INTERIM COMPLIANCE PROCEDURE

VERSION: 2~~1~~.0

EFFECTIVE DATE: 1 January 2024~~31 December 2023~~

VERSION RELEASE HISTORY

Version	Effective Date	Changes	Approved
1.0	31 December 2023		James Campbell-Everden
2.0	1 January 2024	Changes from Interim Procedure consultation process	James Campbell-Everden

TABLE OF CONTENTS

1. Introduction

1.1 Purpose and Scope

See Rule [85; 172; Chapter 12; 307; 308; 309]

1.1.1 This Interim Compliance Procedure (Procedure) is made under Rule 308 and Sub-appendix 4.14 of the Pilbara Networks Rules (Rules) and addresses the Pilbara ISOCo (ISO) ~~ISO's~~ compliance functions outlined in Chapter 12 of the Rules.

1.1.2 The Rules provide ISOs compliance function as being:

(a) The ISO must monitor Rules Participants' behaviour (including its own) for compliance with the Rules (including the Harmonised Technical Rules) and may take enforcement action under Subchapter 12.1 of the Rules;

~~{~~Note: As Rule 85 requires compliance with P~~p~~rocedures, the expression compliance with the Rules includes compliance with the Procedures.~~}~~

(b) The ISO must endeavour to perform its compliance function under Subchapter 12.1 of the Rules with as little formality and as much expedition as reasonably practicable.

1.1.3 The Compliance Procedure may, as outlined in Rule ~~Rule~~ 309 of the Rules, include~~outlines topics which may be included in this Compliance Procedure, including~~:

(a) specify which non-compliances must be reported to the ISO; and

(b) specify a tolerance range for a Facility or Network Element, or a class of either, such that operation which does not comply with the~~se~~ Rules but is within the tolerance range, is not a breach of the~~se~~ Rules; and

(c) provide the circumstances in which self-reported non-compliances are not a breach of the~~se~~ Rules, for example if they have been or are being rectified (if capable of rectification) and, where appropriate, steps are in place or planned to reduce the risk of recurrence; and

(d) permit the ISO to decide, based on specified criteria such as the materiality, frequency, duration and recurrence of non-compliances, whether a breach of the~~se~~ Rules should be investigated or merely logged; and

(e) for logged breaches, permit the ISO to decide the circumstances (for example a further non-compliance) in which a matter should be investigated or otherwise escalated; and

(f) Rule 309 ~~the~~and above does not limit the matters the Compliance Procedure may deal with.

~~{~~Note: This Procedure requires all non-compliances to be reported to the ISO. The ISO will undertake a risk assessment to determine whether a self-reported non-compliance is a breach of the Rules, further outlined in s~~S~~ection 4.4 of this Procedure~~}~~

Other provisions of the Rules that support and apply to this Procedure are those in Subchapter 3.6 {Procedures} and Chapter 11 {Information}.

1.1.4

~~1.1.4~~1.1.5 The *Electricity Industry Act 2004* (WA), the Electricity Industry (Pilbara Networks) Regulations 2021, the Pilbara Networks Access Code and the Rules prevail over this Procedure to the extent of any inconsistency.

~~1.1.5~~1.1.6 In this Procedure, where obligations are conferred on a Rules Participant, that Rules Participant must comply with the relevant obligations in accordance with R~~r~~ule 85, unless the Rules Participant has grounds for non-compliance under R~~r~~ule 172 of the Rules.

1.2 Definitions and Interpretation

1.2.1 Terms defined in the *Electricity Industry Act 2004* (WA), the Electricity Industry (Pilbara Networks) Regulations 2021 (Regulations), the Pilbara Networks Access Code and the Rules have the same meaning in this Procedure unless the context requires otherwise. The ISO does not capitalise or italicise terms defined in the above instruments in this Procedure.

1.2.2 Where there is a discrepancy between the Rules and information on a term in this Procedure, the Rules take precedence.

1.2.3 The following principles of interpretation apply in this Procedure unless the context requires otherwise.

(a) Subchapter 1.2 of the Rules apply to this Procedure.

(b) References to time are references to Australian Western Standard Time.

(c) A reference to the Rules or Procedures made under the Rules, have the meaning given to them in the Rules.

(d) Words expressed in the singular include the plural and vice versa.

(e) A reference to a paragraph refers to a paragraph in the Procedure.

(f) A reference to a rule, subchapter or chapter refers to the relevant section in the Rules.

(g) References to the Rules in this Procedure is bold and square brackets, e.g. **"See Rule [XXX]"** are included for convenience only, and do not form part of this Procedure.

(h) Any explanatory notes are included for context and explanation and do not form part of this Procedure.

1.2.4 Appendix A of this Procedure outlines the head of power rules that this Procedure is made under, as well as other obligations in the Rules covered by the Procedure.

1.3 Related Documents

See Rule [85; 307; 317]

1.3.1 All ISO Procedures are related to this Procedure. Rule 85 requires compliance with Pprocedures, and the expression compliance with the Rules includes compliance with the Procedures. The latest version of ISO's Pprocedures can be found on the ISO's website.

1.3.2 In accordance with Rule 317, the Authority has supported the ISO in the development of this Procedure. This Procedure is based on the Authority's Monitoring Protocol Wholesale Electricity Market (WEM) Procedure, adapted to the Pilbara electricity system. This assists in aligning the approach to compliance across Western Australia's electricity systems and facilitates the Authority's role in investigating ISO's compliance with the Rules and Procedures.

2. Compliance Framework

2.1 Compliance Aapproach

See Rule [309]

2.1.1 The ISO's compliance approach is aimed at encouraging compliance by Rule Participants with the Rules and Procedures with the target of achieving high levels of compliance. Under this approach the ISO will seek to:

(a) assist Rule Participants to understand their obligations, noting that the responsibility for meeting compliance obligations rests with the individual Rule pParticipant;

(b) identify potential breaches, investigate these where appropriate and identify any subsequent education or other prevention or enforcement actions required;

(c) ensure any investigation process is conducted in an efficient and professional manner, including applying procedural fairness and ensuring investigation decisions are informed by the relevant facts;

(d) ensure that its compliance responses to breaches are proportionate to the circumstances of the non-compliant behaviour;

(e) apply a risk-based approach to its compliance activities, including its monitoring processes, investigation processes and enforcement actions.

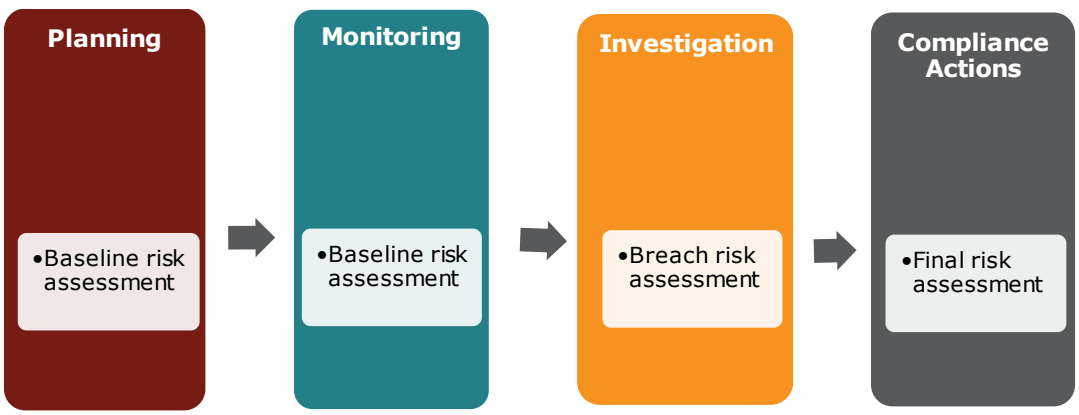
2.2 Risk-based Aapproach

See Rule [309]

2.2.1 The ISO applies a risk-based approach to its compliance function by assessing the compliance risk associated with an obligation or set of obligations under the Rules and Procedures.

2.2.2 This assessment assists ISO in determining planning and monitoring activities, investigation priorities and compliance actions.

Figure 1: Application of Risk Assessments



2.2.3 The ISO's risk-based approach uses the consequence and likelihood tables in Appendix B to assign a risk rating to the Rule and Procedure obligations and alleged or actual breaches of obligations.

2.2.4 Baseline risk assessments are used for planning and monitoring, breach risk assessments are used to determine investigation prioritisation and final risk assessments of confirmed breaches are used to inform compliance actions.

2.2.5 All non-compliances are to be reported to the ISO. The ISO will use a risk-based approach to determine if a self-reported non-compliance is considered a breach of the Rules.

2.3 Baseline R~~r~~isk A~~a~~ssessment

See Rule [309]

2.3.1 The ISO must prepare a register of obligations which sets out the obligations of the ISO, ISO Control Desk, NSPs, Facility Controllers~~controllers~~, Integrated Mining Networks and Connection Point Compliance facilities and excluded networks under the Rules.

2.3.2 The ISO must undertake a baseline risk assessment on each of the obligations to determine:

(a) The baseline risk score of each of the obligations;

~~(a)~~(b) Which non-compliances must be reported to the ISO;

~~(b)~~(c) The timeframe for reporting non-compliances, whether batch reporting is appropriate under section 4.2;

~~(c)~~(d) The ISO's priorities for compliance monitoring;

~~(d)~~(e) Whether a self-reported non-compliance is considered a breach of the Rules;

~~(e)~~(f) Whether an alleged breach will be investigated or logged;

~~(f)~~(g) The prioritisation of the investigation;

~~(g)~~(h) Any compliance action or enforcement following the determination that a breach has occurred.

2.3.3 The ISO will publish the outcomes of the baseline risk assessment on its website. This may be updated from to time to ensure compliance monitoring priorities and investigation functions remain aligned with the NWIS system risks.

2.3.4 When considering the prioritisation of compliance activities, the ISO will generally prioritise higher risk obligations over lower risk obligations. However, there may be exceptions to this as there may be circumstances where lower risk matters may warrant compliance action (for example, repeated low risk non-compliances by the same Rule Participant that may indicate a systemic issue).

2.3.5 In the absence of a published baseline risk assessment in accordance with paragraph 2.3.3 of this Procedure all non-compliances must be reported to the ISO as soon as reasonably~~practicably~~ possible.

2.4 Risk-based Ccompliance Aactivities

2.4.1 Table 1~~The following table~~ provides an outline of ISO's compliance activities as determined by the risk rating of the obligation and potential non-compliance activity.

Table 1: Compliance activities as determined by risk rating

Risk Rating	Monitoring Priority	Reporting	Breach[1]	Investigation / Priority	Enforcement
	Baseline assessment	Baseline assessment	Breach assessment	Breach assessment	Final assessment
Low	Low	Batch	No	No[2]	Education
Moderate	Medium	Batch	No	Maybe / Low	Increased monitoring
Significant	High	20 business days	Yes	Yes / Medium	Warning issued
Extreme	High	20 business days	Yes	Yes / High	Warning issued

[1] If a self-reported non-compliance has a low or moderate risk rating, the ISO may determine it is not a breach of the Rules. However the ISO may determine a breach has occurred if for example it is a repeated low risk non-compliance which has not been rectified.

[2] Generally, the ISO will not investigate breach allegations with a low risk rating. However, the ISO may investigate where it considers it is reasonably required, for example repeated low risk breaches may indicate a systematic issue which warrants investigation.

3. Compliance Monitoring

3.1 Monitoring Pprocesses

See Rule [307; 309; 310]

3.1.1 Rule 307 requires the ISO to monitor Rules Participants behaviour (including its own) for compliance with the Rules.

{[Note: Rule 310 of the Rules requires a Rules Participant to inform the ISO in writing if it considers it has breached the Rules or has reasonable cause to suspect that it may have breached the Rules and must provide details of the breach. This is discussed further in section 4 below]}

3.1.2 The ISO's compliance monitoring activities are designed based on the following principles:

(a) Monitoring activities are carried out with as little formality and as much expedition as reasonably practicable See Rule [307(2)];

(b) Monitoring activities are carried out with minimal resource and regulatory burden on Rules Participants participants (including the ISO); and

(c) Activities focus on high-risk issues and appropriately deal with low level non-compliances.

3.1.3 The ISO prioritises compliance monitoring of the following categories:

(a) Risk-based: Obligations the ISO has identified as requiring monitoring from the risk assessment process; and

(b) Trend-based: Obligations the ISO has decided to prioritise for monitoring based on its observations of compliance breaches.

3.1.4 The ISO monitors Rules Participants compliance using various methods including:

(a) Self-reporting: Rule 310(1) requires a Rules Participant to inform the ISO in writing if it considers that it has breached the rules;

(b) Industry intelligence: Rule 310(2) of the Rules requires a Rules Participant or other person may inform the ISO in writing if it considers that another Rules Participant has breached the Rrules or a Procedure, and may provide evidence of the breach;

(c) Information monitoring: analysing rules related information, data and documents (for example Energy Balancing and Settlement data, post-incident discussions and investigations) which may identify potential areas of non-compliance; and

(d) Targeted monitoring activities: target reviews of Rules Participants may be carried out to assess compliance with specific rule obligations or groups of obligations or areas identified as being of particular compliance concern (i.e. on the basis of risk-based or trend based assessment). If targeted monitoring activities are to be carried out, the

ISO will work with affected Rules Participants on the process, dependent on the circumstances of the compliance concern.

3.1.5 Rules Participants must cooperate with the ISO by providing any information or records ~~data, information or documents~~ in the Rules Participant's possession or control which may assist the ISO to monitor compliance with obligations in the Rules or Procedures within the time requested by the ISO unless otherwise agreed.

3.2 Monitoring ISO's C~~c~~ompliance

See Rule [307; 310; 313; 318]

3.2.1 In accordance with Rule 307, the ISO must also monitor its own behaviour for compliance with the Rules and Procedures.

3.2.2 ISO monitors its own compliance with the Rules and Procedures using various methods including:

(a) The development of an ISO obligations register, which identifies all of the ISO's Rules obligations;

(b) Business planning processes, which identifies how and when the ISO's obligations are being carried out;

(c) Industry intelligence: Rule 310(2)(b) of the Rules outlines that subject to the Compliance Procedure, a Rules Participant or other person may inform the Authority and ISO in writing if it considers that the ISO has breached the rules, and may provide evidence of the breach;

(d) ISO Audit: In accordance with Rule 318 of the Rules, the ISO must appoint an auditor no later than 2 years after the Rules commencement date to undertake an audit of:

i. the ISO's internal Procedures and business processes' compliance with the Rules;

ii. the ISO's compliance with Rules and Procedures;

iii. the ISO's software systems and processes for software management; and

iv. any other matter the ISO considers appropriate.

~~(d)~~(e) ~~ISO's compliance with Rules and Procedures.~~

3.2.3 Taking into account that this Procedure is an Interim Instrument under the Rules and that ISO is still developing capabilities required to perform its functions under the Rules, ISO may reasonably determine that a non-compliance is not a breach of the Rules where the ISO has steps or processes in place or planned to achieve compliance with the relevant Rules.

~~3.2.3~~3.2.4 If the ISO considers that it has breached the Rules and/or Procedures, or has~~d~~ reasonable cause to suspect that it may have breached the Rules or Procedures, the ISO will record details of the breach, and the risk-assessment process that it has undertaken (taking into account that this is an Interim Instrument) to assess whether the breach should be reported to the Authority for further investigation~~ed~~ or any prevention or enforcement action that should be undertaken.

~~3.2.4~~3.2.5 The ISO will inform the Authority in writing if it considers it has breached the Rules or Procedures for an obligation that has a significant or extreme baseline risk assessment rating, provided in Section 2.3 of this Procedure.

~~3.2.5~~3.2.6 Any person may refer an alleged Rules breach by the ISO to the Authority, by written notice given to the ISO and Authority.

4. Breaches

4.1 When to Rreport a Nnon-compliance to ISO

See Rule [310(1); 310(2)]

4.1.1 When a Rules Participant becomes aware of a potential non-compliance, it should assess the incident to determine if it is non-compliant with the Rules or a Procedure.

4.1.2 If a Rules Participant determines that it is non-compliant, or has reasonable cause to suspect it is non-compliant with the Rules or a Procedure, subject to the Compliance Procedure, that Rule Participant must report in writing the non-compliance or suspected non-compliance to the ISO. Any notifications of non-compliance by a Rules Participant must be in accordance with section 4.3 of this Procedure.

4.1.3 A Rules Participant or other person may notify the ISO in writing if it considers that another Rule Participant is non-compliant with the Rules or Procedures. If a Rules Participant or other person reports a non-compliance, they must provide reasonable information in support of that non-compliance, and may provide evidence of the non-compliance. Any notifications of non-compliance by another Rule Participant must be in accordance with section 4.3 of this Procedure.

4.1.4 A Rules Participant or other person may notify the Authority and ISO in writing if it considers that the ISO is non-compliant with the Rules or Procedures. If a Rules Participant or other person reports a non-compliance they must provide reasonable information in support of that non-compliance, and may provide evidence of the non-compliance. Any notifications of non-compliance by the ISO must be in accordance with section 4.3 of this Procedure.

4.2 Timeframes

4.2.1 Once a Rules Participant has formed an awareness that a non-compliance has occurred or becomes reasonably certain that a non-compliance has occurred, for an obligation that has a significant or extreme baseline risk assessment rating, it must submit a self-reported non-compliance notification in accordance with section 4.3 of this Procedure ~~document~~ as soon as practicably possible and within 20 Business Days of becoming aware of a non-compliance or suspected non-compliance of the Rules or Procedure.

4.2.2 If a Rules Participant is unable to submit a self-reported non-compliance notification within 20 business days, it should contact the ISO as soon as possible to request an extension. The ISO will reasonably consider an extension to these timeframes where sufficient justification has been made by the Rules Participant.

4.2.3 For an obligation that has a low or moderate baseline risk rating, a Rules Participant may batch-report notifications of suspected non-compliance matters to ISO on a 6 monthly basis, by 1 April and 30 September each year.

4.3 Process for Rreporting Nnon-compliance

See Rule [309; 310; 311]

4.3.1 A notification of a non-compliance must be in writing and contain the information contained in section 4.3.3 of this Pprocedure. This includes all reporting of non-compliance with the Rules or Procedures, including:

(a) a self-reported non-compliance by a Rules Participant;

(b) reporting a non-compliance of another Rules Participant;

(c) reporting a non-compliance of the ISO to the Authority and ISO;

(d) batch-reported non-compliance notification.

4.3.2 The ISO has created a non-compliance reporting template to support Rules Participants. This template can be found on the ISO's website. This template does not form part of this Procedure.

4.3.3 A notification of a non-compliance must included:

(a) The name of the Rules Participant and contact details for the person responsible for the notification;

(b) The name of the Rules Participant who is alleged to have not complied with the Rules or Procedures;

(c) The specific Rrules or paragraphsclauses in Procedure/s that are alleged to have not been complied with;

(d) The dates and times on which the non-compliance occurred;

(e) A description of the non-compliance with any supporting information for the allegation.

4.3.4 If available, the notification in paragraph 4.3.3 of the Procedure should also include:

(a) If the non-compliance is by the notifying Rules Participant, details explaining:

i. The root cause of the non-compliance;

ii. Any mitigating circumstances;

iii. Whether and how the non-compliance has been rectified; and

iv. Actions planned or implemented to prevent recurrence of the non-compliance;

(b) Details of any known impact to the Rules Participant, or other Rules Participants; and

(c) Any other information considered relevant.

4.3.5 Notifications of all alleged non-compliance are to be reported to the ISO by email to: submissions@pilbaraisoco.com.au

4.3.6 Confidential or personal information included in any notification to the ISO should be clearly marked so the ISO can ensure it is appropriately protected.

4.3.7 On receiving written notification under paragraph 4.3.1 of this Procedure, the ISO will record the details of the suspected non-compliance.

4.3.8 A Rules Participant may, at any time after making a notification of a suspected non-compliance, provide updated information to ISO in writing to submissions@pilbaraisoco.com.au

4.3.9 When investigating the suspected non-compliance in accordance with the processes set out in Ssection 5 of this Procedure, the ISO will consider whether it is appropriate to disclose to the Rule Participant alleged to have committed the non-compliance the identityfy of the Rules Participant reporting the alleged non-compliance. In exercising this discretion, the ISO will take into consideration any request for anonymity from the party alleging the non-compliance.

4.4 Breach Ttolerance

See Rule [309; 311; 313]

4.4.1 Rules Participants must report all non-compliances to the ISO.

4.4.2 The ISO will undertake a risk-assessment to determine whether a self-reported non-compliance is a breach of the Rules. If the risk assessment undertaken by the ISO determines a low or moderate score in accordance with Table 74 in Appendix B2, the ISO may determine it is not a breach of the Rules. The ISO will inform the Rules Participant in writing that no breach has occurred.

4.4.3 If the ISO determines that the self-reported non-compliance is a breach of the Rules, or the non-compliance is reported by another person, the ISO will take the following actions, in accordance with Rule 311 of the Rules:

(a) It must record the alleged breach; and

(b) If required by the Compliance Procedure it must, and otherwise itIt may investigate the alleged breach; and

(c) It may meet with the Rule Participant on one or more occasions to discuss the alleged breach and possible actions to remedy the alleged breach and prevent recurrence.

4.4.4 The risk rating of the alleged breach will determine whether the ISO will investigate the alleged breach, and if so the priority of the investigation.

4.4.5 The following process will be applied by the ISO when assigning the risk rating to a self-reported non-compliance or alleged breach of the Rules or Procedures:

(a) Consider the baseline risk score of the obligation under section 2.3 of this Pprocedure;

(b) Review the information provided in the notification of the non-compliance, to determine if any change to the risk score is required (for example, are the severity of the consequences or whether the non-compliance has been rectified) and then assign an updated risk rating;

(c) Record the risk rating;

(d) The breach risk rating will determine whether the alleged breach will be investigated and the priority of the investigation.

Table 2: Outcomes of a non-compliance notification determined by breach risk assessment

Risk Rating	Breach[3]	Investigation	Investigation Priority
	~~Breach risk assessment~~	~~Breach risk assessment~~	~~Breach risk assessment~~
Low	No	No[4]	Not applicable
Moderate	No	Maybe	Low
Significant	Yes	Yes	Medium
Extreme	Yes	Yes	High

4.4.6 Where a person has referred an alleged non-compliance by the ISO to the Authority under Rule 313, unless the Authority considers the referral to be frivolous, vexatious or not made in good faith, the Authority must investigate the non-compliance.

[3] If a self-reported non-compliance has a low or moderate risk rating, the ISO may determine it is not a breach of the Rules. However the ISO may determine a breach has occurred if it is a repeated low risk non-compliance which has not been rectified.

[4] Generally, the ISO will not investigate breach allegations with a low risk rating. However, the ISO may investigate where it considers it is reasonably required, for example repeated low risk breaches may indicate a systematic issue which warrants investigation.

5. Investigations

5.1 Investigations Powers

See Rule [312; 313]

5.1.1 If the ISO has determined that an alleged breach should be investigated, Rules Participants must cooperate with an investigation by the ISO into an alleged breach and not engage in materially false or misleading conduct in connection with an investigation, see ~~,~~ Rule [312 (4)(a)], including:

(a) Providing the ISO with any information requested in a timely manner; and

(b) Allowing reasonable access to equipment for the purpose of inspection.

5.1.2 As part of an investigation the ISO may:

(a) Require information and records from Rule Participants; and

(b) Conduct an inspection of any Rules Participant's equipment.

5.1.3 At any time during an investigation the ISO may meet with the Rules Participant on one or more occasions to discuss the alleged breach and actions to rectify it.

5.1.4 A Rules Participant must not engage in materially false or misleading conduct in connection with an investigation.

5.1.5 Where the ISO requires information, records or access to equipment or seeks a meeting it will confirm the request in writing by email to the person nominated as the compliance contact for the Rules P~~p~~articipant as provided under section 4.3.3 of this Procedure, or any other appropriate officer from the Rule Participant's organisation that the ISO considers appropriate.

5.1.6 The request from the ISO will indicate a date which the ISO considers timely, by which the information and records should be provided.

5.1.7 Rule Participants may request in writing for the ISO to extend the date to comply with the information requests from the ISO. The ISO must consider the individual circumstances of the request and advise the Rules Participant of whether the extension has been granted, and if so, details of the extension, and if not, the reasons for not granting the extension.

5.1.8 If the Rules Participant fails to cooperate with the investigation, the ISO may appoint a person to investigate an alleged breach and to provide a report or other documentation as the ISO requires, and the ISO may recover the cost of the investigator from the Rules Participant.

5.1.9 When the Authority is investigating an alleged breach by the ISO under Rule 313 of the Rules, the ISO's investigation powers and functions described in this section 5.1 of the Procedure are to be read as references to the Authorities powers and functions.

5.2 Investigation Pprocess

See Rule [311; 312; 316]

5.2.1 Where, using a risk-based assessment, the ISO has determined that an investigation is to occur on an alleged breach, the following investigation process will apply.

Assessment phase:

5.2.2 On becoming aware of an alleged breach the ISO will:

(a) Record the alleged breach; and

(b) Assign a risk rating to the alleged breach to determine if investigation is required and to determine the priority of ~~prioritise~~ the investigation.

Investigation phase:

5.2.3 If the ISO determines that an investigation is required based on the risk assessment and prioritisation process:

(a) The ISO will notify the Rules Participant alleged to be in breach;

(b) The ISO may request further information from the Rules Participant on the alleged breach;

(c) To establish the facts of the alleged breach, the ISO may gather evidence from relevant parties such as:

i. ISO C~~c~~ontrol D~~d~~esk;

ii. Other Rule Participants; and

iii. Any other person.

(d) The evidence gathered will be recorded and stored in the ISO's record management system;

(e) Where the ISO's preliminary findings are that the Rules Participant had breached the Rules or Procedures, the Rules Participant will be given notice of the ISO's preliminary findings including the reasons and rationale for the findings and will be requested to make a submission in response to these preliminary findings.

Submissions must be in writing and made via email to submissions@pilbaraisoco.com.au.

(f) When requesting a submission response to preliminary findings the ISO will work with the Rules Participant to determine a timeframe appropriate to the matter being considered. The ISO will reasonably consider extensions to these timeframes where sufficient justification has been made by the Rules Participant;

(g) The ISO may meet with the Rules Participant alleged to be in breach at any stage during the investigation process;

(h) Any further information provided by the Rules Participant alleged to be in breach will be taken into consideration when finalising the investigation;

(i) At any stage of the investigation, the ISO may suspend or close the investigation in accordance with section 5.4 of this Procedure;

(j) The investigation findings will be documented in an internal investigation report.

Outcome phase:

5.2.4 On conclusion of the investigation phase:

(a) The ISO must determine either that a breach has occurred or no breach has occurred;

(b) The ISO will notify the ~~r~~Rules P~~p~~articipant of the outcome of its investigation;

(c) If an investigation finds that a breach has occurred, the ISO must publish a notice identifying the breaching Rules Participant and, subject to Rule 316, setting out reasonable details of the breach; and may direct the Rules Participant do or refrain from doing a thing in order to remedy the breach or prevent its recurrence See Rule [312(6)(a)(i)]. This notice must meet the requirements of Rule 316, confidentiality of compliance matters;

(d) The ISO will assess the final risk of the non-compliance to determine the:

i. Materiality of the breach;

ii. Appropriate investigation outcome; and

iii. Whether it needs to direct a Rules Participant to do or refrain from doing a thing in order to remedy the breach or prevent its recurrence.

(e) Where the ISO has determined that no breach has occurred, it must record the closed investigation and the reasons for the determination. The ISO must give notice that no breach has occurred to:

i. The Rules Participant that was alleged to have breached; and

ii. To any Rules Participant who notified the ISO of the alleged breach; and

iii. If the Rules Participant that was alleged to have breached is the ISO, the Minister.

(f) When the ISO's compliance action recommends the implementation of any actions by the Rules Participant alleged to be in breach, the ISO may follow up on the progress of implementation of those actions;

(g) The ISO will record the outcomes of its investigation.

5.2.5 Each investigation will be carried out in a manner appropriate to the circumstances of the matters alleged to be in breach and consistent with Rule requirements.

5.2.6 At any time during an investigation, the ISO may suspend or close the investigation in accordance with section 5.4 of this Procedure.

5.3 Investigation Outcomes

See Rule [312] See Regulation [19]

5.3.1 Where the ISO determines a breach has occurred, the ISO will consider the appropriate compliance action in response to the breach.

5.3.2 In accordance with Rule 312(6)(a)(ii), the ISO may direct a Rules Participant to do or refrain from doing a thing in order to remedy the breach or prevent its recurrence. This may include:

(a) education or advice to assist with future compliance;

(b) a compliance program, such as additional reporting, to increase monitoring and prevent recurrence;

(c) issue a warning to the Rules Participant, and record the Rules Participants response to the warning See ~~f~~Rule [312(2)(b) & (c)];

(d) direct the Rules Participant to remedy the breach if it is still occurring See ~~f~~Rule [312(6)(a)(ii)];

~~{f~~Note: The only obligation which currently has a statutory penalty for non-compliance under the Regulations is the requirement to be registered under the Rules, See Regulation [19]~~}~~.

5.3.3 At the conclusion of its investigation, the ISO will notify the Rules Participant in writing of any compliance actions to be undertaken. This will be determined on a case-by-case basis, having regard to the risk assessment and individual circumstances applicable to the matter.

5.3.4 If the breach was not self-reported, ~~T~~the ISO may also notify the Rule~~s~~ Participant who reported the breach of the compliance actions being undertaken~~, if the breach was not self-reported~~, if the ISO considers this to be appropriate and permitted under confidentiality provisions in the Rules.

5.3.5 The following process will be applied by the ISO when determining any compliance action to be undertaken:

(a) Consider the breach risk assessment score of the obligation under section 4.4 of this P~~p~~rocedure;

(b) Review the information identified as part of the investigation, to determine if any change to the risk score is required (for example if remedy action has already been undertaken) and then assign an updated risk rating to the breach;

(c) Record the breach risk rating;

(d) The final breach risk rating will determine whether any compliance action is undertaken.

Table 3: Compliance action determined by risk rating

Risk Rating	Compliance Action
	Final risk assessment
Low	Education or advice to assist with future compliance
Moderate	Education or advice to assist with future compliance Potential for~~to~~ increased monitoring to~~and~~ prevent recurrence Potential to direct R~~r~~ules P~~p~~articipant to remedy the breach, if still occurring
Significant	Warning issued Increased monitoring to prevent recurrence Potential to direct R~~r~~ules P~~p~~articipant to remedy the breach, if still occurring
Extreme	Warning issued Increased monitoring to prevent recurrence Direct R~~r~~ules P~~p~~articipant to remedy the breach, if still occurring

5.4 Suspending or E~~e~~early C~~c~~losure of an Investigation

5.4.1 If an alleged breach was self-reported to the ISO under Rule 310(1) and the ISO is reasonable satisfied that:

(a) If a breach can be rectified, the Rules Participant:

i. Has rectified the alleged breach; or

ii. Undertakes to rectify the alleged breach by taking actions agreed to by the ISO.

(b) When required to by the ISO, the Rules Participant agrees to take actions agreed to by the ISO intended to prevent recurrence of the alleged breach.

The ISO may suspend or close an investigation of an alleged breach.

5.4.2 The ISO may also:

(a) Suspend an investigation if:

i. During the investigation, the risk rating of the alleged breach falls to a moderate or low risk rating~~below the investigation threshold~~; or

ii. The Rules Participant agrees to undertake actions to mitigate or prevent recurrence but has not yet completed those actions.

(b) Close an investigation if:

i. The Rules Participant alleged to have breached the Rules or Procedures is no longer a legal entity; or

ii. An investigation has been suspended for 6 months or more.

5.4.3 When the ISO suspends or closes an investigation, the ISO will:

(a) Notify the relevant Rules Participant of the suspension or closure by email; and

(b) Record the suspension or closure of the investigation, including the reasons for suspending or closing the investigation.

5.4.4 If the ISO suspends an investigation, it will reassess the suspended investigation every 6 months to determine if the investigation should be closed, reopened or suspended for a further 6 months.

5.4.5 A suspended investigation may be closed where:

(a) Rule Participants have completed any outstanding actions agreed to with the ISO;

(b) New information is received that results in a decrease in the risk rating to a moderate or low risk rating of the alleged breach; or

(c) No further alleged non-compliant behaviour has been identified.

5.4.6 A suspended investigation may be reopened where:

(a) Participants have failed to complete outstanding actions by timeframes agreed to with the ISO;

(b) New information is received that results in an increase in the risk rating of the alleged breach; or

(c) The ISO identifies that the alleged breach forms part of a pattern of non-compliant behaviour.

5.4.7 An investigation may be suspended again for reassessment where:

(a) Participants still have outstanding actions agreed to with the ISO; or

(b) There has not been sufficient time for the ISO to assess if the alleged breach forms part of a pattern of non-compliant behaviour.

5.4.8 If the ISO reopens or closes a suspended investigation, it will notify the relevant Rules Participant in accordance with paragraph 5.4.3 of this Procedure.

6. Enforcement

6.1 Warnings

See Rule [312(2)(b)]

6.1.1 Where the ISO determines that a breach of the Rules has taken place, it may issue a warning to the Rules Participant to rectify the alleged breach.

6.1.2 Where the ISO considers that a warning is appropriate the warning must:

(a) Identify the specific paragraph~~clause~~ or paragraphs~~clauses~~ of the Rules or Procedures that are believed to have been or are being breached;

(b) Describe the behaviour considered to be non-compliant;

(c) Request an explanation where the ISO considers it relevant; and

(d) Request rectification of the breach of the Rules or Procedures~~contravention~~, where relevant, including a timeframe that the ISO considers to be reasonable to accomplish the request.

6.1.3 The ISO will provide the warning by email to the person nominated as the primary contact for the Rules Participant under section 4.3.3 of this Procedure or alternatively to any other appropriate officer of the Rules Participant as the ISO considers appropriate.

6.1.4 The ISO will specify in the warning the timeframe within which the Rules Participant is required to provide the explanation referred to in paragraph 6.1.2(c) of this Procedure. The Rules Participant is required to provide the explanation within the specified timeframe. The explanation is required to be in writing and may be provided to the ISO by email to submissions@pilbaraisoco.com.au

6.1.5 The Rules Participant may request the ISO to extend the timeframe to provide the explanation referred to in paragraph 6.1.2(c) of this Procedure in writing.

6.1.6 On receipt of a response to a warning from the Rules Participant, the ISO will record the response of the Rules Participant.

6.2 Electricity Review Board

See Rule [312; 313; 314]

6.2.1 In accordance with Rule 314, a notice published by ISO identifying that a breach has occurred by a Rules Participant under Rule 312(6)(a)(i) or a notice published by the Authority identifying that a breach has occurred by the ISO under Rule 313(4) may be challenged before the Electricity Review Board.

7. Recording and Reporting

7.1 Report to Minister

See Rule [313; 314; 315; 316]

7.1.1 The ISO must annually provide to the Minister a report for the preceding year which includes:

(a) All alleged breaches (including its own); and

(b) The outcome of each investigation; and

(c) Any matter referred to the Authority under Rrule 313(1)~~, alleged rules breach by the ISO~~; and

(d) Any proceedings that have been brought before the Electricity Review Board in connection with ISO's compliance function and the Electricity Review Board's findings and final orders in connection with those matters.

7.1.2 Subject to the confidentiality of compliance matters provided in Rule 316, the ISO must publish this report on its website.

7.1.3 The ISO may from time to time publish a report on any one or more matters referred to in section 7.1.1 of this Procedure.

7.2 ISO Aaudit Rreport

See Rule [318]

7.2.1 In accordance with Rule 318, the ISO must appoint an auditor no later than 2 years after the Rules Ccommencement Ddate to undertake an audit of:

(a) The ISO's internal Pprocedures and business processes compliance with the Rules; and

(b) The ISO's compliance with the Rules and Procedures; and

(c) The ISO's software systems and processes for software management; and

(d) Any other matter the ISO considers appropriate.

7.2.2 In each subsequent audit report, the auditor, having regard to the findings of its audit, is to recommend a period of no more than 5 years, within which the next audit must be conducted.

~~7.2.2~~7.2.3 Within 30 business days after receiving the auditor's report the ISO must publish it, and must either:

(a) Accept the report and any recommendations it contain; or

~~(b)~~ Publish a separate report setting which of the matters raised in the auditor's report the ISO accepts and which it does not accept, and give reasons for that view.

~~(c)~~(b)

Appendix A. Relevant Rules

Table 4~~1~~ details the Rules under which this Procedure has been developed and where an obligation, process or requirement has been documented in this Procedure.

Table 4~~1~~: Relevant R~~r~~ules

Pilbara Networks Rules
85
172
307
308
309
310
311
312
313
314
315
316
317
318
Sub-appendix 4.14
Electricity Industry (Pilbara Networks) Regulations 2021
Regulation 19

Appendix B. Risk Framework and Tables

Risk Framework

Consequence rating table – The consequence of the risk is the effect or outcome to the NWIS of a risk eventuating. Categories are areas that would influence the ability of the NWIS to function. Consequences are rated on a scale of 1 to 5, with 1 being insignificant and 5 being catastrophic. For each consequence category, criteria are defined for each level specified.

Likelihood rating table – Likelihood describes how likely it is that a risk will eventuate with the defined consequences. This is measured on a scale of 1 to 5, with 1 being rare and 5 being almost certain, based on the frequency of the obligation occurring.

Risk matrix tables – Used to assign a risk rating from the risk score. Risks are scored by multiplying the consequence and likelihood ratings to obtain a risk score. The risk score is used to assign a risk rating as per the risk matrix table.

Table 5~~2~~: Consequence Rating Table

Level	Rank	Health and Safety	Damage to P & E	System Security/Reliability	Financial (direct and indirect)
1	**Insignificant**	First aid	No measurable damage to plant and equipment No plant outage	Power system secure state maintained [Rule 164] Technical non-compliance only No load shedding System remains within Frequency Band (49.75 to 50.25 Hz)	No direct or indirect financial impact to participants
2	**Minor**	Medical treatment only	Damage to plant and equipment resulting in a plant outage ≤1 day	No load shedding System is not within Frequency Band (49.75 to 50.25 Hz) but within Frequency Band (49.00 to 51.00 Hz)	Estimated financial consequences: • Offending participant gain ≤ $250k • Other participant loss ≤ $250k

Level	Rank	Health and Safety	Damage to P & E	System Security/Reliability	Financial (direct and indirect)
3	Moderate	Injury requiring ≤ 5 days hospitalisation Ongoing medical treatment	Damage to plant and equipment resulting in a plant outage >1 day - ≤ 3 days Facility fully restored within a week	No load shedding System is not within Frequency Band (49.75 to 50.25 Hz) but within Frequency Band (49.00 to 51.00 Hz)	Estimated financial consequences: • Offending participant gain > $250k to ≤ $1m • Other participant loss > $250k to ≤ $1m
4	Major	Serious injury requiring > 5 days hospitalisation Localised impact on public safety	Damage to plant and equipment resulting in a plant outage > 3 days - ≤ 5 days Facility fully restored within month	Load Shedding occurs (up to 17%) System is not within Frequency Band (49.75 to 50.25 Hz) but within Frequency Band (48.75 to 51.00 Hz)	Estimated financial consequences: • Offending participant gain >$1m to ≤ $5m • Other participant loss >$1m to ≤ $5m
5	Catastrophic	Single fatality Permanent injury Widespread threat to public safety	Damage to plant and equipment resulting in a plant outage > 5days Facility cannot be fully restored	Load Shedding occurs (> 17%) System is not within Frequency Band (48.75 to 51.00 Hz) or black start required.	Estimated financial consequences: • Offending participant gain > $5m • Other participant loss > $5m

Table 63: Likelihood Rating Table

Level	Rating	Description	Control environment
1	Rare	Breach may occur in exceptional circumstances (<10% probability)	No history of breaches. Compliance mechanisms are in place and operating effectively. Controls are strong with no control gaps. The strength of the control environment means that, if a breach eventuates, it is highly likely a result of external circumstances beyond the control of a Participant.
2	Unlikely	Breach is unlikely to occur in most circumstances (10-30% probability)	One or two historical breaches Compliance mechanisms are mostly in place and operating reasonably effectively Controls are strong with few control gaps. The strength of the control environment means that, if a breach eventuates, it is likely a result of external factors not known to the Participant.
3	Possible	Breach may occur, but not expected in most circumstances (30-50% probability)	Few historical breaches Compliance mechanisms are mostly in place but need further improvement There are some controls that need improvement, however, if there is no improvement there is no guarantee that a breach will eventuate
4	Likely	Breach can be expected to occur in most circumstances (50-90% probability)	Multiple historical breaches Compliance mechanisms are not all in place and not further improvement The majority of the controls are weak. Without control improvement it is more likely than not that a breach will eventuate
5	Almost Certain	Breach will occur in most circumstances (>90% probability)	Several historical breaches Compliance mechanisms are not in place and need significant improvement All of the controls are extremely weak and/or non-existent. Without control improvement there is almost no doubt that a breach will eventuate

Table 74: Risk Matrix Tables

			Consequence				
			1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	5	Almost Certain	5	10	15	20	25
	4	Likely	4	8	12	16	20
	3	Possible	3	6	9	12	15
	2	Unlikely	2	4	6	8	10
	1	Rare	1	2	3	4	5

Risk Assessment				
Assessment	Low	Moderate	Significant	Extreme
Score	1-5	6-9	10-14	15-25