Telecommunications (Jersey) Law 2002

Case T-027: Outage of network of JT (Jersey) Limited on 12 July 2020: Decision and Directions to JT (Jersey) Limited

PUBLISHED VERSION

Document No: JCRA 21/38 Date: 17 September 2021

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street
St Helier
Jersey, JE2 3RF Tel
01534 514990

Web: www.jcra.je

Contents

Section

1. Executive Summary

1.1 At 18:55 on 12 July 2020, JT's network on Jersey stopped functioning (the '**Outage**'). Services began to be restored from 21:44 – nearly three hours later. The majority of services to JT's Channel Islands customers were fully recovered by 3am on 13 July 2020, although its international services were not fully recovered until 5pm on 14 July and some remaining mobile issues were not finally resolved until 12 noon on 17 July 2020. The Outage affected many customers, including residential and business customers, across JT's fixed and mobile networks.

1.2 On 22 July, the Authority notified JT that it was commencing an investigation to understand the cause of the Outage, and whether it raised any regulatory concerns about JT's performance of its obligations.

1.3 JT's analysis is that the root cause of the Outage was a failure in a piece of JT's network equipment, that failed to register the 'resetting' of a date measure (the 'week number'). Although the complete picture only became apparent after the event, JT's own analysis is that:

(a) the source of that problem was known prior to the Outage.

(b) JT was conscious of the specific risk of failure arising (due to media reporting).

(c) JT relied on an assurance from one of its suppliers in Q1 2019 that the equipment deployed in the network was not vulnerable to the risk. In April 2019, JT monitored the equipment and as no issue was encountered JT did not believe that there was a future vulnerability.

(d) In the event, that assurance turned out to be wrong.

1.4 The Authority considered material provided by JT (including two technical reports) and also commissioned independent technical advice.

1.5 This Decision sets out the basis on which the Authority finds that JT has contravened the obligations set out in Conditions 9 and 14 in its licence. The Authority is issuing directions to JT on the terms set out in Section 7, Annex 1.

1.6 In summary, the primary reason for finding JT in contravention is that:

(a) In relation to its obligations relating to network resilience (Condition 9), JT's network equipment was susceptible to failure and JT failed to act to a sufficient standard on material information that set out the nature of the failure that could have, and did, occur; and

(b) In relation to its obligation to maintain a continuous 999 service (Condition 14), JT's service was not maintained during the Outage. Whilst JT's call centre was ready and able to take calls throughout, and some customers were able to use roaming on other networks to get through, for some customers (e.g., those on the JT fixed network), 999 was completely unavailable. As with other outages of the 999 service, this is a very serious contravention that necessarily exposes JT's customers to risk of harm or death in an emergency.

1.7 The Authority considered whether JT was additionally in breach of Condition 17 of its licence (relating to operating its network in accordance with international best standards and with specific standards published by international telecommunications bodies). Although the Authority felt that there were strong indications on the evidence that JT had failed in this respect, it concluded that the evidence as it stood was not such as to enable it definitively to conclude that JT breached Condition 17. In any event, a finding of contravention in relation to Condition 17 would not have materially changed the Directions imposed on JT.

1.8 The Authority is particularly concerned by the evidence about the level of rigour and assurance undertaken in relation to JT's reliance on a third party expert to test a critical issue upon which the network's resilience was ultimately found to depend. JT's submission argues that it is required from time to time to rely on third parties in at least some respects to support its network. The Authority does not dispute this. But that makes it all the more important that JT has the requisite skills and processes to manage and verify the outcomes of third party testing. In this case, JT's reliance was on a single email with a less than unequivocal assurance ('*the quick answer is that your equipment should be ok*'). That decision, amongst others, fell materially short of the standard that the Authority expects of licensees when relying on third parties for such critical inputs.

1.9 Because everyone who lives and works in Jersey relies, to a lesser or greater extent, on JT's network, it is particularly important that it is resilient and robust. On that basis, the findings of this investigation merit not only specific consideration of the systems that failed, but also a wider effort to make sure that the network is secure and being operated in a way that is consistent with international best practice and that maintains continuity of service, including in relation to 999 services. The Directions being imposed (which JT has accepted) will put in place a process that will help JT to ensure it is operating a network that operates to the standards that its licence requires and the people who live and work on Jersey would expect.

1.10 The Directions are set out in Annex 1. These Directions address the initial failings identified by the Authority in its investigation. The Authority also has the power to impose a penalty and/or to impose further directions (if that is justified by the evidence). In keeping with its established practice and the terms of the Telecoms Law, the Authority will consider the question of whether to impose a penalty and/or further directions as the next phase of this matter. Any proposed actions will be put to JT in the form of a Notification in accordance with the terms of the Telecoms Law.

1.11 JT has 28 days from the date of this Decision to confirm the necessary steps it will take to comply with the Directions.

2. Regulatory framework

Summary

2.1 This section briefly sets out the main elements of the legal framework relevant to the investigation undertaken by the Authority. It addresses the regulatory obligations that apply to licensed telecommunications operators in Jersey that are relevant to this Decision.

2.2 The key points are that:

(a) JT has clear obligations to adhere to international best practice, to ensure integrity of its network and to ensure that that network provides public emergency call services at all times.

(b) If an operator contravenes a licence condition, the Authority can enforce that condition by issuing a direction and/or imposing a penalty.

(c) The Authority has other relevant powers to enable it to enforce and improve the regulatory regime, including to gather information or modify licence conditions.

Telecoms in Jersey is regulated primarily via licence conditions

2.3 In Jersey, telecommunications are governed by the Telecommunications (Jersey) Law 2002 (the "**Telecoms Law**"). Pursuant to Article 2(1) of the Telecoms Law, a licence is required to run part, or all, of a telecommunications system.

2.4 JT (the "**Licensee**") has a licence authorised by the Authority. JT's modified licence was issued on 4 August 2021 (with a commencement date of 30 June 2017) (the "**Licence**").[1]

JT's relevant obligations

Resilience and standards of operation

2.5 Condition 9 of the Licence is entitled 'Integrity of the Network'. Specifically, Condition 9.1 provides that:

> *9.1 The Licensee shall take all reasonable steps to ensure the integrity of the Network[2] and may refuse to provide the Telecommunication Services which it is obliged to, provided in accordance with Condition 13 of this Licence to a particular User if providing those Telecommunication Services would or would be likely to cause damage or interference to the Licensed Telecommunication System.*

2.6 Condition 17 of the Licence is closely related to Condition 9. It is entitled 'Development of Network and Services'. Condition 17.1 provides that:

> *17.1 The Licensee shall develop and operate the Licensed Telecommunications System[3] so as progressively to achieve standards in line with international best practice and in particular, the Licensee shall achieve and comply with relevant*

[1] Other licensed providers offering voice services are Sure Airtel-Vodafone and Homenet.
[2] As per the Licence, Network means a set of interconnected devices across which a telecommunicated message can be passed.
[3] As per the Licence, Licensed Telecommunication System means the system for the conveyance of messages through the agency of energy which the Licensee is authorised to establish, operate and maintain in the Bailiwick of Jersey.

standards established by ETSI, the ITU and such other international benchmarks as the JCRA may direct from time to time.

Continuity of 999 services

2.7 Condition 14 of the Licence is entitled Public Emergency Calls. Condition 14.1 provides that:

> *14.1 The Licensee shall provide a public emergency call service, being a Telecommunications Service[4] that enables a User at any time and without incurring any charge or using any coin or token, to communicate with the police, the ambulance or fire services or the marine search and rescue services and to notify them of an emergency by using Customer Premises Equipment lawfully connected to the Licensed Network at any place in the Bailiwick of Jersey.*

The Authority can enforce licence conditions by issuing a Direction

2.8 The Telecoms Law provides that:

> *where, in the opinion of the Authority, a licensee is in contravention of a condition contained in a licence, the Authority shall give a direction to the licensee to take steps, or specified steps, to ensure compliance with that condition.[5]*

2.9 According to Article 19(3) of the Telecoms Law, a direction shall:

> *(a) specify the licence to which it relates;*
>
> *(b) name the licensee or specify the class of persons to whom the licence has been granted; and*
>
> *(c) specify the condition contravened.[6]*

2.10 Article 19(2) specifies that, before issuing a direction, the Authority must give the licensee a notification that:

> *(a) sets out the direction which the Authority proposes to give to the licensee under paragraph (3);*
>
> *(b) specifies the period during which the licensee has an opportunity to –*
>
> *(i) make representations about the matters notified,*
>
> *(ii) comply with any conditions referred to in the notification in respect of which the licensee remains in contravention, or*
>
> *(iii) remedy the consequences of any contraventions referred to in the notification.*

2.11 Unless the Authority specifies that it should be shorter or longer under Article 19(2B) or Article 2(C) respectively, the length of the period referred to in Article 19(2) shall be:

[4] As per the Licence, Telecommunications Service means the provision of any telecommunications services to the public.
[5] Article 19(1) of Telecommunications (Jersey) Law 2002.
[6] Article 19(3) of Telecommunications (Jersey) Law 2002.

the period of 28 days beginning with the day after the one on which notification was given.

2.12 Article 19(4) sets out that a direction:

> *(a) Shall require the licensee to act or not to act, according to the nature of the condition and the contravention, in a manner specified in the direction;*
>
> *(b) May require the licensee to take steps, or specified steps, to remedy the effects of the contravention; and*
>
> *(c) May be modified at any time by the Authority, but only by giving a new direction in accordance with this Article.*

2.13 Article 19 also provides for instances in which the Authority should refrain from issuing a direction. Specifically, Article 19(2F) stipulates that:

> *the Authority shall not give a direction or notification under this Article if it is satisfied that its duties under Article 7* [Duties of Minister and Authority] *preclude the giving of a direction.*

2.14 Article 19(2G) allows that:

> *the Authority shall not give a direction under this Article [19] if it is satisfied that –*
>
> *(a) The contravention of the condition is trivial; or*
>
> *(b) The licensee is taking reasonable steps to comply with the conditions and to remedy the effects of the contravention.*

2.15 The Authority's view of Article 19(2G)(b) is that in assessing the reasonable steps that the licensee "*is taking*", the Authority can, and should, consider the steps that were taken before, during and following the contravention – in other words, the words "*is taking*" are not to be constructed narrowly as relating solely to the point in time when the decision to issue a direction is taken (although steps being taken at that point are also likely to be relevant). Instead, what Article 19(2G)(b) requires is that the Authority considers the steps taken by the licensee at each of the relevant points in time considered in the investigation, and assess whether, in the round, those steps fulfil the statutory purposes that would otherwise be served by issuing a direction, so as to render such a direction inappropriate.

2.16 Furthermore, Condition 5.1(b) of the Licence provides that, in addition to complying with the conditions of their respective licences:

> *…. the Licensees shall comply with any direction duly issued by the JCRA….*

The Authority can modify licence conditions

2.17 The Telecoms Law provides for the Authority to modify licence conditions. Article 18(1) of the Telecoms Law specifies that:

> *the Authority may, of its own motion or on the application of any person, modify any condition contained in a licence ……*

2.18 As set out in Article 18(3):

> *the power to modify a condition contained in a licence includes the power to insert a new condition or amend or delete an existing condition……*

2.19 Condition 6.1 of the Licence provides that:

> *the JCRA may from time to time modify, delete or add to any Condition in this Licence. Any modification, deletion or addition to the Conditions shall be made in accordance with Article 18 of the Telecommunications (Jersey) Law and any other requirements under any applicable Law.*

The Authority's power to gather information

2.20 Article 23 of the Telecoms Law provides the Authority with statutory basis upon which it is able to request information. In particular, 23(1)(a) allows the Authority, by notice in writing to:

> *require any person to produce to the Authority, or any person appointed by it for that purpose, any documents specified or described in the notice that are in the custody, or under the control, of the first-mentioned person and specify the time, manner and form in which those documents are to be furnished.*

2.21 Condition 4 of the Licence stipulates that the Authority is authorised to gather information from any licensee.

(a) Condition 4.3 states that:

> *the JCRA may require an examination, investigation or audit of any aspect of the Licensee's business relating to the Licensed Telecommunication System or its compliance with the Conditions and the Laws, and the Licensee shall provide any assistance requested by the JCRA in relation to any such examination, investigation or audit. The JCRA may issue directions with regard to the manner in which such an examination, investigation or audit is carried out, including the creation of financial and/or technical specifications or documentation.*

(b) Condition 4.4 states that:

> *in particular, the JCRA may authorise a person to carry out an examination, investigation or audit or may require the Licensee to arrange for an examination, investigation or audit of any aspect of the Licensed Telecommunication System to ensure compliance with the Conditions. The Licensee shall allow the JCRA's authorised representative to attend at, enter and inspect any premises under the Licensee's or any of its Subsidiaries or Joint Ventures control, and to take copies of any documents and to acquire any information in the control of the Licensee or any of its Subsidiaries or Joint Ventures, as may be required in order to carry out the examination investigation or audit.*

(c) Condition 4.5 states that:

> *the Licensee shall bear all reasonable costs associated with any examination, investigation or audit conducted under this Condition 4.*

The Authority can fine operators who have contravened licence conditions

2.22 Article 19A of the Telecoms Law provides that where a licensee has contravened or is contravening a licence condition, the Authority may, in addition to, or in place of a direction or other remedies,

> *Make an order imposing a financial penalty on the licensee for the contravention.*[7]

2.23 The maximum penalty that can be imposed is 10% of turnover during the period that the licensee was in contravention of the condition, to a maximum period of 3 years.[8]

[7] Article 19A(2) of Telecommunications (Jersey) Law 2002.

[8] Article 19A(4) of Telecommunications (Jersey) Law 2002 provides that '*A financial penalty imposed on a licensee or, if more than one financial penalty is imposed, the total of those penalties, must not exceed 10% of the turnover of the licensee during the period that the licensee was in contravention of the condition contained in the licence, to a maximum period of 3 years.*'

3. The Authority's investigation

Summary

3.1 This section explains the steps taken by the Authority in conducting its investigation. Annex 2 sets out a list of the documents and other material gathered during the investigation and to which the Authority had regard in relation to this decision.

Prior to the investigation

3.2 The Authority was first notified of the Outage at 09:10 on 13 July 2020, shortly before JT provided a Service Incident Report to the Authority, the Guernsey Competition and Regulatory Authority (the "**GCRA**") and the Justice and Home Affairs Department ("**JHAD**") at 09:21.

3.3 The Chair and CEO of the Authority subsequently met with JT's CEO and Director of Corporate Affairs on 14 July at 16:00. At that meeting, JT provided an update on the service incident and the Authority orally informed JT that it intended to undertake a formal investigation into the Outage.

The Authority's Investigation

3.4 Further to its meeting with JT on 14 July 2020, the officers of the Authority prepared a paper for the Authority's Board recommending the appointment of Cognitio Consultants Limited ("**Cognitio**") to undertake an investigation into the 12 July Outage, which would include a technical and governance / management audit. This was approved at a Board meeting on 20 July 2020.

3.5 Formal notification of the investigation was sent to JT on 22 July 2020.

The Technical Investigation

3.6 On 21 July 2020, the Authority commissioned Cognitio to undertake a technical investigation into the root causes of the Outage at JT (the "**Cognitio Technical Report**"), the findings and recommendations of which were provided to the Authority on 17 August 2020 (see paragraphs 4.50 to 4.54). A copy of the Cognitio Technical Report was shared with JT on 6 October 2020 and feedback from JT on that document was received on 16 October 2020.[9]

3.7 During the course of the technical investigation, Cognitio discovered that, in order for JT to have been able to recover the network in the period immediately after the Outage, JT needed to manually change the time on each affected router to replace the incorrect date. This, as well as the time elapsed between the incident and the Cognitio request for log information, resulted in serious gaps in available network logs and records. Consequently, the Cognitio investigation was limited in terms of the information retained and available in the network.[10]

The Management Audit

3.8 On 21 July 2020, the Authority commissioned Cognitio to undertake an audit of management and governance processes at JT and at Sure (Jersey) Limited ("**Sure**"). This was borne out of the

[9] JT's Response, Appendix 1A - Cover Note.
[10] Cognitio Final Report - Technical Investigation page 14.

fact that while the scope of the management audit encompassed the particular issues which arose within JT in relation to the Outage, the actual recommendation for this audit emerged out of the prior investigation undertaken as a result of the 999/112 failures during the period January – April 2020.[11]

3.9 As of the time when the Authority commissioned Cognitio to undertake the management audit, JT had consented to cooperating with the Authority. As such, Cognitio's assessment was limited to JT only. Cognito's presented the results of this assessment (the "**Cognitio Audit Report**") on 26 August 2020.

3.10 The purpose and the scope of the Cognitio Audit Report was to establish whether JT had the correct processes in place and was applying best practice to the management of projects. It specifically did not include an investigation of operations, capabilities and competencies at JT.[12]

The Authority's Proposed Directions – November 2020

3.11 Having considered Cognito's Technical Investigation and Management Audit, as well as JT's own Reasons for Outage Report (including the Addendum to the same) and a report commissioned by JT from Niji S.A. (the "**Niji Report**"; see paragraphs 4.44 - 4.49 for more detail), the Authority issued JT with a Notification of Proposed Directions on 19 November 2020 (the "**Notification**"). In doing so the Authority:

(a) Set out its provisional finding that JT had failed to take all reasonable steps to ensure the integrity of its network, and hence, prior to the Outage, was in contravention of Licence Condition 9;

(b) Set out its provisional finding that JT had contravened Licence Condition 17 on the grounds that it had not adhered to the standards and best practices required of it by that Condition; and

(c) Set out its provisional finding that JT failed to maintain its 999 service during the Outage and was therefore in contravention of Condition 14. Specifically, during the Outage:

(1) From 18:55 to 21.44, JT's fixed customers had no 999 access at all;

(2) From 18:55 to 21:44, JT's mobile customers may have had roaming access to the 999 service provided by other licensees, but no access to a 999 service provided by JT

with some customers unable to access 999 until services were fully restored by 03:00 on 13 July 2020.

JT's response to the Authority's Proposed Directions

3.12 JT provided a written response to the Authority on 18 December 2020 ("**JT's Response**"), which contained the following appendices:

(a) Appendix 1A – Cover Note;

[11] Cognitio Report 1 - Root Cause Investigation into 999, 112 Incidents during first half of 2020, dated 7 July 2020.
[12] Cognitio Final Report – Audit of operator processes supporting network change and key factors underpinning licence obligations, page 6.

(b) Appendix 1B – JCRA Initial Notice - Comments for Response: setting out JT's comments on the Authority's Notification;

(c) Appendix 1C – JT's Comments on Cognitio's Final Report - Audit of operator processes supporting network change and key factors underpinning licence obligations;

(d) Appendix 1D – JT's Comments on Cognitio's Final Report -Technical Investigation;

(e) Appendix 2 – Report undertaken by Craig Newton (the "**Newton Report**"), commissioned by JT on 8 October 2020 to provide an assessment of JT's Synchronisation & Timing (Network Time Protocol) deployment.

The Touchstone Report

3.13 On 13 May 2021, following review of JT's response to the Authority's Proposed Directions, the Authority issued a further information request to gather more detail on the root causes of the Outage and the steps that JT had taken prior to and after the Outage to mitigate the risks which ultimately led to the Outage.

3.14 At the same time, the Authority commissioned an independent expert report by Touchstone Consulting Limited (the "**Touchstone Report**"). The Authority commissioned the Touchstone Report to analyse the events leading to the Outage based on the information provided by JT on 25 May 2021 (and subsequent addenda) in response to the Authority's information request, as well as earlier relevant documents from the investigation.

3.15 The Touchstone Report aimed to:

(a) Provide a brief summary of the Outage;

(b) Identify the root cause(s) of the Outage;

(c) Summarise JT's response to the Outage before and after the event;

(d) Discuss a number of pertinent issues and observations highlighted by the Outage and JT's response to it, which may help to mitigate the risk of future incidents and assure the resilience of JT's network as it continues to evolve to meet future requirements.

The Authority's e-mail to JT – 19 July 2021

3.16 Following JT's review of, and representations on, the Touchstone Report, the Authority wrote to JT confirming that it would move to a Final Decision.

3.17 The e-mail confirmed that the Final Decision would incorporate the findings in the Touchstone Report and that the issues and observations set out in the Touchstone Report would be incorporated into the Authority's Directions annexed to the Final Decision.

3.18 Subsequent to this Final Decision and annexed Directions, the Authority will further deliberate, in consultation with JT, on any further Directions and/or penalties to be applied in this case.

4. Relevant facts

Summary

4.1 This section sets out the Authority's findings of fact relevant to the Authority's investigation. It includes:

(a) Background information, including about JT's network and the Outage;

(b) JT's immediate actions to understand what happened in the Outage and to report on the root causes (including subsequent further reporting as more information about the Outage became available);

(c) A report by Niji that JT commissioned to be an independent review of the Outage, its causes and the remedial steps that ought to be taken subsequently;

(d) Two reports by Cognitio, commissioned by the Authority to provide it and JT with an independent review of the Outage and its causes;

(e) Further information provided by JT following the Authority's information request of 13 May 2021; and

(f) A report by Touchstone Consulting Limited, commissioned by the Authority to provide it and JT with an independent review of the Outage and its causes, following the Authority's further information request.

4.2 These facts have been updated to take into account points raised in JT's response to the Authority's Notification, including its appendices.

Background

JT's network

4.3 JT's services rely on an IP (Internet Protocol) network. JT operates a network composed of around 100 IP routers provided by Cisco and configured to a Cisco approved design.

4.4 These routers, which transport all of JT's fixed and mobile traffic, are connected to two clock sources, known as Network Time Protocol ("**NTP**") servers, through the IP network.[13] These NTP servers had been provided by two different vendors.

The 12 July outage

4.5 At 18:55 on 12 July 2020 there was a malfunction in one of the two NTP servers. This ultimately led to the Outage across the entire JT network.

4.6 JT began to restore its network from 21:44 on 12 July 2020. The network was restored in its entirety at 12 noon on 17 July 2020.[14] The Notification therefore referred to the incident as being the period from 18:55 on 12 July 2020 to 12 noon on 17 July 2020, during which the effects of the Outage continued to persist (the "**Incident**").

[13] JT's Preliminary Outage Report, page 1.
[14] A more detailed timeline of restoration by service is set out at paragraph 4.42.

Immediate Aftermath

4.7 At 01:52 on 13 July 2020 JT informed 999ECH@JT365.onmicrosoft.com by email that its IP Core, fixed and mobile network suffered a critical incident at approximately 19:00 on 12 July.[15] It described the following:

(a) JT fixed line/landline subscribers were unable to make or receive calls, including the inability to make a 999 call from their landline.

(b) JT mobile subscribers lost network services but were still able to make 999 calls from their mobile device. During the Outage, a significant volume of 999 calls were handled by JT agents from JT mobile customers and other service providers and forwarded onward to the Contact and Control Room ("**CCR**") where relevant. Engineers were continuing to investigate attempts made to call 999 from fixed line numbers and would provide these to the CCR where applicable.

(c) Fixed line services were restored in stages from around 22:00 on 12 July 2020.

4.8 At 09:21 on 13 July 2020, JT provided a Service Incident Report to the Authority, the GCRA and the JHAD.[16] This stated that the severity of the issue was "*major*" and that the root cause remained "*under investigation*". It specified the issue as follows:

> *Widespread failure of JT connectivity within Jersey, in and out of Jersey including Landline broadband and mobile services.*
>
> *Failure of Guernsey mobile network.*
>
> *JT customers unable to make 999 on Jersey landlines but 999 available from mobiles.*[17]

4.9 Evidence concerning the availability of 999 services included that:

(a) At 08:36 on 13 July 2020 JT confirmed to the Authority by email that it understood that there had been no fixed line 999 calls during the Outage but that the States of Jersey Police had received 16 mobile calls from JT customers via the Sure network.[18]

(b) In an email from JT to the States of Jersey Police at 14:05 on 14 July 2020, JT confirmed that it had established there were a total of 156 calls to 999 received by JT for call handling between 19:00 and midnight on 12 July 2020. 28 of those calls required a transfer to the CCR - 23 to Police, 4 to Ambulance and 1 to Fire.[19]

4.10 The Chair and CEO of the Authority subsequently met with JT's CEO and Director of Corporate Affairs on 14 July at 16:00. At that meeting, JT provided an update on the service incident. The Authority verbally informed JT that it intended to undertake an investigation into the Outage.

[15] Email from executive at JT to 999ECH@JT365.onmicrosoft.com at 01:52 on 13 July 2020.
[16] Email from senior executive at JT to Authority, JHAD and GCRA representatives at 08:21 on 13 July 2020
[17] JT Service Incident Report.
[18] Email from senior executive at JT to Authority, JHAD and GCRA representatives at 08:36 on 13 July 2020.
[19] Email from executive at JT to representative of the States of Jersey Police and the JHAD at 14:05 on 14 July 2020.

JT's Reasons for the Outage

Preliminary Reason for Outage Report

4.11 At 18:03 on 15 July 2020, JT provided its preliminary Reason for Outage Report ("**Preliminary RFO**") to the Authority setting out its assessment of the Incident as it understood it to be as of 15:00 on 15 July 2020.

4.12 This Preliminary RFO referred to the Incident as "*the most critical JT has ever experienced and… exceptional due to both its size and its duration.*" It stated that those services that JT delivered to its Channel Islands customers had almost been fully recovered by 03:00 on 13 July 2020, with its international services being restored by 17:00 on 14 July 2020. Some ongoing mobile issues remained at the time of Preliminary RFO. [20]

4.13 Describing the cause of the Incident as a "*sequence of events that was almost impossible to foresee,*" the Preliminary RFO stressed that the exact reason for the Incident remained subject to further investigation.[21] It nonetheless stated that it believed that the likely reason for the malfunction in one of the two NTP was because there was "*a hardware failure in the clock (NTP server) which caused a card to reset back to its original factory parameters*."[22]

4.14 While the Preliminary RFO provided reasoning for the Outage and a description of its impact, these details were, to a large extent, repeated in greater depth and with a further degree of clarity in JT's subsequent final Reason for Outage Report and JT's Addendum to that final Reason for Outage Report as provided to the Authority on 23 July 2020 and 4 August 2020 respectively (see paragraphs 4.17 to 4.26).

4.15 The Preliminary RFO described the impact of the Incident on JT's 999 emergency call provision. It stated that JT's 999 emergency call handling contact centre "*continued to operate and successfully transferred incoming emergency calls to the appropriate emergency service throughout*" the Incident and that JT received 156 emergency calls between 09:00 BST and 23:59 BST on 12 July, of which 28 required transfer to the emergency services.[23] According to the Preliminary RFO "*users in Jersey could place 999 calls using mobile telephones from any of the three networks*," (these being JT, Sure or Airtel-Vodafone) whereas fixed line subscribers could not place calls during certain periods of time.[24] JT users making a 999 call on a mobile phone "*were connected via either the Sure or Airtel local Jersey infrastructure under standard GSMA emergency call handling protocols*."[25]

4.16 JT also informed the Authority that the faulty clock (NTP Server) had been decommissioned and that, at the time of writing, JT was operating with just one clock. It stated that a new clock would be installed later during that same week in order to ensure that JT would be able to return to a redundant NTP Server source. It indicated that it had been actively working with Cisco to disable the time-based password mechanism related to the IS-IS feature and that, with Cisco, it had

[20] JT's Preliminary Outage Report, page 1.
[21] JT's Preliminary Outage Report, page 4.
[22] JT's Preliminary Outage Report, page 3.
[23] JT's Preliminary Outage Report, page 1.
[24] These periods of time are set out in a table in the Preliminary RFO albeit that this is not done so in a very clear or comprehensive fashion.
[25] JT's Preliminary Outage Report, page 1.

jointly designed a Method of Procedure which it planned to deploy as an emergency change later than same week. JT stated that, after the completion of that change, its network would "*no longer be vulnerable to the propagation of the wrong time/date stamps*" and that a "*repeat of the incident* [would] *therefore be impossible*."[26]

Final Reason for Outage Report

4.17 On 23 July 2020, JT provided the Authority with its final Reason for Outage report (the "**RFO Report**").

4.18 The RFO Report was largely similar to the Preliminary RFO, although it was extended to cover the actions which JT took subsequent to the 15 July 2020 in order to completely remove the cause of the Outage.

4.19 The RFO Report also went further than the Preliminary RFO in adding clarity and structure to the sequence of events which had led up to the Outage. These were described as follows:

(a) At 18:55 on 12 July 2020, one of the two NTP servers generated a wrong date (actually 27/11/2000, instead of 12/07/2020).

(b) Those routers which had this NTP server as their primary source clock did not switch to the secondary clock source. Instead, they started to propagate this incorrect time stamp to other routers across the JT network.

(c) Information is exchanged between routers across the JT network using a protocol called Intermediate Systems to Intermediate Systems ("**IS-IS**"). In order to secure the IS-IS protocol each router is designed to authenticate with its neighbour using a locally stored password.

(d) The local password can only be considered valid by the IP router from an explicit configured date in the router of 1 July 2012, this being the date which JT believes to be when its first Cisco IP routers were deployed. Given that the date transmitted (27/11/2000) was earlier than the password validity start date (01/07/2012) the router stopped working as it no longer had a valid password to communicate with its neighbours.

(e) Consequently, at 18:55 of 12 July 2020, 15 of JT's 100 routers receiving the wrong date, isolated themselves from the rest of the network and made 35 additional routers unreachable. Having lost around half of the network, inherent resilience was lost which ultimately led ultimately to the outage across the entire JT network.[27]

4.20 In seeking to provide an explanation as to why its clocks had sent an incorrect date, JT repeated the cause that it had referred to in the Preliminary RFO - that there had been a "*hardware failure in the NTP server which caused a card to reset back to its original factory parameters*."[28] JT stated that it had investigated other possible causes included "*the possibility of a GPS malicious spoofing".* However, JT concluded that this has been eliminated as a possible cause on the basis

[26] JT's Preliminary Outage Report, page 4.
[27] JT'S RFO Report, page 2.
[28] JT's RFO Report, page 3.

that there were "*other network elements which use the same GPS signal which remained in full sync with the right date."*[29]

4.21 The RFO Report also gave reasons why JT had limited customer communication during the outage. JT stated that because the Incident had caused it to lose access to all of its corporate services, it could not reach its customer databases or use its email services from the Channel Islands. While some JT personnel located outside the Channel had access to emails, they did not have access to JT's central databases nor to the Business Continuity team. In this regard, the RFO Report concluded that there was a need on JT's part *"for more robust customer communications during service incidents"* going forward.[30]

Addendum to the RFO Report

4.22 On 4 August 2020, JT provided the Authority with an Addendum to its RFO Report (the "**RFO Addendum**"). This confirmed that, while the Preliminary RFO Report and the RFO Report itself had specified that the initial assessment of the reasons for the defect clock source was that it was caused by a "*a hardware failure in the NTP server resulting in a card resetting back to its original factory parameters*,"[31] subsequent investigation by JT uncovered that this was not the case.

4.23 Instead, the NTP server had reset itself to 27/11/2000 on 12/07/2020 as a result of the GPS time system upon which JT's NTP servers obtained their time. The firmware implementation of the NTP server which interpreted the GPS week number (WN) value in turn relied on a counting system which reached the end of its cycle on 12/07/2020. The counter looped back to zero at that point, which had the knock-on effect of setting the clock back to 27/11/2000, resulting in the consequences set out at paragraphs (d)4.19(d) and 4.19(e) above.[32]

4.24 The RFO Addendum went into further detail concerning the reasons why the failure in the GPS based clock system had arisen. These are set out below, as taken directly from the RFO Addendum.

> *JT's NTP servers obtain their time from GPS sources.*
>
> *The GPS Time system uses a count of Week Number (WN) and seconds per week to represent time. This is interpreted by GPS devices (NTP server) to translate the GPS Time to UTC [Coordinated Universal Time] format.*
>
> *The WN parameter is made of ten bits which counts weeks from 0 to 1023*[33] *and increments from a start date.*
>
> *That start date is stored in the device providing the clock (NTP server).*
>
> *The default GPS WN start date is 6/01/1980 and this initiated what is called EPOCH1. The WN value increments to 1023, at which point it rolls over to 0. So*

[29] JT's RFO Report, page 3.
[30] JT's RFO Report, page 3.
[31] JT's RFO Report, page 3.
[32] Addendum to JT's Final Reason for Outage Report.
[33] The counter is a binary counter with ten bits (0 or 1). 210 = 1024 which is the highest value the counter can reach before resetting to zero.

EPOCH2 started after 1024 weeks from the start date and EPOCH 3 started a further 1024 weeks after this, on 6/04/2019.

Prior to the 6/04/2019 WN rollover event, JT had liaised with its support providers to determine the potential impact of the EPOCH transition. JT's NTP support provider conducted tests on the clock to ensure the EPOCH transition would not have any impact on the clock integrity. The tests executed in collaboration with our device distributor were successful.

On 6/04/2019 itself, as part of its standard preventive maintenance practices, JT monitored the behaviour of the platforms which use the NTP source to ensure there was no impact to the network integrity during the EPOCH transition.

On the day of the Incident, the NTP server reset itself to 27/11/2000 instead of 12/07/2020 . This is an interval of 1024 weeks.

The cause of this clock resetting in this defective manner was that the WN register on the NTP server has passed 1024 weeks, looping back to 0.

This event, combined with our time-based password management, caused the damages we have experienced on July 12th.[34]

4.25 The RFO Addendum also set out three reasons why JT missed this issue, specifically:

(a) The existence of a different start date in its NTP server was never called-out nor mentioned to JT in exchanges which it had with those third parties involved.

(b) Devices which use GPS to provide a clock signal have different implementations which are left to the manufacturer's choice.

(c) Because JT had successfully passed the EPOCH3 transition, and had assurance from its support provider, it thought the implementation in its NTP server was able to manage the EPOCH transition.

4.26 JT concluded the RFO Addendum by emphasising the steps which it proposed to take to ensure this issue does not happen again. Specifically:

(a) JT assured the Authority that it had "*already had a replacement of* [its] *synchronisation system…. in* [its] *implementation roadmap in 2020*" and indicated that it was in a position to execute this plan. In particular, JT stated that this plan would include the introduction of timing sources other than GPS.[35]

(b) JT stated that, as a short-term measure, it had "*already implemented 2 NTP servers from different manufacturers*"(see paragraph 4.16 above where JT had already referred to this in the Preliminary RFO) and that it was planning to introduce a third one. JT explained that its reason for taking this action was that "*by having three clock sources,* [its] *router equipment can discard one clock source if it differs from the other two*".[36]

[34] RFO Addendum, pages 1-2.
[35] RFO Addendum, page 2.
[36] RFO Addendum, page 2.

JT's Final Analysis of Clock Reset Cause

4.27 On 28 July 2020, JT provided a further document to the Authority in relation to the cause of the clock reset, entitled JT's Final Analysis of Clock Reset Cause.

4.28 This analysis repeated much of the detail that had already been provided in the RFO Report and the RFO Addendum. However, it went further in making the following points:

(a) JT had been made aware of a risk to GPS timing in October 2018 through information published in the media (theregister.com). In preparing its Final Analysis of Clock Reset Cause for the Authority, JT provided an earlier memorandum from the US Department of Homeland Security which sought to make critical infrastructure owners and operators who obtain UTC from GPS devices aware of the GPS Week Number (WN) rollover events and the possible effects a GPS WN rollover may have on the reliability of the reported UTC in advance of the 6 April 2020 Rollover.[37] The memorandum stated that, tests of some GPS devices revealed that "*not all manufacturer implementations correctly handle the April 6, 2019 WN rollover*" and that while devices should not be affected by the WN rollover on 6 April 2019, some "*may experience a similar rollover event at any future date*". The memorandum strongly encouraged critical infrastructure owners and operators "*to investigate and understand their possible dependencies on GPS for obtaining UTC*".[38]

(b) In addition to the memorandum, in preparing its Final Analysis of Clock Reset Cause JT was provided with a presentation entitled - *CGSIC GPS Week Roll Over Issue - Edward Powers, US Naval Observatory*. This presentation served to further substantiate the warnings set out in the memorandum.[39]

(c) At no point did JT receive notification from Oscilloquartz, its distribution partners, or its support channels relating to a known Week Number Rollover Event issue on the 5581C platform. This resulted in JT consulting with its synchronization / NTP Support provider in March 2019. After testing, the provider concluded that the "*GPS engines will react to the rollover but the shelf does handle the adjustment.*"[40]

(d) JT monitored services on 6 April 2019 to ensure the anticipated roll-over event did not interrupt service or timing on the network. In May 2019, its support provider carried out a health check of the synchronization estate, during which "*no actions were raised relating to the NTP servers or risk from Week Number Rollover Event*."[41]

(e) Subsequent to this, JT commenced a synchronization refresh program, which included temporary replacement of one NTP server. It also set about scoping a replacement synchronization and NTP server solution to ultimately replace the Oscilloquartz 5581C.

[37] US Department of Homeland Security, Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time – Upcoming Global Positioning System Week Number Rollover Event, as referred to in JT's Final Analysis of Clock Reset Cause, dated 28 July 2020.
[38] US Department of Homeland Security, Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time – Upcoming Global Positioning System Week Number Rollover Event, as referred to in JT's Final Analysis of Clock Reset Cause, dated 28 July 2020, pages 1-2.
[39] CGSIC GPS Week Roll Over Issue - Edward Powers, US Naval Observatory, dated 26 September 2017, as referred to in JT's Final Analysis of Clock Reset Cause, dated 28 July 2020, pages 1-2.
[40] JT's Final Analysis of Clock Reset Cause, page 1.
[41] JT's Final Analysis of Clock Reset Cause, dated 28 July 2020, page 1.

JT's response to the May 2021 RFI

4.29 Further information relating to the Outage was provided by JT in its response to the Authority's request for information ("**RFI**") of 13 May 2021 (the "**May 2021 RFI**").

4.30 In this response, JT stated that "*investigations with Cisco continued until the end of 2020, and therefore were not reflected in the original Cognitio reports, and may not have been finalised in the original JT responses to the Authority*".[42]

4.31 JT summarised its findings in relation to the 'Panic Timer' on the Cisco IOS XR NTP Client, namely that:

> *JT's efforts in understanding the root cause, and mitigation steps to take to avoid future incidents have focused on the Cisco NTP Client behaviour, and notably Cisco's decision to not implement the 'Panic Timer' on their IOS XR operating system. Arguably, whilst the NTP server injected an invalid time into the network, it is the NTP Clients filtering and selection algorithms which are responsible for detecting and disregarding falsetickers, and it was the Cisco NTP Clients failure to appropriately handle this which triggered the network incident.*[43]
>
> *[…]*
>
> *Further detailed soak testing, log analysis and debug analysis corroborated that the Cisco IOS XR NTP Client did not implement the 'Panic Timer' that would normally cause an NTP Client to ignore an NTP Server exceeding 1000 seconds variance.*[44]

4.32 JT also undertook an internal Options and Recommendations review (dated November 2020), which was provided as part of JT's response to the May 2021 RFI. In its response to the May 2021 RFI JT summarised that:

> *Whilst every effort can be made to secure the robustness of the NTP architecture, JT believe that a small risk would persist which could be exploited given the Cisco NTP Client behavior with regards the Panic Timer.*
>
> *As such, JT recommend to retain static ISIS passwords until such time (if ever) the option to implement the Panic Timer on the Cisco NTP Client is implemented.*[45]

4.33 In relation to the Oscilloquartz NTP server that failed, JT set out in its response to the May 2021 RFI that:

> *JT were aware that the Oscilloquartz OSA 5581C GPS-SR was end of sale and end of support with the manufacturer... JT were also aware that sourcing hardware replacements for the Oscilloquartz NTP server was becoming problematic. Under a failure condition, if a suitable replacement NTP card could not be sourced, JT's back-up position was to purchase an alternative NTP server.*
>
> *Ahead of the 12th July incident, this scenario had already played out at the JT Central site, where the NTP Server had been replaced with a loan Oscilloquartz OSA 5420 (November 2019), and a replacement NTP Server (Brandywine TFS NTP 80), installed in May 2020.*

[42] JT's response to the May 2021 RFI, page 1.
[43] JT's response to the May 2021 RFI, page 1.
[44] JT's response to the May 2021 RFI, page 5.
[45] JT's response to the May 2021 RFI, page 5.

4.34 JT's response revealed that Edge Networks' assurances that "*We have carried out a lot of proactive simulation testing regarding this matter*" and "*The quick answer is your current equipment should be ok. The GPS engines will react to the rollover but the shelf does handle the adjustment ok*" was provided in a single email dated 26 March 2019.[46] No further details of the simulation testing undertaken by Edge Networks were sought by JT.

4.35 JT also engaged Edge Networks to undertake a Synchronisation Health Check in May 2019. JT does not appear to have provided specific instructions to Edge Networks on the nature of the synchronisation tests that should be conducted.

4.36 JT's reasoning in this respect was that:

> *JT are not synchronisation and timing experts, and would not seek to direct Edge Networks in their testing methodology, tools or procedures. As the support provider for Adva / Oscilloquartz, and experts in synchronisation and timing, JT did not seek further detail once a positive answer had been provided.*[47]

4.37 The response also outlined that JT did not have a support contract for its NTP servers from January 2019 to November 2019, following the failed novation of its support contract from Horsebridge to Edge Networks that had been due to take place by the end of 2018. JT was therefore engaging with Edge Networks on a "good will basis" during this time.[48] Edge Networks was, however, formally engaged to carry out the Synchronisation Health Check.[49]

JT's assessment of the impact of the Incident

4.38 JT stated in the RFO Report that the majority of its services were impacted by the Incident, specifically:

(a) Mobile voice and data for JT subscribers in the Channel Islands or roaming abroad;

(b) Fixed voice and data subscribers in the Channel Islands;

(c) JT internal corporate services;

(d) Internet of Things ("IoT"), FPS and bulk messaging services for international customers; and

(e) Internal communications.

4.39 Amongst the routers impacted were two which terminate JT's submarine cable connections to the UK (London), and one which terminates JT's submarine cable connection to France (Paris). In addition, each of the four routers which are used as "*gateways to JT's georedundant mobile network core systems located in Jersey and Guernsey"* were also impacted.[50]

4.40 In order to restore service, JT engineers had to physically attend the multiple sites where the effected routers are located and manually update the time on each. As such, the majority of services on the Channel Islands themselves were restored by 3am on 13 July 2020. However,

[46] JT's response to the May 2021 RFI, Appendix 5.
[47] JT's response to the May 2021 RFI, page 8.
[48] JT's response to the May 2021 RFI, page 27.
[49] JT's response to the May 2021 RFI, page 8.
[50] RFO Report, page 2.

additional time was required to reach the routers located outside of the Channel Islands, with the JT router in Paris not being corrected until 4pm BST on 13 July 2020.

4.41 Therefore, while the majority of services to JT's Channel Islands customers were fully recovered by 3am on 13 July 2020, its international services were not fully recovered until 5pm on 14 July and some remaining mobile issues were not finally resolved until 12 noon on 17 July 2020.

4.42 The RFO Report provided a table setting out the exact durations of the outage for each of JT's different services. This table is set out below:

Service	Time to partial recover - HR:MM	Time to full recover - HR:MM
FTTP Voice	02:49	04:46
FTTP Broadband	Straight to full	05:57
Guernsey Broadband	Straight to full	05:57
CI Mobile Voice / SMS	02:49	04:46
CI Mobile Data	Straight to full	05:57
CI Private Circuit	05:57	21:00
INT IoT	05:57	42.12
INT Roaming	05:57	42.12
INT FPS	05:57	28:49
INT Bulk Messaging	05:57	TBC
JT Internal communication services - Voice	Straight to full	04:46
JT internal communication services – Data	Straight to full	05:57

4.43 The RFO Report confirmed that JT had acted upon the immediate short-term next steps which it had indicated that it would address in the Preliminary RFO. The RFO Report set these out as follows:

(a) In parallel to taking steps to ensure the full recovery of its service, JT had commenced working actively with Cisco to disable the time-based password mechanism related to the IS-IS feature.

(b) The Method of Procedure, which was jointly designed by Cisco and JT, had been implemented in a maintenance window during the night of 16 / 17 July. This was completed by 5am on 17 July 2020. Having effected this change, JT was confident that

there was no longer any potential risk of the wrong time / date stamp being propagated through its servers, rendering a repeat of the Incident impossible.[51]

Niji Report

4.44 On 24 September 2020, JT provided the Authority with the report of an independent review carried out by Niji S.A. (the "**Niji Report**"), which the JT Board had commissioned on 31 July 2020.

4.45 JT specifically instructed Niji that the review should encompass the following:

(a) To examine the circumstances inside JT leading up to the Incident;

(b) To conduct an independent assessment of JT's handling of the Incident;

(c) To review the action already identified to reduce the risk of incidents and to improve recovery times;

(d) To provide recommendations for further improvements; and

(e) To provide recommendations to improve JT business continuity planning and execution.

4.46 In carrying out its report, Niji undertook interviews with JT personnel, several JT customers (both international and Jersey-based) and JT vendors.

4.47 The Niji Report was published on 23 September 2020 and made the following findings[52]:

(a) JT had conducted an independent test of the NTP server, whose failure led to the Incident, in May 2020. No issues for concern were identified at that point in time and the circumstances which led to the incident with the JT network on 12 July 2020 were "*exceptional*". Niji also noted that, to its knowledge, the circumstances of the Incident had not happened before at JT and that it was "*unaware of this happening elsewhere*."[53]

(b) JT did not have an effective disaster recovery plan for such an incident and due to the total loss of connectivity it was not possible for JT to mobilise its business continuity management ("**BCM**") process. In any event, at the time the Incident occurred this BCM process had not been practiced by JT since 25 September 2019.

(c) The nature of the problems which led to the Incident were diagnosed "*relatively quickly*" by JT's technical team. JT remediated the cause of the Incident on 17 July 2020 by disabling the time-based password management on all IP routers and removing the dependency of IP traffic on clock accuracy.[54]

(d) JT had a major problem with customer communication both during and after the Incident. Specifically, there was a lack of inbound and outbound communication in the early stages. When communication was re-established, the information which was given to customers was "*not always clear, accurate or coordinated*."

(e) As of the date of publication of the Niji Report, many of the immediate high-impact steps necessary to improve resilience and responsiveness had been understood by JT and some

[51] RFO Report, page 3.
[52] JT Incident of 12 July 2020: An Independent Review by Niji, dated 23 September 2020, page 3.
[53] Letter from JT to JCRA dated 24 September 2020 attaching the Niji Report.
[54] JT Incident of 12 July 2020: An Independent Review by Niji, dated 23 September 2020, page 4.

actions had been completed. Some enterprise-wide business processes remained incomplete and there continued to be communication gaps, leading to a higher risk of error.

4.48 In light of its findings, the Niji Report set out a series of recommendations across four principal areas[55]:

(a) Technology

(1) JT should complete its service assurance programme as soon as possible;

(2) JT should conduct a full independent audit of its IP core and major support systems; and

(3) JT should accelerate its plans to deploy tools to achieve better end-to-end visibility and more efficient management of its networks and the services they support.

(b) Process

(1) JT should implement a standards-based business continuity planning (BCP) process that integrates with all major organisational processes, and where appropriate, with the systems and processes of key customers and other stakeholders; and

(2) JT should strengthen processes for technical change management, end-to-end service management, communications and recovery management.

(c) People

(1) JT should capture and codify important knowledge that at present resides in the heads of many of its more experienced staff and enhance its training programmes for technical staff as well as those in customer-facing roles.

(2) JT should review current roles and when necessary, address gaps in areas such as product and service management.

(d) Customers and Other Stakeholders

(1) Within the growing IoT market segment, JT would benefit from working more closely with its clients to better understand the challenges which they face.

4.49 JT has indicated its acceptance of each of the recommendations.[56]

The Cognitio Reports

Technical Investigation

4.50 The Cognitio Technical Report was provided to the Authority on 17 August 2020. Drawing upon information requested of and provided by JT, it assessed the technical issues which contributed to the cause of the Incident, as well as setting out prescriptive recommendations designed to address these issues.

[55] JT Incident of 12 July 2020: An Independent Review by Niji, dated 23 September 2020, pages 3-4.
[56] Letter from JT to JCRA dated 24 September 2020 attaching the Niji Report.

4.51 As regards the root cause of the Incident, the Cognitio Technical Report broadly concurred with JT's own internal assessment, specifically:

(a) The root cause came from the NTP Server whose internal clock had reached its range limit and had automatically cycled back to zero.

(b) This caused the NTP Server to reset its internal calendar to a firmware date implemented by the manufacturer - the reset date - with the intention of re-starting this cycle. Whilst technically a valid date, the reset date was not the actual date.

(c) The NTP Server propagated this reset date to other Servers in the network.

(d) The reset date was outside the recognised range of the internal security protocol operating within the other routers and this then caused authentication to fail, thereby preventing transmissions between connected routers.

(e) This brought to a stop all traffic in JT's core network resulting in the large-scale outage.[57]

4.52 The Cognitio Technical Report also drew attention to the fact that during the major network outage both the Production Network and the Operational Management Networks suffered major outages, which also caused Emergency Services to be critically impacted.[58]

4.53 **[REDACTED]**

4.54 The Technical Report summarised its assessment as follows: **[REDACTED]**

The Audit Report

4.55 The Cognitio Audit Report was provided to the Authority on 26 August 2020.

[57] Cognitio Final Report - Technical Investigation Report, pages 8 – 9.
[58] Cognitio Final Report - Technical Investigation Report, page 14.
[59] Cognitio Final Report - Technical Investigation Report, page 11.
[60] Cognitio Final Report - Technical Investigation, page 15.

4.56 The Audit Report found that JT's project management office ("**PMO**"), operations and security functions are executed in a professional manner which is compatible with industry best practices.

4.57 Nevertheless, the Cognitio Audit Report found that there were key areas for concern. In particular:

(a) That the JT network has delayed upgrades, legacy issues **[REDACTED]**

(b) **[REDACTED]**

(c) That JT offers a tier 1 type service which is "*central to their marketing and proposition*."[62] However, this does not correspond accordingly to the level of service provided. Tier 1 service at the very least requires the provision of basic telephony services for delivery of emergency service traffic (999) at a very high level and grade of service that outperforms other aspects of its service and prioritises those services.[63]

JT's response to the Authority's Notification – December 2020

4.58 JT responded to the Notification on 18 December 2020. While JT accepted the scope of the Proposed Directions (subject to further detail), it took issue with what it referred to as "*technical and/or factual errors"* in the Notification, the Cognitio Technical Report, and the Cognitio Audit Report.[64]

4.59 JT accepted that it had breached Licence Condition 14 and did "*not contest that as a result of the 12 July Incident it failed to provide a public emergency call service during the incident.*"[65]

4.60 However, JT did not accept that it had breached Licence Conditions 9 and/or 17.

4.61 In relation to Licence Condition 9, the JT Response maintained that the Authority had erred in its interpretation of this Condition, arguing that the Condition only applied to control over the network insofar as it was necessary to protect it from third parties and that the Authority was wrong to consider that the Condition concerns network resilience. The Authority considers JT's submissions on Licence Condition 9 in section 5.

4.62 In relation to Licence Condition 17, the JT Response maintained it could not be considered in breach. This was on the basis that adherence to the condition merely provides for a "*mechanism for* [the Authority] *to mandate … the relevant standards*" and to provide direction as regards the international benchmarks which JT as licensee was required to comply with.[66] JT alleged that the Authority had applied this mechanism properly in the past and as a consequence argued "*it would be inappropriate and unfair to penalise JT retrospectively.*"[67]

[64] JT's Response, paragraphs 2 & 3, 31 & 32.
[65] JT's Response, paragraph 60.
[66] JT's Response, paragraph 51.
[67] JT's Response, paragraph 54.

Technical or Factual Errors

4.63 JT's Response argued that it had taken all reasonable steps to ensure that the Week Number Rollover Event issue did not impact on its network. It disputed that it failed to anticipate the issue and that it relied unduly on the actions and assurances of a third party rather than testing the specific concerns relating to the issue itself. JT maintained that it itself "*did not have the expertise or the facilities to determine whether the Week Number Rollover would be an issue*" and therefore appointed a third party specialist (Edge Networks (UK) Ltd) to do so.[68] While JT acknowledged, *"with the benefit of hindsight"*, that Edge Networks' assessment was wrong, it nonetheless maintained that it was "*wholly reasonable for JT to rely on such an assurances, but there was nothing at the time which would or should have indicated to JT that its reliance on such assurances was undue*".[69]

4.64 JT's Response maintained that the findings of the Cognitio Reports contained numerous, fundamental factual and technical errors which in turn were carried through to the Notification.[70] JT alleged that these errors were at least in part due to the fact that Cognitio chose to only have limited engagement with JT during its technical investigation as well as for the purposes of compiling the Audit Report.[71] Instances of what JT deemed to be examples of this limited engagement were set out in broad summary in Appendix 1A of the JT Response.[72]

The Newton Report

4.65 On 8 October 2020, JT commissioned Mr Craig Newton to *"provide an independent assessment of Jersey Telecoms Synchronisation & Timing (NTP) deployment."* The Newton Report was highly critical of the findings of the Cognitio Reports and, by extension, the Notification. In particular, it stressed that:

(a) JT "*have invested considerable time, effort and money in the establishment of a robust, resilient and carrier class synchronisation and timing network*."[73]

(b) JT have "*always procured and operated carrier class network synchronisation and timing equipment.*"[74]

(c) NTPv3, as utilised by JT is not an obsolete standard, indeed NTP by its very nature is not a 'standard', it is a protocol and captured within RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation and Analysis (ietf.org) and is globally accepted and utilised as a timestamp referencing system in a variety of mission critical applications.[75] The OSA 5581C GPS-SR Synchronisation Supply Unit, utilises NTPv3, with good reason, NTPv3 is a fully ratified standard, NTPv4 is not and is still in the ratification process, although it is widely deployed.

[68] JT's Response, paragraph 7a.
[69] JT's Response, paragraphs 8 & 12.
[70] JT's Response, paragraph 14.
[71] JT's Response, paragraph 15.
[72] JT's Response - Appendix 1A, page 3.

The Touchstone Report

4.66 Following the Authority's consideration of JT's responses to the Notification, the Authority issued a further information request to JT in May 2021 and commissioned a further independent expert report by Touchstone Consulting Limited.

4.67 Based on the evidence presented by JT, the Touchstone Report concluded that:

"…the root cause of the Outage were deficiencies in the design and implementation of both the NTP client and NTP server functions by the original equipment manufacturers/suppliers of the Oscilloquartz 5581C NTP server and the Cisco IOS XR NTP client, and a previously unidentified critical dependency of the Cisco ISIS time-based keychain authentication protocol for inter-router traffic on JT's IP Core Network on a reliable NTP time source (providing a time within the validity timeframe of the keychain)."[76]

4.68 The Touchstone Report highlighted a number of issues and observations, in summary that:

(a) The original NTP services were end of life, outside support and kept going on spares. Whilst one of the NTP servers was initially replaced with a loaned NTP server and eventually replaced by a new NTP server in May 2020 – had the WNRO warning prompted JT to replace both NTP servers, the Outage may have been avoided.[77]

(b) The contractual support arrangements with Horsebridge/Edge Networks for the NTP servers were inadequate and JT allowed them to persist for some time before a support contract with Edge Networks was established in November 2019.[78]

(c) JT relied heavily on assurance from Edge Networks that the NTP servers would correctly handle the WNRO issue but did not follow-up to obtain Edge Network's findings from their simulation testing of the WNRO event on the NTP services as supporting evidence for Edge Network's conclusions.[79]

(d) Once JT had received assurance from Edge Networks, and after keeping watch over the rollover event, which passed without incident, there seems to have been no further action taken by JT prior to the Outage, despite a clear warning that WNRO events could happen at other times depending on different implementations.[80]

(e) Following the Outage, whilst the NTP server was taken out of service and the suspected 'faulty' NTP module was tested in another shelf, there seems to have been no further follow-up with Edge Networks or Oscilloquartz/Adva for forensic analysis of the shelf/module firmware to confirm the cause of the time roll-back.[81] This means that a hardware error, rather than a firmware error, remains as a possible alternative explanation.[82]

[76] Touchstone Report, page 2.
[77] Touchstone Report, page 6.
[78] Touchstone Report, page 7.
[79] Touchstone Report, page 7.
[80] Touchstone Report, page 7.
[81] Touchstone Report, page 7.
[82] Touchstone Report, page 8.

(f) Whilst JT has, since the Outage, added a third NTP server (to resolve a potential conflict between two NTP servers showing different times) JT's synchronisation/timing refresh remains outstanding.[83]

(g) The scope of the High-Level Design (HLD) and Low-Level Design (LLD) documents provided by JT are limited to JT's Cisco IP previous/refreshed Core Network, and do not document JT's wider network design. The limited scope of the HLD/LLD documents may have masked a wider understanding of the behaviour of, and any critical dependencies on, non-Cisco network elements interacting with the Cisco IP core network.[84]

(h) LLD Version 1.8 (June 2020) 'highly recommended' that an Out-of-Band (OOB) management capability be implemented to provide an alternative to in-band management, in the event that in-band communication was interrupted, but an OOB management capability was only implemented by JT after the Outage. This meant that each core network location (including those in London and Paris) had to be physically visited by JT's network engineers to set static passwords on the core network routers at all locations.[85]

(i) Points (g) and (h) taken together leads to the following potential consequence: had JT conducted an LLD walkthrough based on a 'what if' assumption derived from the prospect of a WNRO event, the critical dependency between a significant roll-back in NTP time and the starting date for key chain authentication validity could have been spotted – if the dependency could have been identified, reverting to static passwords (as applied after the event) could have led to the Outage being avoided.[86]

(j) Time-based key chain authentication is widely recognised as best practice for IS-IS authentication in IP core networks, it is widely used by other network providers, and should be re-introduced into JT's core network once the issues that caused the Outage have been fully resolved. JT's current practice of using static unchanging passwords should be viewed as an interim solution as it would not be compliant with best practice network security policy.[87]

(k) JT did not seem to have an effective Disaster Recovery Plan for this kind of network incident, and the total loss of internal communications capability within JT due to the Outage meant that JT was unable to mobilise its Business Continuity Process, which led to a slow response by JT, particularly in relation to JT's customers affected by the Outage. JT, in conjunction with the Authority, needs to develop an assurance framework to build and maintain confidence in the ongoing integrity of JT's network as it evolves to grow in capacity and to meet any new requirements.[88]

[83] Touchstone Report, page 8.
[84] Touchstone Report, page 8.
[85] Touchstone Report, page 8.
[86] Touchstone Report, page 8. The Report notes that 'Network behaviour between multiple devices and multiple protocols is inherently complex, making critical dependencies difficult to spot'.
[87] Touchstone Report, page 9.
[88] Touchstone Report, page 9.

JT response to the Touchstone Report – June 2021

4.69 The Touchstone Report was provided to JT for comment on 16 June 2021. On 28 June 2021, JT responded with its comments. Few comments were provided by JT on the Touchstone Report.

4.70 Two of the more substantive comments made by JT were that:

(a) *"JT had no reason to consider that the Cisco NTP client would behave in an abnormal manner. Whilst, with the benefit of hindsight, it can be stated that the dependency and risk 'could have been spotted', JT would counter, that with the information available to it at the time, we would have expected the Cisco NTP client to ignore the falseticker and continue to maintain it[s] system time"*;

(b) *"…the event happened during an exceptional period, notably Covid-19 restrictions, which limited JT and 3rd party access to JT and remote premises. Regardless, JT acknowledge the flaws in invoking the Business Continuity Process and have taken steps as part of the Service Assurance Plan to revise the BCP contact process (including providing key staff with alternative communications devices from another service provider), and taken steps to improve Business Continuity and Disaster Recovery planning."*

4.71 In response to point (a) the Authority observes, per the observations in the Touchstone Report, that JT have not provided evidence that it had been through a detailed process (such as an LLD Walkthrough) prior to the Outage to try to understand whether a WNRO event could have had any adverse consequences on the network.

4.72 In response to point (b) the Authority observes that, whilst the impacts of Covid-19 have undoubtedly had negative impacts on many businesses, Covid-safe measures must have been available to JT which would have enabled it to avoid a complete outage across the JT network. The Authority recognises and welcomes the steps subsequently taken by JT to date.

5. Analysis and evidence of breaches

Summary

5.1 This section sets out the Authority's analysis in support of its decisions concerning contraventions of JT's relevant licence conditions.

5.2 The relevant issues arising are:

(a) Did JT take '*all reasonable steps*' to ensure the integrity of its network, in accordance with the requirements of Condition 9?

(b) Did JT achieve outcomes '*in line with international best practice*' and relevant ETSI and other standards, in accordance with the requirements of Condition 17?

(c) Did JT maintain a 999 service '*at all times*' in accordance with the requirements of Condition 14?

(d) If the answer to any of the above questions is 'no' – what steps are the appropriate steps to require JT to take in a direction that responds to those contraventions?

5.3 The Authority's conclusions are that, in the lead-up to and during the Outage:

(a) JT failed to take all reasonable steps to ensure the integrity of its network, and so contravened Condition 9.

(b) while there are strong indications that JT did not achieve outcomes '*in line with international best practice*', the evidence as it stands does not enable the Authority to conclude with certainty that JT contravened Condition 17.

(c) JT did not maintain a 999 service '*at all times*', and so contravened Condition 14.

(d) The Authority should issue a direction in the terms set out in Annex 1.

JT's reporting was timely and, for the most part, clear

5.4 During the period following the outage, JT provided sequential reports that ultimately built a detailed picture of what happened. Section 4 sets out the relevant points in detail.

5.5 There is no criticism to be drawn from the fact that JT's explanation developed over time and that JT's best available view of the causes of the outage evolved with further information. That said, it is disappointing that additional information on JT's interactions with Cisco only came to light following the Authority's further information request of May 2021. Where there has been such a critical outage in Jersey, the Authority would expect to be kept proactively informed of such developments.

5.6 For the most part, JT's reporting is clear and factually oriented. The Authority has relied on those reports as agreed factual findings in any decision about whether to issue directions to JT (together with the other evidence set out in Section 4).

5.7 There were a few instances where JT appeared to adopt an approach to reporting designed to minimise bad news or draw attention away from the relevant failures or problems. For example, rather than reporting clearly that 999 calls from JT's directly connected fixed customers were not completed, the Preliminary RFO stated that (emphasis added):

It is important to note that throughout the service incident JT's 999 emergency call handling contact centre continued to operate and successfully transferred incoming emergency calls to the appropriate emergency service. Users in Jersey could place 999 calls using mobile telephones from any of the three networks. ***Fixed line subscribers could not place calls during the timings outlined below.*** *JT users making a 999 call were connected via either the Sure or Airtel local Jersey infrastructure under standard GSMA emergency call handling protocols. On the day itself JT received 156 emergency calls between 09:00 BST on the 12th July and 23:59 BST of which 28 required transfer to the emergency services. This compares with an average Sunday when we would expect to see 41 calls and transfer 18 of those.*

5.8 This text does not present the critical (emphasised) fact clearly: despite the fact that JT's CHA operated continuously, during the outage, JT was not able to connect its own customers to that CHA service, and such calls either failed in the case of fixed customers, or were passed via emergency roaming over other networks. Instead, the text switches between a discussion of the CHA element alone in the first sentence, making a point about the services that were not interrupted in the second, before placing the key information in the middle of the paragraph. Furthermore, the placement of this information in the third sentence also relies on the reader having to combine information in the text and table to understand it. The paragraph then switches back to referring to JT users as being able to make a 999 call when in fact it was only JT's *mobile* users, and not fixed subscribers, who could do so. The final sentence deals with how many calls JT actually received, but it fails to address the key fact - that it is unknown how many calls would have been made but were not able to be placed due to the Outage.

5.9 In all contexts but especially in relation to technical/incident reporting, the Authority urges JT to focus on clear reporting, and to avoid presenting factual points in a manner which frames them in a particular light. Such an approach is in direct conflict with the primary purpose of reporting, which is to offer a clear and transparent explanation (including to its customers) of what went wrong and why.

JT's compliance with Condition 9

Approach to assessing compliance with Condition 9

Approach taken by the Authority in the Proposed Direction

5.10 Condition 9 requires JT to '*take all reasonable steps to ensure the integrity of*' its network. It does not require, directly, that a licensee provides a continuous service and the fact that an outage occurs, by itself, is not sufficient to demonstrate a contravention of Condition 9.

5.11 Although Condition 9 contains slightly different wording, it is closely aligned in its objectives with similar provisions contained in other regulatory regimes that also regulate the steps that operators or licensees must take to manage risks to their networks and services and to ensure resilience.[89] In assessing compliance with Condition 9, the Authority therefore intends to have regard to the approach taken by other regulators in relation to these aligned provisions.

5.12 Although in this case, the '*integrity*' of the network arises in relation to the resilience and continuity of services provided over the network, the Authority considers that Condition 9 has

[89] For example, section 105A of the Communications Act 2003 (UK), which sets out rules 'to protect the security of networks and services'.

wider application and is engaged in relation to a range of threats to network integrity, including (for example) the physical security of network infrastructure, cybersecurity, and the protection of key assets such as customer data or the content of communications passing over the network.

5.13 The '*reasonable steps*' taken to ensure the integrity of a licensee's network are, by definition, matters that are taken in advance of problems occurring. By their nature, that means that the steps regulated by Condition 9 include:

(a) Risk assessment and risk management within the licensee's business. This is likely to include both initial risk assessment and mitigation, and also an ongoing programme of risk management;

(b) Accountability and management of risk and security, including whether there are clear lines of accountability up to and including at Board level.

5.14 Condition 9 will continue to apply notwithstanding that some of the steps required by it are also required under other conditions or regulatory obligations. For example:

(a) Because there are applicable standards developed by the telecommunications industry and endorsed by various standards bodies specifically in relation to risk management and security, a failure to adhere to those relevant standards could be both a failure to comply with Condition 9 (because the licensee failed to take steps that those standards require) and Condition 17 (which applies relevant industry standards directly); or

(b) Failure to properly protect data integrity could constitute a failure under data protection law.

JT's submissions on Licence Condition 9

5.15 In relation to Licence Condition 9, the JT Response maintained that the Authority had erred in its interpretation of this Condition in at least two respects. JT argued that:

(a) the Authority had misconstrued the meaning of Licence Condition 9. JT argued that the licensee's obligation is to ensure that it remains in control over the management of its network by preventing third parties who would be likely to cause damage to or interference with the functions of the licensee's network;[90] and

(b) the Authority was wrong in taking the view that Licence Condition 9 concerns the obligation to ensure network resilience. Rather, JT maintain that Licence Condition 9 is only concerned with the ensuring network integrity and that *"when applied to telecommunications, integrity cannot be substituted for the term resilience as the two terms hold separate and distinct meanings."* [91]

5.16 JT's submission noted that:

> *34. On an ordinary reading, Licence Condition 9 refers to the licensee's obligations to ensure that it remains in control over the management of its network. In particular, the mischief at which Licence Condition 9 is directed is to ensure that*

[90] JT's Response, paragraph 34.
[91] JT's Response, paragraphs 35 & 38.

the licensee should not allow third parties to interfere with its functions. This is supported by the reference to third party users who "would be likely to cause damage or interference" to the telecommunication system.

35. Licence Condition 9 is not focused on network "resilience"; not only does the term not appear in the text of the condition, but when applied to telecommunications, "integrity" cannot be substituted for the term "resilience" as the two terms hold separate and distinct meanings in relation to telecommunication systems.

5.17 The footnote to paragraph 35 notes that:

The International Telecommunications Union (the ITU referred to in Licence Condition 17) defines "Integrity" in relation to an integrity protected environment such as the network as "An environment in which unauthorized data alterations (including creation and deletion) are prevented or detectable."; it defines "network resilience" as "The ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation of a given communication network, based on prepared facilities."

5.18 JT also submitted that the Authority's approach to Licence Condition 9 is novel or a departure from the stance previously taken by the Authority.[92]

The Authority's reasoning

5.19 The Authority understands JT's submissions to be, at their core, that:

(a) The term 'integrity' should be read as limited to the absence of specific forms of 'mischief' being third-party interference with the network; and

(b) Specifically, that it is to be read as exclusive of, or distinct from, the concept of 'resilience' (which the Authority considers to be closely related and, in part, overlapping with, 'integrity' of the network).

5.20 The Authority's starting point is that the construction of Licence Condition 9 should apply established principles of law. The meaning given of the term 'integrity' should reflect its context and the nature of the Licence as a document drawing on established principles of telecommunications regulation.

5.21 The relationship between 'integrity' and 'resilience' is widely-documented in telecommunications regulation and the two terms are used in ways that indicate that they relate to the common concern to ensure that networks operate without interruption. For example, consider that Article 23 of the Universal Services Directive is expressed in the following terms:

Article 23

Integrity of the network

[92] See, for example, paragraph 37 of JT's Response.

> *Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations. Member States shall ensure that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.*

5.22 This makes it clear that, in the context of telecommunications regulation specifically, amongst the most important failures of network '*integrity*' is the possibility of '*catastrophic network breakdown*'. It is also notable that such a breakdown is a failure of '*integrity*' even when the cause of the breakdown is outside the reasonable control of the operator ('*force majeure*').

5.23 The Authority does not consider that the example cited by JT is relevant or instructive. The definition from which JT draws its meaning of 'integrity' is taken from a standard dealing with a specific concern about data integrity ('integrity protected environment') that reflects one possible meaning of the term 'integrity'.[93] The document that JT's cited example is drawn from reflects the use of that term in relation to data but does not limit the use of that term in the context of a network. Data integrity is enormously important, but it is not the only form of 'integrity' that is relevant to consider, nor is there any suggestion that Licence Condition 9 is focused solely or exclusively on data integrity.

5.24 Other ITU documents that are more aptly focused on the question of network integrity make the opposite point to the JT submission. For example, Recommendation Y.140.1 notes that

> *The definitions of the terms "security", "availability", "integrity" and "confidentiality" are closely linked together and should be used in the context of the others*

5.25 This is reflected in the approach taken in, for example, the European Electronic Communications Code ("**EECC**"), in which:

> *'security of networks and services' means the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;*

5.26 The EECC notes that '*Competent authorities [i.e., regulators, such as the JCRA] should ensure that the integrity and availability of public electronic communications networks are maintained*'[94], through the use of the obligations they impose on the bodies they regulate (i.e., in the present context in Jersey, via licence conditions).

[93] JT does not provide a specific citation, just referring to the 'ITU', but the relevant definition can be found in, for example, Recommendation X.815, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Integrity Frameworks.

[94] EECC, Recital 28.

5.27 Although it is not directly applicable in Jersey, the EU regime provides a useful example of how a different jurisdiction with closely-related issues and needs views the concept of 'integrity' in relation to networks as being captured within the concept of 'security', in the context of telecommunications regulation. That is consistent with the approach that the Authority has taken in relation to its interpretation and construction of Licence Condition 9.

5.28 In any event, even if JT's narrowly constructed view of 'integrity' were accepted (which it is not), it seems that *even on JT's own construction*, a contravention of Licence Condition 9 appears to have occurred. JT describes that '*Licence Condition 9 refers to the licensee's obligations to ensure that it remains in control over the management of its network*'.[95] The Authority agrees that failure to maintain control over the management of the licensee's network falls within the scope of Licence Condition 9. This seems to describe what happened regarding the Outage reasonably clearly: the components that failed caused JT to lose control over the management of its network.

Conclusion on construction of Licence Condition 9

5.29 Licence Condition 9 is concerned with '*integrity*' of the JT network in a broad sense and in a way that encompasses threats that go beyond data integrity. It includes, specifically, the integrity of the network in the sense of the integrity of its structure and functioning – that is, the protection afforded to the network from external or internal sources of instability or failure. For that reason, the concept of '*integrity*' in the context of Licence Condition 9 is closely related to the concept of '*security*', although it is not necessary to decide on the facts in this case whether all matters that would be threats to 'security' would also be concerns about network 'integrity'. (As a general point, the Authority would expect that JT's approach to its obligations would be to protect its network on an expansive and precautionary basis, and not to approach the question of what it needs to do to protect the integrity of its network on a narrowly constructed basis).

5.30 Licence Condition 9 is engaged in relation to this matter because the Outage arose due to a threat to the integrity of the network caused by the failure of specific equipment on JT's network. The network suffered a loss of integrity, in that its functioning failed.

5.31 In assessing whether or not JT has met this licence obligation in relation to this investigation, the Authority considers that the following questions are relevant:

(a) Were there technically feasible and proportionate additional steps that could have been taken by JT to avoid the Outage?

(b) If so, were these additional steps taken?

(c) If these additional steps were not taken, was it within JT's reasonable control to take them?

5.32 In reaching its conclusions on those questions, the Authority relies substantially on JT's own analysis as to the immediate source of the problem that triggered the incident. The Authority also draws on the findings made in the Niji and Touchstone Reports, and the further material provided by JT in response to the Draft Decision and May 2021 RFI. The findings and

[95] JT's Response, paragraph 34.

recommendations of the various reports and responses referred to below are summarised in Section 4.

Relevant evidence and findings of fact

5.33 The Authority's provisional view was that:

(a) There were technically feasible and proportionate additional steps that JT could have taken, but did not take, to avoid the Outage:

(1) In relation to the short-term, some actions that it could have taken to avoid the specific failure that triggered the Outage are set out below; and

(2) In relation to the long-term approach that JT seems to have taken in relation to its network design, this appears to have been insufficient to meet the requirements of Condition 9.

(b) It was within JT's reasonable control to have taken these additional steps.

JT's submissions

5.34 JT disputes that it failed to anticipate the issue and submits that it took all reasonable steps that could have been expected of it prior to the 12 July incident. JT's submission notes that:

> *6. … JT accepts that in or around October 2018, public media released an article warning of potential faults that may occur in all GPS devices generally on or around 6 April 2019.*
>
> *7. As a result of the generic media warnings, JT undertook steps to understand and to manage insofar as reasonably practicable and in line with the US Department of Homeland Security Recommendations, the risk relating to week number rollover (the **"Week Number Rollover Issue"**):*
>
> *a. JT acknowledged that it did not have the expertise or the facilities to determine whether the Week Number Rollover would be an issue for the network and accordingly it approached its trusted partners to obtain "verification by consultants" (as Cognitio subsequently recommended that it should).*
>
> *b. For JT itself to have carried out sophisticated internal testing would have required JT to source specialised equipment and expertise, which is not (and was not at the time) a reasonable step to take in the circumstances (as illustrated by the fact the even the JCRA's consultants, Cognitio do not recommend it).*
>
> *c. GPS and NTP are specialised fields and within the expertise of Edge Networks (UK) Ltd (**"Edge Networks"**), its professional NTP support provider and a trusted supplier to JT.*
>
> *d. JT contacted Edge Networks, in order to establish whether the clock functions on any hardware supplied by Edge Networks were susceptible to this issue:*

i. Edge Networks are a reputable company providing market-leading services and hardware solutions for the communications technology sector. They are (and were at the time) the support provider and distribution partner for Oscilloquartz (now Adva). They are a specialised, technical expert partner for JT.

ii. In or about March 2019, Edge Networks, advised, in writing, that they had conducted "a lot of proactive simulation testing regarding this matter" which showed that the equipment would be "ok" in the circumstances in that "the GPS engines will react to the rollover but the shelf does handle the adjustment ok". JT shared this with Cognitio during their audit.

iii. Edge Networks gave a specific assurance to JT that on the basis of their testing, no error was expected; they did not recommend that JT obtain any further or more specific advice on this issue.

e. JT drew some comfort from the fact that its network had previously navigated the EPOCH transition in April 2019, without any disruption, and it was therefore not unreasonable in the circumstances for JT to assume that the Week Number Rollover would have similar consequences.

8. We now know, with the benefit of hindsight, that Edge Networks' assessment was wrong.

The Authority's findings

5.35 In relation to the actions regarding the specific hardware issue that triggered the Outage:

(a) JT were aware of the risk of a 'week number' failure and sought advice from a third party supplier to ascertain whether JT's hardware was affected.

(b) In responding to that risk, JT relied on the actions and assurances of a third party rather than taking further steps to assure itself that the testing was sufficiently robust so as to establish the true level of the threat. The fact that an earlier transition had occurred without a failure explains but does not excuse JT opting to rely on a third-party supplier in relation to a component that, if it failed, could cause JT's entire network to fail. As a licence holder and designated network provider, JT is responsible for maintaining the integrity of its network and is accountable for its failure to do so. Where JT contracts with, and relies on, a third party to provide critical assurances and where that third party provides JT with incorrect advice, that may have important implications for the positions of those two contracting parties.[96] But it does not, by itself, absolve JT or mean that the Authority ought to view JT's regulatory obligations differently. In fact, on closer

[96] For example, speaking in general terms, it may be failure to fulfil contractual obligations or be circumstances in which one party is liable to the other.

inspection of the assurances provided by Edge Networks, JT was only able to provide the Authority with one email dated 26 March 2019.[97] On the face of that evidence, there is no basis for concluding that JT engaged in any follow-up with Edge Networks. It appears not to have made any attempt to obtain a more detailed report or to understand the testing which Edge Networks had undertaken. At the time, JT did not have a written support contract in place with Edge Networks and was relying on a 'good will' relationship. The Authority views these arrangements as sub-standard and below the level of assurance expected of an operator seeking to ensure the integrity of its network.

5.36 In relation to this second point, JT argued in its submissions that it could not and did not have the expertise to undertake the testing internally. The Authority recognises that operators do and can rely on third parties to undertaking activities related to their networks. But, at all times, that operator (in this case, JT) remains responsible for the fulfilment of its regulatory obligations. This, in turn, means that where an activity relies on expertise drawn from third parties, it is JT's responsibility to ensure that any such activities carried out by third parties are done to the requisite standards in order for JT to be satisfied that its obligations have been fulfilled.

5.37 In this case, JT fell below that standard; for example, it had no written contract in place with Edge Networks, that would have enabled it to exercise a sufficient degree of control over Edge Networks to satisfy itself that its obligations had been fulfilled. JT also made no attempt to check what Edge Networks had done to reach its conclusion that its equipment would be 'ok'.

5.38 Based on the evidence provided by JT, the Authority does not agree that '*JT undertook steps to understand and to manage **insofar as reasonably practicable** and in line with the US Department of Homeland Security Recommendations, the risk relating to week number rollover*' (emphasis added). JT cannot be said to have tried to '*understand and to manage **insofar as reasonably practicable***' (emphasis added) when it did not check with Edge Networks what testing had been undertaken or give Edge Networks any specific instructions as to the testing that should be carried out (even if this was simply relaying the recommendations), or what the testing needed to determine. The Authority considers that JT's contravention of this licence condition began no later than the point at which JT opted not to follow-up on the email from Edge Networks.

5.39 The approach the Authority is taking to this issue is consistent with the established practice of regulators more widely, and the Authority's approach should not come as a surprise to JT. For example, Ofcom's guidelines deal specifically with the question of where responsibility lies when an operator relies on a third party for a function or activity that is critical to the integrity of their network, noting that:

> *Outsourcing*
>
> *3.51 Many CPs now make extensive use of third parties to provide infrastructure for, and to design and operate, their networks. It is therefore conceivable*

[97] JT's response to the May 2021 RFI, Appendix 5.

that a CP may have less visibility or control over the level of resilience that is put in place, than it would if it kept these activities in-house.

3.52 ***We do not consider that outsourcing to third parties in this way excuses CPs from their obligations*** *under 105A(4). Put simply, a CP cannot contract out of its statutory obligations.* ***As such, they should have sufficient levels of contractual control over third parties in place to ensure they continue to comply with their obligations. We also expect CPs to continuously and rigorously check that actions undertaken on their behalf do not put them in breach of their obligations****.*

5.40 Although recognising that the relationship between JT and Edge Networks was not an 'outsourcing', the underlying point that operators must check that action taken on their behalf does not put them in breach of their obligations is apt in this case.

Conclusion on Condition 9

5.41 The Authority's finding is that JT failed to take all reasonable steps to ensure the integrity of its network, and hence, prior to the Outage, JT was in contravention of Condition 9. The Authority also considers that JT's contravention of this licence condition began no later than the point at which JT opted not to follow-up on the email from Edge Networks.

JT's compliance with Condition 17

Approach to assessing compliance with Condition 17

Approach taken by the Authority in the Proposed Direction

5.42 In its construction of Licence Condition 17, the relevant elements include:

(a) Identifying relevant best practices or standards that are engaged (by industry practice or by adoption by an international standards body of appropriate standing) such that those standards are incorporated into Condition 17; and

(b) Evidence of fact that the licensee's performance was lower or below the relevant standard to a material extent and in a way that relevantly engages Condition 17.

JT's submissions on Licence Condition 17

5.43 In relation to Licence Condition 17, the JT Response notes that:

50. On a proper reading of Licence Condition 17, it is self-evident that there is no agreed single, day-one-achievable, standard for "best practice" in the industry. The Condition notes that "The Licensee shall develop and operate the Licensed Telecommunications System so as progressively to achieve standards in line with international best practice" and then goes on to mandate that "in particular, the Licensee shall achieve and comply with relevant standards established by ETSI, the ITU and such other international benchmarks as the JCRA may direct from time to time" (emphasis added)

51. Accordingly, Licence Condition 17 provides for a mechanism for the JCRA to mandate by way of direction "the relevant standards" and requires JT to provide a development plan and a monitoring plan, to be agreed and

> *approved by the JCRA, to ensure that the network is up to standard. The mechanism for progressive improvement provides for the licensee to submit a plan to the JCRA and in turn the JCRA will approve such plans from time to time (Licence Condition 17.2). Furthermore, it is for the JCRA to "direct the Licensee to update and resubmit the plans from time to time" (see Licence Condition 17.4) and "may amend or replace such directions from time to time" in the plan (Licence Condition 17.5) and it is only when the licensee has not achieved the target levels that the licensee will be in breach of its licence (pursuant to Licence Condition 17.6).*

5.44 JT's submission is that the initial part of Licence Condition 17 ('*The Licensee shall develop and operate the Licensed Telecommunications System so as progressively to achieve standards in line with international best practice')* only bites in the event that the Authority has previously specified the relevant standards to JT as being applicable.

The Authority's reasoning

5.45 The Authority rejects JT's construction of Licence Condition 17 because:

(a) On conventional principles of construction, it gives no effect to the first part of the Licence Condition, rendering it meaningless and ineffective;

(b) It is contradicted by the clear language of the Licence Condition, which specifies that standards nominated by the Authority shall '*in particular*' apply – in other words, such nominated standards are a *subset* of the set of standards in respect of which compliance is required under the Licence Condition.

5.46 JT's assertion that it is 'self-evident that there is no agreed single, day-one-achievable, standard for "*best practice*" in the industry' is not correct, either in law (i.e. as an explanatory statement to make sense of Licence Condition 17), or in fact.

5.47 There is ample evidence that what constitutes 'best practice' in the sector is a widely- understood set of clear and identifiable requirements that can be, and are, incorporated into legally binding obligations (for example, in contracts, as well as in regulation).

5.48 It is precisely the existence of this body of best practice that is essential to the operation of Licence Condition 17. Most obviously, there are standards set by the ITU and relevant regional bodies, as well as relevant standards bodies in other disciplines (e.g. engineering and risk management).

5.49 The existence of a coherent concept of 'best practice' in telecoms is relied on by JT itself elsewhere in its submission, noting, for example:

> *JT relies upon a report from Craig Newton, an independent expert, with nearly 25 years' experience in the telecommunications industry, specifically in the field of Time, Frequency and Network Synchronisation Solutions. A copy of his report is at* ***Appendix 2****. We consider that Mr Newton is well placed to offer an expert opinion as to whether or not the standards and architectures employed by JT were in line with international best practice.*

5.50 On that basis, the Authority does not accept JT's assertion that what is 'international best practice' is non-existent or uncertain in this context.

5.51 Given that best practice exists, it is routine to adopt this body of practice into the regulatory obligations of telecoms operators. That can be done by an exhaustive process of specifying each and every standard that applies (that is the approach taken in the EU, for example).[98] But that is not the only approach, and a perfectly reasonable alternative approach is to nominate that it is a responsibility of the operator (licensee) themselves to equip themselves with an understanding of what represents best practice and/or is standard within the industry, and apply that approach. That is the approach taken in Jersey under Licence Condition 17.

5.52 It is also taken in other jurisdictions, including, for example, Guernsey, where Licence Condition 16.2 of JT's licence in Guernsey is in substantially similar terms:

> *16.1 The Licensee shall develop and operate the Licensed Telecommunications Network so as progressively to achieve standards in line with international best practice and in particular, the Licensee shall achieve and comply with relevant standards established by ETSI, the ITU and such other international benchmarks as GCRA may direct from time to time.*[99]

Relevant evidence and findings of fact

5.53 The Touchstone Report identifies a number of areas where JT's practice appears on the face of the report to fall short of '*international best practice*' (footnotes included):

> *In any event, both of the original Oscilloquartz NTP servers were end of life, outside support, and kept going on spares*[100] *- one of the NTP servers was initially replaced with another loaned NTP server (in late 2019), and eventually replaced by a new NTP server (a Brandywine TFS 80)*[101] *in May 2020, but the NTP server that failed was not replaced prior to the Outage. Had the WNRO warning prompted JT to replace both legacy NTP servers, the Outage may have been avoided.*
>
> *[…]*
>
> *The contractual support arrangements with Horsebridge/Edge Networks for the NTP servers were inadequate,*[102] *and were allowed to persist for some time before a support contract with Edge Networks was established in November 2019.*

[98] It is noteworthy that even those regimes that do rely on an explicit list of applicable standards can also incorporate an element of wider best practice into their regulatory requirements: see for example, the UK's General Condition A2.4, which provides that '*In the absence of such standards and/or specifications referred to in Conditions A2.2 and A2.3 [i.e. specifically named standards], Communications Providers shall take full account of international standards or recommendations adopted by the International Telecommunication Union (ITU), the European Conference of Postal and Telecommunications Administrations (CEPT), the International Organisation for Standardisation (ISO) and the International Electrotechnical Committee (IEC).*' This evidence clearly shows that although the EU and UK regimes do use an explicit list of standards, they do not have to do so – the approach in GCA2.4 could be relied on instead.

[99] GCRA licence issued to JT (fixed) - available at https://www.gcra.gg/media/597630/guernsey-fixed-licence-jt.pdf.

[100] 'End of life' means that the equipment was operating beyond its intended operational lifetime. 'Outside support' means that the equipment was no longer supported by its original equipment manufacturer/supplier or contracted support provider'. 'Kept going on spares' means that the equipment was maintained by using spare parts (as new parts would no longer be available from the original supplier).

[101] JT Response to JCRA RFI 250521, Responses to Section 10 (d) (2).

[102] JT Response to JCRA RFI 250521, Appendix 11.

JT relied heavily on assurance[103] from Edge Networks that the Oscilloquartz 5581C NTP server would correctly handle the WNRO issue, but did not follow-up to obtain Edge Network's findings from their simulation testing of the WNRO event on the Oscilloquartz 5581C NTP server, as supporting evidence for Edge Network's conclusions.[104]

After assurance from Edge Networks, and keeping watch over the EPOCH 3 event (around 6th April 2019) without incident, there seems to have been no further action taken by JT prior to the Outage[105] (despite a clear warning that WNRO events could happen at other times depending on different implementations).

Following the Outage, the Oscilloquartz 5581C NTP server was taken out of service, and the suspected 'faulty' NTP module tested in another shelf (the output time remained at UTC – 1024 weeks, i.e. November 2000),[106] but there seems to have been no further follow-up with Edge Networks or Oscilloquartz/Adva for forensic analysis of shelf/module firmware to confirm the cause of the time roll-back.

[…]

Network behaviour between multiple network devices and multiple protocols is inherently complex, making critical dependencies difficult to spot. However, had JT conducted an LLD walkthrough, led by JT and supported by key suppliers, and based on a 'what if' assumption derived from the prospect of a WNRO event, the critical dependency between a significant roll-back in NTP time (to 27th November 2000 or by 1024 weeks) and the starting date for key chain authentication validity (of 1st July 2012) could have been spotted – if the dependency could have been identified, reverting to static passwords (as applied after the event) could have led to the Outage being avoided.

While Cisco has raised a 'bug report' internally, it is not yet clear whether, how or when the issue with the Cisco IOS XR NTP Client will be resolved to enable JT to return to ISIS time-based keychain authentication.

Time-based key chain authentication is widely recognised as best practice for ISIS authentication in IP core networks, widely used by other network providers, and should be re-introduced into JT's core network once the issues that caused the 12th July 2020 Outage have been fully resolved. JT's current practice of using static unchanging passwords protected by the MD5 hashing algorithm should be viewed as an interim solution, as it would not be compliant with a best practice network security policy – static unchanging passwords are a tempting target for any malicious actors targeting denial-of-service attacks, man-in-the-middle attacks and/or ransomware attacks.

JT did not seem to have an effective Disaster Recovery Plan for this kind of network incident, and the total loss of internal communications capability within JT due to

[103] JT Response to JCRA RFI 250521, Appendix 5.
[104] JT Response to JCRA RFI 250521, Responses to Section 9 (e) (1).
[105] JT Response to JCRA RFI 250521, Responses to Section 9 (f).
[106] JT Responses to JCRA RFI 250521, Responses to Section 9 (g).

the Outage, meant that JT was unable to mobilise its Business Continuity Process, which led to a slow response by JT, particularly in relation to JT's customers affected by the Outage.[107]

5.54 These failures provide indicative evidence that JT has contravened LC17.

Conclusion on Condition 17

5.55 While the findings of the Touchstone Report are highly indicative of a failure by JT to adhere to *'best practice'* the Authority has found that the evidence, as it stands, is not sufficient so as to establish such a failure to a standard that would enable the Authority to make a definitive finding that JT contravened Condition 17.

5.56 The Authority considers that, in any event, it is not necessary for it to make a finding of a contravention of Condition 17, as the Directions it might have imposed in such event would be materially the same as those it has determined to impose in relation to the contravention of Condition 9. The Authority is therefore satisfied that its concerns will be addressed by the current (and any future) Directions and that it would not be efficient, economical, or effective to expend further resources investigating whether a contravention of this Condition by JT occurred.

5.57 While the Authority rejects JT's construction of Condition 17 (see paragraphs 5.45 to 5.52), it considers that it would be in the best interests of JT and of other licensed operators for the Condition to be modified in due course so as to clarify the applicable standards by which the Authority expects licensed operators in Jersey to abide by.

JT's compliance with Condition 14

Approach to assessing compliance with Condition 14

5.58 The approach taken by the Authority to the proper construction of Condition 14 in this investigation is consistent with the approach previously taken in relation to the investigation of various 999 outages by JT and another licensee in early 2020.[108]

5.59 That approach is, in summary:

(a) To interpret Condition 14 in the context of the paramount importance that 999 services play in protecting people on Jersey from risks to life and safety, and other emergencies;

(b) That the obligation on each licensee is to provide an 'end-to-end' service, that enables callers to be connected successfully to the relevant emergency service;

(c) That notwithstanding that the licensee may opt to use a call handling service from an outside organisation (including another licensee), that the licensee remains accountable for the performance of their end-to-end service under Condition 14. If the licensee relies on someone else to provide their CHA, it is for that licensee to ensure that they have secured sufficient oversight and resilience of that service to meet their obligation under Condition 14;

[107] JT Incident of 12 July: An independent Review by Niji, dated 23 September 2020.
[108] See JCRA Final Decision Emergency Call Outages https://www.jcra.je/publications/

(d) Where a third party steps in on a 'Good Samaritan' basis and takes steps to wholly, or partially, restore the 999 service, that may affect the direct harm arising and as such may be relevant to the seriousness of any breach. However, it will not result in a licensee being able to avoid a finding of contravention of Condition 14;

(e) That, notwithstanding that operating a CHA is not an activity that is directly licensed by the Authority, it is a vital activity for the support of 999 services and that the Authority expects (and has an interest in ensuring) that any CHA operation is designed, implemented and managed to suitably high standards; and

(f) Operators who themselves maintain a CHA for their own purposes are in a position of particular responsibility and that this may be relevant to the assessment of seriousness in relation to a contravention of Condition 14 by such a licensee.

Relevant evidence and findings of fact

5.60 The Outage in this investigation was in relation to JT's fixed and mobile access networks. There was no specific issue arising in relation to JT's CHA. It appears to have handled calls from other networks (including, it would appear, calls from JT users using roaming to access 999 via another operator's service) without interruption. JT customers on other services, such as ISDN30< would have been able to make 999 calls as the JT Core network remained connected to the CHA.

Conclusion on Condition 14

5.61 The Authority's view is that JT failed to maintain its 999 service during the Outage and was therefore in contravention of Condition 14. Specifically, during the Outage:

(a) From 18:55 to 21:44, JT's fixed customers had no 999 access at all;

(b) From 18:55 to 21:44, JT's mobile customers may have had roaming access to the 999 service provided by other licensees, but no access to a 999 service provided by JT

with some of JT's customers not able to access 999 until services were fully restored by 03:00 on 13 July 2020.

6. The scope of the Directions

Summary

6.1 This section sets out the Authority's decision in respect of the directions to be issued to JT.

6.2 The Authority considers that it is appropriate to issue directions to JT pursuant to Article 19(1) of the Telecoms Law.

6.3 The Directions will require JT to provide to the Authority, within a defined period, the specific measures which it intends to take in order to rectify the issues to its network which led to the Outage, particularly those relating to emergency call services.

6.4 The Directions will indicate that, in doing so, JT must propose how it will address the recommendations set out in the Niji Report and address the issues and observations set out in the Touchstone Report.

6.5 Furthermore, the Directions will require JT to develop a self-reporting framework through which it will provide periodic reports to the Authority, so that the Authority can effectively monitor JT's progress towards implementing the specific measures.

Directions

6.6 Article 19(1) imposes an obligation on the Authority to give a direction to a licensee to take steps, or specified steps, to ensure compliance with a licence condition wherever, in the opinion of the Authority, the licensee is in contravention.

6.7 The duty under Article 19(1) is subject to two express limitations:

(a) First, by virtue of Article 19(2F) of the Telecoms Law, the Authority shall not give a direction if satisfied that its duties under Article 7 preclude it from doing so. The Authority has considered its duties and is of the view that they favour the giving of a direction in this case.

(b) Secondly, by virtue of Article 19(2G), the Authority shall not give a direction if satisfied that the contravention of the condition is trivial or that the licensee is taking reasonable steps to comply with the condition and to remedy the effects of the contravention.

6.8 The Authority concludes that JT's contravention in this matter cannot be regarded as trivial.

6.9 With respect to the second limb of Article 19(2G), the Authority acknowledges that some steps have been taken to varying degrees by JT in order to remedy the effects of the contravention of Conditions 9 and 14.

6.10 However, the Authority does not consider that these steps are sufficient such as to discharge the Authority's responsibility to issue directions in relation to those contraventions. The Authority takes the view that JT must take further steps to ensure that it robustly complies with Conditions 9 and 14.

6.11 The Authority therefore directs JT under Licence Condition 19(1) as set out in Section 7, Annex 1. Subsequent to this Final Decision and annexed Directions, the Authority will further deliberate, in consultation with JT, on any further Directions or penalties to be applied in this case.

7. Annex 1 - Directions issued to JT (Jersey) Limited

7.1 The Authority directs JT to:

(a) **DIRECTION 1:** Provide to the Authority with 28 days from the date of the Final Decision a proposed set of specific measures which JT intends to take in order to rectify those design issues within its network which led to the outage which occurred on 12 July 2020. In particularly, these measures must address:

(1) JT's provision of emergency call services; and

(2) How JT will ensure the implementation of each of the recommendations set out in the Niji Report dated 23 September 2020 and remedy the issues and observations set out in the Touchstone Report (version 3, dated 5 July 2021).

(b) **DIRECTION 2**: Provide to the Authority within 28 days of the Final Decision a proposed self-reporting framework through which JT will provide periodic reports to the Authority to enable it to effectively monitor JT's progress as regards implementing the specific measures referred to in Direction 1.

(c) **DIRECTION 3**: Make any amendments to the specific measures referred to in Direction 1 or the self-reporting framework referred to in Direction 2 that are required by the Authority.

(d) **DIRECTION 4**: Upon the Authority's review and written consent being given, execute and deliver the specific measures referred to in Direction 1 and provide the Authority with the periodic reports referred to in Direction 2.

8. Annex 2 – Table of evidence relied on by the Authority

Document Number	Date	Document name
1	7 July 2020	Cognitio Report 1 - Root Cause Investigation into 999, 112 Incidents during first half of 2020
2	13 July 2020	Email from executive at JT to 999ECH@JT365.onmicrosoft.com at 01:52 on 13 July 2020
3	13 July 2020	Email from senior executive at JT to Authority, JHAD and GCRA representatives at 09:21 on 13 July 2020
4	13 July 2020	Email from senior executive at JT to Authority, JHAD and GCRA representatives at 09:36 on 13 July 2020
5	13 July 2020	Email from senior executive at JT to Authority and JHA representatives at 12:48 on 13 July 2020.
6	13 July 2020	JT Service Incident
7	14 July 2020	Email from executive at JT to representatives of the States of Jersey Police and the JHAD at 14:05 on 14 July 2020
8	15 July 2020	JT's Incident Report re. Incident of 12 July 2020 - Preliminary Reason For Outage Report
9	22 July 2020	JT Service Incident Update
10	22 July 2020	JT's Final Reason For Outage Report
11	4 August 2020	JT's Addendum to Final Reason For Outage Report
12	28 July 2020	JT's Final Analysis of Clock Reset Cause
12a.	Unknown	US Department of Homeland Security, Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time – Upcoming Global Positioning System Week Number Rollover Event
12.b	26 September 2017	CGSIC GPS Week Roll Over Issue - Edward Powers, US Naval Observatory, 26 September 2017
13	17 August 2020	Cognitio Report 4 - Technical Report Major Outage
14	26 August 2020	Cognitio Report 3 - Audit Report – JT's Management
15	23 September 2020	JT Incident of 12 July 2020 - An Independent Review by Niji
16	24 September 2020	Letter from JT to JCRA attaching Niji Report
17	25 May 2021	JT's response to the May 2021 RFI
18	15 June 2021	Report prepared by Touchstone Consulting Limited
19	28 June 2021	JT's comments to the Touchstone Report
20	5 July 2021	Final version (Version 3) of the Touchstone Report