Market Operations

Annual Service Provider Review

July 2007 to June 2008

This report details information in relation to the wholesale information & trading system, clearing manager and pricing manager functions performed by M-co under contract to the Electricity Governance Board.

Table of Contents

1. Introduction

1.1 Purpose

This report has been prepared for the Board in accordance with section 43 of the Electricity Governance Regulations 2003 (EGRs) and details performance for the year July 2007 to June 2008 of the wholesale information & trading system, clearing manager and pricing manager service providers in respect of their performance standards.

The report also summarises findings of a self-review of performance over the year using the guidelines outlined in sections 44 and 46 of the EGRs.

As M-co commenced reconciliation manager service provision on 1 May 2008, an annual review has not been conducted for the purposes of this report.

2. Overview

Following commencement of the new service provider agreements on 1 July 2007, the 12 month period to 30 June 2008 has focussed on implementing and consolidating the new contracting arrangements.

While not detailed in this report, the establishment of a reconciliation system (RECON) to support the new Part J reconciliation rules was a key focus of activity for the year. This project was delivered on time and within budget allowing for the reconciliation manager to commence operations as scheduled on 1 May 2008.

Other activities over the period involved an infrastructure transition and a number of other operational development activities.

2.1 Infrastructure Transition

Transitioning the WITS, CHASM and RECON applications onto Commission owned hardware was one of the major projects for the year. The project commenced in September 2007 and was extremely complex in that it involved shifting 24/7 systems, used by multiple participants, to new infrastructure hosting environments. A key facet of the project therefore was meticulous early planning in order to minimise system downtime during the changeover.

The project involved:

- Design of hardware platforms, network and security services, and disaster recovery solutions;
- Liaising with multiple stakeholders;
- Purchase/license and implementation of new:
    - network services (routers, switches, console services, load balancers);
    - servers (hardware, operating systems, database software, backup hardware & software); and
    - 3rd party software (Sun Solaris, Oracle);
- Installation of Transpower circuits to the new environments to accommodate GENCO;
- Testing of new hardware and infrastructure environments;
- Migration of applications and data to new infrastructure environments;
- Monitoring and tuning application performance on the new hardware and infrastructure environments; and

- Transition of licence management and support agreements to the Commission.

The WITS, CHASM and RECON applications were successfully transitioned to the new infrastructure environments in April 2008.

2.2 Other Projects

Other major projects worked on during the reporting period were:

- Upgrading the market applications to Oracle10g and Solaris8 operating environments;
- Implementing the publication of the Special Winter Schedule on WITS;
- Implementing the publication of Variable Reserves information on WITS;
- Liaising with Transpower on the application and infrastructure interfaces that will be required for the MSP implementation;
- Working with the Commission on a review of the WITS, CHASM and RECON source codes and documentation;
- Providing IT support to the M-co consulting team for their work on the Commission's LRA project;
- Commenced development of the Risk Management Contract Disclosure module within WITS;
- Undertaking a visit program to all key WITS client users;
- Implementing a number of CHASM system changes to accommodate the new Part J reconciliation rules;
- The selection of ASB Bank to replace Citibank as one of two financial institutions (the other being Westpac) for the holding of participant cash deposits to meet Energy Clearing House prudential security calls;
- Implementing the operational changes arising from the High Spring Washer Price (HSWP) rule change in September 2007;
- Analysing and reporting on the events surrounding high energy prices and the subsequent HSWP event on 24 June 2008 at Western Road; and
- Working with the Commission on the PPIP workstream.

2.3 Future Activities

The focus for the 2008/09 is about the further 'bedding-down' of the service provider functions to improve operational efficiencies. Activities such as targeted investments into staff training, compliance reviews, and business continuity are all planned this year.

System related initiatives include enhancements to the WITS, CHASM and RECON applications based on user feedback. These enhancements are centred on improved functionality and the addition of new datasets.

In addition, the implementation of Transpower's MSP systems will be a major focus of activity in the first quarter of 2009.

3. Compliance with Agreed Performance Standards

3.1 Wholesale Information & Trading System (WITS)

Measure	Actual 2007/08	Standard	Achieved
WITS availability	99.85%	99.72%	✓
WITS 6-month availability (rolling)	99.86%	99.72%	✓
WITS file upload availability	100.00%	99.72%	✓
Average time to publish PDS	4 mins 23 secs	7mins	✓
Average time to publish dispatch prices	26.4 secs	1min	✓
Average time to publish provisional/final prices	19.9 secs	1 min 30 secs	✓

Description

The target level of 99.72% relates to the equivalent of no more than two hours of outages per calendar month. Core functionality denotes all the systems and facilities necessary to fulfil the information system requirements of the EGRs as part of the Wholesale Information & Trading System Service Provider Agreement.

3.2 Clearing Manager

Measure	Actual 2007/08	Standard	Achieved
Wash-up notifications distributed to parties by 5th business day of each month	100%	92%	✓
Invoices released by 6pm on 9th business day	100%	92%	✓
Constrained on/off amounts released to System Operator by 9am on 8th business day	92%	92%	✓
Amounts payable to payees sent through to the bank by 5:30pm on settlement day	100%	92%	✓
Number of invoice calculation errors	1	0	✗
Number of security level calculation errors	0	0	✓

Description

The target level of 92% relates to the equivalent of no more than one instance of missing the deadline within a twelve-month period. The zero standards indicate that the Board expects there to be no calculation errors, in either invoices or the establishment of security levels.

Explanation

During the review period the clearing manager made one invoice calculation error. The error related to an April 2008 reconciliation file for a participant not having been fully deleted from the clearing system before a replacement file was loaded. The result of the error was that certain metering quantities for this participant were not processed in the system. The removal of the original file from the system was a manual process and was caused by human error. A minor change was subsequently made to the system to prevent a reoccurrence. The error was rectified through the washup process.

3.3 Pricing Manager

Measure	Actual 2007/08	Standard	Achieved
Final prices published by 9:30am if no provisional price situation exists	98.75%	97%	✓
Provisional prices published by 10:30am if provisional price situation exists	98.75%	97%	✓
Final prices published within 3 hours of a System Operator/Grid Owner fix to a provisional price situation	99.50%	97%	✓
M-co IT processing time to publish final prices within 5 minutes of sending	100%	97%	✓
Number of price processing errors	0	0	✓

Description

The target level of 97% relates to the equivalent of no more than one instance of missing a listed deadline within a calendar month. The zero standard indicates that the Board expects there to be no errors caused by the pricing manager in the calculation of prices.

3.4 Performance Standards Review

Regulation 43 requires the Board and the service provider to agree a set of performance standards for the next financial year. After discussion with the Commission, it is agreed that the existing standards as set out in the respective service provider agreements produce the right incentives on performance and therefore remain as stated for the 2008/09 year.

4. Self-Review of Performance

4.1 Compliance with Regulations and Rules

As per the requirements stipulated in the regulations, all known rule or regulation breaches by the respective service providers were noted in the monthly service provider reports.

In the 12 month reporting period the clearing manager self-reported two rule breaches and the pricing manager three breaches. Details are as follows:

Clearing Manager

13/08/07 – Late submission of the clearing manager monthly report to the market administrator.
13/9/07 – Late notification of must run dispatch auction results.

Pricing Manager

13/9/07 – Late publication of a provisional price situation notice.
13/4/08 – Late publication of a provisional price situation notice and late publication of provisional prices.

The wholesale information and trading system service provider had no rule breaches to report.

4.2 Operation of the Regulations and Rules

During the 12 month reporting period both the clearing manager and the pricing manager identified areas within the rules that required amending to better clarify respective service provider obligations. These were associated with the monthly reporting requirement of the clearing manager and daily reporting requirement of the pricing manager.

Throughout the review period the pricing manager worked with the Commission on the PPIP workstream and the WITS administrator participated in the Contract Disclosure workshops that resulted in some system design and rule modifications.

4.3 Compliance with Service Provider Agreements

To best of our knowledge, for the reporting period the M-co service providers complied with nearly all of the obligations contained in their respective agreements.

Due to operational oversight however, certain obligations were not met and procedures are now in place to avoid a repeat. These obligations are as follows:

1. The annual clearing manager and wholesale information and trading system user satisfaction surveys were not undertaken during the review period. These are being conducted in November 2008.
2. This annual report was not provided to the Commission within one month after the anniversary of the commencement date of the service provider agreement.

While an annual software audit of the COMIT and CHASM system was conducted in June 2008, discussions are still occurring with the Commission regarding the scope and form of this particular audit.

Appendix 1 details the contractual obligations for each of the services provider and contained in their respective agreements. Compliance, or otherwise, is noted in the table.

Appendix 1 – SPA Performance Requirements

WITS

The following tables provide a summary of the obligations only. Refer to the Service Provider Agreement for the full wording of each obligation.

Service Provider Agreement

General Terms

Clause	Obligation/Requirement	Compliance

3.2.1(a)	The WITS provider agrees to perform the following services in accordance with the SPA, from the commencement date:
	• the services contemplated in operational requirements and functional specification and if there is any inconsistency between the two, or any rule or regulation, the relevant rule of regulation will prevail :
	  ○ the additional requirements; and
	  ○ all other duties of the WITS provider under the SPA (except the hosting and support services; and
	• from the acceptance date, the hosting and support services;
		✓

3.2.2	The WITS provider must promptly perform the services with diligence, efficiency and to a standard reasonably expected of a properly qualified, resourced and experienced WITS provider of services of a similar nature, scope and complexity to the services.	✓
3.2.3	The WITS provider must perform the services in accordance with all relevant legislative and other legal requirements;	✓
3.2.4	The WITS provider must provide the services in accordance with the performance standards and such additional or substitute performance standards as are agreed between the parties: • at the beginning of each financial year in accordance with regulation 43; or • at any other time during a financial year following a request by the Commission to alter the performance standards. Agreement to additional or substitute performance standards may not be unreasonably withheld. IF the parties cannot agree on performance standards within 20 business days of the beginning of each financial year or a request by the Commission, the matter may be referred to dispute resolution under clause 16;	✓
3.2.5	The WITS provider must promptly inform the Commission if: • the WITS provider breaches any rule or regulation, or any requirement of the operational requirements, the functional specification or schedule 4; or • the WITS provider becomes aware of any error or ambiguity in or in respect of the operational requirements or the functional specification;	✓
3.2.6	The WITS provider must co-operate with the Commission's other service providers and other participants to facilitate effective provision of the services and all other services to the Commission; and	✓
3.2.7	The WITS provider must, from the acceptance date, provide the hosting and support services so that the system, on a continuing basis for so long as hosting and support services are to be provided by the WITS provider: • functions, operates and performs so that the services are provided in accordance with the SPA; • meets and satisfies the specifications; and	✓

	• is free from:
	  ○ viruses, to the extent reasonably possible (which includes the WITS provider using its best endeavours to protect and eliminate viruses); and
	  ○ material defects and errors	

3.3.1	The WITS provider will at all times during the term of the SPA provide a representative approved by the Commission to be the WITS Provider's representative. The representative will: • be authorised to receive all directions and instructions in connection with provision of the services on behalf of the WITS Provider; • monitor the performance of the services; • proactively identify and resolve any issues that may affect the provision of the services; and • review risks and agree risk management actions.	✓
3.3.2	The representative will be contactable by the Commission from 8:30am to 5:00pm on business days and outside of these hours in the event of any situation which the Commission reasonably considers requires immediate action by the WITS provider.	✓
3.4.1	The WITS provider will review its performance of the services in accordance with regulation 44 and provide reports to the Commission in accordance with regulation 45. Such reports will include such other information as the Commission reasonably requests.	✓
3.4.2	The WITS Provider will also provide the Commission with an annual report, no later than one month after each anniversary of the commencement date. This annual report will (in relation to the relevant year): • review the WITS provider's performance of the services; and • provide the Commission with such information as it reasonably requires to enable the Commission to review the WITS provider's performance of the services in accordance with regulation 46.	✗
3.4.3	The WITS provider will provide other reports required by the operational requirements in schedule 2 and also provide any other ad hoc reports to the Commission at the Commission's reasonable request, such reports to be paid for at the hourly rates. All reports provided must be presented in a format that can be reproduced on the Commission's website.	✓
3.5	The WITS provider will ensure that the representative appointed in accordance with clause 3.3 of the SPA attends monthly meetings with the Commission (and other additional meetings), to discuss matters relating to the services.	✓
3.7	The WITS provider warrants that: • its employees, contractors and agents have the suitable skills, training and experience for, and are properly supervised in, the provision of the services; and • it is not aware as at the date of the SPA of anything within its reasonable control which might or will adversely affect its ability to perform its obligations under the SPA, the regulations or the rules.	✓
3.9	From the acceptance date, the WITS provider must use the System as required to provide the services to the Commission in accordance with the SPA. To avoid doubt, the WITS provider shall not use the System for any purpose other than to provide services to the Commission.	✓
6.11	The WITS provider may not charge any participant for the services.	✓
7.5.1	Where the WITS provider is providing services at the hourly rates: • the WITS provider will keep proper records of the hours worked by its personnel and provide such records to the Commission on request; and • the number of hours worked by its personnel must be reasonable in the circumstances.	✓

9.1	The WITS provider warrants that: • any material provided as part of the services does not and will not infringe any intellectual property rights of any third party; and • the provision of the services and the use of the services by the Commission and the participants does not and will not infringe any third party's intellectual property rights, provided that this warranty shall not apply to data which the WITS Provider received pursuant to the rules in circumstances where the WITS provider had no knowledge, and could not reasonably be expected to have known, of any infringement of third party intellectual property rights in respect of such data.	✓
9.2	The WITS provider indemnifies the Commission in respect of any costs, including legal costs on a solicitor-client basis, expenses, claims, liabilities, damages or losses incurred by the Commission as a result of a breach of any of the warranties in clause 9.1.	✓
9.3	The WITS provider must not: • obtain any rights to, interest in or ownership of any data received by the WITS provider for the first time on or after the commencement date, or any processed data derived from that data; • except with Commission's written consent, use data or processed data as described in clause above, for any purpose other than for providing the services, provided that no written consent will be required if such data or processed data has entered the public domain; • obtain under the SPA any rights to, interest in or ownership of data which was held under the Information SPA, or any processed data derived from that data; and • except with the Commission's prior written consent, use data or processed data as described in clause above for any purpose other than for providing the services, provided that: o no written consent will be required if such data or processed data has entered the public domain; and o this clause shall not limit any rights to the WITS provider has under the Information SPA to use such data and processed data. The WITS provider asserts that it has interests in the data and processed data received and held by it under the Information SPA, and certain rights to use such data and processed data for purposes other than for providing the services. The commission denies this assertation. The parties will attempt in good faith to resolve this difference and if not resolved within 90 days of the effective date, either party may refer the matter for resolution in accordance with clause 16.	✓
10.1	The WITS provider must: • maintain such arrangements with its officers, employees, agents, auditors and professional advisors as are reasonably necessary to protect the confidentiality of confidential data; • ensure that confidential data is only used for the purposes of the SPA and is not disclosed except: o to such of its officers, employees, agents, auditors and professional advisors as need to know such confidential data for the purpose of providing the services; o as required under the regulations, rules or at law; or o as permitted by the Commission; and • except to the extent it is transferred under clause 10.2 or 13.2, at its own expense store all data and processed data held by the WITS provider under the SPA.	✓
10.4	The WITS provider must not make or release public or media statements, or publish material related to the SPA or the services, without the Commission's prior written approval.	✓
11.1	The WITS provider must have in place at the commencement date and maintain throughout the term of the SPA data and processed data backup arrangements, and a disaster recovery system, that will enable the WITS provider, on a continuing basis, to fulfil its obligations under the SPA with the minimum disruption practicable to the electricity market. The back-up policy and data recovery plan must comply with the operational requirements.	✓

11.2	Without limiting clause 11.1, the WITS provider must perform and comply with the requirements set out in the SPA, including the operational requirements, in respect of: • back-up of all data and processed data and the software; and • disaster recovery (comply with disaster recovery plan in op requirements)	✓
15.1	The WITS provider must from effective date until at least 2 years following expiry or termination of SPA, maintain adequate insurance cover, for all normal commercial risks and in respect of any potential liability it may incur under the SPA or under the regulations or the rules, to ensure that any problems encountered by the WITS provider will not result in disruption of the efficient performance of the SPA. Insurance to be in a form and insurer approved by Commission.	✓
15.2	In respect of the effective date, the commencement date and each anniversary of the commencement date, the WITS provider must: • obtain a certificate from its insurer to establish compliance with clause 15.1; and • provide to the Commission either a copy of the certificate or a letter from the insurer, confirming cover at least 5 business days prior to the relevant date (or, in the case of the effective date within 5 business days after that date). Where a letter is provided under clause 15.2.2(b) a copy of the certificate must be provided as soon as practicable thereafter.	✓
17.1	The WITS provider must not assign any of its rights or obligations under the SPA without the prior written consent of the Commission.	✓

Operational Requirements – Schedule 2

Para	Obligation/Requirement	Compliance
1.1	The WITS system must be built on an industry standard, robust architecture that is reliable and scaleable in the following areas.	✓
1.2	WITS must have separate and independent environments for development, user acceptance testing and production. The user acceptance testing must be available for participants to perform their own testing and staff training. The WITS provider must maintain a standalone "tertiary" facility to process orders in the event of unexpected downtime or scheduled outage.	✓
1.3	The architecture must not contain any components that are no longer supported.	✓
1.4	The architecture must be easily scaleable to accommodate a 10 percent growth in users and transactions per annum, without significantly affecting performance and reliability.	✓
1.5	There must be agreed procedures in place for upgrades to hardware and software. All upgrades must be carefully planned, scheduled, notified to all relevant parties well in advance and implemented efficiently at times that cause minimum disruption to users. The WITS provider must implement all relevant, proven operating system, database and system software upgrades in a timely manner.	✓
1.6	The WITS provider is responsible for the maintenance to the data environment and must ensure functionality is available within the application to reverse the effects of any material errors made by users in loading the data via file transfer. The WITS provider must provide assistance to users in executing any such recovery.	✓
1.7	The WITS system must be designed to cope with at least 200 concurrent online users and the transaction volumes detailed in the appendix II. A breakdown of the costs associated with concurrent usage numbers above 200 must be provided.	✓
2.1	The following types of interfaces must be provided: • a secure web browser user-interface for updating, viewing and downloading information in CSV formatted files;	✓

	• as a minimum, a facility to transfer files in CSV or XML format via encrypted FTP; and • interfaces individually agreed with the relevant service provider: system operator, clearing manager and pricing manager. The WITS provider must co-operate with the System Operator, and any other service provider, when upgrades to any transfer mechanism are proposed.	
3.1	The WITS system must be available and operational 24x7 and designed to provide maximum availability around the critical periods.	✓
4.2	The WITS provider must undertake all preventative, corrective maintenance and the implementation of enhancements outside business hours where possible.	✓
4.3	The WITS provider must provide the Commission a monthly report detailing whether service levels were met during the month and if not, reasons for any failure.	✓
5.1	Backup copies of data must be taken at least daily and stored in a secure location. Copies of the latest version of the software must also be kept offsite. At least weekly, a backup copy of the data and software must be delivered and stored at an offsite location at least 100 kms from the premises used to provide the regular service.	✓
5.2	The WITS provider must keep an up to date disaster recover plan, designed to recover in the event that the WITS provider's site is inoperable. A real-time DR site must be available that provides a ten minute recovery capability.	✓
5.4	The WITS provide must test the DR procedure every six months. The test must include: • restoration of the system to the remote location; • restoration and roll-forward to a known time; and • verification of system availability to an external user. The WITS provider must provide a written report to the Commission, on completion of the DR test, of the results and ensuing actions. At regular intervals the WITS provider must perform "desk-checks" to test smaller components of the DR plans.	✓
5.5	The WITS provider must provide alternative submission and publication facilities to participants and service providers in the event that the primary system is unavailable, as required by the Rules.	✓
6.1	The WITS system must have a framework for the management of user accounts.	✓
6.2	User privileges must be able to control access at both function and specific data level.	✓
6.3	The WITS system must have a security policy in place and have mechanisms that enforce the password standard, account lock-out for unsuccessful logon attempts and/or session timeouts. The security policy must be reviewed each year to ensure it conforms to industry best practice.	✓
6.4	The WITS system must maintain audit logs or user interactions with the system and action all alerts of repeated unsuccessful logons to analyse their own usage patterns of the system. This information must be made available on request.	✓
6.5	The system must maintain the confidentiality of each participant's information by allowing requests only by parties that have been granted authority by participants to access the system on their behalf of the exchange of digital certificates / password authentication.	✓
7.1	There must be a well defined and documented capacity planning strategy in place.	✓
7.2	There must be system management utilities implemented that will measure the capacity of the system, to show trends and therefore assist with predicting future capacity requirements.	✓
7.3	All data is the property of the Commission and the WITS provider must store the data securely and be able to provide it to the Commission on request within a reasonable	✓

	timeframe.	
7.4	The WITS system must maintain history for immediate access for seven years, or longer as agreed with the Commission, after which the information must be archived and available for retrieval on request.	✓
8.1	The WITS provider must store the data securely and be able to provide it to the Commission on request within a reasonable timeframe.	✓
9.	The WITS system must have an audit trail of all data input, confirmations delivered, notifications delivered and the delivery of information to other parties.	✓
10.1	The WITS provider must employ industry service management methodologies, such as ITIL including robust quality assurance processes. Any methodology must cover the service management functions being provided.	✓
10.2	The WITS provider must provide a contact person who is available 24/7 to assist with queries from participants and other service providers. The WITS provider must actively assist all users to resolve their issues promptly, even outside business hours. The WITS provider must respond within 30 minutes of a call being lodged. Response must be by an appropriately skilled person, who is able to fix any problems encountered within the requirements of the SPA. If an incident affects more than one user, the WITS provider must notify all participants.	✓
10.4	The WITS provider must maintain a register of all help desk requests, system faults and other operational incidents reported by each user during the previous 12 month period. The WITS provider must notify users when incidents are resolved or time when expected to be resolved. The WITS provider must develop an incident management process for users to view all incidents and to report any faults. A summary of all incidents and their resolution times must be included in the monthly report on service levels.	✓
11	The WITS provider must follow the change management procedure as set out in appendix I of this document and must be integrated into the internal change management processes with respect to the efficient management and reporting of progress.	✓
12.1	The WITS provider must employ industry standard software engineering practices including robust quality assurance processes. Any methodology must cover the whole SDLC in the development and maintenance of software.	✓
12.2	The software must be designed for flexibility to ensure changes to functions can be made efficiently and cost effectively. The WITS provider must be able to develop custom reports on request from the Commission and from participants.	✓
13.1	The WITS provider must maintain close contact with users, be proactive and provide additional services and support to ensure that the system remains responsive, up to date and consistent with the needs of the industry.	✓
13.3	The WITS provider must develop formal notification channels to notify users and the representative of the Commission of outages and likely timeframes for restoration of service.	✓
13.4	The WITS provider must provide an escalation process for users in the event of either a major failure of the system extending beyond service level thresholds or in the event of continued user service issues.	✓
13.5	During periods when the system is not available the WITS provider must liaise with the representative of the Commission and users not less than daily, including advising of expected times for the resumption of service.	✓
13.6	The WITS provider must develop, distribute and consolidate a survey of all participants that analyses the satisfaction levels of their service provision. The survey is to be conducted annually and the results reported to the Commission.	✓
14	The WITS provider must be able to provide training in the use of the software to new users.	✓

15	The WITS provide must maintain and provide as a minimum: • an up-to-date functional specification against which the software can be audited as per the requirement in clauses 51 to 53 of the Electricity Governance Regulations (Regulations). The functional specification is the 'software specification' referred to in the Regulations. The functional specification and any subsequent changes are the property of the Commission; • a user manual and online help facilities to enable new users to configure their systems correctly and access the system. The documentation must provide sufficient detail for new users to locate and use all the relevant functions. The user documentation must include a troubleshooting guide, frequently asked questions and information on where and how to seek further help; • backup procedures describing alternative methods for the submission and delivery of information as required by the Rules; • a DR procedures manual that describes the procedure, possible impacts on users and their operation and instructions on what users will need to do for business continuity; and • sufficient technical documentation for business continuity in case of the loss of key personnel. This must include a design specification that describes how the system delivers the functions described in the functional specification and operational requirement documents.	✓
16.2	The provider of the software must implement, under the change control procedure, any changes necessary to give effect to any reasonable recommendations made by an auditor, with the objective of constantly improving services.	✓
16.3	The WITS provider must comply with the audit requirements as set out in clauses 51, 52 and 53 of the Regulations with respect to conducting audits of the software, annually, on first-time use and for software changes.	✓
17	For the public (including participants): The WITS provider must provide an online web-based publication service to the general public. The functional specification details the requirements for the publication of real-time prices, historical bids and offers and daily demand files on a public website. However, in addition, the Commission requires that some non-confidential information is also made available via the public website. This information must include, but is not limited to: final prices at selected locations, price trend data, demand charts, hydrology charts and scheduled constraints.	✓

Additional Requirements – Schedule 4

Clause	Obligation/Requirement	Compliance
1	The WITS provider must provide for use by participants: • a trading interface that allows participants to display different types of information at same time on screen, automatically refreshed when information updated and information can be customised by user; • additional validation facilities when submitting bids and offers, particularly around the 2 hour limit, removing the possibility participants will breach these particular rules without having bona fide physical reasons as required by rules; • an alert system notifies users via cellphone or email for prices falling outside user-defined thresholds; and • a 'cellphone interface' to all for submission and publication of information including; ○ the aggregation of information such as total quantities bid and offered;	✓

	○ the publication of pricing trends, averages etc; ○ the publication of Indices – Electricity Price Index, Fixed Price Indices; and ○ a WAN environment for testing new functionality	

Hosting and support Services – Schedule 5

Clause	Obligation/Requirement	Compliance
3.1	The WITS provider must, when providing the equipment maintenance services, perform and comply with the requirements set out in the SPA, including the operational requirements, in respect of disaster recovery.	✓
3.2	The WITS provider must at all times maintain a supply of replacement and spare parts necessary to effect equipment services or maintain hardware maintenance contracts with equipment manufacturers that guarantee an on site response within 2 hour, with 24 hour, 7 days a week coverage and unless otherwise agreed, ensure all replacement and spare parts provided, pursuant to the SPA, will be new parts.	✓
4.1	The WITS provider must: • install and host the System at the sites, including connection of the System to the WITS Provider's network provider of choice and power supply. • provide cabinet space at the sites capable of, and appropriate for, being used for the installation of the System. • agree that the System will not be housed within a cabinet containing the WITS provider's or third party equipment. • fully secure the System by the systems separate from other customers' equipment an also from the WITS provider's equipment, using such measures as the Commission may reasonably require. The security measures required by the WITS provider shall include both physical security measures and network security. • provide the sites with robust, environmentally controlled support systems, which include alarm monitored air conditioning systems, fire alarms and a centrally controlled security system with a reliability that is consistent with the ICT hosting services industry best practice. The WITS provider must ensure that: • it provides electricity to the sites and to all components of the System. • the sites as a whole, or section of the sites housing the System must have its mains grid power supply backed by a UPS of sufficient capacity to power all devices it supports for a minimum of 15 minutes in the event of a main power failure. The UPS must al be capable of issuing a low battery alert in the event of a mains power failure and a generator failure, with processes in place to react to such an alert and power the system back up and begin to recover service when power supply becomes available; • the sites as a whole or the section of the sites housing the System must have its mains grid power supply and UPS backed by a generator of sufficient capacity to power all of the equipment it supports, with at least a 20% margin of excess capacity. The generator must have sufficient fuel to run at full power for 24 hours and processes in place to guarantee fuel and other consumables sufficient to operate for 7 days continuously in the event of a mains power failure and to start automatically and must be tested annually; • the sites will have an automatic water sprinkler system; • the sties as a whole to the section of the sites housing the System will have sufficient heating ventilation and air conditioning systems to maintain the temperature and	✓

	humidity with recommended ranges as specified by the manufacturers of the components of the System; • no third parties, other than those third parties that have prior written approval of the Commission, will have access to the System; • the WITS provider will only access or deal with the System as is strictly necessary to comply with the terms of the SPA and maintain a complete and detailed log of all actions that the WITS provider carries out on the system; and • any changes to the sites, whether associated with the System or not, that increase the operating risk of the System or impact the availability of the System can only be made as a variation under clause 7.	
4.2	The WITS provider must: • protect the System from radio or electrical interference, power fluctuations, abnormal environmental conditions, theft and any other risks of loss or damage; • take reasonable steps to make sure the System is not affected by any virus, power surge/interruption, water damage, dust, shock or other negative factor; • monitor all alarms and hardware error logs, operating system errors, database error logs and application error logs in a proactive manner, and take corrective action where a fault it is indicated; and • manage as part of the System a full application and database backup every 24 hours, and a full operating system backup twice a week, which is to be secured offsite within 24 hours of the beginning of the backup.	✓
4.3	The WITS provider warrants that the environment of the sites is environmentally suited to house the System and that the WITS provider will maintain that environment throughout the term of the SPA. This includes the maintenance of temperature, humidity and dust within the recommended ranges as specified by the manufacturers of the components of the System.	✓
4.4	The WITS provider must not move or relocate the System or the location of the sites except with the prior written approval of the Commission, such approval not to be unreasonably withheld. At least one months notice will be given of any change. Any such new sites must comply with all the terms and conditions of this schedule 5. This clause 4.4 will not apply where Telecom is required to move or relocate the System because of any emergency.	✓
4.5	The WITS provider must provide the Commission and its contractors with reasonable, safe access to the sites and the System, and shall control access to the sites and the System, in accordance with this clause 4.5.	✓
5.1	As soon as the WITS provider becomes aware of any failure to provide the services in accordance with the SPA, the WITS provider must: • use all reasonable endeavours to remedy that service failure; and • perform any accurate and comprehensive root cause analysis to determine the cause of the service failure. The WITS provider will supply the Commission with a written report summarising the results of that analysis as soon as reasonably practicable after the analysis has been completed.	✓

CLEARING MANAGER

The following tables provide a summary of the obligations only. Refer to the Service Provider Agreement and EGRs for the exact wording of each obligation.

Service Provider Agreement

General Terms

Clause	Obligation/Requirement	Compliance
3.1.2	CM functions must be performed through a special purpose company.	✓
3.2.1	From the commencement date, the CM must undertake: • the duties and obligations in the EGRS; • the services contemplated by the operational requirements and functional specifications; • the additional requirements; • all other CM duties set out in the SPA. From the acceptance date, the CM must perform the hosting and maintenance services.	✓
3.2.2	CM must perform services with diligence, efficiency and skill and to a standard reasonably expected of a properly qualified, resourced and experienced provider.	✓
3.2.3	CM must perform the services in accordance with all relevant legislation and other legal requirements – Electricity Act, Companies Act, etc.	✓
3.2.4	CM must agree performance standards at the beginning of each financial year or at any other time during the year following a request from the Commission.	✓
3.2.5	CM must promptly inform the Commission of: • any breaches of the rules, regulations, operational requirements, functional specifications or additional requirements. • any error or ambiguity in the operational requirements and functional specifications.	✓
3.2.6	CM must co-operate with the Commission, other service providers and participants.	✓
3.2.7	From the acceptance date, the CM must provide hosting and support services so that CHASM: • functions, operates and performs so that the services are provided in accordance with the SPA; • meets and satisfies the operational requirements, functional specifications and performance standards; • is free from viruses, material defects and errors.	✓
3..3	CM must provide a Commission approved representative and delegate to receive directions/instructions from the Commission, monitor performance of the services, proactively identify and resolve issues, and review risks and agree risk management actions. The representative and delegate must be available during and after office hours.	✓
3.4.1	CM must conduct a self review of its performance in accordance with regulation 44 and report the results of this review to the Board under regulation 45.	✓
3.4.2	CM must provide an annual report to the Board no later than one month after each anniversary of the commencement date.	✗

3.4.3	CM must provider other reports required by the operational requirements, e.g. • monthly report detailing compliance with the service levels (para 4.3); • annual report containing the results or the annual user satisfaction survey (para 13.6).	✗
3.4.4	CM must provide any ad hoc reports requested by the Commission.	✓
3.5	CM must attend monthly meetings with the Commission, and additional meetings if required.	✓
3.6	CM must co-operate with any Commission-initiated audits regarding the services (not the software). Audits may be held annually or at a greater frequency as reasonably required by the Commission.	✓
3.7.2	CM must re-perform the services regarding any data (at its own cost) if it omits to include all data made available to it at the time.	✓
6.1	CM must provide the Commission with a valid tax invoice for the relevant fees by the 5th business day of the month following provision of the relevant services.	✓
6.9	CM must refund the amount of any monies it has overcharged the Commission, including pay default interest on this amount.	✓
9.3	CM and Commission must resolve data ownership issue within 90 days of contract commencement.	✓
10.1.1	CM must maintain such arrangements with its employees, contractors to protect the confidentiality of all confidential information.	✓
10.1.2	CM must ensure all confidential information is only used for the purposes of the SPA and is not disclosed except in specified circumstances.	✓
10.1.3	CM must, at its own cost, store all data and processed data that it holds as CM, including data held under the previous CM service provider agreement.	✓
10.2	CM must, during the term of the SPA, transfer to the Commission copies of, or grant the Commission access to, the data or processed data (if requested by the Commission).	✓
11.1	CM must maintain data and processed data back-up arrangements, and a disaster recovery system. Both processes must comply with the operational requirements.	✓
15.1	CM must maintain adequate insurance cover for all normal commercial risks and potential liability it may incur under the SPA, regulations and rules.	✓
15.3	CM must maintain fidelity insurance with an insurer, and on terms, approved by the Commission.	✓

Operational Requirements – Schedule 2

Para	Obligation/Requirement	Compliance
1.1	CHASM must be built on an industry standard, robust, architecture that is reliable and scaleable.	✓
1.2	There must be separate and independent environments for development, user acceptance testing and production.	✓
1.3	The architecture must not contain components that are no longer supported.	✓

1.4	The architecture must be easily scaleable to accommodate 10% growth in users and transactions per annum, without affecting performance or reliability.	✓
1.5	Agreed procedures must be in place covering the implantation of upgrades to hardware and software. All upgrades must be carefully planned, scheduled and notified to relevant parties well in advance, and implemented efficiently at times that cause minimum disruption to users.	✓
1.6	CM must ensure that functionality is available within the application to reverse the effects of any material errors made by users in loading data via file transfers. CM must undertake the recovery of any database integrity and corruption issues and correct any errors that occur as a result of CHASM incorrectly processing information.	✓
1.7	CHASM must be designed to cope with at least 70 concurrent online users and transaction volumes detailed in Appendix ii.	✓
2.1	CHASM must provide the following interfaces: • a secure web browser user interface; • a facility to transfer files in CSV format via FTP; • interfaces as required by the service providers in the functional specification.	✓
3	CHASM must be available to end users during business hours, particularly during critical periods.	✓
4.1	CM must achieve the target service levels specified in clause 4.1.	✓
4.2	CM must undertake all preventative, corrective maintenance, and implement enhancements outside business hours where possible. For urgent corrective maintenance, the CM may undertake maintenance at any time upon notifying the Commission.	✓
4.3	CM must provide the Commission with a monthly report detailing compliance against the service levels.	✓
5.1	CM must back up copies of the data daily and store them securely. Each week the CM must store a back-up copy of the data and software at an offsite location at least 100kms from the premises.	✓
5.2	CM must prepare and maintain a disaster recovery plan.	✓
5.3	A real-time DR site must be available that provides a ten minute capability. CM must test the DR procedures every six months, which will involve: • restoring CHASM to the remote location; • restoring CHASM and rolling it forward to a known time; • verifying CHASM's availability to an external user.	✓
6.1	CHASM must have a framework for managing user accounts.	✓
6.3	CM must have a security policy in place (reviewed annually) and have mechanisms that enforce the password standard, account lock-out for unsuccessful logon attempts or session timeouts.	✓
6.4	CHASM must maintain logs of user interactions, and action all alerts of repeated unsuccessful logons to prevent hacking.	✓
6.5	CHASM must maintain the confidentiality of participants' information by allowing requests only by parties that have been granted appropriate authority.	✓
7.1	CM must have a well defined and documented capacity planning strategy.	✓

7.2	CM must implement system management utilities to measure CHASM's capacity to show trends and predict the future capacity requirements.	✓
7.3	CM must promptly advise the Commission if increases in transactional volumes beyond the levels agreed in the SPA threaten the achievement of service levels. CM must take remedial action if service levels cannot be met with the current capacity levels. If transaction and/or database volumes exceed agreed volumes, or if rule changes increase complexity so that the service levels cannot be met, then the CM and Commission must initiate the change control procedures.	✓
8.1	CM must store all data securely and make it available to the Commission on request.	✓
8.2	CHASM must retain historical data for seven years.	✓
9	CHASM must have an audit trail of all data input, confirmations, notifications, etc.	✓
10.1	CM must employ industry service management methodologies.	✓
10.2	CM must make a person available during business hours to assist with user queries.	✓
10.3	CM must provide a fault management service during business hours to rectify operational incidents and system faults. Remedial work must be commenced within two hours of the faults detection and reporting. CM must notify all participants if the incident affects more than one user.	✓
10.4	CM must maintain an incidents register of all help desk requests, system faults and other operational incidents reported by each user during the 12 month period. CM must notify users when incidents are resolved or of the time when they expect to resolve them.	✓
11	CM must follow the change management procedures. CM must integrate these procedures into its internal change management processes (including the management and reporting of progress).	✓
12.1	CM must use industry standard software engineering practices, including robust quality assurance processes.	✓
13.1	CM must maintain close contact with users, be proactive, provide additional services and support to ensure that CHASM remains responsive, up-to-date and consistent with industry needs.	✓
13.3	CM must develop formal notification channels to notify users and Commission of outages and likely timeframes for restoring service.	✓
13.4	CM must provide an escalation service for users for major system failures.	✓
13.5	CM must liaise with Commission and users daily when CHASM is unavailable.	✓
13.6	CM must develop, distribute and consolidate an annual survey of all participants regarding their satisfaction with the CM service. CM must report the results of the survey to the Commission.	✓
14	CM must provide training regarding the use of the software to new users.	✓
15	CM must maintain: • the functional specification;	✓

	• a user manual and online facilities for new users to configure their systems correctly and access CHASM; • maintain a DR procedures manual; • technical documents to ensure business continuity when key personnel leave.	
16.2	CM must implement necessary changes to give effect to any auditor recommendations via the change control process.	✓
16.3	CM must comply with the audit requirements set out in Regulations 52 and 53.	✓

Hosting and support Services – Schedule 5

Clause	Obligation/Requirement	Compliance
3.1	The provider must, when providing the equipment maintenance services, perform and comply with the requirements set out in the SPA, including the operational requirements, in respect of disaster recovery.	✓
3.2	The provider must at all times maintain a supply of replacement and spare parts necessary to effect equipment services or maintain hardware maintenance contracts with equipment manufacturers that guarantee an on site response within 2 hour, with 24 hour, 7 days a week coverage and unless otherwise agreed, ensure all replacement and spare parts provided, pursuant to the SPA, will be new parts.	✓
4.1	The provider must: • install and host the System at the sites, including connection of the System to the provider's network provider of choice and power supply. • provide cabinet space at the sites capable of, and appropriate for, being used for the installation of the System. • agree that the System will not be housed within a cabinet containing the provider's or third party equipment. • fully secure the System by the systems separate from other customers' equipment an also from the provider's equipment, using such measures as the Commission may reasonably require. The security measures required by the provider shall include both physical security measures and network security. • provide the sites with robust, environmentally controlled support systems, which include alarm monitored air conditioning systems, fire alarms and a centrally controlled security system with a reliability that is consistent with the ICT hosting services industry best practice. The provider must ensure that: • it provides electricity to the sites and to all components of the System. • the sites as a whole, or section of the sites housing the System must have its mains grid power supply backed by a UPS of sufficient capacity to power all devices it supports for a minimum of 15 minutes in the event of a main power failure. The UPS must al be capable of issuing a low battery alert in the event of a mains power failure and a generator failure, with processes in place to react to such an alert and power the system back up and begin to recover service when power supply becomes available; • the sites as a whole or the section of the sites housing the System must have its mains grid power supply and UPS backed by a generator of sufficient capacity to power all of the equipment it supports, with at least a 20% margin of excess capacity. The generator must have sufficient fuel to run at full power for 24 hours and processes in place to guarantee fuel and other consumables sufficient to operate for 7 days continuously in the event of a mains power failure and to start automatically and must be	✓

	tested annually; • the sites will have an automatic water sprinkler system; • the sties as a whole to the section of the sites housing the System will have sufficient heating ventilation and air conditioning systems to maintain the temperature and humidity with recommended ranges as specified by the manufacturers of the components of the System; • no third parties, other than those third parties that have prior written approval of the Commission, will have access to the System; • the provider will only access or deal with the System as is strictly necessary to comply with the terms of the SPA and maintain a complete and detailed log of all actions that the provider carries out on the system; and • any changes to the sites, whether associated with the System or not, that increase the operating risk of the System or impact the availability of the System can only be made as a variation under clause 7.	
4.2	The provider must: • protect the System from radio or electrical interference, power fluctuations, abnormal environmental conditions, theft and any other risks of loss or damage; • take reasonable steps to make sure the System is not affected by any virus, power surge/interruption, water damage, dust, shock or other negative factor; • monitor all alarms and hardware error logs, operating system errors, database error logs and application error logs in a proactive manner, and take corrective action where a fault it is indicated; and • manage as part of the System a full application and database backup every 24 hours, and a full operating system backup twice a week, which is to be secured offsite within 24 hours of the beginning of the backup.	✓
4.3	The provider warrants that the environment of the sites is environmentally suited to house the System and that the provider will maintain that environment throughout the term of the SPA. This includes the maintenance of temperature, humidity and dust within the recommended ranges as specified by the manufacturers of the components of the System.	✓
4.4	The provider must not move or relocate the System or the location of the sites except with the prior written approval of the Commission, such approval not to be unreasonably withheld. At least one months notice will be given of any change. Any such new sites must comply with all the terms and conditions of this schedule 5. This clause 4.4 will not apply where Telecom is required to move or relocate the System because of any emergency.	✓
4.5	The provider must provide the Commission and its contractors with reasonable, safe access to the sites and the System, and shall control access to the sites and the System, in accordance with this clause 4.5.	✓
5.1	As soon as the provider becomes aware of any failure to provide the services in accordance with the SPA, the provider must: • use all reasonable endeavours to remedy that service failure; and • perform any accurate and comprehensive root cause analysis to determine the cause of the service failure. The provider will supply the Commission with a written report summarising the results of that analysis as soon as reasonably practicable after the analysis has been completed.	✓

PRICING MANAGER

The following tables provide a summary of the obligations only. Refer to the Service Provider Agreement and EGRs for the full wording of each obligation.

Service Provider Agreement

General Terms

Clause	Obligation/Requirement	Compliance
3.2.1(a)	From the commencement date, the PM must undertake: • the duties and obligations in the EGRS; • the services contemplated by the operational requirements and functional specifications; • the additional requirements; • all other PM duties set out in the SPA.	✓
3.2.1(b)	From the acceptance date, the PM must perform the hosting and maintenance services.	✓
3.2.2	PM must promptly perform services with diligence, efficiency and skill and to a standard reasonably expected of a properly qualified, resourced and experienced provider.	✓
3.2.3	PM must perform the services in accordance with all relevant legislation and other legal requirements – Electricity Act, Companies Act, etc.	✓
3.2.4	PM must agree performance standards at the beginning of each financial year or at any other time during the year following a request from the Commission, and provide the services in accordance with these performance standards.	✓
3.2.5	PM must promptly inform the Commission of: • any breaches of the rules, regulations, operational requirements, functional specifications or additional requirements. • any error or ambiguity in the operational requirements and functional specifications.	✓
3.2.6	PM must co-operate with the Commission, other service providers and participants.	✓
3.2.7	From the refresh date, provide the refresh services.	✓
3.2.8	From the acceptance date, the PM must provide hosting and support services so that the system: • functions, operates and performs so that the services are provided in accordance with the SPA; • meets and satisfies the operational requirements, functional specifications and performance standards; • is free from viruses, material defects and errors.	✓
3.3	PM must provide a Commission approved representative and delegate to receive directions/instructions from the Commission, monitor performance of the services, proactively identify and resolve issues, and review risks and agree risk management actions. The representative and delegate must be available during and after office hours.	✓
3.4.1	PM must conduct a self review of its performance in accordance with regulation 44 and report the results of this review to the Board under regulation 45.	✓

3.4.2	PM must provide an annual report to the Board no later than one month after each anniversary of the commencement date.	✗
3.4.3	PM must provide other reports required by the operational requirements, e.g. • monthly report detailing compliance with the service levels and detailing all system incidents, e.g. faults, helpdesk requests (paras 3.3 and 9.2). • annual report containing the results or the annual software audit (para 1.5.3, Appendix III).	✓
3.4.4	PM must provide any ad hoc reports requested by the Commission.	✓
3.5	PM must attend monthly meetings with the Commission, and additional meetings if required.	✓
3.6	PM must co-operate with any Commission-initiated audits regarding the services (not the software). Audits may be held annually or at a greater frequency as reasonably required by the Commission.	✓
3.7.2	PM must re-perform the services regarding any data (at its own cost) if it omits to include all data made available to it at the time.	✓
6.1	PM must provide the Commission with a valid tax invoice for the relevant fees by the 5th business day of the month following provision of the relevant services.	✓
6.9	PM must refund the amount of any monies it has overcharged the Commission, including pay default interest on this amount.	✓
9.1	PM warrants that: • any material provided as part of the services does not and will not infringe any third party IP rights; • the provision of the services and their use by the Commission and participants does not and will not infringe any third party IP rights.	✓
9.3.2	PM must not use data or processed data described in clause 9.3.1 (i.e. pricing data relevant to this SPA) for any purpose other than for providing the services (unless otherwise agreed by the Commission). The Commission's written consent will not be required if the data or processed data has entered the public domain.	✓
9.3.4	PM will not use data or processed data described in clause 9.3.3 (i.e. pricing data relevant to the previous SPA) for any purpose other than for providing the services (unless otherwise agreed by the Commission).	✓
10.1.1	PM must maintain such arrangements with its employees, contractors to protect the confidentiality of all confidential information.	✓
10.1.2	PM must ensure all confidential information is only used for the purposes of the SPA and is not disclosed except in specified circumstances.	✓
10.1.3	PM must, at its own cost, store all data and processed data that it holds as PM, including data held under the previous PM service provider agreement.	✓
10.2	PM must, during the term of the SPA, transfer to the Commission copies of, or grant the Commission access to, the data or processed data (if requested by the Commission).	✓
11.1	PM must maintain data and processed data back-up arrangements, and a disaster recovery system. Both processes must comply with the operational requirements.	✓
12.4	PM must obtain from the SO: • a licence for the software for the term of the SPA to enable the PM to provide the services; and • a warranty that the software performs in accordance with the software specification.	✓
14	NB: The disengagement service provisions have been omitted from this table as they will only be applicable if the SPA expires or is terminated.	✓

16.1	PM must maintain adequate insurance cover for all normal commercial risks and potential liability it may incur under the SPA, regulations and rules.	✓

Operational Requirements – Schedule 2

Para	Obligation/Requirement	Compliance
1	The provider must obtain from the system operator a licence for appropriate software and warranty that the software performs in accordance with the specification.	✓
3.2	The provider must undertake all preventative, corrective maintenance and the implementation of enhancements outside business hours where possible.	✓
3.3	The provider must provide the Commission a monthly report detailing whether service levels were met during the month and if not, reasons for any failure.	✓
4.1	Backup copies of data must be taken at least daily and stored in a secure location. Copies of the latest version of the software must also be kept offsite. At least weekly, a backup copy of the data and software must be delivered and stored at an offsite location at least 100 kms from the premises used to provide the regular service.	✓
4.2	The provider must keep an up to date disaster recover plan, designed to recover in the event that the provider's site is inoperable.	✓
4.4	The provider must test the DR procedure every six months. The test must include: • restoration of the system to the remote location; • restoration and roll-forward to a known time; and • verification of system availability to an external user.	✓
5.1	The provider must ensure only approved and trained personnel operate the system. The system must have a framework for the management of user accounts.	✓
6.1	There must be a well defined and documented capacity planning strategy in place.	✓
6.2	There must be system management utilities implemented that will measure the capacity of the system, to show trends and therefore assist with predicting future capacity requirements.	✓
6.3	The provider must advise the Commission if transactional volumes threaten achievement of service levels.	✓
7.1	The provider must store the data securely and be able to provide it to the Commission on request within a reasonable timeframe.	✓
7.2	The system must maintain history for immediate access for seven years, or longer as agreed with the Commission, after which the information must be archived and available for retrieval on request.	✓
8.	The system must have an audit trail of all data input, confirmations delivered, notifications delivered and the delivery of information to other parties.	✓
9.1	The provider must provide a contact person who is available during business hours to assist with queries users. The provider must actively assist all users to resolve their issues. Response must be by an appropriately skilled person.	✓
9.2	The provider must maintain a register of all help desk requests, system faults and other operational incidents reported by each user during the previous 12 month period. The provider must notify users when incidents are resolved or time when expected to be resolved.	✓

	The provider must develop an incident management process for users to view all incidents and to report any faults. A summary of all incidents and their resolution times must be included in the monthly report on service levels.	
10	The provider must follow the change management procedure as set out in appendix I of this document and must be integrated into the internal change management processes with respect to the efficient management and reporting of progress.	✓
11.1	The provider must maintain close contact with users, be proactive and provide additional services and support to ensure that the system remains responsive, up to date and consistent with the needs of the industry.	✓
11.2	The provider must provide an escalation process for users in the event of either a major failure of the system extending beyond service level thresholds or in the event of continued user service issues.	✓
11.3	During periods when the system is not available the provider must liaise with the representative of the Commission and users not less than daily, including advising of expected times for the resumption of service.	✓
12	The provide must maintain and provide as a minimum: • an up-to-date functional specification against which the software can be audited as per the requirement in clauses 51 to 53 of the Electricity Governance Regulations (Regulations). The functional specification is the 'software specification' referred to in the Regulations. The functional specification and any subsequent changes are the property of the Commission; • a DR procedures manual that describes the procedure, possible impacts on users and their operation and instructions on what users will need to do for business continuity; and • sufficient technical documentation for business continuity in case of the loss of key personnel. This must include an operations manual.	✓
13.2	The provider of the software must implement, under the change control procedure, any changes necessary to give effect to any reasonable recommendations made by an auditor, with the objective of constantly improving services.	✓
13.3	The provider must comply with the audit requirements as set out in clauses 51, 52 and 53 of the Regulations with respect to conducting audits of the software, annually, on first-time use and for software changes.	✓

Additional Requirements – Schedule 4

Clause	Obligation/Requirement	Compliance
1	PM must provide: • A daily report (business days only) detailing key market data for the previous 8 days; • Publish binding branch and branch group constraints and disconnected nodes.	✓

Refresh Services – Schedule 5

Clause	Obligation/Requirement	Compliance
1	PM must agree a project plan for the refresh services by 10 August 2007.	✓
2.1	PM must supply the Commission with "the server".	✓
2.2	PM must: • deliver the server to the Wellington site; • deliver the documentation to the Commission; • install the server at the Wellington site; • install the software on the server; • carry out the acceptance test plan in relation to the system.	✓
3	PM must carry out the acceptance testing in accordance with this clause 3.	

Hosting and Support Services – Schedule 6

Clause	Obligation/Requirement	Compliance
2.1	PM must perform and comply with the requirements in the SPA and operational requirements when providing equipment maintenance services in respect of disaster recovery.	✓
2.2(d)	PM will, at all times, maintain a supply of replacement and spare parts necessary to effect equipment maintenance services or maintain hardware maintenance contracts with equipment manufacturers.	✓
2.2(e)	Unless otherwise agreed, the PM will use best endeavours to ensure that all replacement and spare parts provided by the PM will be new parts.	✓
3.1(a)	PM will install and host the system at the sites, including connection of the system to the PM's network provider of choice, and power supply.	✓
3.1(b)	PM will provide cabinet space at the sites capable of, and appropriate for, being used for the installation of the system.	✓
3.1(c)	PM agrees that the system will not be housed within a cabinet containing M-co's or a third party's equipment.	✓
3.1(d)	PM will ensure that the system is fully secured by security systems separate from other customers' and its own equipment using such measures as the Commission may reasonably require.	✓
3.1(e)	PM will provide the sites with robust, environmentally controlled support systems, which include alarm monitored air-conditioning systems, fire alarms and a centrally controlled security system with a reliability that is consistent with the ICT hosting services industry best practice. In particular, the PM will ensure that: • it provides electricity to the sites and to all components of the system; • the sites as a whole, or the section of the sites housing the system, have its main grid power supply backed by an uninterruptible power supply of sufficient capacity to power all devices it supports for a minimum of 15 minutes in the event of a main power failure; • the sites as a whole or the section of the sites housing the system must have its main grid power supply and UPS backed by a generator of sufficient capacity to power all of	✓

	the equipment it supports, with at least a 20% margin of excess capacity. • the sites will have an automatic water sprinkler; • the sites as a whole or the section of the sites housing the system will have sufficient heating ventilation and air condition systems to maintain the temperature and humidity with recommended ranges as specified by the manufacturers of the components of the system under normal operating heat outputs for all equipment that the sites or sites section houses. • no third parties other than those who have prior written approval from the Commission will have access to the system; • the PM will only access or deal with the system as is strictly necessary to comply with the terms of this agreement.	
3.2	PM will: • protect the system from radio or electrical interference, power fluctuations, abnormal environmental conditions, theft and other risks of loss or damage; • take reasonable steps to make sure the system is not affected by any virus, power surge/interruption, water damage, dust, shock or other negative factor; • monitor all alarms and hardware error logs, operating system errors, database error logs and application error logs in a proactive manner, and take corrective action where a fault is indicated; • manage as part of the system a full application and database backup every 24 hours, and a full operating system backup twice a week, which is to be secured offsite within 24 hours of the beginning of the backup.	✓
3.3	PM warrants that the environment of the sites is environmentally suited to house the system and that the PM will maintain that environment throughout the term of this agreement.	✓
3.4	PM will not move or relocate the system or the location of the sites except with the prior written approval of the Commission.	✓
3.5	PM will provide the Commission and its contractors with reasonable, safe access to the sites and the system.	✓
4.1	Upon PM becoming aware of any failure to provide services the provider will use reasonable endeavours to remedy the service failure and perform a root cause analysis to determine the cause. The provider will provide the Commission with a written report summarising the results of the analysis.	✓
5.1	The PM will use reasonable endeavours to obtain appropriate software support services from the system operator.	✓