

Electricity Commission

Pricing manager

Draft

Non-functional specification

Version 2.2

July 2006

This document reflects the draft Electricity Governance Rules 2003 (Rules) as at December 2005. Subsequent rule changes and transitional requirements have yet to be included.

Contents

REVISION HISTORY	4
NON-FUNCTIONAL SPECIFICATION	5
PRICING MANAGER.....	5
1. APPLICATION ARCHITECTURE.....	5
2. SERVICE LEVELS	5
2.1 TARGET LEVELS	5
2.2 MAINTENANCE	6
2.3 MONTHLY SERVICE LEVEL REPORTING.....	6
3. RECOVERABILITY AND BUSINESS CONTINUITY.....	6
3.1 BACKUP.....	6
3.2 UP-TO-DATE PLAN.....	6
3.3 RECOVERY TIME.....	6
3.4 DISASTER RECOVERY	6
4. SECURITY AND CONFIDENTIALITY	6
4.1 USER ACCOUNTS	6
5. CAPACITY.....	7
5.1 CAPACITY PLANNING STRATEGY.....	7
5.2 MANAGEMENT UTILITIES	7
5.3 EXCESS VOLUMES.....	7
6. DATA INTEGRITY AND ARCHIVE POLICY	7
6.1 DATA OWNERSHIP	7
6.2 HISTORY.....	7
7. AUDIT TRAIL/TRACEABILITY	7
8. HELP DESK.....	8
8.1 END-USER ASSISTANCE	8
8.2 INCIDENT REGISTER.....	8
9. CHANGE MANAGEMENT	8
10. IMPLEMENTATION AND TRANSITION.....	8
10.1 IMPLEMENTATION PLAN.....	8
10.2 MIGRATION PLAN.....	8
10.3 HISTORICAL INFORMATION	8
11. USER LIAISON.....	9
11.1 CLOSE CONTACT	9
THE VENDOR IS REQUIRED TO MAINTAIN CLOSE CONTACT WITH USERS, BE PRO-ACTIVE, AND PROVIDE ADDITIONAL SERVICES AND SUPPORT TO ENSURE THAT THE SYSTEM REMAINS RESPONSIVE, UP-TO-DATE AND CONSISTENT WITH THE NEEDS OF THE INDUSTRY.NOTIFICATION CHANNELS	9
11.2 ESCALATION PROCESS	9

11.3	DAILY LIAISON	9
12.	DOCUMENTATION.....	9
13.	SYSTEM AUDITS	9
13.1	SPOT AUDITS	9
13.2	AUDIT RECOMMENDATIONS	10
13.3	ANNUAL AND CHANGE AUDITS	10

Revision history

Version	Release date	Description
Draft 1	April 2005	Initial version for discussion by Senior Adviser Wholesale.
Draft 2.2	July 2006	Updated with after comments received from other project groups reviewing their own non functional specifications.

Non-functional specification

Pricing manager

1. Application architecture

The vendor must obtain from the system operator:

- a) a licence for the appropriate software owned by the system operator for the term of the agreement to enable the vendor to provide the services; and
- b) a warranty that the software licence from the system operator performs in accordance with the system specification and will enable the vendor to meet its obligations under the regulations and rules as pricing manager. The warranty must be expressed to be for the benefit of the Commission in pursuant of the Contracts (Privity) Act 1982.

The vendor must operate the software in accordance with the operation and hardware requirements specified by the system operator.

2. Service levels

2.1 Target levels

Measure	Target
Final prices published by 9:30am if no provisional price situation exists	97%
Provisional prices published by 10:30am if provisional price situation exists	97%
Final prices published within three hours of a system operator/grid owner fix to a provisional price situation	97%
IT processing time to publish final prices within five minutes of sending	97%
Number of price processing errors	0%

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

2.2 Maintenance

The vendor must undertake all preventative, corrective maintenance and the implementation of enhancements outside business hours where possible. For urgent corrective maintenance (to fix software faults that are threatening the service levels set out in this document), the vendor may, having notified the Commission, undertake maintenance at any time. Any such unavailability will count against service level targets.

2.3 Monthly service-level reporting

The vendor must provide the Commission a monthly report detailing whether service levels were met during the month and if not, reasons for any failure.

3. Recoverability and business continuity

3.1 Backup

Backup copies of data must be taken at least daily and stored in a secure location. The retention and recycle policy of backup media and the storage location must be agreed with the Commission. Likewise, copies of the latest version of the software should 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 100kms from the premises used to provide the regular service.

3.2 Up-to-date plan

The vendor must develop and keep up to date a disaster recovery plan as agreed with the Commission.

3.3 Recovery time

The disaster recovery plan must be designed to recover in the event that the vendor's site (that contains the system) is destroyed by fire, earthquake or otherwise. Recovery is required of the system within 36 hours following a major disaster.

3.4 Disaster recovery

The vendor must test the disaster recovery procedure prior to the commencement of operation and every six months thereafter. The test must include:

- a) restoration of the system to the remote location;
- b) restoration and roll-forward to a known time; and
- c) verification of system availability to an external user.

4. Security and confidentiality

4.1 User accounts

The vendor must ensure that only approved, trained personnel operate the system.

The system must have a framework for the management of operator accounts that enforces the password standard, account lockouts for unsuccessful logon attempts and session timeouts.

5. Capacity

5.1 Capacity planning strategy

There should be a well-defined and documented capacity planning strategy in place.

5.2 Management utilities

There should be system management utilities implemented that will measure the capacity of the system, to show trends and therefore assist with predicting future capacity requirements.

5.3 Excess volumes

The vendor must promptly advise the Commission if increases in transactional volume beyond the levels agreed in the service provider contract threaten the achievement of service levels. The Commission and the vendor must promptly review the capacity of the system and increase its capacity, if necessary, to maintain the service levels.

If the service levels cannot be met with current levels of capacity, and transaction and/or database volumes are less than those agreed with the vendor, the vendor will be responsible for taking such remedial action as is necessary to meet service levels.

Where transaction and/or database volumes exceed those agreed with the vendor, or rule changes have increased complexity to the extent that service levels cannot be met, then the vendor and the Commission will initiate the agreed change control procedures.

6. Data integrity and archive policy

6.1 Data ownership

All data collected, calculated and published as required in the functional specification is the property of the Commission. The vendor must store the data securely and be able to provide it to the Commission on request within a reasonable timeframe.

6.2 History

The system should retain history for immediate access for seven years after which the information should be archived (onto DVD or other such medium) and available for retrieval on request.

7. Audit trail/traceability

The system must have an audit trail of all data input, confirmations delivered, notifications delivered and the delivery of information to other parties. Audit information should include time, party, method and any other pertinent information to allow for full tracking from source to destination.

8. Help desk

8.1 End-user assistance

The vendor is required to provide a contact that is available during business hours to assist with user queries. The vendor must pro-actively assist users to resolve their issues.

8.2 Incident register

The vendor must maintain a register of all help-desk requests, system faults and other operational incidents reported by each user during the previous twelve-month period. The register should contain the user, time and details of the incident as well as the time and details of their resolution. The vendor will notify users when incidents are resolved or the time when they are expected to be resolved.

If an incident affects more than one user, the vendor should notify all participants.

The vendor should 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 should be included in the monthly report on service levels.

9. Change management

The vendor must follow the change management procedure as set out in Appendix I of this document. The change management procedure must be integrated into the vendor's internal change management processes with respect to the efficient management and reporting of progress.

10. Implementation and transition

10.1 Implementation plan

The vendor must provide an implementation plan that includes:

- key SDLC steps, deliverables and milestones;
- the identification of the project critical-path, any external dependencies and areas of uncertainty;
- regular reporting to the industry project team that will be set up to help the vendor;
- a robust testing strategy that includes sufficient program testing, system testing, acceptance testing by the industry and a market trial; and
- commencement dates and duration when resources will be required, especially from the industry.

10.2 Migration plan

The vendor must develop a migration implementation plan, agreed between the vendor and the Commission.

10.3 Historical information

The vendor will be required to load all the historical information contained in the current system into any new system. At the end of the term of the contract,

the vendor must deliver all the data in the system to the Commission, on request, within an agreed time-scale in an agreed format.

11. User liaison

11.1 Close contact

The vendor is required to maintain close contact with users, be pro-active, and provide additional services and support to ensure that the system remains responsive, up-to-date and consistent with the needs of the industry notification channels.

The vendor must develop formal notification channels to notify users, the representative of the Commission and the market administrator of outages and likely timeframes for restoration of service.

11.2 Escalation process

The vendor 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 Daily liaison

During periods when the system is not available, the vendor must also liaise with the representative of the Commission and users not less than daily, including advising of expected times for the resumption of service.

12. Documentation

The vendor must maintain and provide as a minimum:

- a) an up-to-date functional specification against which the software can be audited as per the requirement in the Regulations clauses 51 to 53. The functional specification and any subsequent changes is the property of the Commission;
- b) disaster recovery 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
- c) sufficient technical documentation for business continuity in case of the loss of key personnel.

13. System audits

13.1 Spot audits

The Commission may carry out audits of the records and procedures of the software within normal working hours on reasonable notice. The vendor of the software must give the auditor access to all relevant facilities, personnel, records and manuals, and provide to the auditor any additional information that the auditor reasonably considers is necessary to enable an assessment of whether or not the software continues to meet the criteria for approval.

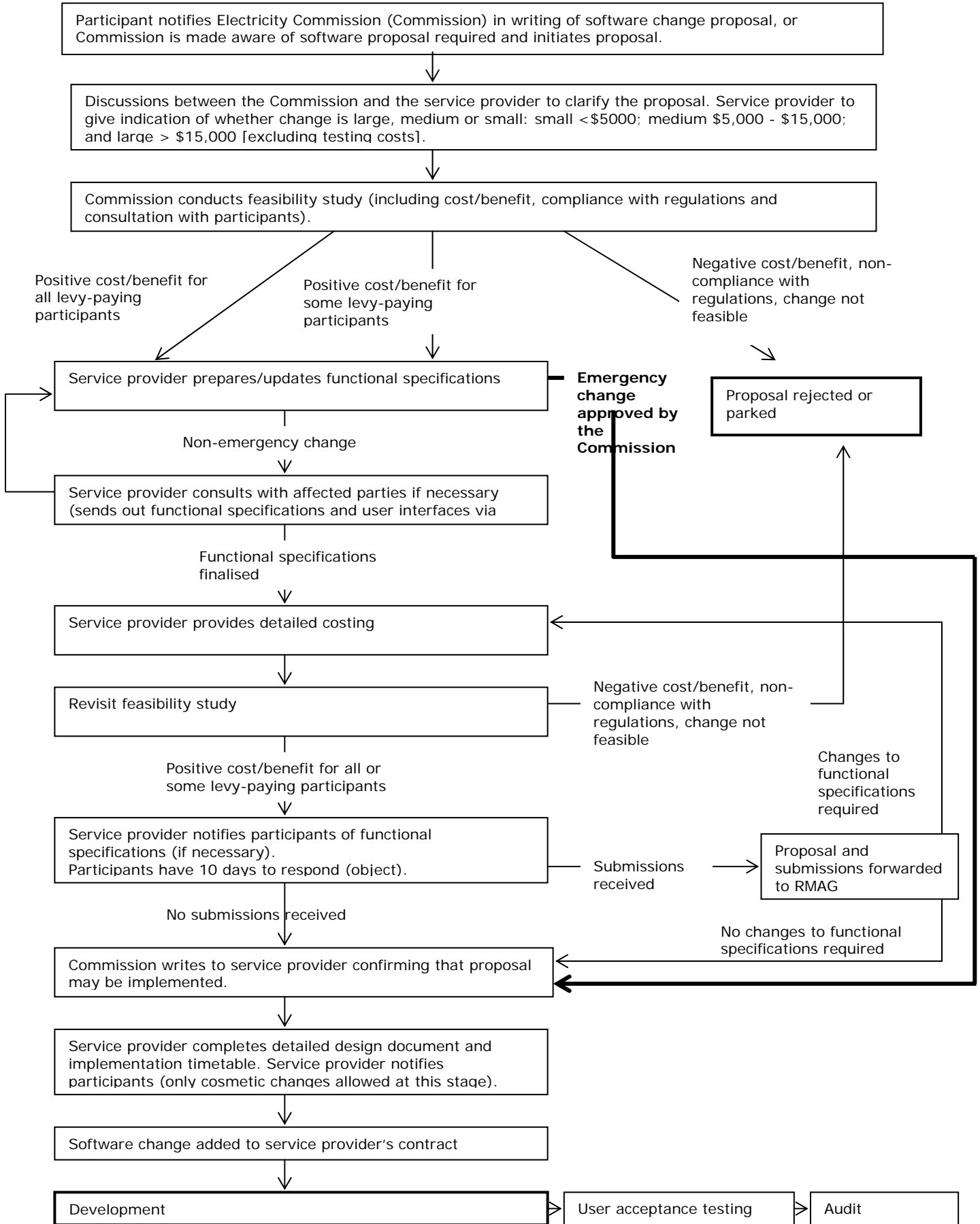
13.2 Audit recommendations

The vendor 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 Annual and change audits

The vendor must comply with the audit requirements as set out in the Electricity Governance Regulations 2003 (Regulations) clauses 51, 52 and 53 with respect to conducting audits of the software, annually, on first-time use and for software changes. The Regulations can be found at www.electricitycommission.govt.nz/rulesandregs/rules.

Appendix I—change control process



Appendix II—operational and hardware requirements (provided by the system operator)