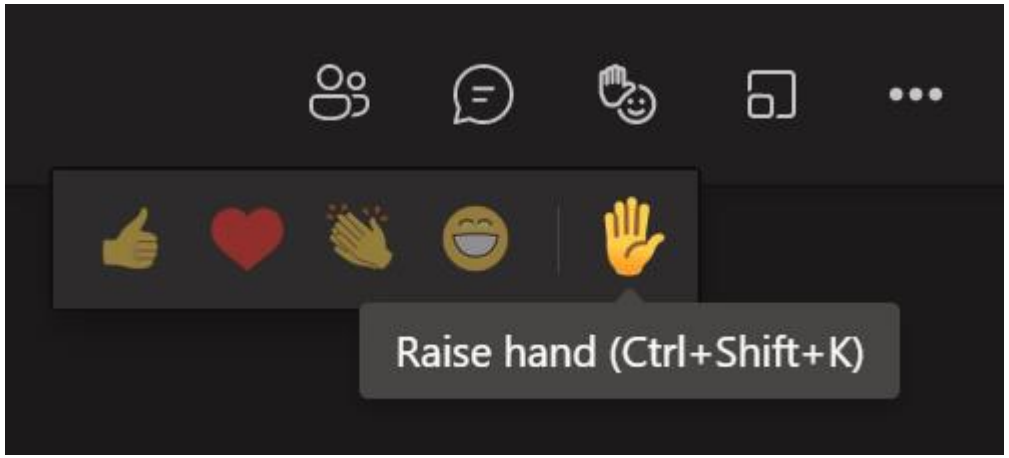
Issue 101 Digital Meeting Etiquette

- Welcome to the Issue 101 Workgroup meeting 15 – we'll start shortly
- No video please to conserve bandwidth
- Please stay on mute unless you need to talk – use the Raise hand feature in the Menu bar in Microsoft Teams if you want to speak, or use the Meeting chat



- Lots of us are working remotely – be mindful of background noise and connection speeds

ELEXON

Issue 101 ‘Ongoing Governance, Funding and Operation of the MHHS Data Integration Platform (DIP) by BSCCo’

Meeting 15

29 February 2024

Meeting Agenda

Objectives for this meeting:

- Discuss feedback from consultation
- Discuss DIP transition plan and implementation

Agenda Item	Lead
1. Welcome and meeting objectives	Lawrence Jones (Chair)
2. Recap of Issue 101	Jenny Sarsfield (Lead Analyst)
3. Summary of Consultation feedback	Jenny Sarsfield
4. Discussion of Consultation feedback and actions	Chris Wood (Market Design, Elexon)
5. Transition Plan and Implementation	Chris Wood
6. Next steps	Jenny Sarsfield
7. Meeting Close	James Stokes

RECAP OF ISSUE 101

ELEXON

Issue 101

- Issue 101 was raised in July 2022

- We held eight Workgroup meetings in the initial Assessment Phase

- We issued a one month consultation on the proposed framework and business requirements in June 2023
  - Included 56 pages of business requirements
  - Twelve responses were received, with the majority agreeing with the proposed framework on each topic

- Five Workgroup meetings were held in the Rules Drafting phase

- We issued a one month consultation on the proposed arrangements and legal text in January 2024
  - 1 BSC Supplement with seven chapters created
  - 6 DIP Subsidiary Documents (DSDs) and 5 annexes created
  - 4 BSC Sections amended
  - A total of 64,936 added words and 239 new pages of rules

- The Issue Report will be presented to the BSC Panel for comment at the March Panel meeting

CONSULTATION FEEDBACK SUMMARY

ELEXON

Consultation Feedback Summary

- Eight responses were received
- Respondents included five distributors, three supplier agents, one supplier, one code manager

Do you agree with the proposed…	Yes	No	Neutral/ No Comment
general DIP arrangements?	**8**	0	1
DIP governance arrangements?	**8**	1	0
DIP connection arrangements?	**7**	1	1
DIP assurance arrangements?	**7**	1	1
DIP change management arrangements?	**6**	2	1
DIP funding and budget arrangements?	**6**	2	1
DIP information security and data management arrangements?	**7**	0	2

Consultation Feedback Summary

Do you agree with the drafting delivers the intention of the proposed…	Legal text			Subsidiary document		
	Yes	No	Neutral/ No Comment	Yes	No	Neutral/ No Comment
general DIP arrangements?	**8**	0	1	-	-	-
DIP governance arrangements?	**8**	0	1	**7**	1	1
DIP connection arrangements?	**6**	2	1	**5**	3	1
DIP assurance arrangements?	**7**	1	1	**6**	2	1
DIP change management arrangements?	**6**	2	1	**6**	2	1
DIP funding and budget arrangements?	**7**	1	1	**6**	2	1
DIP information security and data management arrangements?	**7**	0	2	**6**	1	2

CONSULTATION FEEDBACK

ELEXON

Governance

You Said…	… We did
We agree with the approach taken by Elexon to develop the DIP Rules through a BSC Supplement with standalone DIP Subsidiary Documents to allow future portability	Thank you
We support the DIP Objectives, and in particular the recent changes to extend the scope outside of settlement processes.	Thank you
We support the principles reflected in the legal text.	Thank you
No Clear definition of the service being offered, and a Service Definition (SD) document should be considered. The SD should specify how the DIP will manage message exchange and any associated non functional requirements to enable the DIP Service Provider to be held to account for delivery of the service.	SDs in the BSC are used to hold BSC Agents to account, but that concept doesn't exist with the DIP – there is no equivalency of a BSC Agent (Avanade is a contractor, not an agent and the relationship is commercial, not enshrined by legal obligation). The DIP Manager will under take roles, and have responsibilities there-in, that would traditionally have been held by a BSC Agent – if there are failings, it is the DIP Manager that will be held to account. That being said, where a traditional SD would lay out service provider responsibilities, these sit with the DIP Manager and are set out in the DSDs, and in particular the Annexes to DSD002 We will also add something to start of DSD002 for clarity of what the DIP is and that it is to support multiple Industry Codes and their processes
The SD should also clarify the distinction between DIP Users who need to communicate directly with the DIP and 'DIP Portal Users' who are only seeking to access reports etc.	DSD002 paragraph 2.5 lays out the different levels of User – 'Analytics Reader' will be 'Persons that only have access to review the DIP dashboard feature' and DSD002 A2 Chapter 3 explains how to access the DIP Portal (log-in, MFA) as well as how DIP Users will access the DIP includes detail on message validation, location of the swagger hub, configurable parameters for Message ingress and egress

Governance

You Said…	… We did
There are missing requirements relating to DIP User interactions with the DIP. The MHHS Design includes a large number of requirements. Functional requirements have been reflected within amended provisions in industry codes, whereas the expectation is that non functional requirements and specific rules for interaction with the DIP (as set out in the E2E Solution Architecture Document would be reflected in the DIP Rules.	We are aware that we still need to add some of the detail of the design in DSDs, we intend to have this completed over the spring. We will work with the MHHS Programme to ensure everything is captured
Soften change to DIP Manager & DCAB Terms of Reference so Ofgem isn't approving typo corrections	Housekeeping changes are now an exception to the rule
Suggest caveat so that nominating odd and even years for DCAB don't include initial set-up	This is covered in DSD001 A1 – the transition plan (see later), DSD001 is intended for enduring, and it will actually be easier to remove the whole of DSD001 A1 than some brackets in DSD001 – and we can sunset DSD001 A1
Inconsistency between DIP Chair being able to expel unruly members (DIP Supplement) and needing 2/3 majority approval (DSD001	Nuance of legal text – but admit it is not entirely clear, so will re-word
Add appeal rejection for frivolous, vexatious etc. that is in DIP Supplement to DSD	Done
Access Agreement suggests only DIP Users can raise DIP CRs	Anyone can raise a DIP CR, we have included change as an example of what is included in membership as it is something normally associated with being a full user
Constituency representation is appreciated, and the thought for industry consultation is also.	Noted
Where appointing the 2 x Data Services reps, should it be considered that the appointments ensure all 3 segments are covered – ADS/SDS/UMSDS? Should there also be a similar consideration for Supplier and Metering Service reps?	Yes, and we will take this for action
Where referencing the Unmetered Supplies Data Service in the documentation we suggest the correct Role Code is used when abbreviating it – which is UMSDS – and not UDS as used in places throughout the documents.	We will check and amend any typos

Governance

You Said…	… We did
What the applicable “authorities’ own procedures” are to be regarding appeal resolution. This is mainly on the basis that the DIP is not a standalone code, but one pinned to the BSC, so it is not clear if such appeals are to follow the standard code modification appeal process as set out in the electricity act or something else.	We expect that Ofgem will deal with appeals against a DCAB decision in a similar way that hey deal with an appeal against a Code Panel’s decision, including timelines and publishing of documents etc. https://www.ofgem.gov.uk/publications/ofgem-guidance-self-governance-modification-appeals-process
Upon reviewing all relevant documents to this consultation, we feel that a separate definitions & interruptions DSD should be developed so that users have an easily accessible document to understand what each acronym & term means, in the main we have managed to find reference to these in each DSD however it would be much easier for a reader if this was carved our in a similar fashion to BSC Section X to reference these.	We are open to this suggestion and welcome views from others
The time between completing a DIP CR Final Assessment and the report being made should be at least 10WD unless urgency dictates otherwise	We will incorporate this as it will allow more time for stakeholders to submit their views if they are concerned with our assessments
Similarly, consultation time periods should be at least 15WD unless urgency dictates otherwise (as laid out in the Initial Assessment in the case of a DIP CR)	We will amend the DIP Rules to this effect to allow longer times to consider implications, particularly as some consultations may be quite technical in nature and require time to discuss implications with multiple internal stakeholders

Connections

You Said…	… We did
‘Metering Services’ isn’t consistent with BSC terminology	We have reflected the terms used in MHHS design, and the DIP Roles – but are happy to add translations if required
Confusion over whether Suppliers, DNOs and Meter Operators have to be a DIP User prior to Code Qualification	We will amend the text in the DIP Supplement so that its clear that they won’t move to Production until after qualification i.e. DIP onboarding will complete, then Qualification, then move to Production
We won’t need to revoke DIP access in the event of a SOLR as the Supply license is revoked	A DIP User may have multiple DIP Roles including Supplier, the other DIP Roles will remain extant. While the license may be revoked, the Digital Certificates will still exist, so they will need revoking
Require clarification on the reference to BSC provisions that relate to the DIP being subject to the BSC Modification process	These are the text in Section C, D, F and H we shared as part of the consultation
Will the SwaggerHub be a permeant fixture and updated by the DIP Manager?	We will move the swagger to another location ready for creation of the production environment
DIP Read-Only isn’t defined, nor is there detail on this	This will not be a type of DIP User – there is no requirement for them in MHHS design and is something that was considered (hence included in the draft text) but, our thinking has evolved so that there will be other means of organisations accessing DIP messages for research purposes etc. – more details to follow from Elexon later
Use of ’re-direction’ in the event of SOLR as The DIP provisions define the message recipients and should be routed to the correct Supplier based on registration data received from the CSS (via the SMRS).	Messages will be ‘re-routed’ at 2400 (cross-over time) so long as ISD is updated, specifically Effective to/from dates in ISD #45 and #M16 (see next slide) – we have change ‘redirected’ to re-routed Messages are routed as follows: Primary – sent to a named recipient based on MPID; Secondary – the Supplier associated with a MPAN, based on the MPAN; and Always – the organisations listed as ‘always’ in the always routing rules for the particular Interface

Connections

You Said…	… We did
Onboarding process only refers to BSC and REC for single Code process, not SEC to reflect MDR	We've added SEC to recognise MDR Opt-in following CR023 – we're engaging with SECAS to make sure they're aware of this
Checking whether a DIP Applicant already has a license is not needed as the license will come later	This is for those people that already have a market presence and are applying for DIP access as they expand their business e.g. if a Generator diversifies and wants to become a Distributor too. Or, a gas only Supplier that now wants to do electricity too.
Sharing application information collected by Code Bodies will require provision within the Codes and to agree what is required and how it can be shared securely	We expect Code Bodies to make the required provisions to their Codes - we discussed this last year and it has been in the DSD002 draft since first sharing. The Mechanics don't need to be in the DSD and can be arranged later during the implementation phase
Code Bodies should be able to see what information the DIP manager collects in On-boarding to assist with their Qualification	Have added a sentence to DSD002 paragraph 2.12.5 to accommodate this
Question on whether certain messages need to be sent during DIP On-boarding, In particular they would not expect to see parties required to send messages outside their scope or in an incorrect format in order to test their exception processes.	The DIP Role assignment restricts what messages can and can't be sent and/or received, hence the need to send all messages only applicable to their DIP Role. We're open to discussion about incorrect message formats as this is to assist Code Bodies with Code Qualification
When off-boarding a DIP user, the DIP Manager should consider informing other DIP Users so they can assess any impacts and take mitigating actions.	Agreed – have amended DSD002 Chapter 4 to include this
DSD002 paragraph 4.1.1 should consider the scenario of market exit but where the DIP user doesn't voluntarily off-board. In 4.1.1 (b), in addition to breach of the Industry Code, there should be a provision for Off-boarding following instructions from relevant Codes (especially for roles that don't need a licence - MEMs, etc).	Paragraph 4.1.1 is an overview and uses the term 'include' this implies there are other circumstances. DSD002 paragraph 4.3 goes into more detail such as: data breach; sending invalid data that is having a material impact on settlement operations; compromise of a Private Key; and using the DIP contrary to the Fair Use Requirement

Connections

You Said…	… We did
The Supplier of Last Resort (SoLR) and Trade Sale provisions are very specific to Suppliers and we should consider including trade/portfolio sales of other market roles	SOLR and Trade Sale are, by very definition about Suppliers (Trade Sale is defined in Suppliers Standard License Conditions (SLCs) for both Electricity and Gas Suppliers) However, where we point to the Change of Supplier process for a Trade Sale, we can consider something similar for non-Suppliers; similarly we are happy to consider amending the DIP definition of Trade Sale to point at the SLCs
The description of the SoLR within DSD002 is not clear. References to DIP User in 5.2.2. and 5.2.3 do not clarify if its the Failing Supplier or the Replacement Supplier. Also 5.2.4 should reference the transfer of the MPID and DIP ID from the Failing Supplier to the Replacement Supplier which is what ensures messages are routed to the correct endpoint.	Context makes it clear, but we have added ‘Failing Supplier’ in brackets after ‘DIP User’ to make it absolutely explicit. The DSD002 draft we shared with the consultation already uses ‘Failing Supplier’ and ‘Off-taking Supplier’ where we use those terms in the same paragraph, instead of referring to the respective DIP Users Only the MPID will transfer, not the DIP ID – the DIP ID will remain forever with the Failing Supplier
The transfer of MPIDs will need to occur at midnight when the failing supplier licence is revoked to ensure messages are routed correctly.	Yes this will occur as described in DSD002
DSD002 Paragraph 5.4 implies that the Failed Supplier could retain access to the DIP. This should not occur as the Failed Supplier will have had its Supply Licence revoked and the relevant certificates should be revoked.	It allows that DIP User to retain access in a DIP Role other than ‘Supplier’ e.g. they could still be a Meter agent
Where the list in DSD002 A1 paragraph 1.1.1 has originated from as this has extended beyond the information listed in the original DIP CoCo (which has now been removed from the CoCo). Has this been agreed via the MHHS Security Advisory Group?	These are the requirements that we, as DIP manager, will require and are based on E2E, design and CoCo requirements etc. They haven’t been agreed with the SAG as they are something determined by the DIP Manager for the DIP and as far as we’re concerned, don’t need SAG approval, much like the rest of DSD002 doesn’t need SAG approval. Further, these are connection requirements, not security requirements

Connections

You Said…	… We did
As flagged in previous confirmation, we would like clarity on the requirement for information about logical network schematics of the information systems and services in scope that interact with the DIP. Connection to the DIP is not a physical connection and therefore it is not clear why the DIP Manager would require a logical network schematic. The MHHSP has previously confirmed this is not required	This isn't about physical connections, its about the software systems that interact with the DIP to show how they interact with the DIP. This is still a requirement of the latest Interface Code of Connection (MHHS-DEL1197), but we will remove from DSDs as the Programme documents are updated. In fact, following previous feedback we have removed references to physical controls.
We concur with the logic that each DIP Applicant should send at least one type of each Interface for the role that they are taking – but also propose they should send one of each that is incorrect too to demonstrate they can manage receipt of error messages from the DIP. This concept of error messages, whilst likely to occur in SIT, isn't covered through this testing, so scope of doing this would need to be considering when QT is being defined to ensure this is met.	The second half of 2.11.4 says: "In addition, to sending one of each message format, the DIP Applicant shall send one of each message format that is incorrect to demonstrate that they can manage receipt of error messages from the DIP." Also, this will be covered off further by Code Body Qualification processes – we are e working with Code Bodies to agree how this will work operationally

Connections

You Said…	… We did
Under clause 2.8 there does not appear to be any general company checks for DIP accession, this maybe pertinent if there are costs to be recovered/paid for via a non-code party requiring DIP on boarding. We note that DSD002 paragraph 2.8.2 is open ended enough to enable the DIP Manager to do any other Ad-hoc checks such as the above and so is potentially captured under that, however if DIP On-boarding is done via Code accession (REC/BSC), company checks and company director level sign-off etc. are required, so it should be pertinent to ensure this is an explicit requirement for DIP On-boarding for the same reasons.	As noted, 2.8.2 allows us to essentially do as many checks as we feel necessary until we are satisfied that the DIP applicant is a realistic DIP User. It should be noted that DIP Users that are not party to a Code will be exceptional. We reserve the right to collect the full cost before we allow DIP On-boarding to commence where we may be concerned about a company. A Director will already have agreed with the requirements of the BSC either as a Party, or via the Access Agreement (we will make this explicit), which includes compliance with the DIP Rules, so we have Director level 'ownership' indirectly and we didn't feel that there was value in asking an already busy person to undertake lower-level tasks such as Certificate Admin
Does this document need to consider including requirements regarding the revoking of access to individual users within an organisation, around the scenarios where breaches/data security are considered – and how that impacts that organisation as a whole in terms of having users within each of the required Roles. This would clearly be different to when someone leaves their organisation, where another user would need to revoke access for that person(s).	We are looking at how to achieve this and will likely put in a requirement that DIP Users report what internal actions they have taken to prevent recurrence. Based on that, we may then decide to revoke individual access
DSD002 paragraph 2.10 seems to be a potential issue, as it is not clear if this is constrained at organisational level (umbrella) based on the company registration number or if it is possible for a parent company to allow 2 of its umbrella companies separate DIP connectivity. This is pertinent because our group consists of several umbrella companies, for which at least 2 of its umbrella companies are intending on holding separate DIP connections that are agnostic of one another, this clause seems to conflict with this intention.	Set-up at the highest level is base don domain name e.g. 'elexon.co.uk', which is different to 'emrssettlement.co.uk. In this case, both are part of the Elexon group, but could be spate DIP users. In the example given by the respondent, there companies each have separate domain names, so can be stand-alone DIP Users with multiple DIP IDs for each DIP User

Assurance

You Said…	… We did
Sharing of Message Contents (DSD003 paragraph 3.3) in exceptional circumstances should include provisions for sharing details with Code Managers	This is already permitted under paragraph 3.3 if the Code Body can show there is a legitimate regulatory need
Request that this drafting is clearer and references a notification to the relevant Code Body where there are non compliances identified against a Code Bodies' parties. In addition, there needs to be clarity and agreement on the roles and responsibilities between the DIP Manager and the Code Bodies to ensure vires are clear and do not overlap.	DSD003 paragraph 4.1.2 will allow is to publish a list of non-compliance, that could be the start point for working together to deal with non-compliance. Further, DSD001 para 3.4 requires us to share anything Code Bodies will need to meet their own obligations, and DSD002 allows us to report security breaches to Code Bodies. Notwithstanding, we have added a paragraph to make it explicit that we will report non-compliance to Code Bodies, where it was implied before. We will develop vires with Code Bodies as they develop their enduring PAF arrangements, that being said, the DIP Rules do not afford the DIP Manager punitive/remedial action, stand-fast suspension and removal in exceptional circumstances
DSD003 paragraph 3.2.1 states that the DIP Manager may create and share reports (subject to the requirements of DSD006 'DIP Information Security and Data Management') regarding DIP Users' use of the DIP with organisations such as (but not limited to)… This needs better qualification. It is not just the DIP Users' use of the DIP, the DIP Manager may also need to share reports with Code Bodies to assess compliance with processes facilitated by the DIP. Whilst section 1.1.2 captures this, it should be carried forward in section 3.2.	Code Bodies are specifically named in the list of organisations in paragraph 3.2.1. DSD003 paragraph 3.1 has an initial list of reports we will share. We ae working with Code Bodies to develop a way we can share further performance reports with them and this work is on-going
As a DIP User, we would not be comfortable with an automatic right to publish Confidential information without agreement in advance.	DSD006 paragraph 4.2.3 requires that "consideration shall be given to, and advice/permission sought from, the owner of the data and the owner of the Meta Data (if different)." when considering whether data can be released

Assurance

You Said…	… We did
DSD003 paragraph 2.3.6 requires DIP Users to comply with any findings of Assurance prepared by the DIP Manager. We believe this should include a reference to any such requirements being reasonable and achievable.	if we assume that compliance was achieved at On-boarding, there should be no reason why it can't be re-achieved subsequently. All compliance is reasonable and achievable as they're the rules – if not, now is the chance to tell us what isn't reasonable or practical. If we find something to be unreasonable, or unpractical once we start to run the DIP operationally, we can raise a DIP CR. Further, this paragraphs allows that if believe that adherence is not appropriate (e.g. if we're waiting for a DIP CR to be implemented to remove the need), then we will not direct the DIP User to take action to rectify an assurance finding
We would like to know the assessment procedure in which a Risk is added to the Risk Register – will this be via CIA or another method? Will DIP Users/Non active Market Participants be required to maintain a similar Register? For cohesion the sharing of this document would be a positive engagement.	We will publish guidance this year (and consult on it) regarding how the DIP Risk Register will be compiled and how people can suggest additions. We will publish the DIP Risk Register following update and while we won't normally consult on its contents (we will first time around), we will always welcome feedback form stakeholders. There is no requirement in the DIP Rules for DIP Users to have their own register of DIP related risks - this is a business decision for each DIP User
We do not believe that sharing the Assurance Strategy 1 month ahead (with a 10-day response period) is enough time to assess any feedback, is there scope for publishing this earlier? There is also no mention on the documentation on the next steps where feedback has been received, how/when will this be communicated back to the responder?	Based on feedback form other stakeholders, we are extending minimum consultation periods to 15WD, unless there is reason otherwise One month is worst case scenario – the strategy is implicitly linked to the budget proposal cycle (i.e. will we have enough money to implement the strategy?), which is why there is the NLT one month requirement but, we will try and publish sooner
We suggest the addition of the following into the list of considerations for the DIP Manager when determining the DIP Assurance Strategy: Reported security breaches; and DIP Service Provider service incidents	We will ad this

Assurance

You Said…	… We did
We suggest a minimum period of notice of an intention to undertake an audit should be specified, e.g. 1 month?	We have no objection to this, so have amended the DIP Rules accordingly
It is unclear from the wording used in this list in DSD003 paragraph 2.6.3 whether the results of the audits of each of the DIP Manager and DIP Service Provider would be reported to the DCAB. If this was not the intention, we recommend it should be and that the wording is amended to more clearly reflect this.	We intended for it to be implied from each section, but have clarified it in 2.6 to help alleviate any further potential ambiguity
Additionally we recommend that the learnings from any Security Breach or Dip Provider Service Incidents should be reported.	We will report this to DCAB (being mindful of confidentiality etc.)
We recommend that the annual compliance report should also include: Details of any service incidents affecting the availability or integrity of the DIP; and If not already intended in 'details of audits undertaken and themes in findings' we recommend this also includes the details of any audits of the DIP Manager and or DIP Service Provider.	We have added these to the list and while It was intended for DIP Manager and DIP Service Provider to be included, but have added some text in brackets for clarification
DIP Supplement paragraph 4.2.1 (b) refers to DIP Users and DIP Service Provider in regards to the Assurance Strategy but not DIP Manager	We will amend to reflect this
We agree with the proposed assurance arrangements and support the initial similarity of the arrangements that exist in the BSC PAF as a good starting point to move forward and refine based on learnings and annual review approaches as set out.	This is pleasing feedback
We agree the approach set out provides levels of independent assurance (independent auditor & DCAB input) that need to be in place to ensure a fair & consistent approach to the DIP managers overall function,	Also very pleasing feedback

Change

You Said…	… We did
There should be requirements on the DIP Manager to maintain environments, test harnesses and test data to support change delivery and also Qualification activities.	The non-production environment will remain in existence at all times and can be used for testing and some Changes. Additionally, it will take Avanade an afternoon to build a test environment, so will be included in any IA they submit
We do not agree that it is the Code Bodies responsibility to raise a CR instructing the DIP Service Provider to make a change. Where an industry change is being progressed that impacts the DIP rules, then we would expect the DIP Manager to raise a DIP CR as agreed with the CCAG.	We assume this meant CCSG, not CCAG. We will follow CCSG direction, and liaise with relevant Code Bodies as required. We will amend the text to reflect this
Timing of DIP CRs to be raised whereby a code change impacts – we feel that best endeavours should be made by code bodies to raise CRs at the earliest possible juncture, and that should be a specified obligation on code bodies. Whilst this appears to be the intent it is currently not specified but should be based on recent learnings in the DTN space via DCP 383/DCP 394 meant that DTN dataflows where identified too late to implement the required Dataflows for its original intended delivery, consequently the DTN dataflows resulted in a phased implementation whereby manual processes had to exist for a 6 month period post implementation of the change to allow parties development time to implement said dataflows in system processes.	We aim to mitigate this through membership of CCSG, and requiring Code Bodies to inform us as soon as changes are raised and the requirement in DIP Rules for us to liaise with Code Bodies and respond to their Impact Assessments and consultations. Further, we have streamlined the process so that a formal DIP CR won't actually be needed in these cases and we will treat it as a system only change as there will be no need to change the DIP Rules.
Where a change to a DIP message is progressed, this is not expected to require a change to the DIP rules. We would expect the DIP Manager to manage the contractual arrangements requiring the DIP Service Provider to make the changes to the DIP.	This is correct, a message change will not require a change to the DIP Rules but, it will require a change to the DIP, and we would therefore normally expect a DIP CR Having considered this, and the need to avoid the DIP Governance preventing an industry change, we will treat this in the same way as a system only change as described in DSD004 paragraph 2.14 – we have also re-ordered the paragraphs in this area for readability

Change

You Said…	… We did
DSD004 paragraph 2.4 infers that only the DIP Manager is involved in the decision of whether to rasie a DIP CR, which does not provide for any independence or transparency which could therefore undermine the ethos of anyone being able to raise a change. We would object to such a process however note that there is reference in a later section, 2.5.2, of the publication of an assessment but are unclear as to whether this publication is intended to cover the decision step in 2.4.	It is intended that 2.5 follows 2.4, and 2.4 shall only be a sense check and that the initial assessment will be published regardless of the outcome of the validation – we will make this clear We've also added a new paragraph to 2.2 (2.2.4) to make it clear that an appeal can be raised at any point where a decision is made in the change process
Any Housekeeping changes, where not going for approval or consultation; we believe these should be red-lined so that participants can easily review these ahead of being put live, along with providing the opportunity for the participant to feedback that they don't believe the change is just a housekeeping piece before it is put live.	Agreed, and we will amend the DIP Rules to this effect
DSD004 paragraph 4.2.12 relates to message formats and provides information regarding engagement with the CCSG. We believe the information regarding CCSG should be included in a more generic section as it is not just relevant to change impacting message formats.	We have no argument against this and have given CCSG its own heading and added an explicit obligation to comply with CCSG requirements
RECCo believe it would be clearer to refer to Message Definitions rather than Message and Data Item Formats as changes will apply to more than just the message formats.	We have no objection to this and will defer to RECCo in their capacity as overseer of RTS but, need to check consistency across all Codes
We would like to seek clarification as to whether the DIP Manager is to be directly associated to the CACoP or if its indirectly by virtue of its association of the BSC,	The DIP is not a Code and CACoP isn't a decision making body but more concerned with best practice (and was only ever intended as a stop-gap until CCSG was created) as such we aren't intending to be a CACoP member, but will liaise with them via BSCCo if required.
Clarity on the formation of Workgroups under the DIP – is this to be limited to just DCAB, open to wider industry/non-industry members or limited to associated Code modification workgroup members etc.?	DSD004 paragraph 2.6.1 states "The DIP Manager may invite DIP Participants and other interested stakeholders to form a Workgroup" – essentially anyone with a vested interest can join a Workgroup, much like the BSC

Change

You Said…	… We did
Clarity as to why DIP CRs are not be made publicly available/limited to listed DIP Manager organisational contacts – this may cause challenges with change management processes in each organisation, as DIP On-Boarding/administration contacts may not be responsible for managing industry change, even if impacted by DIP CRs.	We will publish on the web, and we have added this to DSD004 to make it clear
We feel that DIP Supplement 5.1.2 (b) should extended to state that any modification procedures in any related Industry Codes shall not be applicable, as opposed just BSC change procedures. We understand the need to call out BSC specifically given DIPs relationship with the BSC but feel that this should be made clear as this is an avoidance of doubt clause it needs to set out DIP change management is separate to any of the codes.	We understand the reason for this suggestion and will raise it with other Codes, as it will be for them to make changes to their own Codes.
The thresholds for Materiality cost should be included in DSDs to determine whether a Change is Tier One or Tier Two	We are working on this, and welcome feed back - our initial suggestion is where the cost to change is £250,000 for the DIP Manager and/or £100,000 for DIP Users based on Impact Assessment/consultation feedback

Funding

You Said…	… We did
As pointed out, the DIP Payees as they are reflected in the proposed arrangements would prevent needless alternative industry pass through costs	This is pleasing feedback
In general, we agree with the arrangements but we feel that more clarity is required. For example: How the “majority” of DIP Participants defined – is it by number of organisations, number of MPANs represented, is by constituency group (ie DNOs/IDNOs – Suppliers – agents etc)? Is any consideration given to a scenario where some constituents wanted a change but others didn’t see the benefit? Presumably all constituents would gain benefit but not all constituents would contribute?	These are valid points and we are considering how to respond and would welcome input form Issue Group members
It is unclear where the rationale for in year budget change threshold levels have come from, i.e. less than 10% is informed via invoicing process & 15%+ shall be consulted on.	These are figures that we thought were right but, we’re open to suggestions o what they should be
We are resigned (but not supportive) to supplier being DIP payees as per Ofgem’s original intent & proposed funding arrangements. The carve outs requiring DIP Non-Core Service Cost (NCSC) recovery from DIP Payees should be reconsidered as we feel that some of these elements should not be at the discretion of the DIP Manager but mandated for costs to be recovered from the DIP participant	Whether NCSCs are passed on is at the DIP Manager’s discretion but, the examples included for when to charge NCSC leave little room to waiver NCSCs, further more, DSD005 paragraph 3.6.6 requires us to publish whether NCSCs will be charged in any information published e.g. DIP CR Initial Assessments, and DIP Users will be able to share their views on whether our determination is correct.

Information Security

You Said…	… We did
The document makes many references to the ISO 27000 series. The ISO 27000 is also extremely onerous and inappropriate for many entrants. This is appropriate only for the largest entities and will form a barrier to entry. If they want a standard to apply the only appropriate one is the Cyber Essentials Plus, which was created by BEIS for this purpose and is now operated by NCSC. Any non-industry standard will need to be topped up with DIP-specific controls.	We don't need DIP Users to have ISO2700 Certification, but we do expect them to meet the requirements of ISO27000: 2.1.1 - '…adhere to the requirements of the ISO/IEC 27000 series standards to the extent that the standards are applicable to their organisation.' 2.1.2 - 'For clarity, if parts of the ISO/IEC 27000 series are not applicable to a DIP Participant then they are not required to meet those standards. But where something within a standard is applicable, they are expected to meet that requirement and their ISMS shall be set-up and/or operated in the same way as expected in the ISO/IEC 27000 series.' We will provide guidance (and consult on that guidance) on which sections of ISO 27000 series we expect DIP Users to adhere to, as specified in paragraph 2.1.3
To remove ambiguity, we recommend all Information Security Management System (ISMS) requirements be captured in one document to prevent the need for DIP users to refer to multiple documents to identify requirements and also to prevent requirements from being misaligned.	We have already moved a lot out of DSD006 into DSD002, and will consider the remainder
DSD006 paragraph 2.2.2 requires DIP Users to provide their Cyber Incident response plan to the DIP Manager. Incident processes would generally be internal documents. How will the DIP Manager protect this confidential information?	In the same way we protect all data we hold – limited access, destroy when no longer required, don't share outside of those who need to see etc. We'll also be open to any reasonable requests from the DIP User
The DIP Manager should consider that SEC covers information security assurance and therefore there should be an explicit requirement for the DIP manager to rely SEC information security assurance where it exists and only conduct incremental assessments of specific DIP information security controls as a proportionate measure. SEC will always need to retain the higher standards because of the potential implications that SEC issues could cause on the provision of energy, that do not arise through information security issues related to the DIP.	Will ensure this is built into guidance and our internal processes. Where DSD003 allows us to work with other Code Bodies, we could ask SEC for their findings, rather than do our own – but, we will reserve the right to do our own assurance checks. We are engaging with SECAS regarding DIP interaction

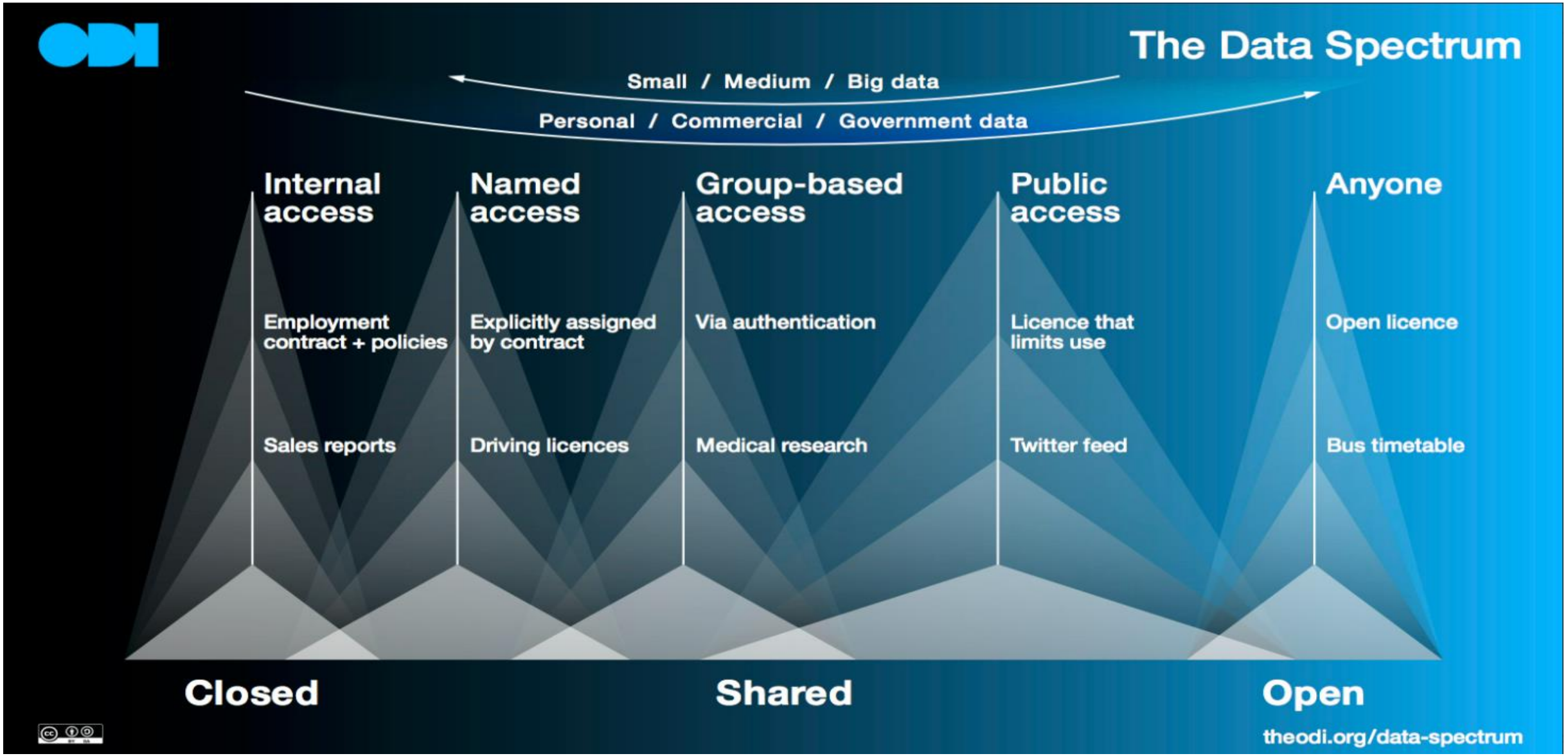
Information Security

You Said…	… We did
Penetration Testing – if using a DCP – is this required of the DIP User? Are we to Pen Test the DIP, or our connection to the adapter?	DIP Users will be expected to conduct Pen testing of their own systems as part of their ISMS
Will there be further qualification for Non Active Participants using DCP or are the expectations the same for all DIP Users?	All of the requirements for On-boarding are laid out in DSD002, there won't be anything extra

Data Management

You Said…	… We did
We understand that the DIP Manager will be identified as a Data Processor rather than the Data Controller. If this is the case, please could you confirm why DIP Users are required to report personal data breaches to the DIP Manager.	Integrity of the DIP, and we will act as a liaison with other DIP Users. Further, from an assurance perspective, if there's a pattern of breaches, we may wish to take assurance/compliance actions, including liaising with Code Bodies and/or the Authority But, recognising there is no legal obligation, have changed 'shall' to 'should'
Reporting on data protection incidents should be qualified so it is relevant to the DIP, not any data protection incident. The current drafting is both onerous and unnecessary.	We thought this was implied, but we've added text to ensure its explicit
DSD006 paragraph 4.2.3 states that data release will seek advice/permission from the owner of the data. However, to provide Code Bodies data for performance monitoring, the DIP manager should not require consent from market participants. Also, the principles of governance to determine appropriate reporting should be defined here in section 4.2 i.e. who holds the final decision on whether a requested report will be shared.	We will be the owner of the data – we will only share performance data e.g. how many messages were sent, whether response X was sent within time from Y, following receipt of message Z etc. DSD006 paragraph 4.4 states the DIP Manager will make the decision however, we have moved for flow of reading
The 'Public' data classification is unclear. Typically, public data would be data in public domain so unlikely to have any restrictions.	This follows ODI data Spectrum and work carried out by the Energy Data Taskforce on behalf of Ofgem and BEIS (as was)

ODI Data Spectrum



Transmission License

Yes	No	n/a
5	1	3

Comments received:

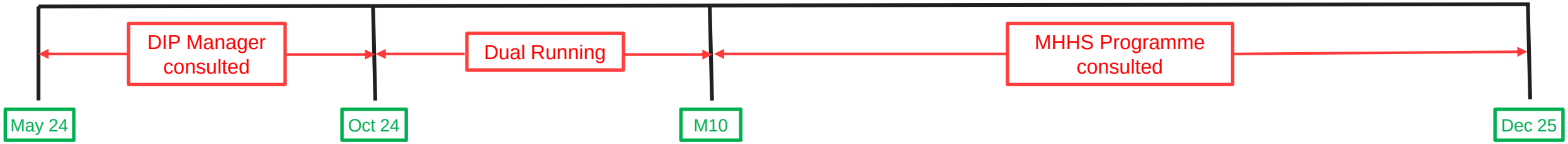
- We believe that there is a requirement for a review of the Transmission area in light of the implementation of the DIP.
- Whilst not relevant to the REC, RECCo believes the change proposed to the Transmission Licence are sensible.
- Our view is and remains that if this should be considered as part of the transition of Elexon's ownership & the FSO licencing requirements/go live currently published pointing towards FSO licence go live over the course of 2024, we acknowledge this is a congested area in terms of overall change in the short term however it is better facilitated in the FSO licence and transition, leaving transmission licence requirements to Transmission Operators and required industry arrangements for the FSO.

THE TRANSITION PLAN

ELEXON

Transition Plan

- Working closely with Programme colleagues for joint plan and we will align with wider MHHS Implementation plan
- At the moment decisions about the DIP design are made solely by the Programme, an DIP Rules reflect Programme's latest position
  - There will be a period form October 2024 where Programme and DIP Manager/DCAB have to agree (we will discuss prima inter pares with Ofgem)
  - Prior to this DIP Manager has to be formally (pro-actively) consulted
  - Following M10, we will formally (pro-actively) consult Programme for their knowledge and experience
    - Open to Programme being temporary DCAB member if Tier One decision
  - Following M16, Programme involvement will fall away
  - Mechanics to be worked out still
- Thinking and timings are evolving - Intend to have 'final' plan by 31 Mar 24



Implementation

- DIP Rules will come into effect on M10 with the exception of:
  - Governance – DSD001/Ch2 of DIP Supplement – Late September 2024 to align with dual running and DIP Manager & DCAB ready dates
  - Change – DSD004/Ch5 of DIP Supplment – Late September 2024 to align with dual running and DIP Manager & DCAB ready dates
- Provisional dates in SCR Direction
  - M10 and early dates
- Use P344 precedence
  - Bulk of rules implemented on Implementation Date
  - Second phase following letter from Ofgem to NETSO to direct implementation
- DIP Manager Proposal:
  - DIP Rules would need to be implemented in September 2024 to allow for Governance and Change
  - Need a caveat that DIP Manager may not use DSD002/3/5/6 (and corresponding DIP Supplement chapters) powers until M10
    - “DIP Rules Effective from Date”, or similar
  - DIP Manager and/or Programme to confirm on track and Ofgem would give go ahead to implement as previously directed – belts and braces
    - Change to BSC implementation dates requires request from BSC Panel and direction from Ofgem to change Implementation Date
- September Implementation Date will allow DIP Manager to issue guidance and make changes/additions to text ahead of M10
    - For example, Design Artefacts are still subject to change and will need to be folded into some DSDs as changes are made
    - We can publish drafts for consultation and hold in-stasis until September

Transition Plan

- Governance matters:
  - DIP Manager will stand-up in October 2024
  - DCAB will be in position by end of November 2024
- DIP Onboarding:
  - Will incorporate MHHS Qualification plan and will support Qualification as we have CIT and SIT
  - Programme responsible until M10 but, in reality it will be a joint plan driven by DIP Manager
- DIP Assurance
  - Strategy and Risk Register to be consulted on pre-M10
- Change Processes
  - Dual decision making on changes ahead of DIP Manager and DCAB taking responsibility
  - DIP Manager to be consulted prior to dual running, similarly DAG will be consulted post-dual running
- Funding Arrangements
  - Will be centrally funded until end of Migration
  - Funding share won't be 'right' until post-migration
- Information Security Management Systems (ISMS)
  - Working closely with Avanade and programme to be in place for M10
  - ISO27000 Series requirements to fall under wider Elexon certification
- We will issue guidance (and consult on it as new documents) to match sub-sections of DSDs prior to M10

NEXT STEPS

Next Steps

- Elexon will publish a summary of responses to the consultation feedback shortly
- The Issue 101 Issue Report summarising the work done will be presented to the BSC Panel on 14 March 2024
- The Issue Report and supporting documentation will be shared with Ofgem for review
- Ofgem will raise the SCR Modification to implement the DIP legal text

MEETING CLOSE

ELEXON

THANK YOU

Jenny Sarsfield

jenny.sarsfield@elexon.co.uk

bsc.change@elexon.co.uk

29 February 2024