

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	OPSG_65_0802_12
Action:	For Decision

OPSG Risk Register – Progress Report

1. Purpose

This paper provides an update on the status of actively managed entries on the Operations Group (OPSG) Risk Register, together with any activities planned to take place during the following month.

The OPSG is requested to note the contents of the paper and next steps in line with the recommendations at the end.

2. New Candidate Risks

This section presents the new Candidate Issues for inclusion on the OPSG Issue log.

Risk Number	Risk Description	Severity Rating
OPSG-016	There is a risk that the full required 2G/3G service will not be provided until the final sunset date at the currently agreed price.	15 (Critical)

At OPSG_64 Risk 016 – 2G/3G Sunsetting, was endorsed by OPSG members for inclusion in the Risk Register and escalation to SEC Panel for its Q4 2021/22 review on OPSG Risks.

Post OPSG_64, the wording in the risk drafting has been amended by SECAS following comments and feedback, including views from DCC. SECAS will present the amendments at OPSG_65 to provide members with the opportunity to discuss the changes and express any final views.

3. Actively Managed Risks

This section presents the Risks which are being actively monitored by OPSG.

Risk Number	Risk Description	Severity Rating
OPSG-006	There is a risk that the CSP N will fail to meet SEC requirements, creating barriers for Service Users when operating at a large scale.	20 (Critical)

Impact

The impact of this risk is the capacity for Suppliers to operate Devices could be impaired. OPSG have limited confidence that services in the CSP N region will be delivered in accordance with the SEC requirements. Concerns have been raised around the design assumptions and how the service actually operates against User expectations and behaviour.

It may not be possible for Users to deploy Emergency Releases at scale in CSPN due to constraints on firmware image processing time which could cause reputational damage to the programme and the SEC.

It may not be possible for Users to execute their Smart business processes in accordance with their reasonable expectations (e.g. prepay top ups).

Mitigation Actions

- Increased monitoring of service performance to detect early signs of any shortfalls, particularly as usage increases. This could be achieved using the Business Process Indicators implemented through MP122A - Ongoing.
- DCC/Arqiva to present a clear Optimisation and Scaling Plan that shows how the service will evolve to meet the needs of users throughout the rollout – Ongoing.
- Dependant on results of the independent review, implementation of remediations identified in the review – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-008	There is a risk that Users and the DCC will be unable to deploy firmware upgrades in a timely manner if the service in CSP N does not consistently achieve the target service level performance (99%) for PM2 'Firmware Payload delivery'.	15 (High)

Impact

Regulatory non-compliance by the DCC and User impacts to deploying Firmware at scale. Suppliers and DCC will be unable to deploy firmware upgrades in a timely manner and will increase the number of retries generating additional cost and effort. It may not be possible for Suppliers to deploy Emergency Releases at scale in CSPN due to constraints on firmware image processing time which could cause reputational damage to the programme and the SEC.

Users are unable to successfully roll out firmware to their portfolio increasing the likelihood of operational issues being left unresolved.

Mitigation Actions

- OPSG to monitor CSP N plans towards 92% SLA with a follow up plan to be required for 99% SLA – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-002	There is a risk that unstable connections between Comms Hubs and HAN devices impedes the Service User's ability to send Commands to the devices and the device's ability to send Responses & Alerts to the Service Users, in a large number of premises as the rollout progresses.	15 (High)

Impact

Communication between Service Users and Devices will be affected, leading to a variety of operational and consumer facing problems (e.g., not being able to set, tariffs, update FW, receive security alerts etc.) and damaging the programme reputation.

Mitigation Actions

- DCC to identify the triggers and their causes via the HANSIT report and present those findings at TSIRS moving forward – Ongoing.
- SECAS to follow TSIRS and actively report developments to OPSG – Ongoing.
- OPSG to sponsor a workstream looking at providing recommendations on measures of Interoperability at a DMC and Device level – Complete.
- SECAS to confirm with the SMDA Scheme Operator what proportion of deployed DMCs have been assured by SMDA and therefore, gain a better approximation of the scale of untested DMCs – Complete.
- SECAS to carry out actions taken from the Interoperability Workshop – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-015	There is a Risk that the DCC's Comms Hubs Supply chain will not be able to deliver to Service User's requirements due to a global component shortage and increasing costs of the components.	15 (High)

Impact

DCC will be unable to meet the User expectations on Comms Hubs deliveries which could have a knock-on impact to meeting roll-out targets.

DCC noted at the June Supply Chain Capacity Working Group that Arqiva will also be impacted by the global component shortage for August 2021 deliveries. The DCC noted a wider risk for next year regarding the increase in component costs and reduced availability.

Mitigation Actions

- Monitor risk via CH Supply Chain Working Group and report updates to OPSG – Ongoing.
- DCC to explore options for better management of supply chain and forecasting with Users – Ongoing (DCC to provide an update to OPSG on progress on remediation and mitigation plans at the August OPSG Main meeting) – Complete.

- DCC to provide an update at the Supply Chain Working Group and OPSG regarding the CH supply chain risk – Complete.
- The DCC to report on the revised plan for TCHODR from the outputs of the consultation – Complete.
- DCC to engage with CSPs and SEC parties to implement new TCHODR – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-001	There is a risk that an increasing number of Device Model Combinations will adversely affect HAN quality or availability leading to issues concerning the interchangeability of Devices, information transfer between Devices and incorrect Data being exchanged.	12 (Moderate)

Impact

Potential for a repeated consumer queries to Supplier regarding lack of consumption information on the Display.

Loss of consumer confidence in the smart metering solution and general consumer confusion. Potential regulatory implications to the Supplier (under SLC49) if not corrected for.

Mitigation Actions

- DCC to identify the triggers and their causes via the HANSIT report and present those findings at TSIRS moving forward – Ongoing.
- OPSG to sponsor a workstream looking at providing recommendations on measures of Interoperability at a DMC and Device level – Complete.
- SECAS to find out from the SMDA Scheme what proportion of deployed DMCs have been assured by SMDA and therefore, gain a better approximation of the scale of untested DMCs – Complete.
- SECAS to follow TSIRS and actively report developments to OPSG – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-004	There is a risk that the proportion of meters that cannot be contacted by the DNOs significantly increases as the rollout progresses (as DNO certificates on the Meters are either incorrect or missing). This Risk potentially concerns DNO systems which may need to be changed.	12 (Moderate)

Impact

Two-way communication between DNOs and the Meters, both Commands as well as Alerts/Responses, is impeded. Suppliers could be breaching their obligations by not placing the certificates or by placing the wrong certificate (excepting for IDNOs).

Mitigation Actions

- DCC to include in its internal Transformation plan efforts to better relationships, communications, and reporting with the DNOs – Complete.
- SECAS to analyse the reporting and data produced by the DCC – Complete.
- DCC to hold a workshop with DNOs and Supplier parties on this issue and follow up with them on why the clean-up of certs (the fixable portion) is not progressing – Ongoing.
- SECAS to present latest figures and progress on engagement with Suppliers with OPSG and continue engagement with the DCC and DNOs to ensure alignment on issues and discussions – Ongoing.
- SECAS to monitor OPSG Issue 004 'Incorrect or Missing Distribution Network Operator Certificates on Meters – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-005	There is a risk that the DCC's delivery capabilities for the POA and PRA Alerts, which inform the DNOs regarding the supply state of the premise, are insufficient to be of greatest value to DNOs. In addition to delivery capabilities, failures can also occur because of manufacturer device problems.	12 (Moderate)

Impact

Lack of regulatory compliance by the DCC. The DNOs do not know supply state of a premise, and this may become a risk as the penetration of smart meters and newer innovations such as Electric Vehicles and Load Control increases.

Mitigation Actions

- SECAS to monitor the progress of [MP096 - 'DNO Power Outage Alerts'](#) – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-009	There is a risk that the CSPs will not meet SEC required (non-PM-2) performance levels and capacity demands at peak rollout/end of rollout. A "sub-risk" exists for a similar concern at the end of the CSP contract	12 (Moderate)

Impact

Service Users do not get the service expected causing additional time and effort with material impacts to the end energy consumer (specifically Prepayment).

Mitigation Actions

- TABASC to monitor the arrival dates for C&S Next Gen Hubs, their relevant communication technology, and timeline of introduction – Ongoing.

- TABASC to undertake a review of the CSP N architecture to assess its scalability – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-003	There is a risk that the number of CH Exceptions significantly exceeds reasonable tolerance as the rollout progresses, causing reputational and regulatory damage.	9 (Moderate)

Impact

Service Users are non-compliant with mandated I/C obligations. Additionally, depending on the type of exception, the CH may not be contactable and be left in an 'unknown' state. Inaccuracies of databases/data in the SMI.

Faults logged to the DCC would fall outside contracted SLAs; CSPs can claim no performance against these hubs. Reputational damage to Suppliers and the programme in case of site visits, CH replacement processes, and incomplete coverage.

Mitigation Actions

- Re-establish PMEL governance as a vehicle for managing this Risk and establishing defined and specific Exception categories– Ongoing.
- DCC to monitor the rates of Exceptions and report at OPSG – Ongoing.
- SECAS/DCC to advise on a theoretical threshold value for each Exception to OPSG to assess the Severity of each type of CH Exception – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-011	There is a risk that critical operational modifications (e.g. MP15, 24, 122, 117) that deliver industry desired processes and improvements or those facilitating innovation are unable to progress due to a lack of clarity around DCC costs, length and time of progression, and the inability from industry to scrutinize.	9 (Moderate)

Impact

Key changes are unable to be introduced due to the sheer scale and variation of costs for the Service Providers.

Mitigation Actions

- Tracked under the SEC Panel Risk Register as Risk 1: "The progression of Modification Proposals is not meeting required timescales due to the delayed completion of activities (e.g. submission of Impact Assessments and any requested information within reasonable timescales from the DCC)" – Ongoing.

- Tracked under TABASC Risk Register as TABASC011.3: "Cost or complexity of upgrading may deter any individual from triggering upgrade, leading to piecemeal enhancement of existing technologies" – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-012	There is a risk that the ancillary DCC services will be inadequate to meet demands related to general service management (e.g. service desk, DCC support services etc.) as the rollout progresses	9 (Moderate)

Impact

Lack of capacity to serve Service Users. Potential for the programme to suffer reputational damage.

Mitigation Actions

- No mitigation actions confirmed yet. Possible candidate for closure subject to OPSG agreement.

Risk Number	Risk Description	Severity Rating
OPSG-010	There is a risk that the SMETS1 DCO will not be able to maintain a consistent and stable service across the different cohorts of Devices, potentially impacting end User systems (e.g. needing to create individual instances in back-end)	8 (Moderate)

Impact

Non-compliance to the SEC required standards. This can lead to Service User and end Energy Consumer impacts (specifically Prepayment).

This can also lead to the prevention or delay in SMETS1 migrations, impacting Service Users processes and ability to maintain the planned schedule of Dormant and Active migrations to meet Suppliers and Industry obligations.

Mitigation Actions

- DCO Stability plan to be presented at and reviewed by OPSG to monitor status of the service and remediations – Complete.
- SECAS and DCC to begin working on the requirements for a SEC Modification and for DCC to start consideration of the change request – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-014	Because it is unlikely that iDNOs will become DCC Users and because these parties will not have SMKI certificates, there is risk	8 (Moderate)

	that certain post-commissioning obligations on Suppliers cannot be fulfilled	
--	--	--

Impact

These meters will be unable to communicate or be communicated to via the smart metering infrastructure by the iDNOs (who are not DCC Users and don't have relevant credentials in the Device).

Mitigation Actions

- Monitor Industry developments on regulatory position on iDNOs becoming DCC Users – Ongoing.
- Exploring SEC Modifications if iDNOs are not required to become DCC Users – Ongoing.

Risk Number	Risk Description	Severity Rating
OPSG-007	There is a risk that the DCC will be unable to execute or maintain scheduled BCDR and necessary arrangements (e.g., site visits, on-site testing) exercises due to government regulations on Pandemic	5 (Low)

Impact

Non-compliance to SEC requirements and untested Disaster Recovery processes. Communications across the WAN network may be severely impeded.

Mitigation Actions

- DCC to present pandemic risks updates and their expected impacts to services at OPSG sessions moving forward – Complete.
- No additional mitigation actions confirmed yet. Possible candidate for closure subject to OPSG agreement.

4. Recommendation & Next Steps

The OPSG is requested to:

- **NOTE** the contents of this paper;
- **REVIEW** the description, impact, and next steps on the new Candidate Risk;
- **ENDORSE** the inclusion of the new Candidate Risk;
- **PROVIDE** any new candidate Risks for consideration; and
- **PROVIDE** any comments on the wording, impact, and severity of any OPSG Risk.

Eugene Asante

SECAS Team

1 February 2022