SCHEDULE 2

NON-FUNCTIONAL SPECIFICATION

ELECTRICITY AUTHORITY
TE MANA HIKO

FTR manager

Non-functional specification

Updated: April 2024

Version control

Version	Release Date	Description
1.0	April 2012	Draft released by Authority in FTR Manager RFP
2.0	July 2013	New version agreed upon System Acceptance and signed as an agreed update to Schedule 2 of the FTR Manager SPA
3.0	November 2018	Various amendments to clauses 4.2, 5.1, 6.4, 10.4, 13,4 and Appendix 2: Performance Standards
4.0	July 2024	Start of new contract 1 July 2024

Contents

1. Introduction and purpose

The purpose of this document is to describe the non-functional requirements of the System provided by the FTR manager (the Provider). The System comprises software and equipment that achieves these functions:

- the FTR grid design;
- the auctions;
- the FTR register;
- determination of the FTR rentals; and
- the interfaces for end-users.

This document should be read in conjunction with the associated FTR manager functional specification.

2. Application architecture

The following requirements apply whether the Provider is offering a bespoke System specifically designed for the Authority or a System based on existing software.

2.1 Industry standard

The System must be built on industry standard, robust architecture that is reliable and scalable in the following areas:

a) hardware infrastructure including production and disaster recovery hardware;

b) operating system;

c) network topology;

d) application software;

e) database;

f) security;

g) systems deployment and management; and

h) external security, firewalls, virus protection, etc.

2.2 Independent environments

There must be separate and independent environments for development, user acceptance testing and production. "Independent" in this context means that activity on the user acceptance testing and development environments must not affect the production environment in any way. The user acceptance testing environment will, upon reasonable request, be available for FTR market participants to perform their own testing and staff training.

2.3 Current components

The System must not at any time contain any components that are no longer supported by the Provider or the relevant licensor or manufacturer.

2.4 Scalability

The System must be easily scalable to accommodate a compounding 10 per cent per annum growth in FTR application users, portal users, and transactions for seven years, without significantly affecting performance and reliability.

2.5 Upgrades

Procedures agreed with the Authority must be in place for the implementation of upgrades to equipment and software. The implementation of all upgrades must be carefully planned, scheduled, notified to all relevant parties well in advance and implemented efficiently at times that cause as little disruption as possible to users of the System. The timetable for the implementation of all upgrades must be approved in writing by the Authority.

The Provider must implement in a timely manner (i.e. within 12 months of release) all available, proven operating system, database and system software upgrades. If the Provider does not consider it appropriate to implement a new release within 12 months, the Provider must promptly notify the Authority in writing that it is delaying implementation and provide a reason that is acceptable to the Authority.

2.6 Data-integrity maintenance

The Provider is responsible for the maintenance of the data environment and must ensure that functionality is available within the software to reverse the effects of any material errors made by users in loading data via file transfer. The Provider must provide assistance to users in executing any such recovery.

The file transfer system into the software must perform a data validation process to ensure that any files that are not consistent with the prescribed format and content are rejected and the user is notified of the rejection.

The Provider must undertake the recovery (where possible) of any database integrity and corruption issues and correct any errors that occur as a result of the System incorrectly processing any information.

2.7 Concurrent users

There are two types of **end-users**:

- **FTR application users** who participate as representatives of the FTR market participants in auctions; and
- **Portal users**, a wider group of users including the bidders, clearing manager and the Authority, who must be registered to use the Provider's website and who will check the results of auctions and query the FTR register via the Provider's website.

The FTR application forming part of the System must be designed, implemented and maintained to cope with at least 35 concurrent online auction bidders (**FTR application users**) for the receipt of auction bids and notification of auction results. The **FTR** website interface must be designed, implemented and maintained to enable and cope with queries of the FTR register by 200 concurrent **end-users**, including **FTR application users** and **portal users.**

In order to show the use of the application, the Provider must provide the Authority with monthly usage figures as part of the monthly report, including:

- Total number of users over a one-month period.
- Maximum page views in a one-hour period.
- Maximum number of concurrent users

3. Interoperability

3.1 User interfaces

The following user interfaces must be provided:

a) a secure web browser user interface for uploading, viewing and downloading information online; and

b) as a minimum, a facility to transfer files in a secure manner.

4. Service levels

4.1 System availability – FTR register

The regular service hours for the System must be 0800 hours to 1700 hours New Zealand Standard Time or New Zealand Daylight Time (as applicable) on **business days** as defined in the Electricity Industry Participation Code.

The availability of the FTR register, via the end-user interface, must be as follows:

a) for localised interruptions of service, to all **end-users**:

   i. during regular service hours, the System must not be unavailable for more than 90 minutes in any one month; and

   ii. outside regular service hours the System must not be unavailable for more than 10 hours in any one month;

b) there can be one planned outage per month taken outside of auction window periods (auction day, plus day afterwards) and of no more than 3 hours duration.

c) there can be one planned outage per month taken outside of business hours, and of no more than 10 hours duration.

d) planned outages in excess of the limits defined in 4.1(b) and 4.1(c) must have the prior written approval of the Authority; and

e) a record must be kept of unplanned outages and included in the monthly report to the Authority.

4.2 System availability – auction bid window

The System availability for auctions must be as follows:

a) the Provider must use all reasonable endeavors to avoid unplanned outages during auctions

b) there must be no planned outages to the auction System during auctions; and

c) a record must be kept of unplanned outages and included in the monthly report to the Authority.

d) in the event of an unplanned outage, the Provider must follow these protocols:

i. Once made aware of an unplanned outage affecting all bidders the Provider must promptly inform the Authority of the issue and then all affected bidders;

ii. From the time that the Provider has been made aware of an unplanned outage, the Provider will have 90 minutes to remedy the issue and return the FTR application to a functional state. If the unplanned outage is of less than 90 minutes duration during an auction window, the Provider will extend the bidding window for the auction by up to 90 minutes in total, and then must notify all bidders and the Authority of the time extension at the time the auction window restarts.

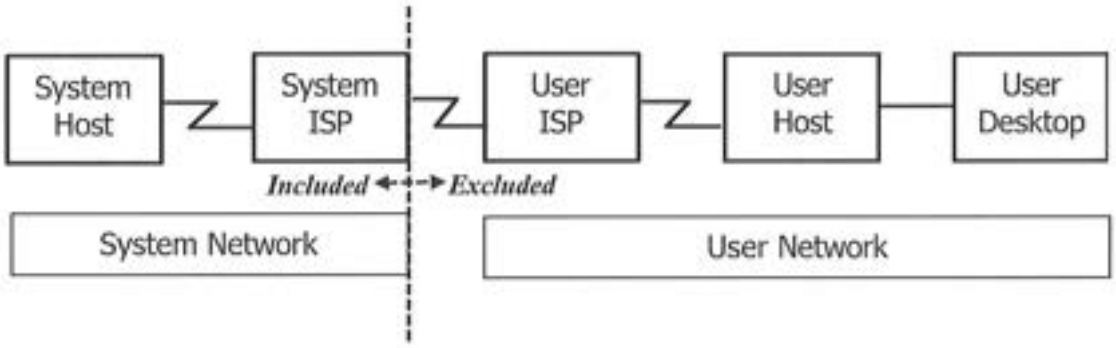
iii. If the unplanned outage is of more than 90 minutes duration, the Authority may, without limiting its powers under clause 13.255 of the Code, direct the Provider to suspend the auction. If the auction is so suspended, the Provider must notify all bidders within 10 minutes of receiving notification of the direction to suspend, and in the notification the Provider must reschedule the auction to the next suitable day, not being a settlement day for the clearing manager or any other day that interferes with other electricity market operations.

4.3 Calculation of outages

Availability and outages for all System components must be calculated as follows:

Both availability and outage service levels are delineated by the point at which any transaction enters or exits the System's subcontracted Internet Services Provider (ISP). All service components, including the System host, internal and wide area networks and ISP, are covered under availability and outage calculations. This is shown in Figure 1.

Figure 1 – Service delineation



Calculation of availability (where expressed as a percentage)

Availability must be calculated based on the number of minutes that the System is substantially unavailable in any one month using the following formula:

$$\%\ availability\ per\ calendar\ month = 100 - \left[\frac{minutes\ outage}{(days\ in\ month\ \times 60\ \times 24)} \times 100\right]$$

Calculation of outages

For the purposes of the calculation of availability of the System, outages occur on each occasion when the System is unavailable due to either:

- a failure of any component of the System host or the System ISP; or
- any planned outage required to perform regular housekeeping or to install upgrades.

If the actions of any FTR market participant have caused the outage to occur, or have contributed to a material extent to the cause of the outage, then the Provider will not be held accountable for the outage only to the extent that it was caused by the intentional action or inaction of any FTR market participant. This includes any actions not taken by an FTR market participant at the request of the Provider, where acting on the recommendation would have avoided or minimised the outage.

In addition to the Provider's obligations under the Code, the following service levels per month must be achieved.

4.4 System response times

The System must achieve the following System response times:

a) the System must upload any one bid portfolio in less than 30 seconds;

b) for all other transactions, including FTR registry file downloads:
   i. Sampled transactions must have an average page load time of less than five seconds.

c) the System must complete all necessary 'housekeeping' and backups by 0730 hours New Zealand time each day.

4.5 Maintenance

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

For urgent corrective maintenance (to fix software faults that are threatening the achievement of 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 the achievement of the service levels.

4.6 Monthly service-level reporting

The Provider must provide the Authority with a monthly report within 10 business days of the end of each month as required by Part 3, clauses 3.13 and 3.14, of the Code.

In addition to the above the Provider is to include the following:

- commentary on the previous month's auctions, assignments, re-assignments,

FTR settlements and unusual bid behaviour

- revenue adequacy for the previous month and commentary on performance against revenue adequacy objectives
- capacity scaling factor for the previous month and commentary on performance against expectations
- any observations that require the Authority's attention, including, but not limited to:
  - risk frameworks (registers, bowties, mitigations, controls etc.)
  - cyber-security work related to the FTR market
  - overall strategic outlook
- Planned and unplanned outage durations, timings and details for current month and planned outage durations, timings, and details for upcoming month

5. Recoverability and business continuity

5.1 Backup

The Provider must take backup copies of data generated or stored by the System at least daily and store such copies in a secure location. The retention and recycle policy of backup media and the storage location must be agreed with the Authority. 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 5kms from the premises used to provide the regular service.

5.2 Up-to-date disaster recovery plan

The Provider must develop and keep up to date a disaster recovery plan as agreed with the Authority, based on the provisions outlined below.

5.3 Recovery time

The disaster recovery plan must be designed to enable recovery of the System at the disaster recovery site in the event that the Provider's primary site (which contains the production System) is inaccessible or unsafe to enter or operate. Recovery is required of the System within 6 hours following a disruption.

5.4 Disaster recovery procedure

A copy of the System, including relevant admin passwords and IDs, is to be stored in a geographically remote (at least 100km distant) location. The disaster recovery System is to be kept synchronized with the primary System and to be typically up to date with daily updates of data from the primary System, and with an update within 10 minutes of the closure of an auction bidding window and with an update at the time of the notification of the auction results.

In the event of a switch-over to the disaster recovery site, the Provider will, within 6 hours of the date and time of the disruption:

a) check back through recent changes and re-apply any recent changes to the disaster recovery copy of the System;

b) reinstate the FTR register user interface and verify that the data is correct as of the date and time of the disruption, or if this is not possible, as of a particular date not being more than one week prior to the date and time of the disruption;

c) confirm that once the System has been brought up that the participants can access it (since there will be network changes);

d) reconfirm the accuracy of data inputs and calculation methodology for determination of FTR grid design and for calculation of FTR rentals prior to those processes being undertaken;

e) publicly notify any relevant market information required for participation in upcoming auctions.

5.5 Disaster recovery testing

The Provider must test the disaster recovery procedure prior to the commencement of operation and every six months thereafter. Disaster recovery reports must be provided to the Authority after each test detailing the test, results and any issues raised during the test. The test must include:

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

b) notification to all FTR registry users of the date and time of the disaster recovery test, and any changes to URLs, addresses etc for the duration of the test;

c) activation of the disaster recovery System at the remote location and transfer of production to the disaster recovery System;

d) verification of System availability and that the System is fully functional to an external user;

e) running a full reporting cycle and testing of file and manual updates; and

f) transfer of production back to the production site at the date and time agreed under a) above.

6. Security and confidentiality

6.1 User accounts

The System must have a framework for the management of user accounts. Any identifiers used for FTR market participants are to be obtained from the market administrator.

6.2 User privileges

User privileges must be able to control access at both function and specific data level.

6.3 Security policy

The auction System must have a security policy in place and have mechanisms that enforce the password standard, account lock-out for unsuccessful logon attempts and session timeouts. The policy must be consistent with the requirements of the New Zealand Information Security Manual (as updated from time to time).

6.4 Logs

The auction System should maintain audit logs of user interactions with the System and action all alerts of repeated unsuccessful logons to prevent hacking. The audit logs must provide information for FTR market participants to analyse their own usage patterns of the System.

By request, all logs for a specified event must be made available to the Authority in an

agreed standard format as required by the Authority.

6.5 Confidentiality

The auction System must maintain the confidentiality of each FTR market participant's information by allowing requests only by parties that have been granted authority by FTR market participants to access the System on their behalf by the exchange of digital certificates and/or password authentication.

6.6 Data encryption

Data transfer between FTR market participants and the Provider must be encrypted to at least 128 bits using SSL.

6.7 External security audit

The Authority may arrange for an external security audit or assessment during the build phase so that if any security design flaws are found, they can be addressed during the design phase. The Provider agrees to co-operate fully with such audit or assessment.

7. Capacity

7.1 Management utilities

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.

7.2 Excess volumes

The Provider must promptly advise the Authority if increases in transactional volume beyond the levels agreed in the FTR manager service provider agreement threaten the achievement of service levels. The Authority and 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 with the Provider, the Provider will be responsible for taking such remedial action as is necessary to meet service levels.

The Provider must trend transaction and database volumes over time. Should this trend indicate that within the next six months that the transaction and/or database volumes may exceed those agreed with the Provider, or if Code changes have increased complexity to the extent that service levels cannot be met, then the Provider must advise the Authority, and the Provider or the Authority may initiate the agreed change control procedures.

8. Data integrity and archive policy

8.1 Data ownership

All data collected, calculated and published as required in the functional specification is the property of the Authority. The Provider must store the data securely and be able to provide it to the Authority on request and at no cost within a reasonable timeframe, being no later than 10 business days after the request, and in the format and with the delivery mechanism nominated by the Authority.

8.2 History

The System should retain history for immediate access for seven years after which the information must be archived (onto an appropriate storage medium) and available for retrieval on request, as per sections 17 and 18 of the Public Records Act 2005. The Provider is required to meet the minimum requirements of any relevant mandatory standards issued under the Public Records Act.

9. 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.

10. Service management

10.1 Industry standard

The Provider should employ industry service management methodologies, such as ITIL (Information Technology Infrastructure Library) including robust quality assurance processes. Any methodology should cover the service management functions being provided.

10.2 End-user assistance

The Provider is required to provide a help desk that is available by phone and email during regular service hours to assist with **end-user** queries. The Provider must proactively assist **end-users** to resolve their issues.

The Provider, acting reasonably, is to prioritise help desk calls and emails. The Provider must send an initial response to the enquiry within five business hours of receiving it, and to include a pathway for resolution, if required. The Provider will inform the customer when resolution has been achieved.

10.3 Fault management

The Provider must provide a fault management service during regular service hours to rectify operational incidents and System faults. Operational incidents are those where the user reports that the System is unobtainable. A System fault means a defect, error or malfunction in the System that renders all or any part of it inoperable or unusable. The Provider must commence work to rectify operational incidents and System faults

within two regular service hours of their detection or reporting.

The Provider must proactively manage all aspects of the service.

If an incident affects more than one user, the Provider should notify all FTR market participants and the Authority as soon as practicable.

10.4 Incident register

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 register should contain the user, time and details of the incident as well as the time and details of its resolution. The Provider must notify users when incidents are resolved or the time when they are expected to be resolved. The Provider 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 must be provided to the Electricity Authority on a monthly basis.

17/11/2020 variation: revised to clarify monthly reporting does not need to be in the report on service levels.

11. Change control process

The Provider must follow the change control process as set out in Appendix 1 of this document. System changes must follow recognised good practice for software change management as noted in paragraph 12.1 below. The Provider and the Authority will agree a development plan for software changes including a schedule for delivery of test and audit reports.

12. Development methodology

12.1 Industry standard

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

For the avoidance of doubt, the systems development life cycle (SDLC) is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.

12.2 Flexibility

The software should be designed for flexibility to ensure changes to functions, as a result of user requests and rule changes, can be made efficiently and cost effectively.

12.3 Historical information and documentation

At the end of the term of the agreement, the Provider must deliver to the Authority:

a) all the data (including any transformation of the base data) in the System, on request, within an agreed timescale in an agreed format. The Provider will be

required to load all the historical information contained in the current System into any new system; and

b) the operating manuals, historical reviews, analysis and models, related documentation, admin passwords and IDs for the Authority's ongoing use, including technical and user documentation in connection with the FTR System held by the Provider.

13. User liaison

13.1 Close contact

The Provider is required to 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 FTR market participants.

The Provider must develop formal notification channels to notify users, the Authority, and any other affected parties of outages and likely timeframes for restoration of service.

13.2 Escalation process

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.

13.3 Daily liaison

During periods when the System is not available, the Provider must also liaise with the Authority and users not less than daily, including advising of expected times for the resumption of service.

13.4 User satisfaction survey

The Provider is required to develop, distribute and consolidate a survey of all FTR market participants including all **end-users** that analyses the satisfaction levels of their service provision, System and FTR market effectiveness, and desired developments. The Provider is to consult with the Authority over the survey questions. The survey is to be conducted annually and the results reported to the Authority within 1 month of 1 April each year.

17/11/2020 variation: reference to the date of the first survey removed.

14. Documentation

The Provider must maintain and provide as a minimum:

a) an **up-to-date functional specification**, which contains all interfaces, processes and descriptions of how systems operate, and must be in the format and content approved by the Authority, against which the software can be audited as per the requirements in clause 3.17 of the Code. The functional specification is the 'software specification' referred to in the Code. The functional specification and any subsequent changes are the property of the Authority;

c) a **user manual and online help facilities** (user documentation) to enable new users to configure their systems correctly and access the System. The documentation should provide sufficient detail for new users to locate and use all the relevant functions. The user documentation should include a troubleshooting guide, frequently asked questions and information on where and how to seek further help;

d) a **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

e) **sufficient technical documentation** for business continuity in case of the loss of key personnel. This must include an **operations manual**.

15. System audits

15.1 Spot audits

The Authority may carry out audits of the Provider's performance of the **services** in accordance with clause 3.6 of the agreement, including records and procedures, within normal working hours on reasonable notice. The Provider 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 Provider continues to meet the **services** specified in the agreement, including the criteria required in the functional specification and in Appendix 2 of this document.

15.2 Audit recommendations

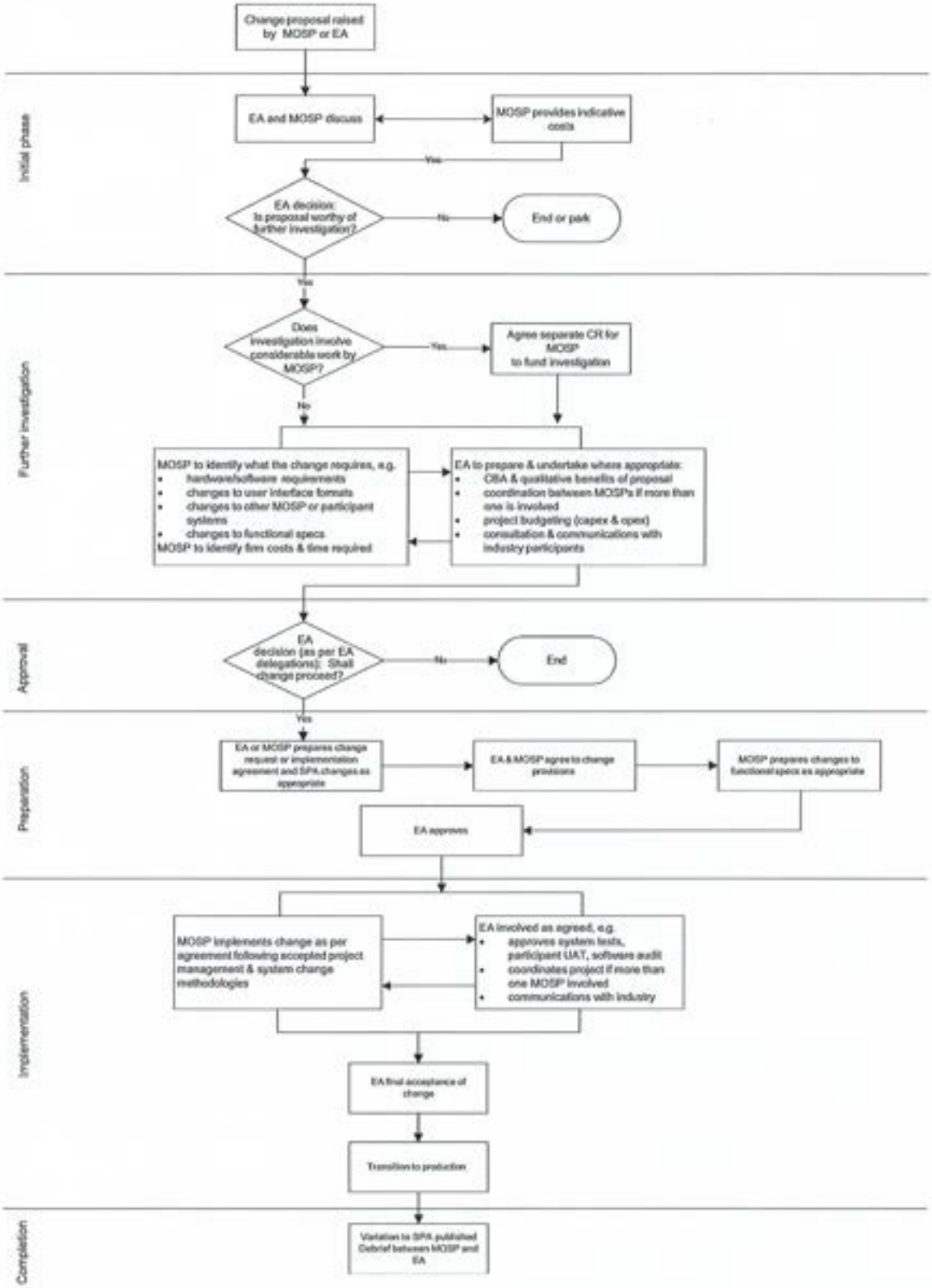
The Provider must implement, using recognised good practice in software change management procedures, any changes necessary to give effect to any reasonable recommendations made by an auditor, with the objective of constantly improving services.

15.3 Annual and change software audits

The Provider must comply with the **software** audit requirements as set out in clause 3.17 and clause 3.18 of the Code with respect to conducting audits of the software on first-time use, and thereafter annually and for software changes. Refer to: http://www.ea.govt.nz/act-code-reqs/code-reqs/the-code/part-3/.

The Provider must send the annual audit report to the Authority within a reasonable period of time mutually agreed following the completion of the annual audit.

Appendix 1 – Change control process



Appendix 2 – Performance standards

The following is a list of the performance standards referred to in clause 3.13(2)(c) of the Code, and other market reporting to the Authority. Reports are required monthly.

Measure	**Performance requirement**
Market performance	
The number of registered FTR market participants and changes to participant numbers in the month.	Numbers
Report on market information as set out in the functional specification.	As set out in RP-010 of the functional specification
Number of FTR market participants in each auction 17/11/2020 variation: replaced reference to "bidders" with "FTR market participants" and deleted number of bids per FTR product. Number of unique end-users using the System each month Maximum number of concurrent end-users on the System during the month	Numbers
17/11/2020 variation: deleted growth incentive.	
System availability	
Report on System availability.	As set out in section 4.1, 4.2 and 4.3 of the non-functional specification
Help desk availability from 0800 to 1700 hours each business day.	100%
Response times	
Report on System response times.	As set out in 4.4 of the non-functional specification
Response and resolution times for help desk calls and emails separated into priority status.	As set out in 10.2 of the non-functional specification
System performance	
Number and details of Code or service provider agreement breaches by the Provider.	Report
Number and details of actions carried out to correct a software-related problem.	Number and details
Number and details of incidents requiring data fixes.	Number and details

Schedule of faults raised giving description, severity, and response.	Schedule
Number and details of FTR participant Code breaches.	Report
Report on disaster recovery procedures, tests, and back-up obligations as set out in the non-functional specification.	Report
Confirmation that the Provider (continues to) meet the minimum requirements of the Create and Maintain Recordkeeping Standard and the Electronic Recordkeeping Metadata Standard under the Public Records Act 2005.	Report
FTR awards, prudential limits and rentals delivered to the clearing manager. ".	As per the Code

Appendix 3 – Software Audit Guidelines

A.1 Purpose of this document

The purpose of this document is to provide the Authority and service providers with guidelines for deciding when software audits are required. Clauses 3.16 to 3.18 of the Code set out service provider responsibilities for software audits. This document 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.

A.2 Definition of software

The term "software" is defined in Part 1 of the Electricity Industry Participation Code 2010 (Code), and for the purpose of this document is interpreted to mean the application software that the service provider uses to deliver the functions defined in the software specification which forms part of the service provider's agreement (SPA) with the Authority.

A.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 software specification (as defined in the Code) and that it conforms to the Code. The Authority may also require the auditor to report on any other matters that the Authority requires.

A.4 Introduction

In accordance with clause 3.17 of the Code, there are three types of audit that service providers are subject to, being:

(a) an initial audit before any software is first used by the service 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 service provider; and

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

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

A.5 Software Change Audit

(a) Software and software specification changes that require auditing

All changes to the software and software specifications must be audited, except both bug fixes and enhancements that fall outside the scope of the core functionality specified within the software specification. All changes must be implemented by following the software change control process as specified in the SPA. Every change must be incorporated into a new release of the software. Details of each new release must be documented 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 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 software specification and that it conforms with the Code. 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.

A.6 Audit process

For a software change audit the auditor must:

(d) ensure that the software specification has been updated in sufficient detail so that the changes made are consistent with the rest of the document. The service provider is expected to keep the software 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;

(e) check that the change to the software conforms with the requirements of the Code;

(f) verify that the software performs as described in the updated software specification. The objective should be to discover whether all the functionality has been delivered as described; however, it should be understood that this will involve only checking a random sample of possible scenarios not all of them; and

(g) 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. Service providers must, therefore, develop and retain test scripts for all changes made to the software and record the results of testing.

A.7 Software change audit report

The software change report must state whether:

(h) the software specification has been updated;

(i) the software change conforms with the Code;

(j) 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.

A.8 Annual audit

Purpose of the 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. 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 service 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 software 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 the SPA 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. Service providers 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 levels 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 service provider and examine the responses. The responses should be positive overall. Any issues mentioned by more than one respondent should have already been addressed or be in the process of being addressed by the service provider.

A.9 Annual audit report

The annual audit report must:

(a) detail whether the software still delivers the functionality described in the software 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.

The provider must send the annual audit report to the Authority by 1 May in the relevant year. The provider shall ensure that each annual audit report includes an up to date list of the equipment of any Authority-owned hardware.

A.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 service 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) System 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 service 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 SPA. The service provider will be required to inform the Authority of these upgrades.

(c) Other enhancements

These are enhancements to the system developed by the service provider that fall outside the scope of the software as defined by the software specification and the Code, and which are therefore not directly auditable. The service provider will be obliged under the SPA to inform the Authority of all such enhancements. 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 software specification is not adversely impacted.

A.11 Auditor

The provider shall ensure that the same auditor (meaning, where the auditor is a company, the same audit lead) is not used for more than two consecutive annual audits under this Schedule 2 except as otherwise agreed by the Authority.