples of such are:

- Implementation of a new feed
- Industry-wide change (e.g. EURO)
- Major symbology changes (e.g., significant increase of symbol size, inclusion of full equity symbol in an options symbol, inclusion of special characters in symbol)

Unspecified changes should default to contractual specified terms as per service level agreements.

5. SCHEDULED INTERRUPTIONS AND CHANGE MANAGEMENT

A scheduled interruption is a planned change to normal service (e.g. due to essential maintenance the service on 5th November will not be available, etc.). Change management refers to the processes and procedures which control modifications to a service.

This section encompasses all planned changes to normal operating schedules and procedures and describes recommendations for the minimum appropriate requirements associated with the management of those changes.

5.1. Planned Changes

5.1.1. Notification Requirements

The Information Provider should provide all direct feed recipients with a calendar of trading days, established holidays, and all Scheduled Interruptions or Events – covering major and minor infrastructure or feed changes, and new data and service releases (The Calendar) that are known for the following year. The Calendar should be released no later than November 1st of the previous calendar year with updated versions sent out as required to provide appropriate advance notification as per FISD industry recommended standards (i.e. 60 days for a minor change and 120 days for a major change) for all additional or altered Scheduled Events.

5.1.2. Reminder Communications

Any change in service availability due to circumstances described above in the Calendar should be followed up with a reminder communication to the direct recipient at least 5 business days prior to the effective date.

5.2. Change Management

5.2.1. E-Mail Distribution List

To facilitate efficient implementation of scheduled interruptions and ongoing maintenance, the Information Provider should send notification and supporting documentation via e-mail to an established and up-to-date distribution list supplied by the direct recipient. In addition, the data recipient should be provided with an updated list of situationally relevant escalation contacts from the Information Provider. The Information Provider **and direct recipient** should verify distribution list contacts on a quarterly basis and provide appropriate contact information for recipient initiated contact changes.

5.2.2. Web Site Posting

All supporting documentation and complete schedules should be posted on the Information Provider's web-site.

5.2.3. Documentation Versioning

All supplied documentation should be clear and concise and contain version control identifiers and document history. All documents should additionally have a section summarizing all changes from the previous version **at the beginning of the document**. Changes within the body of the document should be easily identifiable. All changes to documentation should be communicated using the established communication procedures. **Previous versions of documentation also need to be made available if requested.**

5.2.4. Source Notification in English

All technical specifications and change management notification documentation should be provided in English as well as the appropriate local language.

5.2.5. Official Communications

All official communications should be sent electronically as described in Section 5.1.1 above, except where contracts specifically state otherwise, and made available in hard copy if requested by direct recipients.

5.3. Documentation

In all cases of scheduled changes identified in The Calendar, the Information Provider should provide full and final documentation as described in the sections below in conjunction with official notifications as per FISD industry recommended standards (i.e. 60 days for a minor change and 120 days for a major change). Documentation should include:

5.3.1. Data feed specification

This should include communication protocol information, application level protocol and data format details, glossary, well defined code tables, trading hours, timeline of when the messages are sent and connectivity requirements for the direct recipient.

5.3.2. Implementation plan

This should entail a high-level plan for rollout of changes. This should include timelines for feed connectivity, testing, parallel running and live switchover. In addition, the Information Provider should provide contact phone numbers of Information Provider staff involved in the implementation as well as schedule periodic conference calls to invite questions and provide feedback.

5.3.3. Test schedule and plan

This should include details of any conformance testing required by the Information Provider, capacity and loading tests, a day in the trading life of the Information Provider, any weekly, monthly, quarterly activities such as contract rollovers and test scenarios which cover market events or Information Provider system events.

5.4. Recipient Testing

5.4.1. Testing Availability

Test facilities for planned changes should be provided to the direct recipient as a minimum 30 days before a minor change and 90 days before a major change, including changes to original specifications.

5.4.2. Test Feed

For data feed changes the Information Provider should provide a feed to be used for test purposes by the direct recipient. The feed should be an exact replication of the new data feed with the same characteristics (i.e. content, message ordering, data rates) as the old live feed. The test feed should be made available as a permanent service and provide full redundancy. If this is not feasible then test data/scripts are required at least 30 days prior to production/hot cut. Direct feed recipients prefer parallel test periods to be set up for approximately 30 days to facilitate real time testing.

5.4.3. Test Data Format

Test data should be provided in the form of a file or set of files. Full coverage of message types, market and system events should be covered, (e.g. open, close, market period transitions (auctions), market suspension, resets and heartbeats). Test data should be fully supported by the Information Provider staff, and file(s) should be accompanied by contact names and phone numbers for assistance in the event of operational problems.

5.4.4. Test Documentation

Tests should be documented with a reference to the test data, file, or scripts that have been pre-tested and are used to subsequently validate the test results.

5.4.5. Testing Schedule Changes

Any subsequent changes to the issued feed specification or problems found with the feed during direct recipient testing will require the Information Provider to revise their live date or extend their parallel run period. Revised dates should be communicated with direct recipients via official notifications ASAP.

5.4.6 API Based Service

It is generally recommended that an Application Programming Interface (API) based service NOT be used. Those Information Providers that do utilize API should know that test quality is very important in these situations and therefore a high quality test environment is required.

5.5. Change Implementation

5.5.1. Parallel Implementation

Whenever practical, and especially for major and exceptional changes, direct recipients should be provided with a 'time window' to cutover to new or upgraded services. That is, the legacy and revised versions of the product should be made available for parallel access by recipients to test and cutover to the new product. For minor changes this parallel period should be a minimum of 7 days, for major changes it should be a minimum of 30 days. It is understood that in order to subscribe to both versions, recipients may need additional bandwidth during the overlap period.

5.5.2. Fallback Capability

If a parallel implementation is not feasible, it is preferable that Information Providers provide fallback capability for all changes. **This means that a data source can fall back to a previous version of the product in event of problems.** The Information Provider should provide notice of fallback with as much lead time as possible of changes regardless of type (major, minor or day to day listing maintenance) to all direct recipients. The Information Provider should consult with all key direct recipients to ensure the desirability and feasibility of a fallback, and notify ALL direct recipients of the fallback's status including availability, use, and discontinuation (if used).

5.5.3. Implementation Cutover

The data source should especially avoid a "Hot Cut" implementation if they cannot provide fallback capability. "Hot Cut" denotes cutting over to a new version of a feed with no parallel implementation.

5.5.4. Go/No-go Announcement

Regardless of the notification period, the data sources should publish a "Go/No-Go" statement regarding the proposed implementation date at least two (2) weeks prior to the proposed date. That is, at least two (2) weeks before the proposed implementation date the data source will either:

- a) indicate it has **any and all regulatory requirement approvals in hand** and remains **highly confident** that the change will be implemented on the previously announced date; OR
- b) it will provide notification that the change is postponed and also announce a new date of implementation that provides at least two (2) weeks of notice from the time of announcing the date of change and the date of change itself, OR
- c) it will announce that the proposed change has been cancelled with no expected implementation for the foreseeable future.

This advance notice will allow the Vendors to ensure that the correct systems are in place and notify clients with enough lead time that they can take (or avoid taking) actions to prepare for the new behavior.

If the Information Provider issues a postponement for implementation and it is unable to provide a rescheduled date at that time, it should still provide a two week notice for the rescheduled implementation date when it is announced.

5.5.5. Backward Compatibility

It is strongly recommended that a Information Provider's implementation of product changes facilitate backward compatibility so that Vendors can deploy their new systems prior to the Information Provider's implementation with the only consequence being the non-receipt of new data which is not yet being provided. For instance, adding new fields or message types can be implemented by downstream applications in a backward-compatible way. Conversely, changing the basic encoding or interpretation of existing message types is not backward-compatible.

5.6. Ongoing Services

5.6.1. Two Data Feeds for Production

The Information Provider should provide a minimum of two copies of any data feed they supply to the direct recipient. Two copies allow the direct recipient to implement a resilient solution. The feeds should be provided via different access points within the Information Provider distribution infrastructure and should be independent of each other to ensure that there will be no single point of failure, enabling full redundancy.

5.6.2. One Data Feed for Disaster Recovery

The Information Provider should provide the direct recipients a minimum of one data feed line for business continuity and disaster recovery purposes. It is acceptable that this line only broadcasts in disaster recovery situations, and as such should not represent an additional charge by the Information Provider unless utilized.

6. UNPLANNED INTERRUPTIONS

The best practice recommendation on unplanned service interruptions covers any interruption to or degradation of a Information Provider's delivery stream that would cause the loss of messages; stoppage or delay of updates; corruption of message formats or errors in content during normal operations. Content is defined as the data and information normally delivered to recipients under the service contract and described in the Information Provider's data feed specification. Normal operations are defined as the hours of operation detailed in the daily message schedule for the Information Provider's data feed.

The members of FISD believe that market data Information Providers have sufficient incentive in their business continuity goals to ensure they will do all they can to quickly restore service following an unplanned outage. However, they may be so focused on that objective that they neglect to notify direct and indirect customers of the incident. As such, these recommendations are limited to issues related to notification schedules/communication processes and include the following elements:

- Initial notice of problem including what is affected and an estimate for restoring service.
- The requirement for contact names, numbers, points for escalation, and an open conference line that direct recipients can dial into wherever possible (**active only during actual events, not continuously**).
- **Periodic follow-up until the problem is resolved**
- Notice when service has been restored
- Preliminary and final description of the problem and how/when it will be/was fixed, also providing a full root cause analysis.

Note that it is expected for all these elements that the elements of communication and notification outlined in this section are preserved even in event of a disaster recovery situation. **Exchanges should maintain and update a database of emergency contacts at direct data recipients – distinct from database of contacts for system change announcements.**

6.1. Initial Notice

6.1.1. Immediate Notification

The Information Provider should immediately (simultaneously with notice to internal personnel responsible for restoring service) notify direct recipients of any unplanned interruption to service. Initial notice should describe the problem, outline what content is affected and describe which systems are affected (particularly if the Information Provider provides multiple feeds or services). Information Providers should provide estimated resolution times and provide customer statements to direct recipients (who can in turn pass on to their customers) for all outages. Timeliness of notification should supersede completeness of information when Information Providers are faced with such a trade off.

6.1.2. Communications Systems or Equipment

If the outage is the result of a communications problem, the Information Provider should provide details of the entity responsible for fixing the problem (i.e. the communications vendor, the IT department at the Information Provider or recipient) and describe whether a restart of downstream devices or restart of an IP session is required.

6.1.3. Dedicated Resource for Communication

A dedicated point of contact at each Information Provider should be designated on every shift within core hours to initiate notices to recipients and respond to any necessary inquiries from direct recipients. This person should not also be responsible for recovery of the service to ensure that there is no conflict with the requirement for customer notification and support.

6.1.4. Notification Procedure

While notice should be via **the appropriate** electronic mechanisms including telephone, e-mail, web site, beeper (etc), notice via logically formatted messages in the data feed is the recommended method if the service itself is still capable.

6.1.5. Restoration Projection

Notice (or reasonable projection) of when service will be restored is needed as soon as possible. If this is not possible then the next projected status update time should be provided.

6.2. Periodic Follow-up

6.2.1. Notification

For longer outages, the Information Provider should provide periodic status updates indicating progress toward resolution and an estimate of the resolution timeframe. The frequency of these updates should be provided based on the estimated resolution times as per the following schedule:

Estimated Resolution Times	Frequency of Updates
< 3 hours	Every 30 minutes or less
3 to 24 hours	Every hour
24+ hours	Daily updates

6.2.2. Restart Requirements

If resolution also requires recipients to restart a system or an IP session, it must be communicated to direct recipients.

6.3. Service Restoration

6.3.1. Notification

The Information Provider should provide notice that the service has been restored as soon as possible. The notice should indicate whether restoration is partial or full. It should also distinguish any data elements that remain corrupted from the universe that is accurate and reliable for client use. The notice should provide updated or corrected times of when the incident began and when it was resolved.

6.3.2. Retransmission of Data

The Information Provider should be capable of retransmitting data to fill in gaps when messages are missed or to restore service after an outage. [See section 8.9 for a more complete treatment of this topic.]

6.4. Problem and Resolution Description

6.4.1. Preliminary Description

Within an hour of the resolution of the problem, the Information Provider should provide a written preliminary post mortem on the incident describing the cause of the problem and the fix. If the fix is a temporary work-around with a permanent fix to come, this should be explained and dates should be provided for the final resolution.

6.4.2. Under Investigation

If the matter is still under investigation, this should be explained and further updates should be provided to fill in missing details.

6.4.3. Final Description

Many end-users require market data Vendors to provide written explanations of major problems and their resolution. Within 24 hours of the preliminary problem description, Information Providers should provide a final, written description setting out the root cause of the problem, the permanent fix and any other steps, such as procedural, communications, hardware or software changes that have been or will be implemented to prevent a recurrence.

7. NOTIFICATION PERIODS – GENERAL ACTIVITIES

7.1. Annual Schedule

The Information Provider should inform the direct feed recipient of the trading calendar for the next year, including trading/exchange holiday dates as part of The Calendar described in section 5.1.1 above. Direct recipients should be notified of any unscheduled holidays at least one day in advance (if at all possible) via direct e-mail distribution and website posting.

7.2. Market Coverage

The Information Provider should provide notification of, and necessary details for, routine changes to market coverage (add/modifications/deletions) at least two business days (48 to 72 hours) prior to first trading day. Electronic bulletins should provide details of the changes, including the reason for, and importance of, the change and its impact on the direct recipients as required.

7.3. New Listings

For major new listings, new symbols additions and distribution messages provided by the Information Provider (e.g. proposed Blue Chips, top tier, indices, options etc.); the Information Provider should provide advanced notification at

least 10 business days prior to the effective date. This should include all data elements required to provide precise and unique identification the minimum of which are:

- Ticker Symbol
- ISIN (or national number such as CUSIP or SEDOL) – **this assumes that the contractual and commercial situation allows for dissemination**
- Place of Official Listing
- Place of Trade

7.4. Non Regular Changes

For non-regular corporate actions (mergers, delisting, splits, rights issue, and bonus issue) and changes in contract details of derivatives, advance notifications at least 48 hours to 72 hours before the effective date. The necessary details for non-regular corporate actions should follow ISO 15022 standards (<http://www.iso15022.org/>). For changes in contract details of derivatives, the minimum field requirement is the SIC (Symbol Identification Code) as well as the actual field change(s).

8. SYSTEM CONSIDERATIONS

When an Information Provider implements any technological solution to its data distribution system, there are a number of considerations which need to be taken into account in the design, development and management of the solution. This section outlines these recommended system considerations and appropriate best practices.

8.1. Hours of Service

8.1.1. Core Hours Designation

The Information Provider should define the core hours of continuous service for the data-feed, during which there will be no anticipated interruptions to the service, other than those identified in The Calendar.

The definition of these core hours should provide a safety zone at least one hour before the start and one hour after the end of data being broadcast on the feed. It is expected that only “heartbeat” messages will be transmitted and that no test messages would be received during this time.

8.2. API Format

It is generally recommended that Information Providers not utilize an Application Processing Interface (API) service format.

8.3. Capacity Management

8.3.1. All Service Types

Analysis and Communication

The Working Group notes that communications related to message rates and ‘output’ probably would vary depending upon the size of the Information Provider (or at least dependent upon the magnitude of output by the Provider). The possibility exists that suggested recommendations on communicating capacity issues might vary depending upon these differences in size.

Information Providers should perform regular analysis of the data levels on their feeds.

It is critical that Information Providers provide at least the following information to direct recipients on a monthly basis:

- Peak **message rates** usage across the entire trading day, for each trading session, and per second during the core hours.
- Peak number of bytes per second across the entire trading day, for each trading session, and per second during the core hours.

8.3.2 Fully Managed Services

Although not critical, it is helpful for Information Providers to provide the following information to direct recipients on a monthly basis:

- Message rate highs occurring in any single millisecond, 10 millisecond, 25 millisecond, 50 millisecond, 100 millisecond timeframe across the entire trading day, for each trading session, and distinctly for pre and post market hours.
- Message rate highs should be accompanied by timestamps and date of occurrence. Sub second highs should be accompanied by the message per second rate that occurred across the whole second in which that subsecond high occurred..
- The open and closing time of actual market activity should be provided.

Historical statistics going back at least two calendar years for the categories identified above should be made available to direct recipients via a web site in so that recipients can download the data into Excel form and carry out their own data modelling and analysis.

Forecast vs. Actual

Each Information Provider should provide capacity forecasts of growth in message traffic for 6m and 12m future periods including some narrative on why rates are expected to change (normal growth, new products, different quote methods, smaller trading lots, etc.). This forecast should be issued monthly to ensure a continuous 12 month rolling schedule of predicted data rates.

In addition, each Information Provider should provide forensic 'Forecast vs. Actual' reports following each period with some explanation for any significant variance from forecast.

New Product Forecast

Data sources should provide traffic estimates for new products.

Maximum Bandwidth

Information Providers should provide figures for maximum bandwidth and message rates that could be transmitted during exceptional circumstances of high activity.

Maximum Output

Information Providers should provide figures for maximum output of messages over the course of the day.

Capping and Throttling

If an Information Provider has any intention or plan to cap or throttle bandwidth and/or message rates, details of how and under what circumstances this capping or throttling would be effected (e.g. delaying of data or filtering of data) should be provided to the data recipients.

Both the capacity of the Vendor and its downstream end-users should be considered by the content provider when making changes. Frequently this requires market providers to initiate early consultation with downstream Vendors and consumers prior to finalizing plans for changes. Members of the Working Group recognize that not all upgrades and other changes to the Network are equal. Some changes are minor and other changes are major. Information Providers should strive to provide ample notification to downstream customers and vendors regarding these changes. Some major changes require as much as 120 days of advance notification for proper planning and implementation.

8.3.2. Fully Managed Service

A fully managed service is defined as the Information Provider providing, maintaining and remaining responsible for all technology between the points of data collection within the institution itself through to the point of presentation within a direct recipients data centre.

Information Providers should ensure the bandwidth on any communications circuit for fully managed service is sufficient for maximum potential bandwidth requirements for current data rates and that upgrades to headroom associated with forecasted growth rates are planned and notification is provided in accordance with FISD industry recommended standards (i.e. 60 days for a minor change and 120 days for a major change) as appropriate.

8.3.3. API Based Service

The Information Provider should determine and quarterly re-evaluate the current minimum hardware specification on which software using that API should be run. Clients should be notified in accordance with FISD industry recommended standards (i.e. 60 days for a minor change and 120 days for a major change) for any required change as appropriate.

8.3.4. Institution Provided Hardware

If a Information Provider provides any additional hardware to execute software provided by the Information Provider or otherwise interact with their systems, then the Information Provider should quarterly re-evaluate the minimum specification for this hardware, notification of the need to upgrade or replace hardware should be in accordance with FISD industry recommended standards (i.e. 60 days for a minor change and 120 days for a major change) as appropriate.

8.4. System Reliability

8.4.1. All Services

Performance Uptime

The Information Provider should attempt to provide the client with an operational and correct feed during 100% of the core hours of service but a minimum of 99.98% of uptime is **recommended as a standard** in any rolling month.

Failure Management

The Information Provider should ensure that there is no single point of failure anywhere within their system between the point of data generation and the point of presentation to the direct recipient, this should include, but is not limited to:

- The use of multiple redundant systems (e.g. two or more independent, and geographically remote data centres) that should provide automatic fail-over such that the time taken to do so is reduced to a minimum, and direct recipients do not miss any data generated during this period.
- Any communications within the system should have multiple routes to their destination (on any WAN connections, these routes should be via confirmed distinct communications providers)

Feed Monitoring by Recipient

The Information Provider should ensure that the feed can be effectively monitored by the data recipient through their own software to identify if and when a problem has occurred on the feed including, but not limited to the following areas:

- **Heartbeat Messages:** In order to facilitate the detection of a "hung" data feed where physical connectivity is not lost, the data feed should supply heartbeat messages at regular, predefined intervals. These should be available prior to, during and after core hours to allow end consumers to verify full end-to-end connectivity and dataflow.
- **Message Timestamps:** In order to allow the detection of network issues or other system problems that may give rise to abnormal latency, it is recommended that all messages contain a message creation timestamp to millisecond granularity. This timestamp should be passed on, without modification, by any intermediate data-Vendors to end user data feed consumers.

8.4.2. Fully Managed Service

Maintenance

The Information Provider should execute performance checks on a monthly basis on any and all communications circuits for which they are responsible, including but not limited to the testing of latency and quality of signal.

Communications Redundancy

The Information Provider should ensure that all messages provided are duplicated and delivered by distinct communications providers via different routes.

8.4.3. Institution Provided Hardware

Hardware Management

If an Information Provider provides any additional hardware to execute software provided by the Information Provider or otherwise interact with their systems, then they should comply with the follow:

- The hardware must not constitute a single point of failure within the system as a whole (for example, there should not be one piece of hardware taking data from the two feeds).
- Provision should be made to enable a direct recipient to monitor this hardware, preferably using a standard monitoring technology.
- Such hardware should additionally be monitored remotely by the Information Provider.
- The Information Provider should be prepared to react to alerts and alarms, or otherwise provide support, preferably 24/7 but at a minimum during the core hours of service (Market hours plus 1 hour before open and 1 hour after close).

8.5. Data Quality

8.5.1. Data Accuracy

Data items transmitted on the feed should be a full and accurate representation of the activity within the Information Provider, a minimum of 99.9% of all data items transmitted by the system over the period of a rolling month should be correct at time of transmission.

8.5.2. Corrections

Corrections should be handled via the data feed on the day of error rather than requiring manual correction by the direct recipient, if the Information Provider is unable to provide correction on the same day this must be appropriately communicated to direct recipients along with the correct values to be applied. The process of correction provision should be designed to incorporate as little human intervention as possible on the part of the direct recipient.

8.5.3. Manual Verification

Any data entered manually into the system should go through a verification and correction process before release. Each Information Provider should be able to provide evidence of verification/validation as required.

8.5.4. Numeric Values

Numeric values should be transmitted to the maximum precision possible from the data generated within the system.

8.5.5. Threshold checking

Data from Information Providers should be threshold checked before dissemination to direct recipients to prevent spikes in intraday data from being passed downstream.

8.5.6. Data Quality Investigations and Root Cause Analysis

Each Information Provider should be responsible for the root cause analysis and subsequent resolution of any data quality issues identified by direct recipients through their data quality monitoring and analysis of Information Provider data. Each Information Provider should make available to direct recipients the contact names and numbers of those responsible for data quality and capable of addressing identified issues.

8.6. Network Latency

8.6.1. Latency Definition

End-to-end latency is defined as the period of time measured from the moment of electronic data generation within the Information Provider to the point of presentation to the customer; such as a router within the Information Provider (from which point the customer supplies their own circuitry) or a router within the customers data centre (where the institution is responsible for the circuits).

8.6.2. Latency Standards

Each Information Provider should ensure that data services provided to the direct recipient are as timely and accurate as possible but a minimum target of no more than 200 ms latency over 99.98% of the trading day is recommended.

8.6.3. Latency Monitoring and Reporting

A Information Provider should monitor and perform regular monthly reviews of the latency incurred within their systems, ensuring that any changes (planned or unplanned) are properly communicated and described as per FISD standards (i.e. 60 days for a minor change and 120 days for a major change). Additionally, an Information Provider should provide within the feed specification for data recipients the capability to monitor the latency of the feed.

Each Information Provider should provide, as required by direct recipients, monthly summary reporting of latency figures collected from their monitoring systems including average values, variation from previous months, and maximum latency times encountered during the month along with root cause analysis and action plans for any significant degradation.

8.7. Business Continuity and Testing

An Information Provider should be able to demonstrate that they have an effective disaster recovery strategy and are able to support their market data stream and direct recipients during a disaster Business Continuity situation. The disaster recovery plan should be reviewed, updated and tested whenever a major change is implemented. Under static conditions, Information Providers should perform annual testing of their disaster recovery plan.

8.7.1. BCP Communication

As any Disaster situation will arise as an Unplanned Outage, direct recipients should be informed of the situation and supported as per the guidelines in that section above. If the Information Provider switches to a BCP scenario, direct recipients should be informed that the Information Provider will be running in disaster recovery through an official communication, including a Customer Statement, sent to all appropriate distribution lists of recipient contacts as described in section 7.1.4 above.

Note that implementation of the plan should not require changes to hardware, software or configuration on the recipient site.

8.7.2. BCP Communication with Clients

Clients should be offered the opportunity to take part in a simulated disaster recovery exercise at regular intervals, providing feedback from which the institution can improve their plan.

8.8. Data Backup

8.8.1. Record Keeping

- Information Providers should keep an electronic record of all data messages transmitted over a period of at least 30 business days, to be made available to direct recipients (as outlined in section 8.9 below).
- Information Providers should maintain historical records of their data, that can be made available to direct recipients as requested (e.g. for the seeding of an historical price database or historical price auditing/confirmation). Where applicable, these historical records should stretch back 10 years.
- As with other systems, Information Providers should have more than one store of historical data records to ensure availability in the event of a disaster recovery situation.

8.9. Data Recovery

In order to provide complete and consistent data to consumers of market data, it is critical that each Information Provider provide a mechanism or means to direct recipients that will allow those who ingest the data feed to identify missing messages and recover any lost information. As the information loss may be caused by communications or hardware failure and may affect one or many processors, recovery of missing data must not interrupt the continued flow of real-time information to any recipient.

8.9.1. Contiguous and Sequential Numbers

Information Providers should provide a reliable and accurate method for the identification, requesting and processing of lost messages. The provision of a sequential and contiguous sequence number for each record disseminated within a clearly defined data stream has a number of advantages and is the best practice recommendation. A number of alternative methods are currently in use and described below, however these do not meet the requirements of direct recipients.

- *Restart Feed from Point of Loss*
While this method does allow for complete recovery of missing data, it has an adverse effect on the continued processing of real-time data. Effectively, downstream users will fall behind in real time processing until the feed catches up. In addition, where the processor is maintaining tick history, accumulated volume, high, low, last etc., it is necessary to rewind the accumulated data back to the restart point.
- *On Demand, or Cyclical Summary Messages*
For some applications, the ability to apply a source summary containing the latest view of the data ensures that the processor is now in line with the market. This method of recovery does not provide each missing tick, which is used by some intra-day and performance application, such as best execution analysis. This method also fails to address other data types, which may be included in a real-time stream (suspension information, new listings, and announcements) which do not normally form part of the summary information.

The use of a sequential and contiguous sequence number system allows data recipients to actively manage service gaps, and, in conjunction with a recovery mechanism at the source, explicitly recover lost messages. Additionally, the use of a sequential and contiguous sequence numbering, standard across all versions of the real-time stream has the additional benefit in that it allows arbitration between two or more streams of data from the same source, to produce one complete and correct stream.

8.9.2. System Communication

The data recipient must be able to communicate directly with the Information Provider and request missing messages these should then be resent either commingled with the live stream, or via a predetermined alternate communications link.

Such a system should be designed to minimise the need for human intervention.

8.9.3. Data Retransmission

The Information Provider should have in place a method to resend missed data to direct recipients (both retransmission to a single customer, or to all direct recipients should the need arise) upon request. The nature of the recovery method should form part of the specification document for the data feed, as such there should be a full definition of the format and test data should be available.

- For current data (data less than 24 hours old), this retransmission should begin as soon as retransmission is requested. A feed specification should contain provision for identifying this retransmission.
- Where data is historical, the institution should provide a method for direct recipients to access this data within 24 hours after the request has been received.

9. ADMINISTRATIVE AND POLICY CHANGES

9.1. Changes in Pricing

9.1.1. Major Change

Information Providers should provide data recipients with at least 120 days notice prior to introduction of major changes in pricing. The following are examples of major pricing changes:

- Significant increases to an existing fee
- Creation of new fee
- Fee change that will likely be “passed” to downstream customers.

9.1.2. Minor Change

Information Providers should provide data recipients with at least 60 days notice prior to introduction of minor changes in pricing. The following are examples of minor pricing changes:

- Increase to an existing fee that is typically not passed directly through to downstream customers (e.g., connection fees, application fees, etc.)

9.1.3. Exceptional Change

These changes represent fundamental modifications to the Data Provider’s fee structure(s) and should involve significant discussion and interaction between the parties involved.

- Changes to pricing metrics
- Changes that require significant operational or administrative changes for Vendors or their customers
- Introduction of a fee for a product or data set that was not previously fee-liable.

9.2. Audit Notification

Information Providers must reserve the right to audit at the minimum notice periods specified per contract, but best practice may require longer notice periods, to allow for effective audit planning and preparation.

Information Providers should only audit at short notice where there is reason to suspect non-compliance or by agreement between the parties. Adequate advance notice will be given for routine audits including verification of client site data feed controls and declarations. This may involve up to 90 days prior notice for complex audits involving both Vendor and client sites.

9.3. Changes in Billing and Invoicing

9.3.1. Major Change

Information Providers should provide data recipients with at least 120 days notice prior to introduction of major changes in billing and invoicing. The following are examples of major changes in this category:

- Significant change in payment delivery requirement
- Changes to file formats for electronic invoices

9.3.2. Minor Change

Information Providers should provide data recipients with at least 60 days notice prior to introduction of minor changes in pricing. The following are examples of minor changes in this category:

- Slight changes in layout of invoice
- Change in Payment address

10. BEST PRACTICES FOR END USERS

10.1 Best Practices for Managing Exchange Driven Changes (EDCs) Affecting Market Data Infrastructure

Since 1994, Clearnet has produced the Clearnet Calendar, a consolidated report of planned changes to market data feeds. It is used by large trading firms, market data vendors, and independent systems vendors to manage their market data systems and infrastructure.

As firms have worked with Clearnet, a number of best practices to manage notifications have emerged. These support the goal of eliminating “Severity 1” trading outages...the most serious...caused by a failure to respond adequately to an EDC.

10.1.1 Obtain Earliest Notice

Receive notices for planning and management at the earliest possible time. This means that you want to get them when released by the exchanges. The benefit is that the firm becomes proactive and can query internal support staff and external systems vendors as to their plans to handle the EDC, assuring a coordinated and timely response.

10.1.2 Compare Multiple Sources

Review two or more sources of EDC notifications. Compare one to the other to make sure nothing is missed or incorrectly tracked. The benefit is that looking for differences exposes potential mistakes in the firm’s development schedule.

10.1.3 Filter Notices

Screen out the noise and focus on just the exchanges and notices that affect your floor and systems. Reviewing hundreds of emails each week is mind-numbing and increases the risk of missing a notification. The benefit is that staff spends less time reviewing emailed notifications that are irrelevant.

10.1.4 Create a Master Calendar, Enterprise-wide

Maintain a master calendar showing all relevant notices and due dates by exchange and by date so that your staff sees the big picture of project implementation as well as the detail. More eyes reviewing the master schedule offers improved chances of catching anomalies or mistakes. Use the same format enterprise-wide. The benefit is collaboration and communication: there is a single management tool that guides and tracks notification processing.

10.1.5 Track Progress in Handling Notifications

Starting with early posting of an EDC project to your Master Calendar, track progress by updating the notification with current status, comments, and problem resolution. Create a “project life cycle” for handling notifications and define phase and status codes such as: Not Applicable; Pending Analysis; In Development; User Acceptance Test; Complete. The benefit is that notifications and follow-ups do not get lost in the process.

10.1.6 Create a Supporting System and Database of Notifications

Make underlying notices accessible via hyperlink from the Master Calendar so that the Calendar becomes the focal point for referencing EDC notices as well as tracking progress. The benefit is that everyone...new employees as well as old employees...knows where the information is located and can access it easily.

11. CONCLUSIONS AND NEXT STEPS

As this represents an initial draft by FISD and various members, the next steps are to ensure clear and accurate representation from a wider range of members/sources for industry wide reference and adoption. This will encompass regional forums and reviews with sources sponsored by FISD. Feedback will then be gathered and any necessary

revisions will be incorporated and made publicly available on the FISD website. Once all revisions have been made and agreed upon, this document will represent the Best Practices by which the financial industry should aspire to.

The members of FISD believe that the adoption of the core principles contained herein will benefit the whole financial industry by strengthening the lines of communication between Exchanges, Third Party Information Providers, Direct recipients and End-Users which will in turn greatly reduce delays, misinformation and customer confusion in the event of major interruptions, feed changes or system outages. If adopted by market participants, the FISD will communicate to the financial industry that those participants have met or exceeded the identified requirements.

Due to dynamic nature of the financial industry, it is expected that the current FISD Service Steering Group will continue to be in effect to ensure the relevance of this document.

Examples of Best Practice

We have a few examples currently of best practice in the area of reporting service interruptions. Perhaps the best is NASDAQ. NASDAQ uses both its NasdaqTrader web site and an e-mail "push" facility to issue notices of service interruptions. While NASDAQ does not routinely supply all of the elements listed in Section 7 on Unplanned Interruptions, it does provide good notices. NASDAQ should consider supplying a final written explanation after a major service problem is resolved, as described in 7.4.3 above.

The Chicago Mercantile Exchange also provides e-mail updates of service problems which are quite helpful. The CME's notices are very helpful in tracking service problems but are not as timely as NASDAQ's. Like NASDAQ, CME does not routinely provide a final written notice. However, they are ahead of nearly all other sources in taking on the proactive notice to direct recipients and end-users. The FISD needs to recognize both NASDAQ and CME as good examples of best practice when it comes to service interruption notification and encourage them to continue to enhance their offerings in this regard.

Examples of four NASDAQ notices for a service incident that occurred June 4 are shown below. The date and time plus the significant text for each are highlighted for clarity. This shows the timeliness of NASDAQ's reporting and how the reports track the event from start to conclusion.

1) 06/04/2004 09:36:27 AM

From: Trader Website <traderfeedback@nasdaq.com>
Subject: NASDAQ Market Systems Status
SendTo: traderfeedback@nasdaq.com

NASDAQ Operations has recently updated the status of the following NASDAQ Market System(s) to the NASDAQ Trader website:

NASDAQ is currently investigating a potential problem with Market Center executions. NASDAQ will advise.

Please refer to the link for additional system status updates.

<http://www.nasdaqtrader.com/asp/systemstatus.asp>

For more information you may reply to this Email or call the Web Help Desk at (800)777-5606.

Note: The text beginning with "http" in this mail message is a link to a NASDAQTrader.com page. If you can't click on the link in this message, cut and paste it into your browser's "Address" box (near the top of the browser window).

You may also have to cut and paste the link into the browser's "Address" box if it appears truncated.

2) 06/04/2004 09:39:22 AM

From: Trader Website <traderfeedback@nasdaq.com>
Subject: NASDAQ Market Systems Status
SendTo: traderfeedback@nasdaq.com

NASDAQ Operations has recently updated the status of the following NASDAQ Market System(s) to the NASDAQ Trader website:

NASDAQ is investigating a problem with executions in the range SPDE - STGSW. Executions do not seem to be taking place for this range of securities.

Please refer to the link for additional system status updates.

<http://www.nasdaqtrader.com/asp/systemstatus.asp>

For more information you may reply to this Email or call the Web Help Desk at (800)777-5606.

Note: The text beginning with "http" in this mail message is a link to a NASDAQTrader.com page. If you can't click on the link in this message, cut and paste it into your browser's "Address" box (near the top of the browser window).

You may also have to cut and paste the link into the browser's "Address" box if it appears truncated.

3) 06/04/2004 10:00:11 AM

From: Trader Website <traderfeedback@nasdaq.com>

Subject: NASDAQ Market Systems Status

SendTo: traderfeedback@nasdaq.com

NASDAQ Operations has recently updated the status of the following NASDAQ Market System(s) to the NASDAQ Trader website:

NASDAQ is currently opening the stocks in the range SPDE - STGSW.

Please refer to the link for additional system status updates.

<http://www.nasdaqtrader.com/asp/systemstatus.asp>

For more information you may reply to this Email or call the Web Help Desk at (800)777-5606.

Note: The text beginning with "http" in this mail message is a link to a NASDAQTrader.com page. If you can't click on the link in this message, cut and paste it into your browser's "Address" box (near the top of the browser window).

You may also have to cut and paste the link into the browser's "Address" box if it appears truncated.

4) 06/04/2004 10:02:01 AM

From: Trader Website <traderfeedback@nasdaq.com>

Subject: NASDAQ Market Systems Status

SendTo: traderfeedback@nasdaq.com

NASDAQ Operations has recently updated the status of the following NASDAQ Market System(s) to the NASDAQ Trader website:

All securities have now received an open and are trading normally.

Please refer to the link for additional system status updates.

<http://www.nasdaqtrader.com/asp/systemstatus.asp>

For more information you may reply to this Email or call the Web Help Desk at (800)777-5606.

Note: The text beginning with "http" in this mail message is a link to a NASDAQTrader.com page. If you can't click on the link in this message, cut and paste it into your browser's "Address" box (near the top of the browser window).

You may also have to cut and paste the link into the browser's "Address" box if it appears truncated.

The next examples are from the Chicago Mercantile Exchange in March.

1) **03/25/2004 10:33:25 AM**

From:

Subject: ALERT NOTICE From CME Market Data Operations

*****ALERT NOTICE*****

Due to a technical issue, CME experienced difficulty in transmitting market data on channel's one, two and three of the MDN from 9:05:41 A.M. to 9:23:24 A.M.

CME will retransmit the recovered data from the period mentioned above beginning as soon as possible. These messages will have your own unique Vendor ID in the message header.

Thank you.

2) **03/25/2004 12:23:59 PM**

From:

Subject: ALERT NOTICE From CME Market Data Operations

*****ALERT NOTICE*****

DUE TO TECHNICAL ISSUES AT CME, PLEASE RECYCLE YOUR MDN FEED.

Thank you.

3) **03/25/2004 02:37:50 PM**

From:

Subject: ALERT NOTICE From CME Market Data Operations

*****ALERT NOTICE*****

CME will retransmit the recovered data from the period mentioned below after 3:15 p.m. today. These messages will have your own unique Vendor ID in the message header. If this is going to cause you problems, do not process these messages.

Due to a technical issue, CME experienced difficulty in transmitting market data on channel's one, two and three of the MDN from 9:05:41 A.M. to 9:23:24 A.M.

INDEX

Capacity Management	13
Change	
Change Implementation	8
Exceptional Change	9
Major Change	7
Minor Change	7
Planned Change	8
Data	
Backup	17
Quality	16
Recovery	17
Documentation	9
Hours of Service	13
Interruptions	
Scheduled	8-9
Unplanned	11-12
Latency (Network)	16
Notification Periods	
Annual Schedule	12
General Activities	12
Market Coverage	12
New Listings	13
Non-Regular Changes	13
Quality (Data)	16
Reliability (System)	13
Testing	
Business Continuity	17
Recipient Testing	9
Test Data Format	9