Data Communications Company

DCC Performance Measurement Report

Performance Measurement Period:

December 2019

Version:	**V1.0**
Date:	**05/02/2019**
Security Classification:	**DCC Controlled – Panel, Ofgem, BEIS and SEC Parties Only**

Table of Contents

Control Sheet

Table below details all enduring changes made to the report this month.

Page No.	Change

1 Introduction

1.1 Purpose

The Smart Energy Code (SEC) sets out the operational Service Levels which DCC needs to meet when providing services to DCC Users. This report provides details of the Service Levels achieved in respect of the Code Performance Measures set out in Sections H13.1 and L8.6 of the SEC and such Service Provider Performance Measures as are specified in the Reported List of Service Provider Performance Measures document[1].

Service Levels are reported following the end of each calendar month and this report is provided within 25 working days following the end of each calendar month.

This report is provided to the Panel, SEC Parties, the Authority and (on request) the Secretary of State.

1.2 Content

A Target Service Level and Minimum Service Level apply to each of the Code Performance Measures and to the Service Provider Performance Measures in the Reported List of Service Provider Performance Measures[2]. This report sets out the Service Levels achieved in respect of each Performance Measure[3].

Where the Service Level achieved for a Performance Measure is less than the Target and/ or Minimum Service Level, the report provides the reasons for this. Where the Service Level achieved is less than the Minimum Service Level the report also outlines the mitigating actions DCC is taking to prevent re-occurrence.

Where the Service Level achieved is less than the Target Service Level, Service Points are accrued by the DCC Service Provider. Service Points are then converted into Service Credits (monetary amount). Any Service Credits due from the DCC Service Provider are treated as a reduction in their charges and may be reflected in a reduction in DCC's Internal Costs and/ or External Costs. The method for calculating Service Points and Service Credits is detailed in the DCC Service Provider contracts in Schedule 2.2.

[1] The Reported List of Service Provider Performance Measures document was provided 18th December 2015 to Parties, the Panel and the Authority by the Secretary of State and identifies itself as being produced for the purposes of Section H13; it can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures.
[2] The Target and Minimum Service Levels are defined in Sections H13.1 and L8.6 of the SEC and in the Reported List of Service Provider Performance Measures document.
[3] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

1.3 Scope

This document reports on the performance of the DCC Service against the Performance Measures for December 2019.

1.4 Confidential Information

This report is classified as DCC Controlled in accordance with the confidentiality provisions under Section M of the SEC. Where the Service Level achieved is below the Target / Minimum Service Level and the reasons for this or the mitigating actions being taken by DCC are classified as DCC Confidential, this shall be reported in an annex to this report which shall be available on request.

2 Executive Summary

Code Performance Measure (CPM) Summary

CPM1 measures Percentage of On-Demand Service Responses delivered within the applicable Target Response Time, the Service Level achieved is 98.05% and is below the Target Service Level, further details provided in Section 3.1.1.

CPM3 measures Percentage of Alerts delivered within the applicable Target Response Time, the Service Level achieved is 98.84% and is below the Target Service Level, further details provided in Section 3.1.2.

CPM4 measures Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time, the Service Level achieved is 75.00% and is below the Minimum Service Level, further details provided in Section 3.1.3.

The Service Levels achieved for CPM2, CPM5, CPM6, CPM7 and CPM8 are all above the Target Service Level.

Service Provider Performance Measures Summary

S1SP Capgemini PM2.2 Percentage Service availability – CP Service (Production Environment), reported Service Level is 99.81% and is below Target Service Level. Further details are provided in Section 9.1.1

Where the Performance Measure is reportable, all other Service Provider Performance Measures are above the Target Service Level.

Any Service Credits accrued for this measurement period are detailed in Section 11 of the report.

Key Incidents – December Closed in Period

Incident Reference	**INC000000526144 – Category 1**
Problem Reference	**PBI000000118607**
System(s) Impacted	Loss of Network in the Northern Region
Incident Start Date / Time (Logged in Remedy)	05/12/2019 00:18
Incident Resolved Date / Time	05/12/2019 08:59
Outage Start	04/12/2019 23:41
Outage End	05/12/2019 02:17
Incident Closure Date	11/12/2019
Major Incident Duration	8 hours 44 minutes

Regions Impacted	North
Resolved within SLA	Yes

Summary of High Category Incident
At 00:43 DCC Service Centre informed DCC IM that CSP North had raised a severity one ticket. DCC IM contacted CSP North IM who advised the network in the north had gone down completely following patching work on their RNI servers (carried out under low risk change reference: CRQ119304) CSP North stated that service had restored at 00:41 following a restart of the RNI servers. DCC IM joined the technical bridge and the northern network was seen to fail again at 01:05 DSP joined the technical bridge at 01:13 who had raised a severity 3 ticket INC000000526075 where they had proactively seen the northbound queue starting to increase. The rate of messages queueing was manageable at that time (approx. 20,000 to 30,000 messages) CSP North rolled back the patching activity and restarted their RNI servers restoring service. DSP reported normal traffic was flowing.
Reported Customer Impact
All Service Users in the northern region would not have been able to send/ receive any SRV's or receive alerts. At the time of this incident, traffic across the solution was low. No Service Users reported any impact.

Actions Completed to Recover Service		
Item	Description.	Owner
1	The patching on the RNI servers was rolled back and a reboot of the RNI servers restored service	CSP North

Incident Reference	**INC000000520567 – Category 2**
Problem Reference	**PBI000000118404**
System(s) Impacted	DCC Service Centre Send/Receive email failure
Incident Start Date / Time (Logged in Remedy)	22/11/2019 11:29
Incident Resolved Date / Time	25/11/2109 12:10
Outage Start	22/11/2019 11:02
Outage End	22/11/2019 14:56

Incident Closure Date	01/12/2019
Major Incident Duration	3 days 0 hours 42 minutes
Regions Impacted	N/A
Resolved within SLA	Yes

Summary of High Category Incident
DCC Service Centre experienced issues when sending email. Capita IT&N were engaged to investigate the issue. Initial thoughts were this was because of the change of email address from '.co.uk' to '.com'. This then progressed to also affect inbound email. It was found that the mailbox had reached capacity and was at 99.05GB of 100GB of storage. Data cleansing and Archiving of data was introduced. Once sufficient cleansing and archiving had taken place service was restored.

Reported Customer Impact
70% of DCC contact by Service Users is via email, this issue reduced this contact substantially. However, Service Requests (Work Orders) and Incidents were not affected.

Actions Completed to Recover Service		
Item	Description.	Owner
1	Mailbox data cleanse, archive activities	DCC SC / Capita IT&N
2	E3 Licence applied increasing the mailbox back to 100GB after archiving reduced the mailbox to 50GB	Capita IT&N

Incident Reference	**INC000000530859 – Category 2**
Problem Reference	**PBI000000118516**
System(s) Impacted	SSI - Service Audit Trail functionality
Incident Start Date / Time (Logged in Remedy)	16/12/2019 13:03
Incident Resolved Date / Time	16/12/2019 14:06
Outage Start	16/12/2019 13:00
Outage End	16/12/2019 13:40

Incident Closure Date	22/12/2019
Major Incident Duration	1 hour 3 minutes
Regions Impacted	All
Resolved within SLA	Yes

Summary of High Category Incident
At 13:03 on 16/12/2019 a service user raised a Category 2 ticket as they were getting the following error when attempting to use the Service Audit Trail (SAT) in SSI/SSMI: A database error occurred that has prevented your request from being fulfilled. DSP were engaged and, following the restart of a service component, SAT began fulfilling requests again.

Reported Customer Impact
During the incident it was understood that a single service user was unable to complete Install & Commissioning activities. However, it is now known that the service user in question uses the SAT service to support their engineers during installs and is not imperative to the I&C process.

Actions Completed to Recover Service		
Item	Description.	Owner
1	Service component restarted following unplanned server reboot.	DSP

Incident Reference	**INC000000518930 – Category 2**
Problem Reference	**PBI000000118411**
System(s) Impacted	Service Requests in the CSP North Region
Incident Start Date / Time (Logged in Remedy)	20/11/2019 11:31
Incident Resolved Date / Time	06/12/2019 15:23
Outage Start	20/11/2019 11:31
Outage End	26/11/2019 16:20
Incident Closure Date	22/12/2019
Major Incident Duration	16 days 3 hours 52 minutes

Regions Impacted	North
Resolved within SLA	No

Summary of High Category Incident

On 20/11/2019 at 11:31 DCC received reports from a Service User of widespread issues with installs in the North. Both ESME and GSME were commissioning with significant delays and multiple retriggers. Reports from other Users followed shortly after.

There was a high number of scheduled reads failing to be sent to the CSP North gateway as a 'too busy / HTTP500' error was being returned, the reads would then be retried. The high number of retries meant that the meter reads were encroaching into working hours (the scheduled read window is midnight to 06:00, however there is a 24-hour SLA for delivery of scheduled reads). This caused excessive traffic to the gateway which was impacting the delivery of other SRVs including those used in the I&C process.

Also, the queue of scheduled meters reads was not clearing, a high number were not delivered and expired after 24 hours (Up to 24k)

It was initially thought that this incident was triggered by an approved DSP change (CRQ000000119920 DSP - PROD Increase DSP Fetch Queue Limits). This changed overnight scheduled reads being sent to CSP North to a more consistent flow. The work was completed in the early hours of 20/11. Preliminary investigations suggested that this had caused a 'configuration mismatch' between DSP and CSP North

Several actions were performed to mitigate the impact:

- Pausing the sending of scheduled meter reads for 3 hours as a short-term solution to mitigate the impact to I&Cs
- Changing the rate of meter reads sent per second from 30 to 15
- Turn off the 'Short Business Retry'
- Changing the rate of meter reads sent per second from 15 to 6
- Roll back of the DSP change (later reintroduced)

Although some improvements were seen these actions did not have the desired effect. Service Users continued to report intermittent delays with SRVs completing during commissioning. Therefore, the DSP change was not the cause of this issue.

Plans were made to expedite planned multi-channel tuning activity to reduce congestion on the transmitter equipment.

CSP North also produced a list of the top 50 chatty devices generating a large number of alerts with a view to disabling the devices. 45 of these devices belonged to a single

SU, they were contacted, and they carried out clean up activity (6.4.1 SRs sent) on them and 380 other devices generating 8F3E alerts (8.7.2 SRs sent). This clean up activity reduced alerts by approx. 30% easing the congestion on the transmitters and reducing the 'too busy' failures to normal levels. Technical restoration was achieved 16:20 at 26/11/2019 Manual multi-channel tuning was completed on 29/11/2019 which further reduced the congestion on the transmitters leading to a further decrease in the number of 'too busy / HTTP500' errors returned
Reported Customer Impact
DCC Service Users reported delays and failures to SRVs sent during install and commissioning activities. A delay in the sending of scheduled meter reads was also reported

Actions Completed to Recover Service		
Item	Description.	Owner
1	Service Users suppressed excessive traffic from their chatty devices (6.4.1s to stop the 8F01 alerts & 8.7.1/8.7.2 to stop the 8F3E alerts)	Service Users
2	CSP North completed multi-channel tuning activities. 215k comms hubs were moved across different channels to spread the traffic and clear congestion.	CSP North
3	DSP made amendments to the rate of scheduled meter reads per second. First to decrease the rate so reads were spread out throughout the day. After the 2 actions above were completed the rate was increased so the majority of reads were completed in the 'scheduled read window'	DSP

Key Incidents – December Excluded Through PMEL

Not DCC Resolution

Incident Reference	**INC000000524184 – Category 2**
Problem Reference	**PBI000000118605**
System(s) Impacted	Service Requests for Single Service User
Incident Start Date / Time (Logged in Remedy)	01/12/2019 09:20
Incident Resolved Date / Time	01/12/2019 17:24

Outage Start	01/12/2019 09:20
Outage End	01/12/2019 11:11
Incident Closure Date	07/12/2019
Major Incident Duration	8 hours 3 minutes
Regions Impacted	All
Resolved within SLA	Yes

Summary of High Category Incident

At 09:45 DCC Service Centre informed DCCMIM that the northbound queue had been building up over some time and that there were over 2 million messages for a Service User, it was suspected that this was related to upgrade work on the Service User's data links into DSP.

DCC IM contacted DSP MIM at 10:09, DSP MIM setup technical bridges to discuss removal of 8F3E alerts from the northbound queue for the effected Service User. A further bridge was convened with the provider of the Service Users data link. During this call it was seen that the link had returned to service at 11:11 on 01/12/2019. This was confirmed by the Service User.

All parties (DSP, DCC, Data link Provider, Data link Provider's 3rd Party and the Service User) have stated that they had not taken any corrective actions.

Reported Customer Impact

One Service User was completely isolated from the Smart Metering infrastructure, they were unable to receive alerts or send messages. They were also unable to access SSI.

There was no impact to other Service Users.

Actions Completed to Recover Service		
Item	Description.	Owner
1	No corrective actions were taken by DSP, Service User or their providers to restore service.	N/A

Incident Reference	**INC000000530634 – Category 2**
Problem Reference	**N/A**
System(s) Impacted	Queuing of Service Requests within DSP's Northbound Message Store
Incident Start Date / Time	15/12/2019 09:05

(Logged in Remedy)	
Incident Resolved Date / Time	15/12/2019 16:07
Outage Start	15/12/2019 05:30
Outage End	15/12/2019 15:00
Incident Closure Date	22/12/2019
Major Incident Duration	7 hours 2 minutes
Regions Impacted	All
Resolved within SLA	Yes

Summary of High Category Incident
Multiple Service Users are currently carrying out internal planned works which has resulted in excessive messages queuing in the DSP Northbound Message store. All SRV's and alerts are not being accepted by the Service User's whilst they are carrying out their planned works, causing DSP's queue to increase. These Planned Outages for Service Users do not go through the DCC Change Management process.

Reported Customer Impact
As this incident occurred on a Sunday there is very little customer impact. Install and Commission activity is very low, Sunday is not a recognised installation day. Scheduled Reads there was no impact as they take place overnight. On Demand Reads were either queued in CSP Central and South or processed. AD1 workflow API timed out from CSP Central and South when the interface was closed down from DSP side but once this was re-established everything processed successfully.

Actions Completed to Recover Service		
Item	Description.	Owner
1	Preapproved script in place to discard 8F3E's during uncontrolled Service User Planned works. .	DSP

Incident Reference	**INC000000530467 – Category 2**
Problem Reference	**PBI000000118518**
System(s) Impacted	Queuing of Service Requests within DSP's Northbound Message Store
Incident Start Date / Time (Logged in Remedy)	15/12/2019 11:05

Incident Resolved Date / Time	15/12/2019 11:18
Outage Start	15/12/2019 05:30
Outage End	15/12/2019 15:00
Incident Closure Date	21/12/2019
Major Incident Duration	13 minutes
Regions Impacted	All
Resolved within SLA	Yes
Summary of High Category Incident	
This is a duplicate of INC000000530634. Please refer above for further details	
Reported Customer Impact	
As above	

3 Code Performance Measures

3.1 Service Levels Attained

This section reports the Service Levels achieved in December 2019 against the targets specified in Sections H13.1 and L8.6 of the SEC.

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM1	**Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.**			**95.04%**	**98.05%**	**99.00%**	**96.00%**
	PM1.1	Percentage of DSP Service Request Times within relevant TRT	DSP	99.94%	99.65%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP SIE	96.95%	99.13%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP Capgemini	99.98%	99.98%	99.00%	96.00%
	PM1.4	Percentage of DCC Service Request Times within relevant TRT	DSP	99.97%	99.96%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPN	59.55%	84.71%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPC	97.15%	98.89%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPS	97.01%	98.74%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPN	100.00%	100.00%	85.00%	80.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPC	99.95%	99.74%	99.00%	90.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPS	99.95%	99.73%	99.00%	90.00%
CPM2	**Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time**.			**99.91%**	**99.92%**	**99.91%**	**96.00%**
	PM1.2	Percentage of DSP Service Response Times within relevant TRT	DSP	100.00%	100.00%	99.00%	96.00%
	PM1.3	Percentage of DSP Service Request Scheduling Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	99.99%	100.00%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	99.03%	99.30%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	100.00%	100.00%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPC	100.00%	99.99%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPS	100.00%	99.98%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPC	99.99%	99.94%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPS	99.99%	99.94%	99.00%	96.00%
CPM3	**Percentage of Alerts delivered within the applicable Target Response Time.**			**98.33%**	**98.84%**	**99.00%**	**96.00%**
	PM1.5	Percentage of DSP Alert Response Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	99.95%	99.98%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP SIE	99.16%	99.59%	99.00%	96.00%
	PM1.7	Percentage of S1SP SMETS1 UTRN Response Times within relevant Target Response Time	S1SP SIE	No Events	No Events	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	92.64%	94.74%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	99.96%	99.94%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	99.93%	99.95%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM4	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**87.50%**	**75.00%**	**100.00%**	**85.00%**
CPM5	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 3, 4 or 5 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**91.98%**	**93.64%**	**90.00%**	**80.00%**
CPM6	**Percentage Availability – Self Service Interface**			**100.00%**	**100.00%**	**99.50%**	**98.00%**
	PM2.4	Percentage Service availability – Self Service Interface (Production Services)	DSP	100.00%	100.00%	99.50%	98.00%
CPM7	**Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.**			**100.00%**	**100.00%**	**99.00%**	**96.00%**
	PM1.1	Batch requests for device certificates maximum 375,000 for RA system received 07:00-18:00 available by 06:59 next day	TSP	100.00%	100.00%	100.00%	95.00%
	PM1.4	Single certificate requests via RA System 100% within 30 seconds	TSP	100.00%	100.00%	100.00%	99.00%
	PM1.7	Single certificate request via system to system interface in Core Service Hours (maximum 12 certificate requests/second) 100% within 15 seconds	TSP	100.00%	100.00%	100.00%	99.00%
CPM8	**Percentage of documents stored on the SMKI repository delivered within the applicable Target Response Time for the SMKI Repository Service.**			**100.00%**	**100.00%**	99.00%	100.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM13	Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service.	DSP	100.00%	100.00%	99.00%	96.00%
	PM1.8	Processed certificate or binding is made available to PKI repository within 10 seconds	TSP	100.00%	100.00%	99.00%	96.00%

Table 1 - DCC Code Performance Measures

3.1.1 Service Level below Minimum – CPM1

Percentage of On-Demand Service Responses delivered within the applicable Target Resolution Time

The Service Level reported for CPM1 is 98.05% and is below the Target Service Level.

CSPN PM2 reported Service Level was 84.71% and is below Minimum Service Level.

The above measures have been affected by the volume of alerts coming across to the CSPN from a small percentage of the estate. The volumes of these are 30x that specified in the design. A Problem record PBI000000116412 has been raised. The issue requires a firmware upgrade to resolve but this can't be done over the air and requires the service user to visit the site. Other alerts (8F3E's) are being investigated within the test labs along with the meter manufacturer.
Service Users have been advised not to install this model of Communications Hub whilst investigations are on-going.

CSPC PM2 reported Service Level was 98.89% and is below Target Service Level.

CSPS PM2 reported Service Level was 98.74% and is below Target Service Level.

The reason for the difference between the regions is that the south region was Amber in the September reporting period causing a high multiplier to be applied.

The performance for this measure has improved but it has missed the target due to continued user submission of single requests (instead of batch requests) and error timeouts caused by suspected aborted installs. CSP continues to work with users to identify and address these installations.

3.1.2 Service Level below Minimum – CPM3

Percentage of Alerts delivered within the applicable Target Resolution Time

The Service Level reported for CPM3 is 98.84% and is below the Target Service Level.

CSPN PM3.2 reported Service Level was 94.74% and is below Minimum Service Level.

The above measures have been affected by the volume of alerts coming across to the CSPN from a small percentage of the estate. The volumes of these are 30x that specified in the design. A Problem record PBI000000116412 has been raised. The issue requires a firmware upgrade to resolve but this can't be done over the air and requires the service user to visit the site. Other alerts (8F3E's) are being investigated within the test labs along with the meter manufacturer.

3.1.3 Service Level below Minimum – CPM4

Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.

The Service Level reported for CPM4 is 75.00% and is below the Minimum Service Level.

This was impacted by INC000000518930.

INC000000518930 exceeded the target resolution time as the incident was caused by multiple factors causing congestion on the CSP North infrastructure. Time consuming actions were required to ease the congestion and restore service to expected levels. CSP North expedited the completion of multi-channel tuning activity on the transmitter equipment. This involved moving 215k Comms Hubs to different channels over the course of several days. DCC Service Management were also engaged to coordinate with Service Users to reduce the high number of alerts being generated by 'chatty' devices by sending specific Service Requests.

Please see section 2 "Key Incidents" for further details of this event.

3.1.4 Category 1 and 2 Incident Resolution – CPM4

For clarity please note, to ensure operations boards are furnished with the most recent information, data provided to them utilises the "Start Date". The PMR utilises the "Closed Date" as the formal service level performance on Incident Resolution can only be calculated on closure. This can result in discrepancies between operational reporting and contractual reporting in instances where Incidents are Opened in one month and Closed in another.

Incident Volumes – Closed in Measurement Period

CPM4 measures Incident resolution performance for Category 1 and 2 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA
Category 1	1	1	0
Category 2	3	2	1
Total	**4**	**1**	**1**

Table 2 - CPM4 Incident Count

For Information only: Prior to any Performance Measurement Exclusions Applied

Category	Total Incident Count	Within SLA	Failed SLA
Category 1	1	1	0
Category 2	6	5	1
Total	**7**	**6**	**1**

Table 3 – CPM4 Pre-PMEL Incident Count

3.1.5 Category 3, 4 and 5 Incident Resolution - CPM5

Incident Volumes – Closed in Measurement Period

CPM5 measures Incident resolution performance for Category 3, 4 and 5 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA
Category 3	25	21	4
Category 4	111	106	5
Category 5	1,107	1,037	70
Total	**1,243**	**1,164**	**79**

Table 4 - CPM5 Incident Count

3.1.6 CPM4 and CPM5 – Incidents Re-Opened after Closure

Where an incident that has been closed and their Service Level reported on in a previous period, and re-opened and Closed in this reporting period, the Service Level reported may be subject to change. The new Service Level will be documented below:

No Incidents Closed in this period have been re-opened and reported in a previous period.

3.1.7 Incident Resolution Information – CPM 4 & 5

For information only

Incident Volumes - Raised at any point in time and in a Resolved Status at the point of extract. (Point of Extract: 1st of the Month following the reporting period)

Category	Within SLA	Failed SLA	SLA Pass %
Category 1	0	0	N/A
Category 2	2	2	0.00%
Total	**2**	**2**	**0.00%**

Table 5 - Incidents Relating to CPM4

Category	Within SLA	Failed SLA	SLA Pass %
Category 3	17	7	58.82%
Category 4	8	0	100.00%
Category 5	205	26	87.32%
Total	**230**	**33**	**85.65%**

Table 6 - Incidents Relating to CPM5

Incident Volumes assigned to Service Users – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 June					1	**1**
2018 July					2	**2**
2018 August					48	**48**
2018 September					76	**76**
2018 October					141	**141**
2018 November				1	230	**231**
2018 December					351	**351**
2019 January				1	588	**589**
2019 February					398	**398**
2019 March				2	562	**564**
2019 April					675	**675**
2019 May				2	560	**562**
2019 June				5	1,359	**1,364**
2019 July				12	1,570	**1,582**
2019 August			2	4	1,775	**1,781**
2019 September			2	3	2,540	**2,545**

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2019 October			10	1	2,940	**2,951**
2019 November			28	2	2,791	**2,821**
2019 December		1	42	11	4,199	**4,253**
Total		**1**	**84**	**44**	**20,806**	**20,935**

Table 7 - Aged Incidents Assigned to Service Users

Analysis of these aged incidents show that the top 3 issues are;

Incorrect Communications Hub Variant Installed – 7,852
Incorrect Credentials Loaded on to Device – 9,781
DUIS Service Request 8.14. not received – 1,337

The Incident into Problem plan was shared at the Customer Forum in January and received positive feedback. The plan is now to be taken back to OPSG in February to seek agreement to proceed. In the meantime, Service Management are putting a plan together to have a lead Service Manager assigned to each Aged Incident problem type to drive engagement; mirroring the success on the Alerts initiative.

Incident Volumes assigned to Service Providers or DCC Resolver Teams – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 May					1	**1**
2018 August					1	**1**
2018 September					3	**3**
2018 October					1	**1**
2018 November					19	**19**
2018 December					29	**29**
2019 January					91	**91**
2019 February				1	34	**35**
2019 March					100	**100**
2019 April					86	**86**
2019 May			1		84	**85**
2019 June					137	**137**
2019 July					177	**177**
2019 August				2	257	**259**
2019 September			4	4	142	**150**
2019 October			2	2	235	**239**
2019 November			6	7	175	**188**

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2019 December			4	11	323	**338**
Total			**17**	**27**	**1,895**	**1,939**

Table 8 - Aged Incidents Assigned to Service Providers or DCC

DCC Incident Management have a process whereby the aged incidents are split into Service User and Service Provider. These are worked through on a daily basis in an attempt to bring the number of aged incidents down.

3.2 Performance Level Exemptions

In accordance with the Performance Measurement Methodology document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below.

No Service Providers requested exemptions this period.

3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time.

Exception Type	Total Incidents
User Responsibility	542
Total	**542**
Exclusion Type	
Alert / Event Monitoring (For Information only)	2,509
Duplicate	623
Cancelled	117
Production Proving / Testing	6
Internal to DCC – Non DCC Impacting	16
Total	**3,271**
Grand Total	**3,813**

Table 9 - PMEL Exclusions Detail

4 Reported List of Service Provider Performance Measures DSP

4.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service availability – DCC Data Service	Monthly	100.00%	100.00%	99.95%	99.00%
	2.2	Service availability – DCC User Interface	Monthly	100.00%	100.00%	99.95%	99.00%
	2.3	Service availability – DCC Service Management	Monthly	100.00%	100.00%	99.50%	98.00%
	2.4	Service availability – Self Service Interface	Monthly	100.00%	100.00%	99.50%	98.00%
	2.5	Service availability – Average Interface (DCC Internal availability	Monthly	100.00%	100.00%	95.00%	90.00%
	2.7	Service availability - Test services	Monthly	100.00%	100.00%	99.00%	98.00%
Application Management	3	Category 1 or 2 Incidents directly related to a change release within 30 days of release[4]	Monthly	0	0	0	5
Anomaly Detection	11	Anomalous Service Requests	Monthly	100.00%	100.00%	99.00%	96.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2019 Q2	Latest Qtr. Service Level 2019 Q3	Target Service Level	Minimum Service Level
Service Management	7	Notification of Planned Maintenance events[5]	Quarterly	100.00%	92.31%	100.00%	90.00%

Table 10 - DSP Reportable Performance Measures

[4] DCC are reviewing the contractual definition of this DSP Performance Measure
[5] Measurement Period is a Calendar Quarter

4.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

5 Reported List of Service Provider Performance Measures CSP North

5.1 Service Levels Attained

*Performance Measures are reported monthly unless otherwise specified.

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	94.38%	99.24%	80.00%	70.00%
	1.2	First time SMWAN connectivity within 30 days	Monthly	99.94%	99.82%	90.00%	80.00%
	1.4	SMWAN connectivity Level	Monthly	99.97%	**99.99%**	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	99.14%	99.07%	99.00%	95.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	99.84%	99.71%	99.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	375.48%	385.39%	99.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	100.00%	100.00%	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	100.00%	No Events	99.00%	95.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2019 Q3	Latest Qtr. Service Level 2019 Q4	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.3	First time SMWAN connectivity within 90 days	Quarterly	99.99%	100.00%	99.00%	95.00%
Service Management	10	Notification of Planned Maintenance events within required target[6]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 11 - CSPN Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 385.39%. CSPN had a total of 14,751 CH power outages reported, in December, and 14,708 were sent to DSP within SLA. CSPN MET (100%).

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

[6] Measurement Period is a Calendar Quarter

Using the calculation above PM12.2 = 100 * (14751/ ((14751 – 50) * 0.25) + 50) = 385.39%

5.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[7] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

5.2.1 In Period Exceptions

5.2.1.1 PM1.4 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.4 (CSPN)	15,205	Failure to follow maintenance as per CHIMSM	These figures are for the reporting period (not cumulative)

Table 12 - CSPN PM1.4 Exclusions

15,205 x CH excluded for December 2019 due to several reasons, covering: -

- Incomplete Communication Hub Install – 5,395
- Communication Hub installed on non-consumer premises e.g. Live Lab – 17
- Communication Hub in Low Coverage database – 83
- Communications Hubs where JSR is incomplete – 40
- Communications Hubs where no incident has been raised for outage – 7,065
- Issue started and ended in prior month – 2,605
- Data Error – 4,530
- Not Active – 9

Explanations for the exclusions mentioned above are as follows:

[7] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

Incomplete Communication Hub Install

Installations that have been aborted by the service user, but no service requests submitted. If the installation results in an install and leave then the SU should be submitting and 8.14.2 service request. If the install is fully aborted then an 8.14.3 service request should be submitted. This is being investigated as part of problem ticket.

Communication Hub installed on non-consumer premises e.g. Live Labs

Hubs install is confirmed as not in scope because it not installed on a consumer's premises, i.e. Live Labs.

Communication Hub in Low Coverage database

Comms Hub is installed in a low coverage area.

Communications Hubs where JSR is incomplete

CH insufficient address details / none at all provided in order to determine if the install was compliant and in line with CSPN recommendation. This is caused by address field being optional in DUIS but in the CSPN contract it states that this is a Mandatory requirement.

Communications Hubs where no incident has been raised for outage

CSPN see the comms hub appear on its network but then do not see any traffic to or from the comms hubs for more than 10 days. This is mostly driven by service users powering on a comms hub and either not completing the install or correctly decommissioning it. As soon as the CSPN system sees the CH on the network, it will be looking for it forever. This is being investigated as part of problem ticket.

Issue started and ended in prior month

Comms Hubs where the outage incident started and ended in a previous month but are showing the in current reporting month. This reporting issue is being investigated by CSPN.

Data Error

Comms Hubs where the data shows that an additional outage started prior to the previous one ending. This is an error and is under investigated by CSPN.

Not Active

Comms Hubs where the Operational Status in the CSPN system is not set to Active, to be included in PM1.4 the device must be Active. These are devices where the SU has started the Returns Process

5.2.2 Total Estate Exceptions

No events or periods of time were identified as an Allowed Exception

6 Reported List of Service Provider Performance Measures CSP Central

6.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.98%	99.98%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	100.00%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	99.16%	99.02%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	100.00%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	395.66%	396.23%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	No Events	No Events	99.90%	99.50%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	No Events	No Events	99.00%	95.00%
Performance Area	**Performance Measure Number**	**Performance Measure Name**	**Measurement Period**	**Previous Qtr. Service Level 2019 Q3**	**Latest Qtr. Service Level 2019 Q4**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	100.00%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[8]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 13 - CSPC Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 396.23%. CSPC had a total of 15,776 CH power outages reported, in December, and all were sent to DSP within SLA (100%).

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (15776/ ((15776– 50) * 0.25) + 50)) = 396.23%

[8] Measurement Period is a Calendar Quarter

6.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[9] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

6.2.1 In Period Exceptions

6.2.1.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPC)	5,177	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 14 - CSPC PM1.1 Exclusions

5,177 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,208
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 271
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 30
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 294
- CHIMSM Not Followed – Associated with NEP – 2
- CHIMSM Not Followed – 8.14.2 on Cellular – 9
- There were no, or incomplete address details provided by the Service User – 3,363 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

[9] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

6.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPC)	5,177	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 15 - CSPC PM11 Exclusions

5,177 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,208
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 271
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 30
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 294
- CHIMSM Not Followed – Associated with NEP – 2
- CHIMSM Not Followed – 8.14.2 on Cellular – 9
- There were no, or incomplete address details provided by the Service User – 3,363 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

6.2.2 Total Estate Exceptions

6.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	53,059	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 16 - CSPC PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

53,059 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 8,698
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 3,945
- Aborted Installation – 206
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 562
- Installed out of region – 5
- Test Lab installations – 2
- There were no, or incomplete address details provided by the Service User – 39,641 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7 Reported List of Service Provider Performance Measures CSP South

7.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.95%	99.97%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	98.89%	99.01%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	100.00%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	394.25%	396.86%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	No Events	No Events	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	No Events	No Events	99.00%	95.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2019 Q3	Latest Qtr. Service Level 2019 Q4	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	100.00%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[10]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 17 - CSPS Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 396.86%. CSPS had a total of 18,969 CH power outages reported in December, and all were sent to DSP within SLA (100%).

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

[10] Measurement Period is a Calendar Quarter

Using the calculation above PM12.2 = 100 * (18969 / ((18969 – 50) * 0.25) + 50)) = 396.86%

7.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[11] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

7.2.1 In Period Exceptions

7.2.1.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPS)	6,467	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 18 - CSPS PM1.1 Exclusions

6,467 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,604
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 565
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 31
- CHIMSM Not Followed – 8.14.2 on Cellular – 15
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 220
- There were no, or incomplete address details provided by the Service User – 4,032 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

[11] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

7.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPS)	6,467	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 19 - CSPS PM11 Exclusions

6,467 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,604
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended - 565
- CHIMSM Not Followed – CH Never connected but received 8.14.1 - 31
- CHIMSM Not Followed – 8.14.2 on Cellular – 15
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 220
- There were no, or incomplete address details provided by the Service User – 4,032 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7.2.2 Total Estate Exceptions

7.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	57,888	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 20 - CSPS PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

57,888 x CH excluded for December 2019 due to a number of reasons, covering: -

- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 8,940
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 4,283
- Aborted Installation – 129
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 400
- Installed outside of region – 2
- CHIMSM Not Followed – Given UPRN is not available – 1
- Test Lab installations – 1
- There were no, or incomplete address details provided by the Service User – 44,132 *

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

8 Reported List of Service Provider Performance Measures S1SP SIE

8.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.2	Service Availability – RPS Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.4	Percentage Service availability – S1SP Management Interface Availability (Production Services)	Monthly	100.00%	100.00%	99.50%	98.00%
	2.7	Service Availability - Test services	Monthly	100.00%	100.00%	99.00%	98.00%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level	Latest Qtr. Service Level	Target Service Level	Minimum Service Level
Service Management	7	Planned Maintenance events	Quarterly	N/A	100.00%	100.00%	90.00%

Table 21 – S1SP SIE Reportable Performance Measures

8.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

9 Reported List of Service Provider Performance Measures S1SP Capgemini

9.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.2	Percentage Service availability – CP Service (Production Environment)	Monthly	100.00%	99.81%%	99.95%	99.17%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5

Table 22 – S1SP Capgemini Reportable Performance Measures

9.1.1 Service Level Below Target Service Level

PM2.2 Percentage Service availability – CP Service (Production Environment), reported Service Level is 99.81% and is below Target Service Level due to P3 Incident INC000000528522. The incident was a result of additional storage being allocated to the app hosts in the UK Cloud while the auto scan feature was enabled. This resulted in a high level of traffic be generated causing storage disconnects and the virtual servers to enter into a read only state. The autoscan feature was subsequently disabled and service was restored.

The outage did not directly impact the DCC due to migrations being suspended during the period in which this incident occurred.

9.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

10 Reported List of Service Provider Performance Measures S1SP Vodafone

10.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability		Monthly availability of the Radio Network across VF-UK network	Monthly	99.60%	99.71%	TBC	TBC
		Combined monthly IoT Core and Management Service Availability	Monthly	99.92%	99.90%	99.70%	99.70%
		Monthly IoT Core availability (Voice/Data/SMS)	Monthly	99.92%	99.95%	99.90%	99.90%
		Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal)	Monthly	100.00%	99.95%	99.70%	99.70%
		Monthly Availability of DCC dedicated fixed links	Monthly	No Events	TBC	TBC	TBC

Table 23 – S1SP Vodafone Reportable Performance Measures

10.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

11 Service Credits

The calculation of Service Credits is subject to certain contractual exemptions.

The CSPs have exemptions relating to the installation of Communications Hubs as detailed below;

- CSP South, Performance Measure 1.3 (First time SMWAN connectivity within 90 days) and Communications Hub Performance Measures PM1.1 (Number of Communications Hubs delivered to DCC Service Users according to schedule each Delivery Month) and PM1.2 (Number of Communication Hubs accepted by DCC Service Users in each Delivery Month) exempt from Service Credits until the cumulative number of Communication Hubs installed at the end of any measurement period is greater than or equal to 550,000.

For all other Performance Measures, the Service Credits accrued for this measurement period are as follows:

CSP (N) failed to meet the Target Service Level for four Performance Measures. These Performance Measures are:

CSP PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 84.71%. This failure resulted in the accrual of 150 Service Credit points which equate to Service Credits of £38,894. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP PM3.2 – Category 3 Alerts delivered to the DCC WAN Gateway Interface. The Target Service Level for this PM is 99% and the Actual Service Level achieved was 94.74%. The Service Credit Points for this measure is 263, with Service Credits of £68,195. (This Performance Measure contributes to Code Performance Measure 3.)

Regarding CSP PMs 2 & 3.2, discussions are ongoing between DCC and CSPN regarding the installation by Service Users of meters outside of the agreed derogation areas. Until Phase 2 of ARQCR1028 is implemented, CSPN are unable to automate the exclusion of these non-compliant meters from Performance Measure results. It is therefore proposed that no Service Credits are paid against these Service Measures. DCC to issue a formal position around these performance measures.

CSP PM7.3 – Percentage Incident Resolution of Severity 1 and Severity 2 Incidents within requirement based on Severity level. The Target Service Level for this PM is 99% and the Actual Service Level achieved was 0.00%. The Service Credit Points for this measure is 100, with Service Credits of £25,930. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP PM9 - Delivery of Change Requests. The Target Service level for this PM is 100% and the Actual Service Level achieved was 50%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

These failures equate to Service Credits of £133,019.

CSP (C) failed to meet the Target Service Level for two Performance Measures. These Performance Measures are:

CSP PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 98.89%. This failure resulted in the accrual of 3 Service Credit points which equate to Service Credits of £12,110. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP PM9 – Delivery of Change Requests. The Target Service level for this PM is 100% and the Actual Service Level achieved was 86%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (S) failed to meet the Target Service Level for two Performance Measures. These Performance Measures are:

CSP PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service level for this PM is 99.0% and the Actual Service Levels achieved was 98.74%. This failure resulted in the accrual of 14 Service Credit points which equate to Service Credits of £37,584. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP PM9 - Delivery of Change Requests. The Target Service level for this PM is 100% and the Actual Service Level achieved was 86%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

These failures equate to Service Credits of £49,694.

DSP No Service Failures have occurred during the month. Therefore, no Service Credits have accrued this month.

Note: Whilst discussions on an appropriate measurement method for PM10 continue, it has been greyed out and will not count as either a pass or a fail. This will be revisited once the PM10 performance measure is agreed.

A summary of last 12 months Service Credits is provided in the table below:

Month	Arqiva	BT	CGI	Telefonica	Total
Jan-19	£0	£0	£2,235	£82,097	**£84,332**
Feb-19	£21,402	£0	£0	£0	**£21,402**
Mar-19	£16,510	£0	£2,429	£93,216	**£112,155**
Apr-19	£14,369	£0	£9,333	£93,230	**£116,933**
May-19	£30,078	£0	£4,859	£93,185	**£128,122**
June-19	£53,883	£0	£12,146	£41,975	**£108,004**
July-19	£75,974	£0	£14,771	£86,321	**£177,066**
Aug - 19	£0	£0	£29,758	£86,321	**£116,079**
Sep - 19	£82,975	£0	£17,005	£6,188	**£106,168**
Oct – 19	£94,125	£0	£20,201	£0	**£114,326**
Nov – 19	£100,607	£0	£0	£44,523	**£145,130**
Dec – 19	£133,019.	£0	£0	£49,694	**£182,713**

Table 24 – Service Credits

12 DCC's Internal Costs and/or External Cost

There is no impact on DCC's Internal Costs.

DCC's External Costs in the period of this report are reduced by the Service Credit total of £182,713.

13 Appendices

13.1 Appendix A – Open Problem & Incidents relating to Prior Periods

13.1.1 PBI000000113808

February Report - Key Incident **INC000000429217**

Device Searches Outage - Invalid Business Objects

Problem: Device searches were not returning any information within SSI (Self Service Interface) and SSMI (Self Service Management Interface). This query allows the users to search for Smart Metering devices by various inputs, then view full details of any devices that the search locates. Users are unable to perform the searches to locate the devices.

Root Cause was confirmed as Objects are becoming invalidated in reporting databases as a symptom of a workaround for application/database Production triggered processes not being able to be fully applied to Disaster recovery. This is a workaround that was developed early on in the development phase by DSP, it has always existed and was not introduced following go-live or under a problem or change. This is the first time the skip rules cause an issue like this and it's being investigated by DSPs Vendor. Transactions are skipped from applying on the reporting databases to prevent synchronisation halting and the Transactions that contain DDL (Data Definition Language) on certain tables are causing packages/views to become invalid at 10pm and 1am.

A fix has been implemented by the DSP to correct the issue at 10pm which was caused by a maintenance job and it was this view becoming invalid that caused the Incident. Mitigating has been completed to introduce new alerting to catch invalid objects before they cause a service impact. A fix has been defined to correct the issue at 1am for the possibility of the ERROR_LOG functionality to be separated out to dedicated tables within the database. The code fix to complete resolution activities is due in DSP release 43, scheduled for deployment into Production on 17th March 2020.

Latest: Target Completion Date 20/03/2020

13.1.2 PBI000000113813

February Report - Key Incident **INC000000430724**

Problem: Failure of inbound SR's from DSP to CSP North. This Problem Record is with CSP North. Loss of Inbound SR (Service Request) traffic from DSP to CSP North approx. 15:05 - 17:17 on Monday 18th February 2019. Outbound service was unaffected. No customer impact reported by SU's (Service Users).

The Root Cause has been confirmed as a bug in a Firewall software that caused memory leak [due to unnecessary logging profile configuration updates]. This led to Out of Memory Killer having been invoked 3 times in an attempt to free up swap memory which closed off enough processes to result in the Firewall crashing and going offline.

The fix for this issue requires the unnecessary logging profile configuration updates bug to be fixed. Software upgrade/patching and testing to confirm the fix has begun. This issue is not service affecting, unless a device crashes again before fixed, but the last two times it

has been tested it has failed over without impact. The enduring fix will require a prolonged test phase across multiple environments before promoting to Production which may ultimately coincide with Technology refresh in April 2020. No impact has been seen post incident. A precautionary restart of the Firewall has been successfully carried out on 19th of December 2019 and will be scheduled periodically via Change Process until the permanent solution is put in place.

Latest: Target Completion Date 30/04/2020

13.1.3 PBI000000115702

June Report - Key Incident **INC000000456123**

SR's returning an error status on the 24th May due to Master Key Store (MKS) issue.

Problem: This Problem Record is with the DSP. On Friday 24th May an issue arose within the DSP infrastructure which impacted the flow of traffic, Northbound and Southbound, through the DSP Motorway. It was discovered that a network connection to the Master Key Store (MKS) was causing issues, a restart of the MKS application was carried out to restore service. Some Service Requests (SR's) that required a cert from MKS failed, however instead of returning an error to the Service User, they timed out after 60 seconds.

The Root Cause has been identified as a behavioural/code issue. After the initial 60-second time-out DSP systems completed a number of retries and waits for those to also fail before sending any final error message back to the Service User. It seems in this case that the Service User didn't wait for the full DSP-retry cycle before deciding that the SR had failed. A code change was required to ensure an appropriate response to Service Users in the event of connection/application performance issues. The fix was included within DSP#36, deployed into Production on 27th August 2019. DCC are working with DSP to ensure mitigation is in place to avoid potential reoccurrence.

Latest: Target Completion Date 28/02/2020

13.1.4 PBI000000116409

June Report - Key Incident **INC000000459622**

Service Users unable to run SMI and SAT queries

Problem: This Problem Record is with the DSP. Multiple Service Users were unable to run SMI (Service Management Interface) and SAT (Standard Acis Text file) queries. The queries were running but not completing due to the request timeouts. No corrective action was taken to restore service as the incident self-cleared.

The Root Cause has been found. ESI reports run long running queries on the reporting database and lock tables whilst doing so, this prevents online queries from returning within expected timeframe however, some of the ESI reports were not designed to run with the volume of data now present in the system which is contributing to the long running queries. A workaround to run the ESI reports on the DR Reporting DB server is being used until a permanent fix can be devised.

The solution has been delivered via a code fix.

Latest: Target Closure Date changed to 07/02/2020 to support testing and confirmation of issue resolution.

13.1.5 PBI000000116302

July Report - Key Incident **INC000000457675**

An intermittent fault on the CSP Central & South Smart Metering Wide Area Network service

Problem: This Problem Record is with the CSP (Central & South). This has been raised to track investigation for the High priority incident on 03/6/19. The EPG (Evolved Packet Gateway) failed on the previous night. The incident was mitigated by draining the Comms hub off the EPG. As a result, this caused the Comms Hub to perform reboots. The high number of reboots caused an influx of Service Requests to be sent causing a backlog.

The Root Cause has been identified. The large influx of messages onto the system was due to CH (Comms Hub) behaviour post a vEPG (virtual Evolved Packet Gateway) drain. This influx of traffic caused queues on the CSP servers, which delayed Birth Event traffic and other System and Service User requests. The traffic loss on the EPG was due to protocols failing that direct traffic through the system. A configuration issue was identified and fixed on all 4 of the links.

Latest: Problem Closed

13.1.6 PBI000000116812

August Report - Key Incident **INC000000479406**

DCC SMS, SSI and SSMI service degradation

Problem: This Problem Record is with DSP. DCC Service Management System, Service Management Interface and Self-Service Management Interface observed service degradation when a power outage was experienced throughout the UK which impacted a single rack in DSP Data Centre causing multiple DCC systems to alert.

The Root Cause has not been identified. DSP has confirmed that they have exhausted all testing that can be done without a strategic / planned failover of the F5s with packet captures and sniffers in place. DSP have been unable to see anything other than packet loss / output drops but need to confirm if the loss is enough to have caused this issue. At this stage it is not believed that further testing will add any value to Root Cause Analysis without a failover and captures for analysis. Ahead of any future failover requirements DSP need to provide assurances that a repeat of the impact seen at failover will not be seen, however at this stage no definitive Cause has been confirmed – as a result of the testing completed there has been no fault found to date therefore no further solution to implement in response. What has been identified is that output drops increase only under periods of high traffic output. A recreation of the Incident in a controlled environment is believed to be needed to investigate further, but this will have to be planned and co-ordinated under a planned change. Failover of firewalls is going to be pursued in isolation, under a controlled change, in order to troubleshoot and resolve any outstanding issues with the system management firewalls.

Latest: Target Root Cause Date Expired 27/08/2019

13.1.7 PBI000000117102

September Report - Key Incident **INC000000486219**

CSP North RNI infrastructure (Degradation)

Problem: This Problem Record is with CSP North. On 30th August 2019 DSP flagged an increase in E21's being generated from CSP North infrastructure. Degradation of the Radio Network Interface (RNI) was found and DCC estimate 600 installs in the North were impacted. Service was declared restored following a number of restorative actions being carried out by CSP North. Mitigation for this issue involves 4 hourly checks of Network Controller disk space with check point actions marked should disk space increase pass a threshold. Disk space was also doubled to 300Gb.

The Root Cause has due to CSP North disk space become full. An increase in installs and daily throughput through the NC's (Network Controllers) caused Partition File sizes to gradually increase over time. The log rotation configuration has worked correctly over the last year or so (since its introduction due to a previous incident). However, the increase in file size now means the rotation configuration was no longer suitable and allowed the Partition to fill. Monitoring was in place to capture Partition disk space issues but it had incorrect thresholds settings resulting in the CSP not receiving alerts prior to the issue becoming service impacting.

A further 150GB has been added to each NCs (Network Controllers) since the incident (300GB in total including a 150GB increase to restore the incident). There has been a recommendation to increase by a further 250GB per NC taking total storage for the partition up to 700GB. The CSP have been reviewing requirements for enhanced alerting and are raising amending the threshold alerts from 95% to 70%. This will be requested across all partitions and will need to be tested after to confirm the alerts correctly pull through at the right times. Automatic alert thresholds are being reviewed and long-term solution is still being defined.

Latest: Target Completion Date for this Problem is 28/02/2020

13.1.8 PBI000000117205

September Report - Key Incident **INC000000491661**

Primary host down invoking failover

Problem: This Problem Record is with DSP. A host failover occurred in the late hours of 12th September 2019. The primary core host for the North, Central and South went down at 23:05, which recovered with no corrective action required.

Root Cause was confirmed as a capacity issue. The primary Host failed over to the secondary due to swap memory exhaustion. The North switch failed to work correctly due to missing Hardware Security Module (HSM) keys, added under a Change via Problem Record PBI000000117120, that had not been replicated to the secondary nodes due to a missing step in the Process (now rectified).

The switch vendor has stated that the swap memory exhaustion is related to disk space exhaustion. The 'BIG IP Analytics' process was sending tens of thousands of temporary files to be processed by the 'MySQL' process. The 'MySQL' process also appeared to crash due to disk exhaustion (a single mysql.err.log at 1.5GB). This prevented the processing of the temp files, which resulted in the continual growth of the disk space until it had also been exhausted. A system upgrade to latest version is currently under review, which may resolve the issue with the 'MySQL' process that played a part in the failure. This work needs to be considered in conjunction with Hardware Security Module (HSM) and Load Balancer upgrades currently being progressed across the environments. DSP plan for an enduring fix be completing F5 upgrades across the estate, that programme is very large and will be completed in 3 Phases.

Latest: Target Completion Date for this Problem is 31/03/2020

13.1.9 PBI000000117128

September Report - Key Incident **INC000000493155**

Delays when birthing Comms Hubs in the CSP North region

Problem: This Problem Record is with CSP North. Multiple Service Users experienced delays when birthing Comms Hubs in the CSP North region. Service was restored by restarting the nodes one at a time in the Comms Hub Manager (CHM) infrastructure where a hung process was identified.

Root Cause Analysis investigations continue for this issue. Hourly monitoring of Comms Hub Manager was put in place until an automated monitoring notification would be implemented. This was implemented 26/09/2019 and provides CSP-North with an early warning notification in case of future issues.

Strategic Solution around increased virtual memory capacity commenced on 07th of November 2019, all activities carried out under strict governance and change control. The long term plan is to optimise additional memory allocation for Comms Hub Manager. An upgraded version of Comms Hub Manager is being planned for mid-February and will provide additional improvements to mitigate against this issue.

Latest: Target RCA Date for this Problem Record breached on 22nd October 2019

13.1.10 PBI000000117117

September Report - Key Incident **INC000000487736**

S1SP/SIE Migration failures due to Key Rotation Error

Problem: This Problem Record is with SIE/S1SP. SMETS 1 migrations were suffering from failure with the error message ETO8. On Friday 7th September 27 of the 119 planned migrations failed with the ET08 error. The remaining migrations were then paused to stop any further failures whilst a fix was developed and Implemented.

The Root Cause of this issue was due to the sub sessions being opened with DCO. These sessions were required to be opened separately, however, they were opening at the same

time which was causing the connections to be refused. Other contributory factors have been identified:
1. It was found that there were 4000 open connections on the active load balancer.
2. A race condition was identified between the session managements on two of the S1SP components: Foundation Engine and Migration Manager.

A configuration change was completed to add a delay into the Foundation Engine component to avoid both sessions to DCO being open simultaneously. Measures have also been to be completed to deal with contributory factors. SIE have completed all tasks related to this Problem.

Latest: Closed

13.1.11 PBI000000117305

September Report - Key Incident **INC000000491743**

Service User Message queue increase

Problem: On 13th September at 08:10 DSP reported that they could see message queues for a specific set of Service Users increasing. Initial checks by DSP indicated that the issue could be due to how a Service User was handling message acknowledgements, as all the affected Service Users are hosted through their connection.

The Root Cause is confirmed to be a configuration issue. The Service Users capacity for handling uncharacteristically large queue sizes. For BAU activity this is not an issue, however, should an event happen in any space that results in increased queue sizes, the Service User could experience similar issues in the future.

It was discovered that the message acknowledgement service at the Service User was working as designed but struggling to handle the increased volume (backlog) of messages resulting from a 90-minute interruption to the DSP service provision overnight. The Service User made changes to their acknowledgement process and the backlog reduced as message throughput increased. DCC are coordinating efforts with DSP, DCC Service Management and the Service User to insure repeat incidents don't occur. Work has been completed for the service user to upgrade their primary gateway bandwidth. The upgrade of the Secondary link has to be coordinated with a relocation of equipment in a datacentre due to capacity constraints, this issue has delayed completion of this Problem.

Latest: Target Completion Date for this Problem is 28/02/2020

13.1.12 PBI000000117135

October Report - Key Incident **INC000000495738**

CSP Central and South Comms Hubs not birthing with DSP

Problem: A Service User contacted the DCC to advise that Comms Hubs were not birthing in the Central and South region. This was directly affecting Service Users ability to complete install and commissioning activities. The issue was due to a database full-table scan on the CSP Meter Firmware Operation Logging table. This caused other messages to queue while this scan completed. The reasons behind the full-table scan starting and why it was long-running are under investigation.

The Root Cause of this issue was a configuration change from a CSP release. CSP C&S completed a change release (R8.5) where additional logging was introduced to capture 'Force Time Sync' data issues, this caused the table space to increase significantly. This resulted in increased query times when high volumes of requests were submitted in parallel, in this incident single meter firmware jobs, caused extensive queuing. (90 sec + query times across 1000's of transactions).

CSP C&S technical team added Indexes to the table (per their vendors recommendation). Before the Indexes were added each job could took between 90 and 1200 seconds, following the Indexes going in this has dropped to 11 milliseconds. Long term enhancements are also being devised and a change has been raised to address the main issue of optimising the search API query response times. The change required for the fix has been successfully implemented, this change was to enable a higher number of bulk uploads to be complete in one go. CSP Central and South are now looking to test to confirm the issues are resolved.

Latest: Target Completion Date 28/02/2020

13.1.13 PBI000000117240

October Report - Key Incident **INC000000503961**

CSP Central and South Comms Hubs not birthing with DSP

Problem: A Service User contacted the DCC to advise that Comms Hubs were not birthing in the Central and South region. This was directly affecting Service Users ability to complete install and commissioning activities. The issue was due to a database full-table scan on the CSP Meter Firmware Operation Logging table. This caused other messages to queue while this scan completed. The reasons behind the full-table scan starting and why it was long-running are under investigation.

The Root Cause of this issue was a configuration change from a CSP release. CSP C&S completed a change release (R8.5) where additional logging was introduced to capture 'Force Time Sync' data issues, this caused the table space to increase significantly. This resulted in increased query times when high volumes of requests were submitted in parallel, in this incident single meter firmware jobs, caused extensive queuing. (90 sec + query times across 1000's of transactions).

CSP C&S technical team added Indexes to the table (per their vendors recommendation). Before the Indexes were added each job could took between 90 and 1200 seconds, following the Indexes going in this has dropped to 11 milliseconds. Long term enhancements are also being devised. DSP is still working with the Vendor to ascertain the best upgrade options. DSP has confirmed that the HSM (Hardware Security Module) upgrade is still under analysis with the Vendor as testing of the new client software was unsuccessful. At this stage DSP cannot proceed any further without a re-compiled version for the supporting software. A new testing phase / acceptance test review is required; DSP are currently awaiting a timeline and expect this from the Vendor in the coming weeks.

Latest: Target Completion Date 31/03/2020

13.1.14 PBI000000117151

October Report - Key Incident **INC000000504708** & **INC000000506818**

CSP North - Delayed CH Birthing

Problem: SU's (Service Users) reported delays of Install and Commission activities exceeding 30 minutes in CSP Norths' area. Service was restored; however, symptoms were seen intermittently over the next two days. Only SUs who use “Commission Status Check” step in their orchestration process were affected.

The Root Cause has proven this was as a result of CSP North carrying out tuning activities on a number of CH’s (Comms Hubs) which highlighted code issue that caused TK’s (Transmitter Kit) to disconnect and reconnect resulting in thousands of messages flooding the system. The number of messages being received was greater that what the Comms Hub Manager throttle allows to be passed to DSP Per minute and thus caused a backlog of Install Alerts.

A patch fix for the TK code issue has been deployed via Change Control.

Latest: Closed

13.1.15 PBI000000117601

October Report - Key Incident **INC000000508103**

CHM - Fuse components - Unable to birth in North Region

Problem: This Problem investigates issues with Comms Hub Device Manager related to Fuse components. Install Alerts not progressing through CSP North to DSP on 25th of October 2019 that impacted Service Users (SU's) Comms Hubs installations.

The Root Cause is under investigation. A series of changes has been completed by the CSP North:

1 - Automatic Reboots of the Nodes (4 hourly) - Implemented - Provided the stability and resilience to the systems
2 - CHM Fuse and ActiveMQ JVM optimisation Change 1 - Implemented - Memory utilisation has improved
3 - CHM Fuse and ActiveMQ JVM optimisation Change 2 - Implemented - Memory utilisation has improved
4 - CHM Fuse and ActiveMQ JVM optimisation Change 3 - Implemented - Memory utilisation has improved, No more Hang & Abort of the process routes
5 - Frequency of SLA Cron decreased from 1 Minute to 1 hour to observe the SLA processing - Implemented - No significant improvement observed
6 - Data Fix to invalid data records in the CHM - Implemented - Database contention Improved
7 - Optimisation of Code (CRON SLA) for efficient data processing - Implemented - Resource Utilisation improved as this exclude invalid Records
8 - Throttler Increasing the gap between cycles and the number of SRs per cycle (While Keeping the max count of SR Identical) - Implemented - Improved throughput of the system

The CSP are now looking to reduce the frequency of the reboots currently in place to ensure the changes made have stopped issues reoccurring.

Latest: Target RCA date breached 15/11/2019

13.1.16 PBI000000117154

October Report - Key Incident Excluded **INC000000502214**

SMETS1 Provisioning transactions taking longer than expected

Problem: An incident was raised by the S1CSP Monitoring team as they detected issues during daily health-checks. The provisioning transactions were observed to be taking longer than expected.

Root cause of this Problem is twofold, initially this was identified to be a core network failure on the S1CSP network. S1CSP implemented a change to resolve the core network issue by increasing capacity on a provisioning platform. Further issues were seen & reported post the change. S1CSP proceeded to identify high CPU and memory utilisation on an associated server. The cause of that issue was confirmed as a client activity (of the S1CSP) leading to delays with transactions completing. S1CSP suspended their client's activity and also initiated a code fix to implement to prevent impact from these transactions on the network again.

Enduring fix has been completed via a code change. A full database table scan for provisioning requests was being completed. Due to this, there were many OTA bulk requests submitted that contributed to the creation of an unexpected and excessively resource utilisation on the database. This was permanently optimised after the database tables were indexed. Lessons learnt and improvement tasks have been completed.

Latest: Closed

13.1.17 PBI000000117610

November Report - Key Incident **INC000000510213**

Intermittent Service request failures from DCO

Problem: Following a deployment of a planned DCO (Dual Control Organisation) release in to Production, intermittent Server (error 500) errors were being seen by S1SP in response to the heartbeat service requests (for SMETS1). The deployment was rolled back but issues continued to occur. The Migration of SMETS1 devices could not continue until the incident was resolved.

There are 2 separate unrelated issues within DCO that both contributed to the "Server 500 errors" seen following rollback.

The first was a reoccurrence of the Cryptocontainer issues being investigated in PBI117226 (Bug in the behaviour of the Crypto API (application programming interface) which throws an exception if an error is encountered loading Codesafe against the list of HSMs (Hardware Security Module). An enduring fix is currently being progressed by DCO & its vendor), this was resolved by Container restarts in PROD-B. The second was after the container restarts in PROD-B, any incoming service requests failed, resulting in the

error responses seen by S1SP. This issue was due to an application memory issue, there was a memory limit set to 8Gb and the automating application deployment Memory limit was sent to 4 GB. This caused container memory to be throttled at 4GB when the container was expecting to have 8gb available, causing the container to restart when the 4GB memory usage was reached.

There are two issues to resolve:
1) PBI117226 is dealing with the Bug in the behaviour of the Crypto API (application programming interface) which throws an exception if an error is encountered loading Codesafe against the list of HSMs (Hardware Security Module). The solution proposed is a change of behaviour to note the exception and continue to retry the remaining available HSMs (Hardware Security Module) rather than stopping. This is currently being progressed with DCOs & its vendor.
2) Memory Configuration was amended for the pods within the application servers in the PROD B environment.

The HSM Defensive Solution update is progressing via a commercial CR (Change Request)

Latest: Target Completion Date 30/04/2020

13.1.18 PBI000000117408

November Report - Key Incident **INC000000510226**

CSP-N - UIT-A Environment – No traffic received from Firewall

Problem: Traffic coming to CSP's North UIT-A (User Integration Testing) environment through fronthaul Firewall was being dropped, resulting in Service Users not being able to utilise UIT-A Environment.

The Root Cause is under investigation. CSP North carried out investigations into root cause, which could not be identified.

Firewall policies have been reapplied to restore the service and can be reapplied at any time given issues reoccur. There is monitoring in place, but it is currently impossible to capture the issues before the impact is noticeable. Service has been stable since.

Contractual agreements regarding testing environment are being reviewed by DCC Service Management.

Latest: Target RCA date breached 22/11/2019

13.1.19 PBI000000117609

November Report - Key Incident **INC000000510715**

Delay with Install and Commissions across all regions

Problem: Service Users reported latency with installs and monitoring identified a reduction in Install and Commissions in all regions.

The Root Cause was identified as latency being observed and caused by available sockets. The socket timeout settings are under analysis as if these timeout quicker, they release quicker, leading to sockets being more readily available. On this occasion, the sockets were held for too long, which led to latency and impact on the motorway. Due to resources running out as a result of blocking procedures currently in place. Queries and associated threads to database should be 'non-blocking'.

Making the second Database call asynchronous would resolve this issue. This should mean that DSP don't run out of threads, and although a slow response back to be invoked, it is within the http timeout so calls actually succeed. The fix is currently targeted for DSP#43 Release, scheduled for deployment into Production on 17th March 2020.

Latest: Target Completion Date 20/03/2020

13.1.20 PBI000000117612

November Report - Key Incident **INC000000510869**

UIT-A Not Available For Testing

Problem: On 31st October at 18:49 an incident ticket was raised for the UIT-A environment as users were unable to carry out testing activities. The incident was due to a service user's ESME device in the CSP North UIT-A area generating an excessive amount of alerts (approximately 18,000 alerts). Once this device was turned off normal service resumed. Testing activities in UIT-A had to be suspended until the issue was resolved.

The Root Cause was due to capacity limit being breached. One service user ESME device in the CSP North UIT-A area of the DCC North Test Lab was generating excessive alerts (approximately 18,000 alerts). Once this device was turned off normal service resumed.

DCC are working with DSP to determine what can be done differently to spot and stop these nuisance alerts from impacting the UIT test environments in the future. Contractual agreements regarding testing environment are also being reviewed by DCC Service Management.

Latest: Target Completion Date 28/02/2020

13.1.21 PBI000000117128

November Report - Key Incident **INC000000511840**

Delays when birthing Comms Hubs in the CSP North region

Problem: Multiple Service Users experienced delays when birthing Comms Hubs in the CSP North region. Service was restored by the CSP restarting the nodes one at a time in the Comms Hub Manager (CHM) infrastructure where a hung process was identified.

The Root Cause is under investigation.

Automated monitoring notification on Comms Hub Manager was implemented on 26th of September 2019 and provides CSP-North with an early warning notification in case of

stopped process scenario. Automated resets of these processes at the adjusted timings agreed to accommodate the case when the process is in hanged status rather than being stopped, this has been taking place successfully to date.

Monitoring in place to report on Install and Commission Alert message delay of 4 minutes, to proactively address any Comms Hub potential Issues before they have impact on Service Users. A strategic solution around increased virtual memory capacity commenced on 07th of November 2019 with implementation on PIT-A - under 48 hours review prior to further increase (all activities carried out under strict governance and change control). The Long-term plan is to optimise additional memory allocation for Comms Hub Manager.

A Comms Hub Manager FW update is currently being planned for mid-February and will provide additional improvements and a CPU increase change has been completed to assist mitigation.

Latest: Target Root Cause Date Expired 09/10/2019

13.1.22 PBI000000117807

November Report - Key Incident **INC000000514505**

CSP-N Production Core Firewall high CPU usage and on demand SR's failing

Problem: High CPU (Central Processor Unit) usage on CSP-N Production Core Firewall and high number of connections impacted live service with all on demand Service Requests failing for Service Users.

CSP North vendor identified a memory leak issue within the upgraded firmware that was causing the CPU spike.

CSP Norths vendor have confirmed they now have a fix ready for the CPU issues however they continue to work on memory issues and will be looking to release both fixes at the same time.

Latest: Target Completion Date 28/02/2020

13.1.23 PBI000000117900

November Report - Key Incident **INC000000515630**

CSP-N loss of connectivity to multiple 3G sites

Problem: Over a hundred 3G sites have dropped off the network.

The Root Cause has been identified as incorrect roaming load on the cellular network with CSP North's Vendor. Once the load issue was resolved there was a prolonged impact as the CSP Norths vendors fault left additional manual work to be carried out by CSP North in order for full connection to re-establish between onsite routers and CSP North's infrastructure.

Investigations are ongoing to look at how similar issues can be prevented against in the future and to ensure the correct impact is identified under Incident Triage.

Latest: Target Completion Date 28/02/2020

13.1.24 PBI000000118607

December Report - Key Incident **INC000000526144**

RNI failure following Server patching change

Problem: Failure of multiple RNI (Radio Network Infrastructure) nodes was spotted on the monitoring resulting in no incoming or outgoing traffic on the CSP-North Network. Monitoring also showed shutdown/ heartbeat failures.

The Root Cause has been identified as Human Error during the implementation of a low impacting Planned patching change. The change went through the Non impacting change process however human error lead to an impact.

CSP North change process is under review to accommodate changes to work instructions, work patterns and supervision of change implementers as well as improvements to the current process.

Latest: Target Completion Date 28/02/2020

13.1.25 PBI000000118404

December Report - Key Incident **INC000000520567**

DCC SC Send/Receive email issue

Problem: DCC SC (Service Centre) experienced issues in sending emails (22/11). The issue then progressed to impact them receiving emails.

The Root Cause has been identified as a Capacity issue. It had been found that the mailbox had reached its 100GB limit of storage capacity.

Solution methods have been defined by the DCC service centre to complete regular housekeeping,

Latest: Problem Closed

13.1.26 PBI000000118516

December Report - Key Incident **INC000000530859**

SAT Query Delay

Problem: It was reported that Service Users were experiencing delays when running SAT queries which impacted the ability to view the history of Service Requests on their devices, however, Installs and commissions were not impacted. It was identified that a server had unexpectedly rebooted and required a restart of the application to successfully restore Service.

The Root Cause has been identified as Human Error. The server restart was completed by a technical team member entering the wrong command to a machine.

A change has been created to disable the command on the virtual machines to avoid a repeat issue.

Latest: Target Completion Date 28/02/2020

13.1.27 PBI000000118411

December Report - Key Incident **INC000000518930**

SAT Query Delay

Problem: It was reported that Service Users were experiencing delays when running SAT queries which impacted the ability to view the history of Service Requests on their devices, however, Installs and commissions were not impacted. It was identified that a server had unexpectedly rebooted and required a restart of the application to successfully restore Service.

The Root Cause has been identified as Human Error. The server restart was completed by a technical team member entering the wrong command to a machine.

A change has been created to disable the command on the virtual machines to avoid a repeat issue.

Latest: Target Completion Date 28/02/2020

13.1.28 PBI000000118605

December Report (Excluded through PMEL) - Key Incident **INC000000524184**

Gamma link failure

Problem: Gamma link was down leaving 2 Service users unable to communicate with the DSP system, which meant they were unable to perform any installation or commissioning of SMETS-2 devices or process any Service Requests. No service impact reported as this was Northbound queue affecting.

The Root Cause was a failed Change. The Service User bandwidth upgrade required a Third Party to perform a hub switch and for the Vendor to configure the new bandwidth requirement. Investigation has shown that the hub switch did not work successfully due to a software defect with the Third-Party Portal that is used to automatically request and carry out hub switches.

The Vendor have changed their process so that when upgrading bandwidth involving hub switches, they will do the primary link one day and the secondary link a subsequent day to ensure that in the event of an issue, there is always one link available. Additionally, a Process change has been made to ensure that going forward, this type of work goes through the DSP Change Management Process and receives DSP and DCC CAB approval to ensure that everyone is aware of the work and any risks.

Latest: Target Completion Date 28/02/2020

13.1.29 PBI000000118518

December Report (Excluded through PMEL) - Key Incident **INC000000530634**

Service User Planned Works - Alert Build-up

Problem: Multiple Service Users carried out internal planned works which has resulted in excessive messages queuing in the DSP Northbound Message store. All SRV's and alerts were not being accepted by the Service User's whilst they are carrying out their planned works, causing DSP's queue to increase.

The Root Cause is a Data Issue. Service User Planned works resulted in a high amount of data alerts being stored by DSP and to mitigate against the alerts crashing their systems they tool mitigating actions. DSP ran 4 scripts in parallel to discard/remove 8F3E alerts for the Service Users. DSP also temporarily shut down the CSP Central and South connections to stop the number of alerts increasing which allowed DSP to reduce their queues to within acceptable levels. There should not be this level of alerts on the system to store during outages.

Solutions are being devised. Dealing with alert volumes and finding and implementing solutions is ongoing already. Storm Alert Protection filters being available to DSP to use are under consideration.

Latest: Target Completion Date 28/02/2020