Pricing manager

Schedule 2 –Non-functional specifications

30 October 2015

Market Services

Introduction

This document describes the non-functional features and attributes that the **Authority** requires of the pricing manager (PM).

This document is part of the pricing manager service provider agreement, and must be read in conjunction with that **agreement**, including the associated schedule 3 – Pricing **functional specification**.

Contents

Tables

1 Statutory Objective alignment

When providing the **services**, the **Provider** must provide those services in a way that assists the **Authority** to give effect to the **Authority's** statutory objective under section 15 of the **Act**. Nothing in this clause permits or requires the **Provider** to act in a manner that is inconsistent with the **Provider's** obligations under the **Act**, the **regulations**, the **Code**, elsewhere in the **agreement,** or any applicable law or regulation.

2 Application architecture

2.1 The **Provider** must obtain from the system operator:

(a) a licence for the SPD software owned by the system operator for the term of the **agreement** to enable the **Provider** to provide the **services**; and

(b) a warranty that the software licenced from the system operator performs in accordance with the system specification and will enable the **Provider** to meet its obligations under the Regulations and **Code** as pricing manager. The warranty must be expressed to be for the benefit of the **Authority** pursuant to the Contracts (Privity) Act 1982; and

(c) a stand-alone installation of the SPD software for analysis purposes

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

3 Websites, email addresses and branding

3.1 External communication with **users** and the public related to the **services** must include the **Authority's** approved logo, in a position on that communication type agreed with the **Authority**. This includes but is not limited to websites, templates for notices and **documentation** but excludes emails.

3.2 Website and generic email addresses relating to the **services** (except personal email addresses for the **Provider's** staff) are the property of the **Authority**. Where those addresses, including email addresses, use the **Provider's** registered domain, the **Provider** must cease using those addresses immediately if this **agreement** is terminated or expires.

For 12 months immediately after the agreement is terminated or expires or any transition period ends, whichever is the later, the **Provider** will forward any emails to the email address specified by the **Authority** and will post a message on the website directing viewers to a website address specified by the **Authority**.

4 Interoperability

4.1 Core Interfaces

Interfaces are documented in the **functional specifications**.

4.2 Extended System Interfaces

(a) All inbound and outbound interfaces to the **system** must be efficient and secure. The interfaces must be designed using loose-coupling principles to ensure that the interfaces can be modified or re-implemented with minimal disruption, and so that the **system** can be easily separated with minimal disruption and cost from the other market operations service provider (**MOSP**) roles provided by the **Provider** to enable contestability of the MOSP roles.

(b) All interfaces must be documented in the **functional specification** including source, target, format, mechanism and frequency.

5 Service level requirements

5.1 The pricing manager process is a daily process as set out in the **Code** and **functional specification**. The **Code** sets out the minimum service levels however the parties may agree higher service levels in this **agreement**

5.2 Additional service level targets

Timely publication of provisional and interim prices is an important element of the **services**. The **Provider** is often in the position to publish prices substantially earlier than **Code** defined deadlines. Therefore the **Provider** will meet the following price publication service level measures:

(a) interim prices published by 09:20 am, provided there is no provisional price situation, and the input information has been received by 07:30 am

(b) on a weekday, provisional prices published before 10:20 am, provided the input information has been received by 07:30 am

(c) on a weekend day, provisional prices published before 09:20 am, provided the input information has been received by 07:30 am

(d) a price that has been published as provisional will be republished as interim on the same day that a revised data notice is received, provided that a notice is received before 3:00 pm.

5.3 Additional service level measures.

(a) no more than one late publication in a rolling three month period for each of the targets in paragraph 4.2

(b) zero price processing errors in a calendar month

(c) an average time to recommend to the **Authority** a resolution to a pricing error claim, of two business days over a rolling 12 month period. This target takes into account the time required to obtain additional information from the system operator, participants and the Authority, and to undertake legal review of the **Provider's** recommendation.

(d) no more than six months between tests of disaster recovery plans (standby systems for standalone SPD, and testing back-up pricing at Transpower)

(e) zero unplanned **system** outages, and all planned outages coordinated with the system operator

(f) zero breaches of the service management levels contained in paragraph 11.2

(g) all data specified in paragraph 9.2 is provided to the Authority by the agreed timeframes

5.4 Service levels reported monthly.

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

Table 1: Service levels reported monthly

Measure	Report
Number of interim or final prices published late	Number for the reporting month Number for the rolling 12 months (the current and 11 previous months)
Number of price processing errors	Number
Average time to recommend to the **Authority**, a resolution to a price error claim	Days
Number of price error claims received	Number
Disaster recovery and backup obligations	Achievement
Total outages both planned and unplanned	Number unplanned; Number planned; Number planned without system operator coordination
Service management targets	Count of incidents of each severity level and number of targets not met
Number of data files provided to the **Authority** late	Number

5.5 Maintenance

The **Provider** must undertake all preventative, corrective maintenance and the implementation of enhancements outside **business hours** where possible.

For urgent corrective maintenance (to fix **system** faults that are threatening the service levels set out in this document), the **Provider** may, having notified the

Authority, undertake maintenance at any time. Any such unavailability will count against service level targets.

6 Recoverability and business continuity

6.1 Backup

Backup copies of all **data** and **processed data** must be taken at least daily and stored in a secure offsite location. Copies of the latest version of the **software** must also be kept offsite. At least weekly, a backup copy of the **data**, **processed data** and **software** must be delivered and stored at an offsite location at least 100km from the premises used to provide the regular **services**.

Alternatively, backup copies of the **data** and **processed data** can be stored in a cloud based facility, subject to approval by the **Authority** and compliance with Government Chief Information Officer (GCIO) standards for cloud based computing services.

The **Provider** must have a plan in place to restore backup **data**, **processed data** and recover lost **data** up to the actual time of restoration. The plan must be available to the **Authority** as part of the **documentation**.

6.2 Business continuity plan

The **Provider** must develop and keep up to date a business continuity plan (**BCP**). If the **system** includes a cloud based computing environment, then the **Provider** must provide assurance that the cloud provider maintains a fault-tolerant environment that meets the **Authority**'s required service levels or can demonstrate a failover of the environment to another cloud based computing environment.

The BCP must:

(a) be aligned with the current version of ISO 22301 or NFPA1600 or another recognised standard for business continuity planning;

(b) be regularly tested (at least annually, but may be more frequently if required) and the results of each test reported to the **Authority** in the next monthly report;

(c) be provided to the **Authority** before the initial BCP or any changes are implemented, and the **Provider** will consider any feedback provided by the **Authority**;

(d) contain contact details for the **Provider** nominated contact person, including backup contacts. The contact details are to include multiple methods of contact including physical location and access details for all physical locations where the contact may be located when providing the **services**.

6.3 Recovery time

The BCP must include a disaster recovery plan designed to recover the **system** in the event that the **Provider's** site (that contains the **system**) is inoperable. A real-time disaster recovery **system** must be available to commence **services** within a period of two hours from failure of the production **system** and must ensure that no more than ten minutes of pre-failure **data** or **processed data** is

lost in the event of the production **system** failing, and must ensure the lost **data** is restored with the cooperation of **users**.

6.4 Disaster recovery testing

The **Provider** must test the disaster recovery plan and disaster recovery **system** prior to the commencement of operation and every six months thereafter. The test must include:

(a) obtaining the prior written approval from the **Authority** for the date and time of a disaster recovery test;

(b) activation of the disaster recovery **system** at the remote location;

(c) transfer of the production environment to the disaster recovery **system** for a period of at least two **business days** at the date and time agreed under (a) above;

(d) testing of files, updates and transfers; and

(e) transfer of the production environment back to the production **system** at the date and time agreed under (a) above.

The **Provider** must provide a written report to the **Authority**, in the next monthly report after completion of the disaster recovery test, of the results and ensuing actions.

7 Security and confidentiality

7.1 User accounts

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

7.2 Authority Policies

The **Provider** must comply with the **Authority** policies as updated from time to time, related to information and security where those policies and updates are provided by the **Authority**. The policy outlines the **Authority's** expectations for managing personnel, physical and information security. The **Provider** may provide feedback to the **Authority** about the application of those policies. If the application of those policies will result in changes to the **services** or impose material costs on the **Provider**, the **Provider** may initiate the change management process to implement those changes.

7.3 Confidentiality

The **Provider** must ensure that all **data** and **processed data** remain confidential to the **Provider**, the **Authority** and the participant that provided the **data** unless the **services** or **Code** explicitly require the **Provider** to publish or release the **data** or **processed data**

7.4 Security and confidentiality incidents

Security and confidentiality related events will be reported to the **Authority** and a service management event created in GoToAssist according to the Service Management Procedure.

8 Capacity

8.1 Capacity planning strategy

The **Provider** must have a well-defined and documented capacity planning strategy in place to ensure that the **system** always maintains enough capacity for the predicted amount of **data** and **processed data** and processing requirements plus a margin to ensure the service levels are always met.

8.2 Management utilities

The **Provider** must use system management utilities that will measure the capacity of the **system**, to show trends and therefore assist with predicting future capacity requirements.

8.3 Excess volumes

The **Provider** must promptly advise the **Authority** if increases in transactional volume beyond the levels agreed threaten the achievement of service levels. The **Provider** 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, the **Provider** 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 **Provider**, or **Code** changes have increased complexity to the extent that service levels cannot be met, then the **Provider** and the **Authority** will initiate the agreed change control process if any changes to the **services**, **system** or **fees** are required.

9 Data management

9.1 Data ownership

The **Provider** must store **data** and **processed data** securely, manage **data** and **processed data** according to a lifecycle agreed with the **Authority**, and provide it to the **Authority** via SFTP or a secured online portal as agreed. The rights around use and ownership are defined in clause 9.7 of the **agreement**.

Data and **processed data** must not be used by the **Provider** for any unauthorised use.

9.2 **Data** provided to the **Authority**

(a) The **Provider** will send to the **Authority**:

(i) final pricing cases sent through the WITS system – as they are generated (at least per day but usually 2 or 3 per day) .

(ii) a file containing the status of the prices daily

(b) Unless agreed otherwise this **data** and **processed data** will be sent via SFTP.

(c) If the **data** being provided will be late or missing, or there is an outage or disruption (planned or unplanned) to the system providing the **data**, the **Provider** will inform the appropriate **Authority** representative:

(i) as soon as practicably possible for unplanned outage, late or missing **data**

(ii) at least one **business day** prior to a planned outage.

9.3 Archiving and restoring **data** and **processed data**

The architecture must allow historic **data** and **processed data** to be archived and restored without impacting the operation of the **system**.

9.4 History

The system must retain **data** and **processed data** for immediate access for a minimum of seven years, after which time the information may be permanently archived via an **Authority**-approved mechanism and provided to the **Authority** with appropriate metadata attached as agreed by the **Authority**.

10 Audit trail/traceability

The **system** must maintain an audit trail of all **data** and **processed data** input, added or changed, confirmations delivered, notifications delivered and the delivery of information to **users**. Audit information must include time, **user**, method and any other pertinent information to allow for full tracking from source to destination.

11 Service management

11.1 Industry standard

The **Provider** must employ best practice such as ITIL (Information Technology Infrastructure Library) for service management, including robust quality assurance processes.

11.2 Service management standards

The following service management standards set the minimum standards for fault reporting and restoration of the **services**. As the **Provider** would be both performing the **services** and supporting the **system** the service management standards apply equally for internal and external users of the **system**.

The service management standards are show in Table 2.

Table 2: Service management standards

Severity level of Fault	Definition	Service Level response and response time

Severity level of Fault	Definition	Service Level response and response time
1	**Business Critical Failures:** An error in, or failure of, the **system** that: a) materially impacts the operations of the **service**; b) prevents necessary work from being done; or c) disables major or critical functions of the **system**.	**Level 1 Response:** Acknowledgment of receipt of a support request within 15 minutes. **Level 2 Response:** Appropriately skilled person to respond within 1 hour of the support request. **Level 3 Response:** The **Provider** shall work on the problem continuously and implement a solution within 6 hours of receipt of the support request. If the **Provider** delivers a solution by way of a workaround reasonably acceptable to the user, the severity level assessment shall reduce to a severity level 2 or lower.
2	**System Defect with Workaround:** a) a critical error in the **system** for which a work-around exists; or b) a non-critical error in the **system** that affects the operations of the **user** service.	**Level 1 Response:** Acknowledgment of receipt of a support request within 2 hours. **Level 2 Response:** The **Provider** shall, within 1 **business day** after the Level 1 Response time has elapsed, provide an emergency fix or workaround which allows the **user** to continue to use all functions of the **system** in all material respects. **Level 3 Response:** The **Provider** shall provide a permanent fix as soon as practicable and no later than 20 **business days** after receipt of the support request.
3	**Minor Error:** An isolated or minor error in the **system** that: a) does not significantly affect **system** functionality; b) may disable only certain non-essential functions; or	**Level 1 Response:** Acknowledgment of receipt of the support request within 1 **business day**. **Level 2 Response:** The **Provider** shall provide a permanent fix within 40 **business days** after the Level 1 Response time

Severity level of Fault	Definition	Service Level response and response time
	c) does not materially impact the **user's** operation of the **system**.	has elapsed.
4	**Non-disruptive error** An isolated or minor error in the **system** that has agreement from the **Authority** and the **user** that reports the error to leave the fix until the next convenient release	**Level 1 Response:** Acknowledgment of downgrade of severity to level 4 within 1 **business day** of downgrade. **Level 2 Response:** The **Provider** shall provide a permanent fix at the next convenient opportunity as agreed with the **Authority**.

11.3 Communication

The **Provider** must provide an escalation process for **users** in the event of either a failure of the **system** extending beyond service level thresholds or in the event of continued **user** service issues.

For severity 1 and 2 incidents the **Provider** must also liaise with the representative of the **Authority** and **users** not less than daily, including advising of expected times for the resumption of the **services**.

11.4 Incident reporting

A summary of all incidents and their resolution times must be included in the monthly report on service levels.

The **Provider** will provide the **Authority** access to view (as a minimum) relevant entries on the GoToAssist system change and issue register

12 Technology currency

12.1 The **Provider** will ensure all infrastructure hardware is kept current and up to date, and that all infrastructure operating systems and other supporting software are maintained at current supported versions. The **Provider** will ensure that vendor support is in place continuously for all aspects of the systems

12.2 The **Provider** will provide to the annual auditor, confirmation that all infrastructure is current and that vendor support is in place for the coming year

12.3 The **Provider** will not transition any infrastructure to a cloud based solution (or any non-**Provider** owned solution) without first obtaining the **Authority's** approval. This provision is to ensure that as technology develops in the future, the government standards for data integrity and security current and in development at the time will be taken into account as part of the development of the solution

13 Changes to the services or system

13.1 Change control

For changes to the **services** or the **system**, the **Provider** must follow the change control process as set out in Appendix A of this document. The change control process must be integrated into the **Provider's** internal change management processes with respect to the efficient management and reporting of progress.

13.2 Which form of document is used to record a change.

All changes to the **services** or **system** must be agreed in writing by the **Provider** and the **Authority**, and that agreement will be recorded in either a change request (CR) or a system delivery agreement (SDA). Generally a CR will be used when the change is of low complexity, low impact or low cost. A CR will be used if:

(a) the cost of the change is below $250,000; and

(b) less than 10% of the functionality of the **system** or **services** is being altered; and

(c) less than 10 % of the source code of the **software** is being altered; and

(d) there is low probability of the scope or the charge to the **Authority** changing as the project progresses; and

(e) the change is not a material part of a major **Authority** policy implementation; and

(f) a formal warranty period is not required; and

(g) there is no material impact on the participants to implement the change in their systems.

These are general guidelines and the **Provider** and the **Authority** may agree to use a CR if these thresholds are exceeded. However the **Provider** and the **Authority** must give explicit consideration to using a SDA, and if a CR is used, the reasons for doing so must be recorded in the CR.

The **Provider** and the **Authority** may agree to use a SDA for changes below these thresholds.

13.3 Industry standard

The **Provider** must employ industry standard software engineering practices including robust quality assurance processes. Any methodology must cover the whole system development lifecycle (SDLC) in the development and maintenance of software.

13.4 Flexibility

The **software** must be designed for flexibility to ensure changes to functions, as a result of user, participant or **Authority** requests and **Code** changes, can be made efficiently and cost effectively. The **system** must have a modular design which allows changes to specific business processes to be isolated to those areas only with minimal impact on other parts of the **system** or external interfaces.

The **Provider** must be able to develop custom reports, both one-off and for regular delivery, on request from the **Authority**.

14 Design consultation

The **Provider** must provide input to the design process for the **Authority's Code** amendment initiatives to promote efficient **Code** design. This is limited to a high level assessment of initiatives proposed by the **Authority**, and will require the **Provider** to proactively keep up to date with the **Authority**'s initiatives .

Consequent changes to the **services** will be dealt with using the change control process, and therefore detailed input will be provided as part of the change control process, and is not required as part of the design consultation.

The **Provider** must respond constructively to requests for change from the **Authority** or other market operation service providers (MOSPs) by assessing the potential impact and cost and engaging in dialogue to achieve efficient design.

The **Provider** must proactively propose any changes that it perceives will improve efficiency of delivery of the **services**.

15 Audits under clause 3.17 of the Code

Audits required under the **Code** must be carried out in accordance with the software audit guidelines in Appendix B.

16 Government standards

16.1 The **Provider** must demonstrate alignment with the Records Management and Security Standards as referred to in the GEA-NZ standards.

16.2 Historical information

The **Provider** will be required to maintain all the historical **data** and **processed data** contained in the system immediately prior to 1 May 2016 for use in providing the **services** relating to periods prior to 1 May 2016.

16.3 The **Provider** will provide and keep updated an ICT operations risk assurance plan, consistent with the recommendations of the GCIO. This plan is to be included in the **documentation**.

17 User liaison

17.1 Operational Relationship

The **Provider** is required to maintain close contact with the **Authority**, be proactive, provide advice on future functionality and ensure that the **system** remains responsive, up to date and consistent with the needs of the industry.

The **Provider** will allow reasonable access for **Authority** staff to become familiar with the **Provider's services**. This may involve short term secondments,

shadowing the **Provider's** staff, including developers and **system** support staff, or spending time and discussing the **services** with the **Provider's** staff while the **services** are being performed.

17.2 Participant Relationship

The **Provider** is required to receive and process pricing error claims. This requires as a minimum,

(a) liaison with participants, the **Authority**, the system operator, other MOSPs, and the grid owner during business hours for initial discussion, reporting, investigation and resolution to pricing error claims and the resultant impact on other MOSPs;

(b) liaison with participants and the **Authority** in the event of a delay to final pricing; and

(c) provision, receipt and maintenance of price error claim forms.

17.3 User group

The **Provider** will set up a user group for participants that use the **services**. The user group will be open to all participants including the system operator and the **Authority**. The user group will meet regularly, at least biannually. The **Provider** may combine the user group meetings with similar meetings from the **Provider's** other market operations service provider roles.

17.4 User satisfaction survey

The **Provider** is required to develop, have approved by the **Authority**, and distribute a survey of all **users** that analyses the satisfaction levels of the **service** provision. The results must be consolidated and the report must include the actions the **Provider** proposes to take to resolve any unsatisfactory results. The report must be completed and provided to the **Authority** annually before the end of March, in a form agreed by the **Authority**.

17.5 Key stakeholder meetings

The **Provider** will conduct face to face stakeholder meetings with key stakeholders. These meetings will be conducted at least annually. The **Provider** may conduct additional stakeholder meetings at any time. The **Provider** and the **Authority** will agree the key stakeholders to be met and may agree to combine meetings with similar meetings required from the **Provider's** other MOSP roles. The **Provider** will report the outcomes of these meetings to the **Authority**.

18 Industry information

18.1 The PM will publish daily pricing and weekly reports containing summary information and graphs. The contents and format of these reports are to be agreed with the **Authority**. As at the **commencement date** the format daily report will be the same as that published on or about 25 May 2015 (the day the proposal was submitted).

18.2 These reports will be sent to subscribers and available to non-subscribers on a relevant website.

18.3 The purpose of these reports is to provide relevant information to participants and potential participants to help inform their market and trading decisions.

19 Training

19.1 The **Provider** must make available structured Industry training beyond basic use of **software**, at the cost of the **user**. The training course will cover:

(a) a brief introduction to the **Provider's** role and its place in the 'big picture'

(b) a reasonably thorough review of key role processes

(c) an overview of important **user** obligations relevant to each role

(d) introduction to, and basic use of each role's participant **user** interface

(e) practical hands-on experience in a UAT type environment

(f) how to contact the **Provider's** team both for day to day operational issues and to engage in the development of the **systems**

19.2 The **Provider** will provide basic training materials on line at no cost to the **user** by 1 October 2016.

19.3 The **Provider** will provide online help for the PM related functions on WITS to include full and detailed information about each aspect of the system including:

(a) data definitions

(b) setup information

(c) FAQs

(d) **system user** guide

(e) troubleshooting guide

(f) contact information, and

(g) business continuity information.

This includes a searchable help system allowing **users** to easily locate the content they need. All of this material will be geared towards new **users** but will also be relevant to existing **users**.

19.4 The **Provider** must present to two one-day **Authority** initiated industry forums in Wellington per annum at no cost. The details of the forum and the material to be presented will be agreed at the monthly meeting at least one month prior to the scheduled forum date.

20 Documentation

20.1 Required documentation

The **Provider** must develop, maintain and provide as a minimum to the **Authority**:

(a) an up-to-date **functional specification** against which the **software** comprised in the **system**, including input and output interfaces, can be

audited as per the requirement in clauses 3.17 and 3.18 of the **Code**, and to assure the **Authority** that additional requirements are being provided correctly. The **functional specification** is the 'software specification' referred to in the **Code** as well as the document in which additional requirements requested by the **Authority** is recorded. The **functional specification** and any subsequent changes are the property of the **Authority**;

(b) a **user manual** and online help facilities to enable new **users** to configure their systems correctly and access the **system**, to the level of detail agreed with the **Authority**. The **user manual** must provide sufficient detail for new **users** to locate and use all the relevant functions. The **user manual** must include a troubleshooting guide, frequently asked questions and information on where and how to seek further help;

(c) backup procedures describing alternative methods for the submission and delivery of **data** and **processed data** as required by the **Code**;

(d) a business continuity process manual that describes the procedure, possible impacts on **users** and their operations, and instructions on what **users** will need to do for business continuity; and

(e) 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.

(f) up to date, technical documentation that details the hardware, infrastructure and **software** configurations and settings. The purpose of this documentation is to enable the **Authority** to set up the **software** on a system with another provider without delay if this **agreement** is lawfully terminated, and to ensure the contestability of the pricing manager role at the natural expiry of this **agreement**.

(g) business process information that covers all business processes required to perform the **services**, not just **software** based **services**.

20.2 Access to documentation

(a) All **documentation** must be readily accessible at all times to **Authority** staff through the **Provider's** 'Provider Information Portal' (PIP). The **Provider** will ensure the PIP has the ability for the **Authority** to make copies of any **documentation** for its own use. The **Authority** will only use the **documentation**, including any copies, in accordance with the requirements of the relevant clauses of this **agreement** and the **Documentation Licence Agreement.**

(b) The **Provider** must annotate any contents of the **documentation** that it considers may allow or facilitate unauthorised access to the **systems** if it was released by the **Authority**. The **Authority** acknowledges that annotated documentation is sensitive and the security of the **system** may be vulnerable if the **Authority** does not keep the annotated portions of the **documentation** confidential.

20.3 Software source code

(a) The **Provider** will supply to the **Authority** a full copy of the **software** source code, including any associated scripts, on 1 May 2016.

(b) The **Provider** will supply to the **Authority** an updated copy of the **software** source code, including any associated scripts, whenever the **software** or scripts are changed

(c) The **Provider** will supply to the **Authority** a full copy of the **software** source code, including any associated scripts, on 1 November 2016, and every six months thereafter, and whenever requested by the **Authority**

21 Upgrade and improvement services

The **Provider** will provide Upgrade and improvement services to the **Authority**. These services are intended to advance **Authority** initiated programs and implement **Authority**, **Provider** or participant requested changes to the **Provider's systems** or **services**.

In managing the Upgrade and improvement service program, the **Authority** and the **Provider** will participate in a joint development process. This process will be governed by its own terms of reference and will regularly engage in joint development process (project coordination) meetings. The joint development process will, at a minimum, manage multiple project resource conflicts and priorities, and will agree a joint project lifecycle process. The parties agree that the project deliverables and project artefacts defined and agreed as part of the joint project lifecycle process from time-to-time will form part of the **agreement** deliverables.

22 Third party innovation

22.1 The **Provider** may offer related services to **users** that use the **software**, **system**, **data** or **processed data**.

22.2 The **Provider** must ensure that any advice it gives or services it offers to **users** as part of **user** innovation is, to the extent possible, consistent with enabling the **user** to comply with their obligations under the **Code**. The **Provider** must advise any recipient of the third party innovation in writing that the responsibility for ensuring compliance with the **Code** lies with the participant.

22.3 When offering or providing third party innovation, the **Provider** must contract directly with the **user**. The **Authority** will not be liable for any costs associated with providing the third party innovation that the **Provider** may incur and will not be liable for any loss, claim, demand, damage, cost, expense or liability in connection with the third party innovation.

22.4 In providing the third party innovation, the **Provider** must not disclose any **data**, **processed data**, **documentation** or other related information that is not normally available to the client that is receiving the third party innovation. No services may be offered that result in **data** being reported to the client that the client could not access through standard reporting.

22.5 Unless paragraph 22.6 applies, all additional functionality that a client requests the **Provider** to develop:

(a) may be for the exclusive use of the **user** for a period of no more than six months

(b) must be available for all **users** to use, once any exclusivity period ends

(c) must follow the change control process and be audited in accordance with Part 3 of the **Code** and documented in the **functional specification**

(d) is part of the **software**, **system** and/or **documentation** as appropriate

22.6 Any additional functionality that a client requests the **Provider** to develop and is for the continued exclusive use of the **user**:

(a) must be external to the **services** and the **system**, and will not be recorded in the **functional specification** or included in the **Authority's** software audits:

(b) must not detract from **system** performance or negatively impact any other **user's** use of, or access to, the **system**:

(c) will not be considered in any subsequent changes made by the **Authority** to the **services** or the **system**.

22.7 If any additional functionality developed by the **Provider** for exclusive use by a **user** requires modification or testing as a result of an **Authority** requested change to the **services**, such modification and testing must not negatively impact the delivery of **Authority** requested changes to the **services**.

22.8 If the **Provider**, or a client of the **Provider**, identifies any issue or defect with the **system**, or if a **user** requests any **system** enhancements, the **Provider** must pass that information on to the **Authority**. The **Authority** will prioritise any issue, defect or enhancement in the same way as it does others coming from any other **user**.

22.9 When developing additional functionality for a client, the **Provider** is responsible for making the client aware of the impact of sections 22.5, 22.7, and 22.8.

23 Performance management

23.1 Establishing a joint goal setting framework

The **Provider** will work with the **Authority** to develop a meaningful and workable joint goal setting framework. This will be focused on the **Provider's** service provision activities or functions that will have the greatest impact on supporting the **Authority's** priorities for any given period and also which advance the **Authority's** statutory and organisational objectives. These goals may be short term focussed, or alternatively, span over several years.

Once established, the **Provider** and the **Authority** will regularly review progress at the monthly meetings. Annually, the **Provider** and the **Authority** will formally discuss results and set new or confirm ongoing goals and measures for the coming year

23.2 Timing for performance management components

Activity	When
Establish goals	Annually in August
Establish measurement system	Annually in August
Self assessment and **Authority** review	Monthly meetings
Formal review and recognition	Annually in July or August

23.3 Systems roadmap

Annually the **Provider** will prepare an up-to-date strategic plan (road map) for the PM role. While this process will be led by the **Provider** the plan will be developed and reviewed in close collaboration with the **Authority**. The road map process is intended to allow the **Provider** or the **Authority** to address issues of a longer term strategic nature

24 Provider contacts

The **Provider** will advise the **Authority** of all changes in operational and management personnel used to provide the **services**, including contact details for new personnel. The **Provider** will provide to the **Authority**, and keep up to date, the **Provider's** most current organisational structure for personnel used to provide the **services**

25 Monthly Report

The Provider will provide a monthly report by the 10th business day of the month, reporting on the monthly activities for the previous calendar month. The monthly report will be published by the **Authority**, should not include specific reference to any **users**, and will contain:

(a) a report on the status of the **functional specification**

(b) the report on service levels as specified in paragraph 5.4

(c) a summary of PM service activities and relevant market information

(d) confirmation that the backup requirements have been met or if not, the reasons for not

(e) details of any BCP or disaster recovery testing performed

(f) details of any security breaches and attempts at breaching the security of the **systems**

(g) measure of the **system** capacity and utilisation of that capacity

(h) a summary of all service management incidents and their resolutions

(i) a summary report of the status of all CRs and SDAs

(j) a summary of all design consultation provided including the number of chargeable hours for each staff member for which the **Authority** will be charged

(k) details of the number of hours used for Upgrade and improvement services for each resource for the month, and the year to date totals

(l) a summary of any user group meetings held and the items discussed

(m) a list of any key stakeholder interviews planned for the coming month and a report of discussions and resultant actions from any key stakeholder interviews conducted

(n) the status of any **Provider** initiated audits performed during the month, and the status of action on recommendations from previous **Provider** or **Authority** initiated audits

(o) breaches of the **Act**, regulations, **Code**, or **agreement**

(p) events that may highlight an area where a change to the **Code** may need to be considered

(q) any other matters reasonably required by the **Authority**

25.2 Combining Monthly reports

The **Provider** may combine monthly reports for multiple MOSP roles it holds. A combined report must contain all the required information for each role

26 Meetings

26.1 Monthly operational meeting

Operational representatives from the **Provider** and the **Authority** will meet monthly, generally towards the end of the month. These meetings should not be cancelled but may be moved up to one week to suit availability of staff. Alternates may attend in place of unavailable staff, but those alternates must familiarise themselves with the discussion topics prior to the meeting. The purpose of these meetings is to build and maintain an excellent working relationship between the operational teams. Standing agenda items will include:

(a) review the issues register

(b) review any open change requests

(c) update and inform the operational teams of progress on any projects managed outside the operational teams

(d) discuss any items of interest from the monthly report

(e) discuss progress on any actions resulting from a **Provider** initiated or **Code** mandated audit.

26.2 Joint development programme (project coordination) meeting

Project and operational management representatives from the **Provider** and the **Authority** will meet regularly, but no less often than two monthly. The purpose of these meetings is to:

(a) review and manage resource allocations for all changes that are in progress or are shortly to start, including managing prioritisation requests from requestors of change

(b) coordinate projects that involve multiple MOSPs and/or the system operator

(c) review the use of resources against available Upgrade and improvement services hours, and agree if unused hours will be transferred to the following financial year

26.3 Regular relationship managers meeting

Relationship managers or executives will meet regularly but no less often than two monthly. The purpose of these meetings is to:

(a) ensure there is open dialogue and no surprises between the **Provider** and the **Authority**

(b) ensure there is an excellent working relationship between the **Provider** and the **Authority**

(c) address any escalated issues

26.4 Annual meeting

Representatives from the **Provider** and the **Authority** will meet annually to:

(a) review the previous year's performance

(b) set any new or changed **performance measures**

(c) discuss the planned number of hours, project programme and project priorities for the Upgrade and improvement services

(d) discuss technology currency and vendor support arrangements

(e) review the **Provider's** alignment with the **Authority's** statutory objective, and agree any actions for the coming year to increase alignment

(f) review the **Provider's** plan for **Provider** funded enhancements, **system** maintenance and infrastructure lifecycle maintenance

(g) review the ICT operations risk assurance plan and the systems roadmap

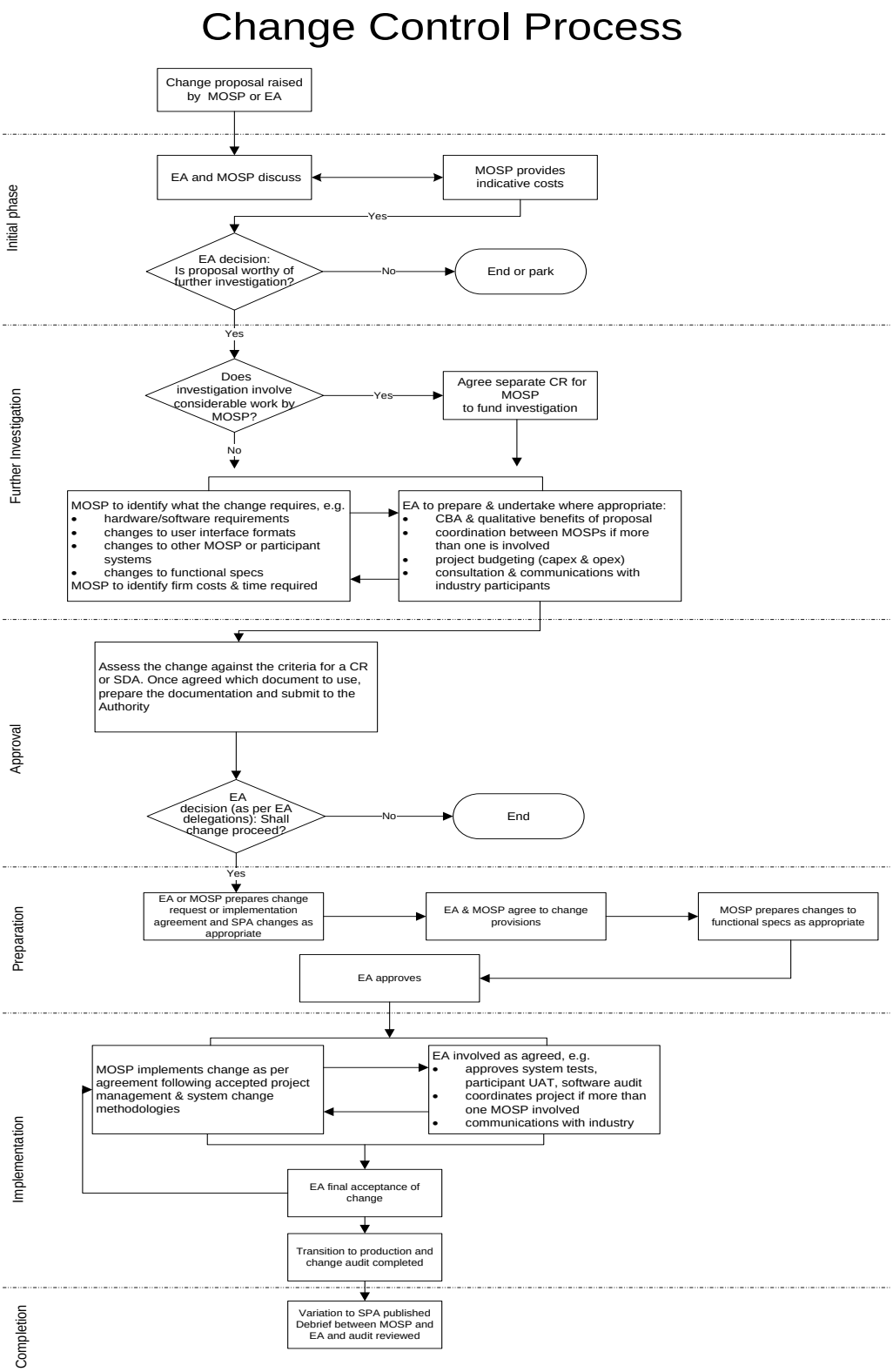
(h) for any year in which **Provider** initiated audits (or any part thereof) will be performed, set the scope of the audit(s)

26.5 Combining meetings from different roles

The **Provider** and the **Authority** may agree to combine the above meetings with similar meetings from the **Provider's** other MOSP roles.

Appendix A Change control process

A.1 If the change proposal is identified by the **Provider**, an initial assessment of materiality and cost is made. If the materiality and cost is low, or the change is to remedy a failure of the **Provider** to meet the terms of this **agreement**, then the change is at the **Provider's** cost. The **Provider** may consult with the **Authority** as part of this initial assessment process.



Appendix B Audit guidelines

(For audits under clause 3.17 of the **Code**)

B.1 Purpose of this appendix

The purpose of this appendix is to provide the **Provider** with guidelines for deciding when **software** audits are required. Clauses 3.16 to 3.18 of the **Code** set out **Provider's** responsibilities for **software** audits. This appendix considers in more detail what should be the extent of an annual audit, exactly what types of **software** changes should require a software audit and how **software** changes that do not require auditing should be treated.

B.2 Definition of software

The term "software" is defined in Part 1 of the **Code**, and for the purpose of this appendix is interpreted to mean the application **software** that the **Provider** uses to deliver the functions defined in the **functional specification** that forms part of this **agreement**.

B.3 Purpose of software audits

The purpose of software audits is to give assurance to the **Authority** that the **software** delivers the functions described in the **functional specification** and that it conforms to the **Code** and the Electricity Industry Act 2010 (**Act**).

B.4 Code mandated Audits

In accordance with clause 3.17 of the **Code**, there are three types of audit that the **Provider** is subject to:

(a) an initial audit before any **software** is first used by the **Provider** in connection with the **Code**, and Part 2 and subpart 1 of Part 4 of the **Act**

(b) an annual audit (within 1 month after 1 March in each year) of all **software** used by the **Provider**

(c) an audit of any changes to the **software** or the software specification, before it is used by the **Provider**.

The following software audit guidelines relate items (b) and (c) only.

B.5 Software Change Audit

(a) **Software** and **functional specification** changes that require auditing

All changes to the **software** must be implemented by following the **software** change control process as specified in this **agreement**.

All changes to the **software and functional specifications** must be audited, except bug fixes and enhancements that fall outside the scope of the core functionality as described in section B.10 "Not-auditable changes" below. Every change must be incorporated into a new release of the **software**. Details of each new release must be documented (as release notes) and published to all participants prior to its deployment into production.

Each release must be uniquely identified by its own release number. It should be noted that, in accordance with the **Code**, the **software** must be

fully audited before being released into production for the first time. This will be a special case of a **software** change audit: one that reviews not only every function of the **software** but also the **software** development and **system** implementation processes

(b) Purpose of the software change audit

The purpose of a software change audit is to provide assurance to the **Authority** that the requested change has been implemented as described in the updated **functional specification** and that it conforms with the **Code** and the **Act**. In addition, while it is not part of a software change audit to test the software for bugs, the audit must determine whether the **software** has been adequately tested.

B.6 Audit process

For a software change audit the auditor must:

(a) ensure that the **functional specification** has been updated in sufficient detail so that the updates made are consistent with the rest of the document. The **Provider** is expected to keep the **functional specification** up-to-date, such that it always reflects the current state of the **software** and to maintain it at the same level of detail as in the original version of the document

(b) check that the change to the **software** conforms with the requirements of the **Code** and **Act**

(c) verify that the **software** performs as described in the updated **functional specification**. The objective should be to discover whether all the functionality has been delivered as described; however, it is agreed that this will involve only checking a representative sample of possible scenarios

(d) review the test scripts and test results from the testing stages of the change control process to determine whether all reasonable tests have been conducted and signed off correctly. The **Provider** must, therefore, develop and retain test scripts for all changes made to the **software** and record the results of testing.

B.7 Software change audit report

The software change report must state whether:

(a) the **functional specification** has been updated

(b) the **software** change conforms with the **Code** and the **Act**;

(c) the **software** change was tested properly.

The **Provider** must send the software change audit report to the **Authority** within one month following the completion of the software change audit.

B.8 Annual Audit

Purpose of the annual audit

The purpose of the annual audit is to provide assurance to the **Authority** that there has been no detrimental impact arising from changes made to the **software** during the previous year, and that the **software** is still compliant with the **Code**

and the **Act**. It will also provide an opportunity to review the performance of the **software** during the previous year and to comment on any areas of concern or any trends identified or areas that the **Authority** directs. The objective of this should be to encourage the **Provider** to make improvements where possible.

(a) Audit process

For the annual audit the auditor must:

(i) Check that all the functions described in the latest version of the **functional specification** are still being delivered by the **software**, in order to provide extra assurance that the changes made throughout the year have not adversely affected any of the other functions

(ii) Examine the fault log required under this **agreement** to discover what faults have occurred and whether they have been adequately tested and fixed. During the lifetime of the **system** the number of faults should fall rapidly. Once stable, new faults should be rare; however, when major changes are made there may be a temporary increase in the number of faults found. Any deviation from this general pattern could indicate problems with the **software**

(iii) Review the change history of the **software** for the previous year. The **Provider** must keep a log of all changes made to the **software** and also all upgrades of the development environment, database, communications and operating system software. Each change must have a set of relevant test scripts and signed test results

(iv) Examine the monthly performance reports and check that **performance standards** have been met and are being measured correctly. Any drops in performance must be explained. The overall trend should be one of constant or improving performance through the year. If this is not observed then it may indicate that the capacity of the **system** needs to be upgraded

(v) Check whether a user survey has been conducted by the **Provider** and examine the responses. The responses should be positive overall. Any issues mentioned by more than one **user** should have already been addressed or be in the process of being addressed by the **Provider**

(vi) confirm technology currency and vendor support arrangements

B.9 Annual audit report

The annual audit report must:

(a) detail whether the **software** still delivers the functionality described in the **functional specification**

(b) summarise all the changes that have been made to the **software** during the previous year, including any changes that are still in progress, and their cumulative effect, if any, on the **software** as a whole

(c) comment on performance and any discernible trends

(d) summarise all the fault activity that has occurred, highlighting any perceived problem areas

(e) comment on the level of **user** satisfaction with the **software**, noting any particular concerns of **users** and how these issues are being addressed

(f) confirm technology currency and vendor support arrangements.

The **Provider** must send the annual audit report to the **Authority** by 1 May in the relevant year..

B.10 Not-auditable changes

(a) **Software** bugs

Software bugs remain in programs as a result of inadequate testing and, as such, are the responsibility of the **Provider**. The annual audit will offer an opportunity to check that bugs have been fixed and tested properly and allow the auditor to form at least a partial opinion about the overall quality of the **software** and the likelihood of future problems.

(b) Infrastructure Software Upgrades

This category includes upgrades to database management, operating system, communications and other third-party software. Although these upgrades should not require auditing, it is expected that the **Provider** will perform extensive testing before putting them into production, as any incompatibilities between the upgrade and the **software** may adversely affect the performance levels specified in the **agreement**. The **Provider** is required to inform the **Authority** of these upgrades.

(c) Other enhancements (additional functionality)

These are enhancements to the system developed by the **Provider** that fall outside the scope of the **software** as defined by the **functional specification** and the **Code**, and which are therefore not directly auditable. Depending on the exact nature of the proposed enhancement, the **Authority** may decide that a **software** audit is warranted in order to ensure that the existing functionality described in the **functional specificatio**n is not adversely impacted.

B.11 Auditor

The **Provider** shall ensure that the same auditor (meaning, where the auditor is a company, the same person leading the audit) is not used for more than two consecutive annual audits except as otherwise agreed by the **Authority**.

Appendix C Indicative volumes as at 1 March 2015

C.1 Pricing manager service provider reports will give some operational detail on the issues involved with management of prices. These are available at http://www.ea.govt.nz/operations/market-operation-service-providers/wits-manager/wits-monthly-reports/

C.2 Pricing nodes

- Number of pricing nodes published on WITS = 253
- For month of December 2014
  - number of solves = 46
  - number of solves not published = 9
  - number of solves published as provisional = 6
  - number of solves published as final = 31
  - number of pricing error claims = 0

C.3 Pricing publication times

- For month of December 2014
  - 1st solve published same day before 9:22 = 17
  - 2nd solve published same day before 12:00 = 10
  - 2nd solve published same day before = 17:00 0
  - 2nd solve published interim 1st business day following weekend or weekday provisional = 4
  - Interim solve publication delayed more than one business day = 0

C.4 Pricing error claim management

- Number of pricing error claims managed per year = 12

C.5 Provisional price management

- For month of November 2014
  - number of infeasibility situations = 12
  - number of metering situations = 4
  - number of high spring washer price situations = 1
  - number of SCADA Situations = 0