

# Project EDGE

Technology and Cybersecurity  
Assessment

May 2023

## Important Notice

### Purpose

This Technology and Cyber Security Assessment has been prepared for Project EDGE by EY.

The Project EDGE hypothesis relating to data exchange in a high DER future is that an industry data hub is an alternative, more efficient, solution to facilitate DER data exchange at scale for various use cases than a point-to-point exchange approach. Project EDGE is testing two versions of an industry data hub: centralised (conceptually akin to the existing eHub operated by AEMO) and decentralised. This Technology and Cyber Security Assessment provides a theoretical assessment of the different approaches to DER data exchange.

### Disclaimer

The Project EDGE participants (including AEMO, Mondo Power Pty Ltd and AusNet Electricity Services Pty Ltd) (each Project Participant) have commissioned this Technology and Cyber Security Assessment by EY for the purposes of Project EDGE. Each of the Project Participants has made reasonable efforts to ensure the quality of the information in this Technology and Cyber Security Assessment but it is not the author of this report and cannot guarantee that the information, forecasts and assumptions contained it are accurate, complete or appropriate for your circumstances. This Technology and Cyber Security Assessment does not include all of the information that an investor, participant or potential participant in the national electricity market might require, and does not amount to a recommendation of any investment.

Anyone proposing to use the information in this Technology and Cyber Security Assessment (which has been prepared by EY, and includes information and forecasts from EY and other third parties) should independently verify its accuracy, completeness and suitability for purpose, and obtain independent and specific advice from appropriate experts.

Accordingly, to the maximum extent permitted by law, each Project Participant and its officers and employees:

- ▶ make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this Technology and Cyber Security Assessment; and
- ▶ are not liable (whether by reason of negligence or otherwise) for any statements, opinions, information or other matters contained in or derived from this, or any omissions from it, or in respect of a person's use of the information in this Technology and Cyber Security Assessment.

The views expressed herein are not necessarily the views of the Australian Government, and the Australian Government does not accept responsibility for any information or advice contained herein.

### Acknowledgement

Project EDGE received funding from ARENA as part of ARENA's Advancing Renewables Program.

Each Project Participant acknowledges:

- ▶ the work of EY in preparing this Technology and Cyber Security Assessment; and
- ▶ the support, co-operation and contribution of the other Project Edge participants and consultants in providing data and information used by EY to prepare this report.

### Copyright

© 2023 Australian Energy Market Operator Limited. The material in this publication may be used in accordance with the copyright permissions on AEMO's website.

Important Notice .....	i
Purposei	
Acknowledgement .....	i
Copyright .....	i
EY NOTICE .....	vi
Use of this Report .....	7
1. Executive Summary .....	8
1.1 Purpose of this report .....	9
1.2 Summary of theoretical assessment outcomes .....	9
1.3 Cyber threat assessment .....	11
1.4 Resilience & Compensatory Controls .....	12
1.5 Feasibility of transitioning to decentralised data exchange .....	13
1.6 Next steps .....	14
2. Background .....	16
2.1 Scale of DER growth ahead .....	16
2.2 DER data exchange use cases .....	17
2.3 Project EDGE hypothesis .....	18
2.4 UK Energy System Digital Spine initiative .....	19
2.5 Purpose of this report .....	20
2.6 Out of Scope .....	20
2.7 Assumptions .....	20
3. Theoretical assessment of data exchange options .....	21
3.1 DER Data Exchange problem statements .....	21
3.2 Data Exchange Options .....	22
3.3 Assessment Approach .....	27
3.4 Theoretical Assessment .....	28
3.5 Assessment Summary .....	38
3.6 Transition to Decentralised Energy System and Technology .....	39
4. Cyber Security Threat Assessment .....	41
4.1 AEMO Risk Assessment Method .....	41
4.2 Key Risks .....	41
4.3 Summary of Risks .....	44
4.4 Detailed Risks .....	52
5. Data Exchange Resilience and Compensatory Controls .....	73
5.1 Definitions and scope .....	73
5.2 Assessment Approach .....	75
5.3 Data Exchange Resilience .....	76
5.4 Compensatory Controls .....	81
5.5 Summary of Resilience and Compensatory Control Assessment .....	87
6. Risk, benefits and feasibility of implementing decentralised data hub for DER .....	89
6.1 Practical considerations of a decentralised data hub for DER .....	90
6.2 Risk Analysis .....	91
6.3 Benefits Assessment Approach .....	96
7. Conclusion .....	103
8. References .....	106
Appendix A DER Data Exchange Detailed Problem Statements .....	108

Appendix B	AEMO Risk Rating Guidelines .....	122
Appendix C	Risk Assessment Approach .....	123
	Risk Analysis .....	124
	Scope, Context and Criteria .....	125
	Risk Criteria: .....	126
	Categories of risk.....	126
	Risk Assessment .....	126
	Risk Identification .....	127
	Risk Causes.....	128
	Risk Management Framework for Maintenance.....	128
Appendix D	Compensatory Controls supporting material.....	130
	Compensatory Control Scenario .....	130
	Summary of Data Exchanged.....	130
	Scenario: Failure/loss of communication to the aggregator/customer representative .....	131
Appendix E	Glossary of Terms .....	139
Figure 1:	DER capacity projections.....	8
Figure 2:	Theoretical assessment framework .....	9
Figure 3:	Summary of theoretical assessment of data exchange options .....	10
Figure 4:	Conceptual roadmap for phased implementation of DER Data Hub.....	14
Figure 5:	2022 Integrated System Plan resource mix.....	16
Figure 6:	SA Operational Demand and Resource Mix – Sun 16-Oct-2022 .....	17
Figure 7:	High Level DER industry data exchange use cases.....	17
Figure 8:	Project EDGE data exchange efficiency hypothesis .....	19
Figure 9:	Functional DER marketplace interactions .....	23
Figure 10 -	Point-to-point architecture (with agreed standards) .....	24
Figure 11 -	Centralised data hub .....	25
Figure 12 -	Decentralised Data Hub (DDH) .....	26
Figure 13:	Assessment Framework .....	28
Figure 14:	DLT Core Concepts .....	40
Figure 15:	Distributed Identity Management .....	74
Figure 16:	Dynamic Operating Envelope (DoE) Passthrough .....	75
Figure 17 -	Project EDGE Data Exchange Design Principles.....	75
Figure 18:	Resilience and Compensatory Controls Assessment Approach .....	76
Figure 19:	Compensatory Control Overview.....	83
Figure 20:	Example Data Quality Measures .....	85
Figure 21:	Benefits Delivery Diagram .....	97
Figure 22:	Conceptual roadmap for phased implementation of DER data hub .....	104
Figure 23:	AEMO Risk Rating Guidelines.....	122
Figure 24:	Risk framework .....	124
Figure 25:	Risk Assessment Process .....	127
Figure 26:	Risk Management.....	129

Figure 27: Compensatory Control Scenario.....	130
Figure 28: Scenario - Loss of Aggregator .....	131
Figure 29: Failure/loss of total communications across the data exchange .....	133
Figure 30: Failure/loss of communication to a DNSP .....	134
Figure 31: Failure to meet the requirements of a market arrangement .....	135
Figure 32: Communication Redundancy Requirements .....	137
Table 1: Core Data Concepts .....	23
Table 2: Data Exchange Options – Theoretical Assessment by Stakeholder Source: EY (2022) .....	37
Table 3: Assessment Summary .....	38
Table 4: DLT Energy Projects.....	39
Table 5: Detailed Summary of Risks.....	51
Table 6: Detailed Risk Format.....	52
Table 7: Vulnerabilities in DER marketplace software leading to confidentiality, integrity and availability based attacks .....	54
Table 8: Malware and Ransomware attacks.....	56
Table 9: Attacks due to weak transmission and communication protocols .....	57
Table 10: Attacks due to weak initial DER device configurations .....	59
Table 11: Data exposure and unauthorised access attacks .....	61
Table 12: Blockchain-based attack .....	62
Table 13: Supply Chain attacks .....	63
Table 14: Compromise of Critical Assets.....	64
Table 15: Insider attacks/Internal threats.....	66
Table 16: Lack of appropriate User Access Management processes could lead to disclosure of DER Marketplace data.....	68
Table 17: Weaknesses in Security Operations could lead to cyber-attacks not being identified or having greater impact .....	70
Table 18: Threat actors targeting weak onboarding and registration processes to gain access to the DER Marketplace .....	72
Table 19: Data Exchange Scalability .....	79
Table 20: Data Exchange Redundancy and Failover .....	79
Table 21: Data Exchange Complexity.....	81
Table 22: Summarised Initial Risk Rating.....	91
Table 23: Summarised Residual Mitigation Risk Rating.....	91
Table 24: Risk Assessment Matrix.....	95
Table 25: Benefits Impact and Achievability Matrix .....	97
Table 26: Benefits Register.....	101
Table 27: DER Data Exchange Problem Statements .....	121
Table 28: Risk Impact and Likelihood Matrix .....	125
Table 29: Summary of Data Exchanged.....	131

Table 30: Scenario - Loss of Aggregator .....	132
Table 31: Failure/loss of total communications across the data exchange .....	134
Table 32: Failure/loss of communication to a DNSP .....	135
Table 33: Failure to meet the requirements of a market arrangement .....	136
Table 34: Communication Redundancy Requirements .....	138

## EY NOTICE

EY was engaged by the Project Participants under a Shared Consultancy Agreement dated 8 August 2022 to conduct an assessment of Technology and Cyber Security.

The results of EY's work, including the assumptions and qualifications made in preparing the report, are set out in this report. You should read the Report in its entirety including any disclaimers and attachments. A reference to the Report includes any part of the Report. No further work has been undertaken by EY since the date of the Report to update it.

Unless otherwise agreed in writing with EY, any third party accessing this Report or obtaining a copy of this Report ("Recipient") agrees that its access to the Report is provided by EY subject to the following terms:

1. This Report cannot be altered.
  2. The Recipient acknowledges that this Report has been prepared for the Project Participants and may not be disclosed to any other party or used by any other party or relied upon by any other party without the prior written consent of EY.
  3. EY disclaims all liability in relation to any party other than a Project Participant who seeks to rely upon this Report or any of its contents.
  4. EY has acted in accordance with the instructions of the Project Participants in conducting its work and preparing this Report, and, in doing so, has prepared this Report for the benefit of the Project Participants, and has considered only the interests of the Project Participants. EY has not been engaged to act, and has not acted, as advisor to any other party. Accordingly, EY makes no representations as to the appropriateness, accuracy or completeness of this Report for any other party's purposes.
  5. No reliance may be placed upon this Report or any of its contents by any party other than the Project Participants. A Recipient must make and rely on their own enquiries in relation to the issues to which this Report relates, the contents of this Report and all matters arising from or relating to or in any way connected with this Report or its contents.
  6. EY have consented to this Report being provided to ARENA and/or published for informational purposes only. EY have not consented to distribution or disclosure of the Report beyond this.
  7. No duty of care is owed by EY to any Recipient in respect of any use that the Recipient may make of this Report.
  8. EY disclaims all liability, and takes no responsibility, for any document issued by any other party in connection with Project Edge.
  9. A Recipient must not name EY in any report or document which will be publicly available or lodged or filed with any regulator without EY's prior written consent, which may be granted at EY's absolute discretion.
  10. A Recipient:
    - a. may not make any claim or demand or bring any action or proceedings against EY or any of its partners, principals, directors, officers or employees or any other Ernst & Young firm which is a member of the global network of Ernst & Young firms or any of their partners, principals, directors, officers or employees ("EY Parties") arising from or connected with the contents of this Report or the provision of this Report to the Recipient; and
    - b. must release and forever discharge the EY Parties from any such claim, demand, action or proceedings.
  11. If a Recipient discloses this Report to a third party in breach of this notice, it will be liable for all claims, demands, actions, proceedings, costs, expenses, loss, damage and liability made or brought against or incurred by the EY Parties, arising from or connected with such disclosure.
  12. If a Recipient wishes to rely upon this Report that party must inform EY and, if EY agrees, sign and return to EY a standard form of EY's reliance letter. A copy of the reliance letter can be obtained from EY. The Recipient's reliance upon this Report will be governed by the terms of that reliance letter.
  13. If, and to the extent of, any inconsistency between the Shared Consultancy Agreement and the terms of this EY Notice, the Shared Consultancy Agreement will prevail.
- Ernst & Young's liability is limited by a scheme approved under Professional Standards Legislation.

## Use of this Report

This Report is intended solely for the use of the “Project Participants”). We understand that the Project Participants may wish to make this report available to other third parties. We are not privy to the interests, technical knowledge and commercial or other objectives of these third parties. Hence, the specific needs and requirements of any such third parties have not been taken into account in preparing this report. In addition, any third party who may have sight of the report will not have the benefit of the detailed discussions and mutual exchange of information, which will inevitably occur between EY and the Project Participants in the course of preparation of the report.

The Project Participants may not use our report for any other purpose without our prior, written approval.

EY’s observations do not constitute a pre-certification or certification audit in accordance with attainment of any accreditation/certification.

EY assumes no responsibility whatsoever in respect of any negligence, fault, breach of contract or breach of duty or otherwise to any user of this report other than the Project Participants. Any person who chooses to rely on this report does so entirely at their own risk. Any references to EY or our report(s) in Marketing or promotional literature or any material to be disseminated to the general public must be approved in advance in writing by EY.



# 1. Executive Summary

Project EDGE (Energy Demand and Generation Exchange) is a multi-year project to demonstrate an off-market, proof-of-concept Distributed Energy Resource (DER) Marketplace that efficiently enables DER to provide both wholesale and local network services within the constraints of the distribution network.

The DER Marketplace is not a single, AEMO-run platform or capability. Rather, it is an integrated digital ecosystem that links many systems and capabilities across various industry actors to enable the efficient and scalable exchange of data and services between industry actors.

The primary use cases being tested in Project EDGE are the exchange of Dynamic Operating Envelopes (DOEs) and operational telemetry between Distribution Network Service Providers (DNSPs), Market Operator and customer agents / aggregators, but the use cases could expand as retailers seek to communicate with customer agents / aggregators to manage PV exports during negative price periods, and electric vehicle (EV) customer models proliferate.

Efficient and scalable digital infrastructure upon which aggregators, DNSPs and other market participants can securely and reliably exchange information and services, may deliver better user experiences for industry participants and more efficient outcomes for consumers. This is particularly important given that AEMO’s 2022 Integrated System Plan forecasts over 100 GW of DER in the National Electricity Market (NEM) by 2050, and >50 GW in the next 10 years.

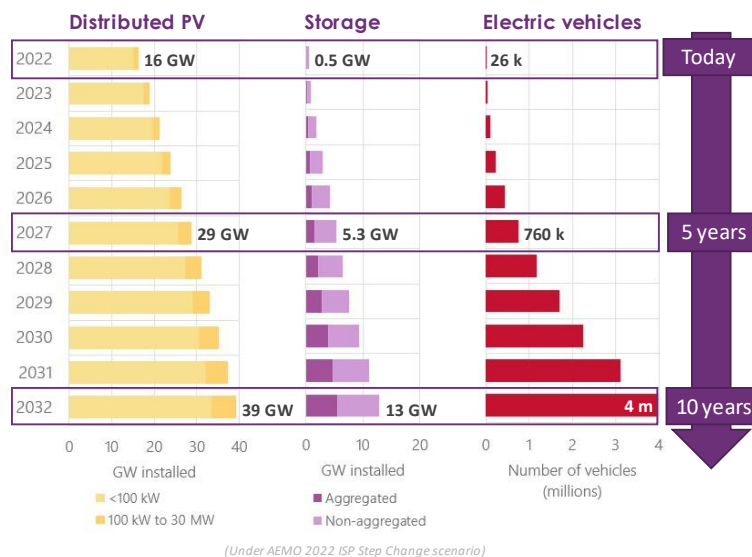


Figure 1: DER capacity projections  
 Source: AEMO 2022 Integrated System Plan

## 1.1 Purpose of this report

The Project EDGE hypothesis relating to data exchange in a high DER future is that an industry data hub is an alternative, more efficient, solution to facilitate DER data exchange at scale for various use cases than a point-to-point exchange approach. Project EDGE is testing two versions of an industry data hub: centralised (akin to the existing eHub operated by AEMO) and decentralised.

EY has been engaged to conduct a theoretical assessment of these different approaches to DER data exchange. EY has developed an overarching assessment framework that considers the National Electricity Objective, the Project EDGE data exchange principles, and uses assessment criteria that focus on the four categories of data exchange characteristics (shown in Figure 2 below). EY has conducted this assessment in the context of the high DER future anticipated in the DER capacity projections in Figure 1, and has also conducted more detailed assessments relating to cyber security, resilience and compensatory controls, and the feasibility of establishing decentralised data exchange infrastructure for DER.

Assessment Framework: Data Exchange Options			
Success Criteria: Industry Alignment	Assessment Criteria	Assessment Rating	
<b>National Electricity Objective (NEO)</b> To promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to: <ul style="list-style-type: none"> <li>Price, quality, safety and reliability and security of supply of electricity</li> <li>The reliability, safety and security of the national electricity system.</li> </ul>	<b>Scalable, Stable &amp; Resilient</b> <span style="float: right;">1</span> Ability for the integration approach to handle ad-hoc load (peaks and troughs incl. instability) without impacting the performance, stability and reliability of the national energy system	Each data exchange option will be assessed against the each of the four assessment criteria.  The assessment rating will be measured utilising Likert scale response anchors of:  <b>Unlikely, Neutral, Likely</b>  in respect to the likelihood of the approach being suitable in achieving the purpose of the assessment criteria and the intentions of the success criteria.	
<b>Project EDGE: Data Exchange Principles</b> <ul style="list-style-type: none"> <li>Reduce cost, and complexity of data exchange</li> <li>Agree and implement standards</li> <li>Decouple actors and avoid hidden coupling</li> <li>Reduce barriers to entry</li> <li>Consistent user experience across regions</li> <li>Ensure data privacy, security and quality</li> </ul>	<b>Interoperable, Modular &amp; Flexible</b> <span style="float: right;">2</span> Ability for the integration approach to support connection and communication across a diverse heterogeneous energy network (devices, systems and networks) in a coordinated and structured manner.		Point to Point Data Exchange
	<b>Secure, Trustworthy &amp; Auditable</b> <span style="float: right;">3</span> Ability for the integration approach to enable privacy-preserving energy scheduling that can be trusted to ensure the integrity of the national energy system in a transparent, integral and where required, confidential way. This includes mitigations against and considerations for cyber attacks across the future distributed national energy system		Centralised Data Exchange
	<b>Standardised, Accessible &amp; Fair</b> <span style="float: right;">4</span> Ability for the integration approach to enforce standardised communication protocols across the network while supporting the long term interests of consumers through ensuring market accessibility (low barrier to entry) and equitable governance and operations		Decentralised Data Exchange
<b>Project EDGE: Research Plan</b> <ul style="list-style-type: none"> <li>Wholesale market participation enabled at scale</li> <li>Distribution network limits in wholesale dispatch considered</li> <li>Efficient and scalable trade of local network services enabled</li> <li>Efficient, scalable and secure data exchange enabled</li> <li>Integrated technology</li> </ul>			

1

Figure 2: Theoretical assessment framework

## 1.2 Summary of theoretical assessment outcomes

The overarching assessment scored each data exchange approach against the criteria in the assessment framework, and also scored from the perspective of different industry participants.

Point-to-point data exchange solutions scored lowest in each of the categories, indicating they are not suitable in a high DER future envisaged by the Integrated System Plan. Point-to-point integrations may be manageable for individual use cases at small scale, such as a small number of aggregators integrating with one DNSP to obtain DOEs, but the following factors associated with a high DER future mean point-to-point approach could lead to inefficient outcomes for consumers:

- ▶ Proliferation of aggregators needing to obtain DOEs from all DNSPs across the NEM.
- ▶ Proliferation of use cases, such as:
  - a. Retailers sending zero export limits to customer agents to manage negative price exposure

<sup>1</sup> Note: NEO objectives may vary overtime. For example, a potential change being considered is to add a sustainability / emission reduction element to the NEO.

- b. DNSPs sending dynamic network prices to EV charge point operators to manage peak charging risks.

Scoring between centralised and decentralised approaches was closer, but a decentralised approach can theoretically deliver greater benefits than centralised in each of the four categories assessed:

1. **Scalable, stable and resilient:** Decentralised architectures have no single source of failure, and are highly resilient as integrated mechanisms for data storage and access enable easy restoration if there is a node outage.
2. **Interoperable, modular & flexible:** Decentralised architectures enable high interoperability for users, are modular and flexible as any party can design, implement, and maintain their system or project in line with the feature set provided by the decentralised ecosystem. Furthermore, the underlying decentralised infrastructure can support any data model or communication protocol that is chosen by the governing body.
3. **Secure, trustworthy, and auditable:** A decentralised integration method offers the most trustworthy system of all three approaches. Like a public Distributed Ledger Technology (DLT) platform, no single entity has complete control to view, write, or modify the protocol. In a permissioned platform any change conducted can be seen and verified by other parties which results in a highly transparent ecosystem, furthermore any change or modification is also immutable increasing trust and auditability in the platform.
4. **Standardised, accessible & fair:** Decentralised architectures adopt ecosystem wide standards that are not easily changed/manipulated. Accessibility for a permissioned system would be similar to a centralised approach as the governing body would determine access. With regard to cost recovery, in a decentralised approach the infrastructure and associated costs can be decentralised to participants. As a result, the costs to host the infrastructure may be allocated more directly to the customers that benefit from it.

	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABLE, STABLE &amp; RESILIENT</b>	1	2	3
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>	1	2	2
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>	1	2	3
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>	1	2	3
<b>AVERAGE</b>			
	Point-to-point	Centralised	Decentralised
<b>INTEGRATION HUB AVERAGE</b>	1 Unlikely	2 Neutral	2.75 Likely

Figure 3: Summary of theoretical assessment of data exchange options

It is important to note that this is a theoretical assessment in the context of a proliferation of DER in the medium to long term, and ‘enterprise -grade’ decentralised technologies in the energy space are not yet widely available.

While DER data exchange is relatively small there is less distinction between centralised and decentralised options, but there may come a tipping point where the advantages of decentralised approaches outweigh the costs and complexities of transitioning towards decentralised technologies.

A key question relates to the timing of those net benefits, and whether there is sufficient confidence in those benefits to advance a pathway of decentralisation before the tipping point in order to reduce the costs and complexities of the transition. This would also need to be considered in the context of broader developments in the electricity industry system architecture.

A balanced approach may involve implementing a phase 1 DER Data Hub in a centralised model, but using technology that gives optionality to support a smooth transition to a decentralised approach if

appropriate in future. The detailed design for a phase 1 implementation should consider the option value that technology solutions can provide for future development.

### 1.3 Cyber threat assessment

The evaluation included a separate cyber security threat assessment on the data exchange approaches. This assessment reviewed a number of potential cyber security risks associated with DER data exchange and outlined a number of mitigating controls that could result in a lower residual risk level.

The most material risks related to the fact that DER uses public communication infrastructure (public internet), rather than dedicated SCADA networks used by large-scale resources:

- ▶ Vulnerabilities and weaknesses in the multiple software ecosystems leveraged in the DER ecosystem could lead to unauthorised access to disclosure of sensitive information.
  - Mitigating control: Implement Secure by Design principles across software development processes. The DER ecosystem should also follow Zero-Trust methodology and frameworks to ensure DER entities continue to work in a fail-safe manner in an event of a security incident.
- ▶ Lack of appropriate management of Supply Chain risks could lead to data disclosure or unavailability of key DER resources.
  - Mitigating control: cyber security requirements should be established for key suppliers according to industry better practices and information sources should be monitored to identify and address supply chain threats and risks.
- ▶ Lack of asset and entity classification processes could lead to inappropriate application of security controls thereby increasing the impact of a potential cyber-attack.
  - Mitigating control: Each entity across the DER Marketplace should perform a Business Impact Analysis (BIA) to understand the criticality of their assets and thereby implement appropriate controls to ensure critical assets have the right level of protection against cyber-attacks.

Although the scope of Project EDGE was limited to considering DER data exchange between key industry (actors, aggregators, DNSPs and AEMO) for specific use cases such as the exchange of DOEs, the critical risks identified above relate to the full supply chain for data exchange that includes aggregator/customer agent to end device communications.

Project EDGE has tested some of the key concepts of a decentralised approach to DER integration, such as Decentralised Identities (DIDs) and a decentralised data hub, to automatically assign DOEs sent by DNSPs (assigned at the NMI level) to the right aggregator without the need for a centralised broker, but this has been done at small-scale so the scalability of these concepts has not been tested practically. Furthermore, the full potential of a decentralised approach has not been comprehensively and practically examined due to the scope restriction outlined above.

#### Longer-term and broader considerations

A more comprehensive application of DIDs at the device level, which has not been tested in Project EDGE, may deliver a range of further benefits for the industry and consumers, including:

- ▶ **Secure integration with the DER ecosystem:** Devices and entities with a DID could automatically upload their standing data and credentials to an updated DER Register as they first connect to the internet, saving time, effort and errors in manually uploading data.
- ▶ **End to end visibility and auditability across the DER ecosystem:** DIDs and Verifiable Credentials (VCs) at each level of the supply chain (for example, device and aggregator / retailer level) enables greater integrity checking and isolation of operation via revocation of VCs if a security threat is identified.

- ▶ **Secure interoperability across the DER ecosystem:** An extended capability of DIDs and VCs may enable any retailer/aggregator to send control signals to compatible devices if they have correct VCs, customer consent and are connected to an industry data hub. This would give customers freedom to switch between providers and enable aggregators to easily coordinate numerous different device types within their portfolio.
- ▶ **Compliance with industry standards:** DIDs and VCs may provide traceability of settings and firmware upgrades for compliance to standards (for example, AS 4777.2.2020 or CSIP-AUS).

## 1.4 Resilience & Compensatory Controls

Each of the three data exchange approaches has been assessed for their resilience, and their ability to monitor triggers for compensatory control as well as enact compensatory control. The pre-conditions and post-condition considerations for the enactment of compensatory control have also been defined.

The Project EDGE Design Principles seek to ensure a safe, reliable, and secure supply of electricity while providing a low barrier to entry, cost effective and consistent user experience. With consideration of these principles the future DER data exchange approach must be scalable, resilient and not overly complex, while simultaneously enabling the compensatory control of DER in the event of communication loss.

When considering the Project EDGE design principles for data exchange and the requirements for compensatory control, this assessment finds point-to-point data exchange to be a low fit for ensuring safe, reliable and secure DER data exchange at scale. Tight coupling of market participants, limited resilience and inability to monitor triggers for compensatory control at scale reduce the suitability of a point-to-point approach as a grid-scale solution for DER data exchange.

A Decentralised Data Hub (DDH) conceptual data exchange approach was found to be the best fit to the intended resilience goals. The DDH approach best enabled trusted participation and DID management. This is based on ensuring loose coupling (a data exchange design principle) and the decentralised worker approach for use cases such as DOEs partitioning which should enable the scalability of data exchange for a future full NEM-wide DER roll-out and market participation.

The Centralised Hub (CH) conceptual data exchange options shared many of the high fit characteristics of the DDH including loose coupling and a low barrier to entry, however it was found to have a medium fit for scalability without the decentralised worker approach to use cases such as DOE partitioning. A key advantage of blockchain-based solutions is that they reduce the amount of human involvement required to create and execute transparent and verifiable transactions through the use of self-executing contracts between buyers and sellers written directly into code. The outcome being, elimination of intermediaries, while raising the assurance of execution and enforcement processes. By automating a transaction in a fully verifiable framework (the blockchain) the transactions can have legal validity even at high frequency – a key enabler for network management required as part of the energy transition. Further work is required to understand the threshold/scale at which a decentralised approach becomes more efficient than a centralised approach, which could be considered in the Industry Data Exchange and DER Data Hub & Register projects as part of the NEM 2025 program.<sup>2</sup>

With regard to compensatory controls, SA Power Networks (SAPN) have adapted IEEE2030.5's "DefaultDERControl" as a failsafe to revert DER to minimal export on the loss of communications. This approach can be applied under either of the three data exchange mechanisms assessed and is not a differentiating factor in the assessment.

It is recommended that AEMO work with DNSPs so that:

<sup>2</sup> AEMO, 2022. NEM2025 Implementation Roadmap. Available at: [https://aemo.com.au/-/media/files/stakeholder\\_consultation/working\\_groups/other\\_meetings/reform-delivery-committee/nem-2025-implementation-roadmap---initiative-briefs.pdf?la=en&hash=050682860B56F94913AAF1CA99129D58](https://aemo.com.au/-/media/files/stakeholder_consultation/working_groups/other_meetings/reform-delivery-committee/nem-2025-implementation-roadmap---initiative-briefs.pdf?la=en&hash=050682860B56F94913AAF1CA99129D58)

- ▶ A consistent approach to DER compensatory controls is adopted across DNSPs, so that DOEs can still be applied even when communications are lost.
- ▶ An operational procedure between DNSPs and AEMO control rooms is developed as DER penetration gain further scale to communicate the settings applied and impact of an extended communication outage on aggregated DER operations.
- ▶ To agree different DefaultDERControl settings to apply under different seasons or operating conditions, if appropriate.

## 1.5 Feasibility of transitioning to decentralised data exchange

As the DER industry is currently on a path of point-to-point data exchange proliferation, the first priority is to understand and articulate:

- ▶ Whether there are long-term inefficiencies for consumers in remaining on this path.
- ▶ The long-term benefits to consumers of a DER Data Hub.

An independent cost benefit analysis (CBA) on Project EDGE has evaluated that a DER Data Hub would deliver significant customer benefits when compared to a point-to-point data exchange approach.<sup>3</sup>

If a DER data hub approach is recognised as a more efficient and scalable way to facilitate data exchange across numerous use cases, then the following realistic options may be considered:

- ▶ Centralised approach: adding DER data exchange use cases (such as the DOEs) to the existing eHub, Shared Market Protocol and consideration of how that should evolve towards a target state following the Industry Data Exchange project.
- ▶ Decentralised approach: establishing an alternative decentralised data hub for DER use cases that can operate in parallel, and separately, to the eHub. In order to enable consistent user experiences for stakeholders that need to interact with each system (for example, a retailer or DNSP), consistent approaches should be prioritised for elements such as Identity and Access Management (for which there is a project in the NEM 2025 program). This, and consideration of how these two approaches could converge over time, should be explored further in the Industry Data Exchange project.

There is also a spectrum of technology choices available, between conventional centralised to fully decentralised technologies including, for example, conventional technology choices deployed in containers to mitigate single point of failure risks.

Utilisation of decentralised technologies for a shared DER Data Hub is feasible and it is considered worthwhile to invest time, effort and resources to explore an implementation in more detail given the potential consumer benefits identified in this report.

It is important to not lose sight of the scale of effort required to develop a detailed design and business case for implementation as there are layers of detail that have not been considered to date. Hence further research and small-scale implementations will be required to explore ways in which various frameworks and models can be applied.

A phased implementation of a DDH is considered the most appropriate approach, rather than a single 'big bang' approach, starting with a small number of use cases and participants. A successful small-scale implementation may pave the way to add further use cases and scale the solution as rapidly as required by industry, noting that economies of scale may not be achieved until later phases.

---

<sup>3</sup> Deloitte Access Economics, 2023. Project EDGE Cost Benefit Analysis. Available: <https://aemo.com.au/en/initiatives/major-programs/nem-distributed-energy-resources-der-program/der-demonstrations/project-edge>

In considering the case for the first small-scale implementations, it is important to consider the potential long-term benefits of decentralisation if beginning the journey down such a path, taking all stakeholder impacts into account together rather than considering individual use cases on a stand-alone basis.

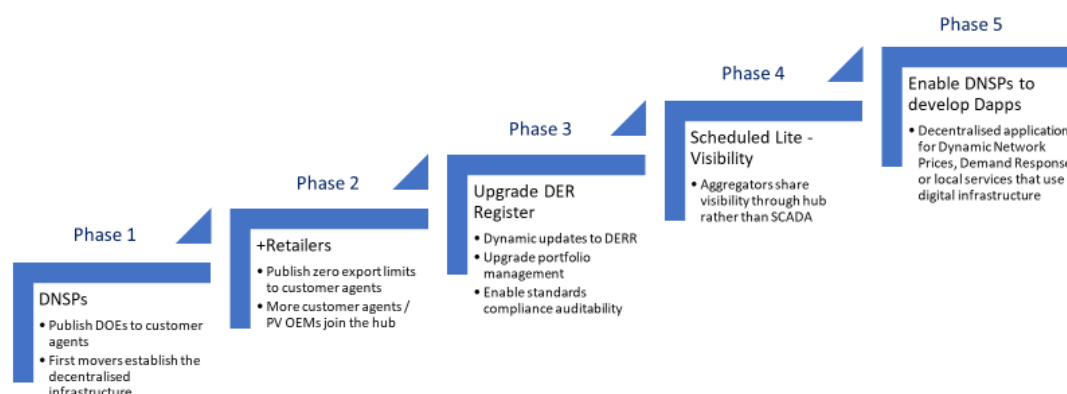


Figure 4: Conceptual roadmap for phased implementation of DER Data Hub

In designing a phased implementation roadmap in more detail, it is important to also consider use cases in adjacent sectors that could deliver greater efficiency gains for consumers. For instance, sharing of standing and operational data from EV charge points, similar to the National Charge Link<sup>4</sup> concept, could be highly efficient in a decentralised DER data hub particularly since those charge points would need to receive DOEs from DNSPs in future.

Australia is not alone in exploring these concepts. For example in the UK:

- ▶ An Energy Digitalisation Taskforce made ambitious recommendations for the UK Government to “create a radically different energy system, driven by open-source software and open standards,” facilitated through the deployment of a “Digital Spine” (including an Energy Asset Register and Energy Data Catalogue) that would create a network of connected nodes to share data across the energy sector.<sup>5</sup>
- ▶ The Department of Transport is establishing an EV Chargepoint Datahub, after industry consultation<sup>6</sup>, so that standing and operational charge point data is made openly available to enable consumers to locate available and working charge points easily.

The Digital Spine and Open EV Chargepoint Datahub are very similar concepts to the data exchange hub that Project EDGE is examining, and each deserves more detailed investigations to validate whether this public interest digital infrastructure is in the long-term interests of consumers.

## 1.6 Next steps

This independent theoretical assessment and the independent CBA on Project EDGE have identified that a DER Data Hub is more aligned to the long-term interest of consumers than a point-to-point approach for DER related data exchange in a high DER future. The practical trial has also demonstrated, at small scale, how a DDH could work to facilitate emerging DER use cases across many industry actors.

To advance industry thinking on how to implement a production grade DER Data Hub, next steps may include the following:

<sup>4</sup> National Charge Link: Available: [https://issuu.com/racefor2030/docs/national\\_charge\\_link](https://issuu.com/racefor2030/docs/national_charge_link)

<sup>5</sup> UK Energy Digitalisation Taskforce. Available: <https://es.catapult.org.uk/report/delivering-a-digitalised-energy-system/>

<sup>6</sup> UK Department for Transport, Consumer Experience at public chargepoints. Available: <https://www.gov.uk/government/consultations/the-consumer-experience-at-public-electric-vehicle-chargepoints/the-consumer-experience-at-public-chargepoints>

- ▶ Identify appropriate use cases and voluntary participants for a phase 1 implementation.
- ▶ Develop detailed design for a minimum viable product (for phase 1 implementation), that includes Enterprise and Solution Architecture (conceptual and logical).
  - Detailed design should determine whether to adopt centralised, decentralised or hybrid technology solutions considering the option value of solutions that can enable a transition to alternative approaches as needed in future.
  - It should also examine governance, ownership and cost recovery models, and requirements for stakeholder engagement and education.
- ▶ Design a more detailed implementation roadmap on which use cases could be added and when.
- ▶ Link with other activities, such as the development of Public Key Infrastructure for DER or the exploration of an EV charge point data hub like the National Charge Link<sup>7</sup> proposal, to identify opportunities to integrate initiatives to deliver more efficient outcomes.

These activities could all be progressed within the broader context of the Industry Data Exchange and DER Data Hub and Registry Services projects in the NEM 2025 Program, and through engagement with industry stakeholders.

---

<sup>7</sup> RACE for 2030. National Charge Link. Available: [https://issuu.com/racefor2030/docs/national\\_charge\\_link](https://issuu.com/racefor2030/docs/national_charge_link)



## 2. Background

Australia is in the midst of a once-in-a-century transformation in the way electricity is generated and consumed in Australia. Legacy assets will be replaced by low-cost renewables, energy storage and other new forms of firming capacity, and the grid will be reconfigured to support two-way energy flow from Distributed Energy Resources (DER) such as Solar Photovoltaics (PV), wind generation, and batteries connected to distribution networks.<sup>8</sup>

### 2.1 Scale of DER growth ahead

AEMO's 2022 Integrated System Plan (ISP) projects that DER will be as influential as large-scale resources on market dynamics by 2050 as:

- ▶ Coordinated DER may represent 50% of dispatchable capacity.
- ▶ Distribution connected resources may represent 40% of total capacity.

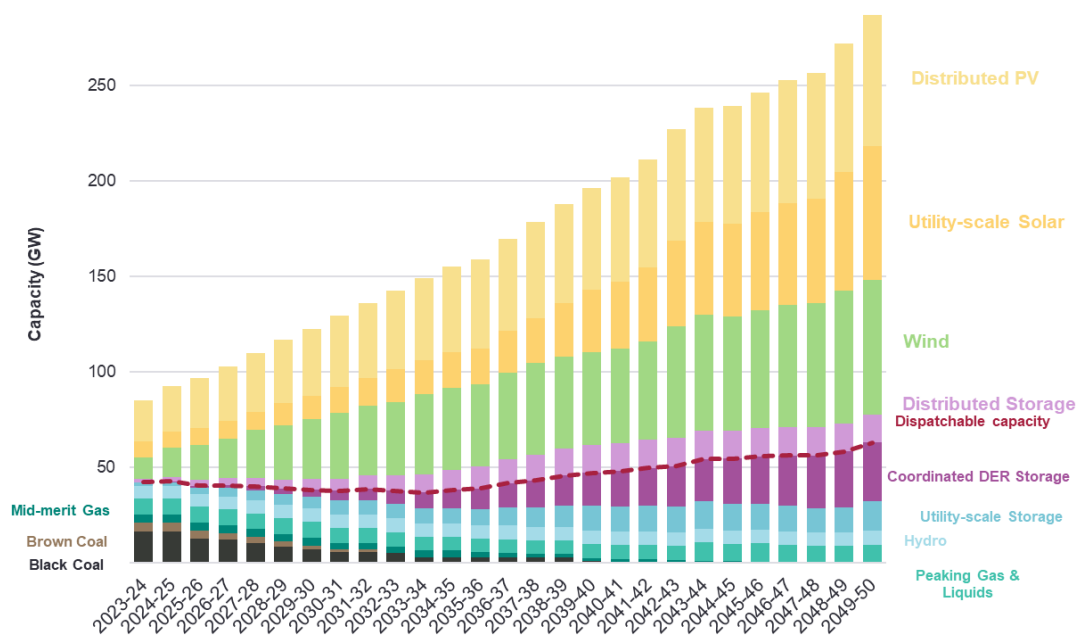


Figure 5: 2022 Integrated System Plan resource mix

Source: Figure reproduced from AEMO (2022)

However, exponential growth of DERs brings several challenges that must be overcome. These challenges include balancing real-time variable supply with flexible demand, managing distribution network power flows with very high DER penetration to remain within secure limits, maintaining power quality at such times, and establishing a governance model that promotes fair and economically viable distribution of resources.

For example, even with current levels of rooftop PV, South Australia Power Networks needs to actively manage rooftop PV using its flexible exports program to support AEMO in managing system security during minimum demand times. The systems to support this capability will need to scale up to support a five-fold increase in rooftop PV anticipated in the 2022 ISP.

<sup>8</sup> AEMO 2022 Integrated System Plan

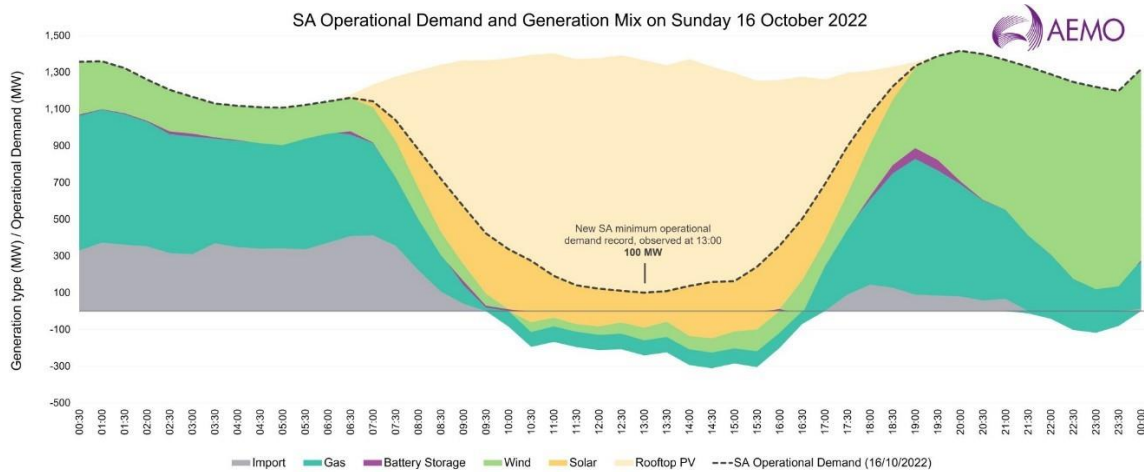


Figure 6: SA Operational Demand and Resource Mix – Sun 16-Oct-2022

Source: Figure reproduced from AEMO (2022)

Each Distribution Network Service Provider (DNSP) or Distribution System Operator (DSO) will eventually need to develop capabilities to calculate and communicate Dynamic Operating Envelopes (DOEs) to aggregators/customer agents, so that customers can keep installing rooftop PV and power flows remain safe and secure.

## 2.2 DER data exchange use cases

There are many use cases relevant to a very high DER future where different actors will need to exchange data with each other, as outlined in the figure below.



Figure 7: High Level DER industry data exchange use cases

In a world with over 100 GW of DER and a fully electrified economy, including land transport, the scale of data exchange required to support simple and valued customer experiences will be orders of magnitude greater than today.

Exchanging data without consistent data models, controls and commands would add unnecessary and material costs to consumers, whilst restricting innovation and raising barriers to entry.

As such, Australia's smart grid system of the future, its digital energy spine, is required to be scalable, efficient, and mitigate against heavy computational and communicational burdens. All the while establishing a secure, private, highly available and trust-worthy operational environment to support data exchange across the industry.<sup>9</sup>

To achieve this, market participants and regulatory bodies require access to the energy systems data in various timeframes to make strategic, operational, and regulatory decisions. The framework to facilitate this data liquidity must ensure the National Electricity Objective (NEO) is upheld; a safe, efficient, reliable, and secure national electricity system that serves the long-term interests of consumers.

## 2.3 Project EDGE hypothesis

AEMO is collaborating with Ausnet Services and Mondo to trial/experiment different versions of a DER Data Hub to support a DER Marketplace concept. Participant roles in this pilot include AusNet Services as the DSO, Mondo as an aggregator of DER services and AEMO as the Market Operator (MO).

The central hypothesis in relation to industry data exchange in Project EDGE is that the current data exchange approach between DER industry actors - point to point integrations – is not efficient and scalable in a >100 GW DER future. This is based on the complexity of administering and managing millions of DER devices, as opposed to a few hundred large scale resources.

Under the status quo, AEMO, DNSPs and every other actor that wants to communicate with customer agents or other entities must develop bespoke IT integrations with each other. This can be made more efficient if each actor uses a similar data model or communication protocol, such as the Australian Common Smart Inverter Profile, which is gaining traction in Australia.<sup>10</sup> An increased adoption of this standard or alternative standard utilising the today's point-to-point architecture will not deliver an optimal solution in a high DER future.

A common approach to complex integration problems is to create a data integration hub, often called an enterprise service bus, in which heterogeneous point-to-point connections between systems are replaced with standardised integrations.

The Project EDGE hypothesis is that an industry data hub is a more efficient way to facilitate data exchange at the GW scale for the various use cases outlined in Figure 7 above than the current approach. Furthermore, Project EDGE is testing two versions of an industry data hub: centralised and decentralised.

---

<sup>9</sup> Mollah et al., 2021

<sup>10</sup> ARENA, 2022. Available: <https://arena.gov.au/knowledge-bank/common-smart-inverter-profile-australia/>

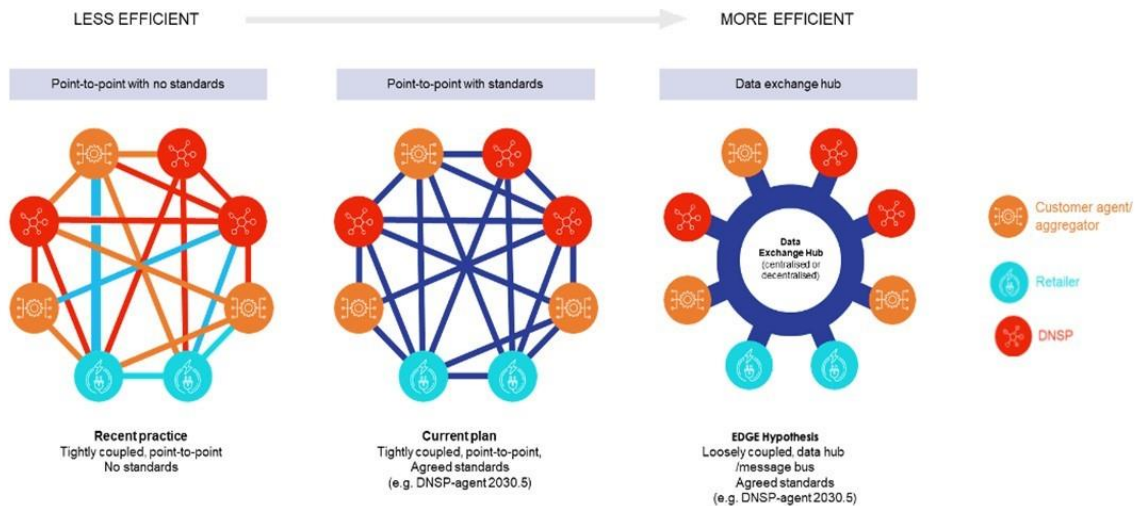


Figure 8: Project EDGE data exchange efficiency hypothesis

Source: Figure reproduced from AEMO (2022)

## 2.4 UK Energy System Digital Spine initiative

The concepts being explored in Project EDGE are very similar to recommendations from a UK Energy Digitalisation Taskforce to develop a digital spine for the energy system, “to enable plug and play options, encouraging whole system interoperability and standardised data sharing.”<sup>11</sup>

The UK Government, Ofgem and Innovate UK are now initiating a joint response<sup>12</sup> to the energy digitalisation recommendations that includes commissioning a feasibility study on the digital spine concept.

The Request for Tender document for the digital spine feasibility study states that:

*“A digital net zero energy system, built on principles of data openness, sector-wide interoperability and security by design, can help to create an efficient whole-system approach to sharing data. Everyone can benefit from the digitalised exchange of data, with improved knowledge, insights and analysis driving improvements in energy products, services, entrepreneurial opportunities and policy-making.”<sup>13</sup>*

The Energy Digitalisation Taskforce report describes ‘a digital spine’ as:

*“a thin layer of interaction and interoperability across all players which enables a minimal layer of operation critical data to be ingested, standardised and shared in near real time”<sup>14</sup>*

The Energy Digitalisation Taskforce also recommends the establishment of the following elements that are complementary to the digital spine concept:

- ▶ Energy Asset Register and Energy Data Catalogue
- ▶ Data sharing ‘fabric’ - governance, administrative and consistent technology solutions to share data across organisations

<sup>11</sup> Catapult Energy Systems, 2022. Available: <https://es.catapult.org.uk/news/energy-digitalisation-taskforce-publishes-recommendations-for-a-digitalised-net-zero-energy-system/>

<sup>12</sup> UK Government Department of Business, Energy and Industrial Strategy, 2022. Available: <https://www.gov.uk/government/publications/digitalising-our-energy-system-for-net-zero-strategy-and-action-plan/energy-digitalisation-taskforce-report-joint-response-by-beis-ofgem-and-innovate-uk>

<sup>13</sup> UK Government Department of Business, Energy and Industrial Strategy, 2022. Available: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1109954/energy\\_system\\_digital\\_spine\\_scoping\\_study.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1109954/energy_system_digital_spine_scoping_study.pdf)

<sup>14</sup> Catapult Energy Systems, 2022. Available: <https://es.catapult.org.uk/news/energy-digitalisation-taskforce-publishes-recommendations-for-a-digitalised-net-zero-energy-system/>

- ▶ Network Data standards and Flexible Asset standards.

These concepts are all explored in Project EDGE in which the DER Data Hub would include an upgraded DER Register, as well as data standards and appropriate governance arrangements to support the establishment and ongoing development of the DER Data Hub.

## 2.5 Purpose of this report

This report is intended to provide an assessment of the theoretical options for a DER data exchange architecture for Project EDGE, and it aims to guide an architect/designer in solution choices and decisions.

## 2.6 Out of Scope

This theoretical assessment of data exchange options report does not evaluate the following:

- ▶ Assessment of other integration architecture approaches/patterns or specific implementations of each integration approach.
- ▶ Assessment of all variations of DLT architecture including core components; nodes, transactions, consensus protocols (governance mechanisms), and data structures as it relates to decentralised data exchange.
- ▶ Assessment of elements required to establish a target state operating model such as governance mechanisms, onboarding & offboarding, complete system technical landscape and roles & responsibilities relating to market actors.
- ▶ Assessment of standards, such as IEEE 2030.5, IEEE 1574-2018, AS/NZS 4777.2:2015 concerning the data exchange and the assessment options within this report.
- ▶ Assessment of the specific data exchange solution for Project EDGE provided by Energy Web.
- ▶ Cyber Security Threat & Risk assessment report does not evaluate either an in-depth analysis of the technical solutions implemented as part of Project EDGE, or a detailed assessment of AEMO's current e-Hub implementation and architecture.
- ▶ Assessment of broader AEMO programs such as Industry Data Exchange, Operational Data Exchange and hence are not considered in this assessment.

## 2.7 Assumptions

The assumptions underpinning the assessment are as follows:

- ▶ Due to the complexity and scale of the Australian energy market, it is assumed that usage of multiple integration approaches may be appropriate based on specific use cases. Therefore, the reading of this report should be in context to the specific use case of enabling a scalable DER marketplace as per Project EDGE's objectives.
- ▶ Further assessment in the context of a full market solution and conditions will be required to ensure the suitability and feasibility of an integration approach to ensure scalability, security, and efficiency as intended by the NEO.

### 3. Theoretical assessment of data exchange options

This section summarises a theoretical assessment of data exchange options, and is structured to examine the following:

- ▶ DER Data exchange problem statements.
- ▶ DER data exchange high level options.
- ▶ Assessment approach and framework.
- ▶ Theoretical assessment.

In this section, three possible data exchange options are assessed:

1. Point-to-Point.
2. Centralised Hub (CH).
3. Decentralised Data Hub (DDH).

All three options are assessed equitably using common assessment criteria.

#### 3.1 DER Data Exchange problem statements

Project EDGE consulted with DNSPs, aggregators and retailers via multiple stakeholder engagement forums to identify and define problem statements that industry is currently (or may soon be) faced with in the transition to a more distributed two-sided market.

Those problem statements identified as high-priority by industry are summarised below, with a detailed outline of all problem statements developed and considered by the project provided in Appendix A.

##### DER Data Inconsistency across Industry Participants

Today DER standing data is replicated across multiple independent systems, and although processes exist to transfer data among these systems based on certain events, they are limited, and discrepancies inevitably arise over time. These inconsistencies create significant operational challenges and inefficiencies across AEMO, DNSPs, retailers and customer agents, as DER standing data represent the foundational inputs for nearly all other market and Business to Business (B2B) transactions.

##### High Data Exchange Costs

Currently, market participants incur significant costs implementing and maintaining a series of bespoke, bilateral data exchange integrations with DNSPs and AEMO. This presents barriers to entry for new participants, and burdens for existing ones.

These costs manifest directly as excessive administrative overhead for VPPs seeking to deliver electricity services, which in turn contribute to higher market prices due to diminished DER participation, and ultimately result in foregone revenue opportunities for customers.

Furthermore, these barriers are anticipated to increase - due to ever complicated data exchange integrations - in order to achieve the Energy Security Board's DER Implementation Plan, which includes the following initiatives that seek to reward customers for their flexibility and enable them to engage multiple service providers to meet their energy needs:

- ▶ Delivering new ways to trade: Flexible trading arrangements that will remove barriers and make it easier for smaller players to engage with the market. This will include scheduled lite

reform that will encourage smaller players like aggregators managing direct load control, or local community batteries, to voluntarily give information on decentralised generation size, availability, and operation to AEMO so it can safely and efficiently ensure supply and demand is balanced.

- ▶ Change with technical and process reforms: to enable fit-for-purpose consumer protections so consumers can safely try different products and switch providers if they want to, simply, safely and securely.

### Visibility of DER (for B2B)

Under the status quo, DER operational data is fragmented across multiple IT systems including proprietary VPP / DER management systems (operated by aggregators), metering databases (operated by DNSPs), third-party telemetry systems (operated by DER manufacturers), and communication / dispatch platforms (operated by AEMO and in some cases, DNSPs). Throughout the stakeholder engagement process, all parties identified the lack of access to certain DER datasets as a challenge that inhibited their ability to effectively perform their respective functions. As mentioned previously, the fundamental issue is not that critical DER operational and relational data are wholly unavailable, but rather it is costly and complicated for industry participants to selectively and intentionally disclose data amongst each other under specific conditions.

### Maintaining cyber security in a decentralising power system (for B2B)

Stakeholder consultation relating to cyber security highlighted that DER operation and coordination increasingly blurs conventional boundaries between “information technology” and “operational technology”, introducing new security and reliability requirements for digital systems. All stakeholders must maintain secure and reliable communication infrastructure that extends to DER “control points” (either aggregators, or devices themselves). In the absence of widely adopted (or mandated) standards, the inherent variation in the (mostly proprietary) DER platforms and protocols currently used by DNSPs and aggregators makes it challenging to establish uniform, controlled, and auditable data exchange systems that are guaranteed to implement security and reliability standards.

## 3.2 Data Exchange Options

This section contains definitions and descriptions, summarising each network topology explored in this report, which are point-to-point, centralised, and decentralised. These have been provided to establish the necessary context to ensure alignment with the assessment of each option.

### 3.2.1 Business functions and data flows in a DER Data Hub

**Error! Reference source not found.** Figure 9 below indicates the business functions and data flows that a DER Data Hub must enable to support the DER Marketplace concept.

Each of the participants engage with the DER Marketplace for the following reasons:

- ▶ AEMO: to receive wholesale bids and offers, send dispatch instructions and receive operational telemetry (since DER is not SCADA connected).
- ▶ DNSP/DSO: to send DOEs, and also to engage aggregators in delivering network support services through the Local Services Exchange part of the DER Marketplace.
- ▶ Aggregators: to subscribe to DOEs from DNSPs/DSOs, interact with the wholesale market and engage with DNSPs/DSOs through the Local Services Exchange. As the customer representative, the aggregator has the most interactive role by delivering in both wholesale and local services.

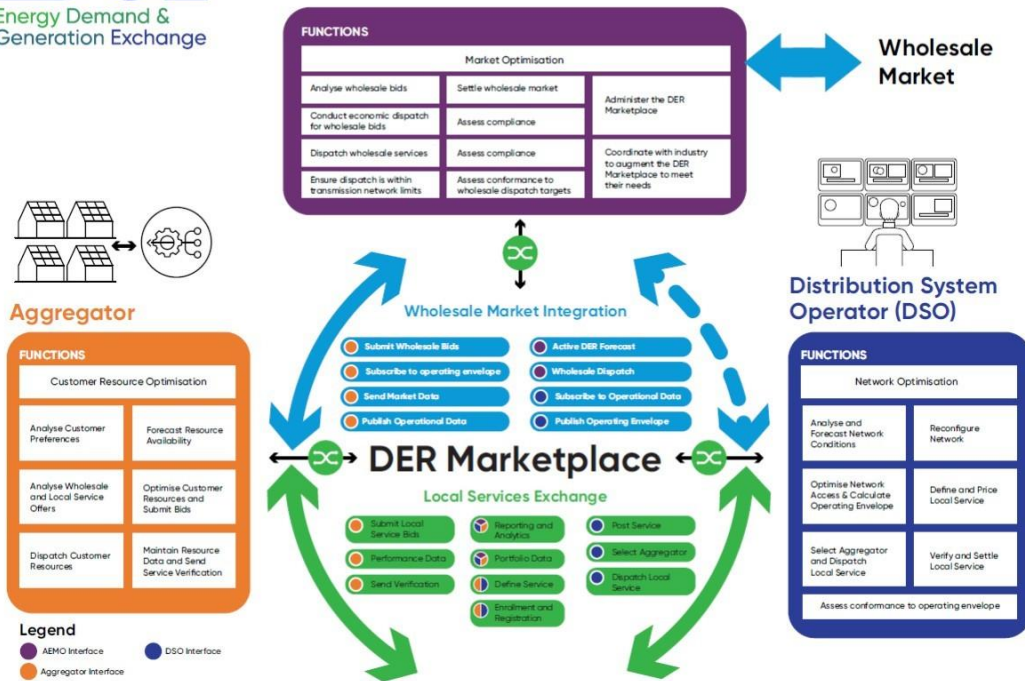


Figure 9: Functional DER marketplace interactions  
 Source: Figure reproduced from AEMO (2022)

### 3.2.2 Data Concepts

The core data concepts provide context for the scope of this report and are listed in Table 1. These data concepts indicate core data exchange concepts that represent data exchange between entities within the ecosystem.

Data Concept	Definition
Identity	Digital identities attached to all value chain actors including participants, DER devices, connection points etc. which enable permission based roles/actions to be defined.
Telemetry	Operational data at the DER device or connection point level
Dynamic Operating Envelope (DOE)	(DOEs are published by the DNSP and are provided to Aggregator and AEMO to apply distribution network limits to participant imports and exports
Standing Data	Business Rules and Reference data are specific to a participant's profile, and can be attached to the digital identities
Market Data (Bids, Offers, Dispatch)	<p><b>Bids and Offers (Boffers)</b> are submitted to the market operator (AEMO) by the Aggregator indicating their intention to deliver Wholesale Energy services for a given 5 minute interval at a specific <b>bid/offer</b> price based on their existing portfolio.</p> <p><b>Dispatch</b> instructions sent by AEMO to the Aggregator to orchestrate their DER fleet to deliver energy services at specific target levels based on the respective Boffer for a given 5-minute interval.</p>

Table 1: Core Data Concepts  
 Source: EY (2022)



### 3.2.3 High Level target state options

A Target State architecture is yet to be defined in detail. **Error! Reference source not found.** below outlines the different high level target state architecture options considered:

- ▶ Option A: Point-to-point integration
- ▶ Option B: Centralised Hub (for example, the existing e-Hub model)
- ▶ Option C: Decentralised Data Hub (DDH)

A brief description of each of these options is provided below.

#### Point-to-point (with agreed standards)

Point-to-point integration architecture is a direct connection between two or more endpoints (systems). Each further system requires its own direct connection, tightly coupling each system together with limited reuse. Point-to-point integration can be made more efficient when applied across multiple parties if a common standard for data exchange models/communication protocols is used. For example, usage of 2030.5 Common Smart Inverter Profile as a messaging protocol, with each DNSP maintaining and managing dedicated connections with each Aggregator.

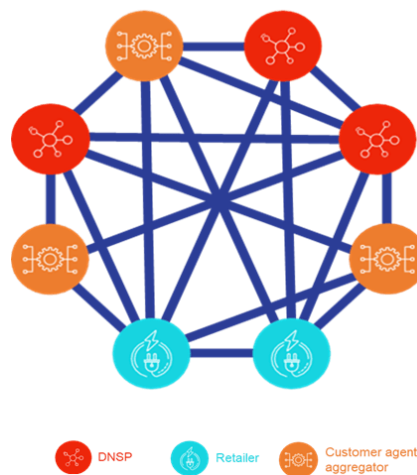


Figure 10 - Point-to-point architecture (with agreed standards)

Figure 10 represents a point-to-point design approach and demonstrates that a large network of communication channels are required in order for the system to operate at scale. Each participant needs to maintain their own data, portfolio, and communication channels to remain operational.

#### Centralised data hub

A centralised integration architecture utilises a central 'hub' to act as a broker of information between systems in place of many point-to-point connections, also known as a hub and spoke model for which the most common representation is an Enterprise Service Bus (ESB).

This architecture allows for a centralised governance authority to develop, dictate, and expose services to enabled system integrators. This typically makes data consistency and accuracy easier at the cost of centralised ownership, control, and redundancy.

Figure 11 represents a centralised design approach where AEMO is the operator and gatekeeper of the system whereby they control the integration layer over which data is transferred as well as the underlying platform infrastructure.

### Customer agent/aggregator

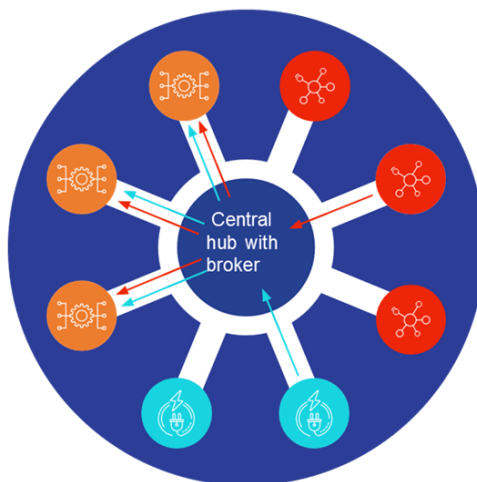
- Operates customers' DER on their behalf - either the original equipment manufacturer or their aggregator - by connecting to the centralised data hub

### DNISP

- Connects to the centralised data hub in order to communicate Dynamic Operating Envelopes to customer agents
- DOEs provide customer agents with the operating limits permitted for DER under their control in any given interval
- Connecting to the hub enables DNISPs to send DOEs to any customer agent also connected to the hub

### Retailer

- Also connects to the centralised data hub in order to communicate control signals to customer agents
- Control signals will request customer agents to reduce or stop exports from the premises to the grid at certain times (Dynamic Export Limits (DELS))
- In future retailers could also communicate dynamic "free charging" periods to EVs in their customer base (Dynamic Charging Signals (DCS))



**CHub** All connect to an industry data hub

- In a centralised data hub a broker is required to operate and manage the hub
- The broker receives data/messages from participants and directs them to the correct recipient
- For instance, the DNISP could send a list of DOEs linked to NEMs for a time period, and the broker would package and send the DOEs for each customer agent (using NEMs in their portfolio)

Figure 11 - Centralised data hub

As shown in the diagram, and as compared with the P2P topology, the hub model allows for a considerable reduction in the number of integration points required for the system to operate leading to increased efficiency and reduced costs.

In this scenario, each network participant manages and maintains their own data, portfolio, and communication channel but the AEMO provides the backbone of the infrastructure by providing standardisation and relaying information.

Example: AEMO already operates a centralised industry data hub known as the e-Hub to support a standardised B2B data exchange between market participants (for example, retailers and DNISPs to facilitate the customer switching process) and B2M data exchange between participants and AEMO.

Importantly the e-Hub also supports backward compatibility message translation so that different participants can maintain different versions of the data schema and still exchange data through the e-Hub. This is an important requirement that a future DER Data Hub should support.

The current AEMO e-Hub is governed by the Information Exchange Committee that is Chaired by AEMO but has representation from across the industry.

## Decentralised data hub

A decentralised integration architecture removes the need for a centralised broker/hub, both in terms of operations and hosting. A decentralised architecture can utilise multiple technologies to enhance scalability and platform resilience while enabling market participants to transact securely. These include:

- ▶ **Distributed Ledger Technology (DLT):** A distributed ledger is a consensus of replicated, shared, and synchronised digital data geographically spread across multiple sites, or institutions. There is no central administrator ensuring reliability and resilience. Data is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures. This is extremely hard to attack because all of the distributed copies need to be attacked simultaneously for an attack to be successful. Records are resistant to malicious changes by a single party. (Alternatives are Traditional Databases (SQL, NoSQL)).

- ▶ Decentralised Identity (DID): A trust framework in which identifiers, such as usernames, can be replaced with IDs that are self-owned, independent, and enable data exchange using distributed ledger technology to protect privacy and secure transactions. The objective is to allow a subject such as an individual or device to create their identity and manage it under their control. (Alternatives are Siloed Identities (Centralised ID, Federated ID)).
- ▶ Decentralised Data Exchange: A component which provides seamless and secure data exchange in a distributed and decentralised manner. It supports small payload - high frequency, and large payload - low frequency data exchange.

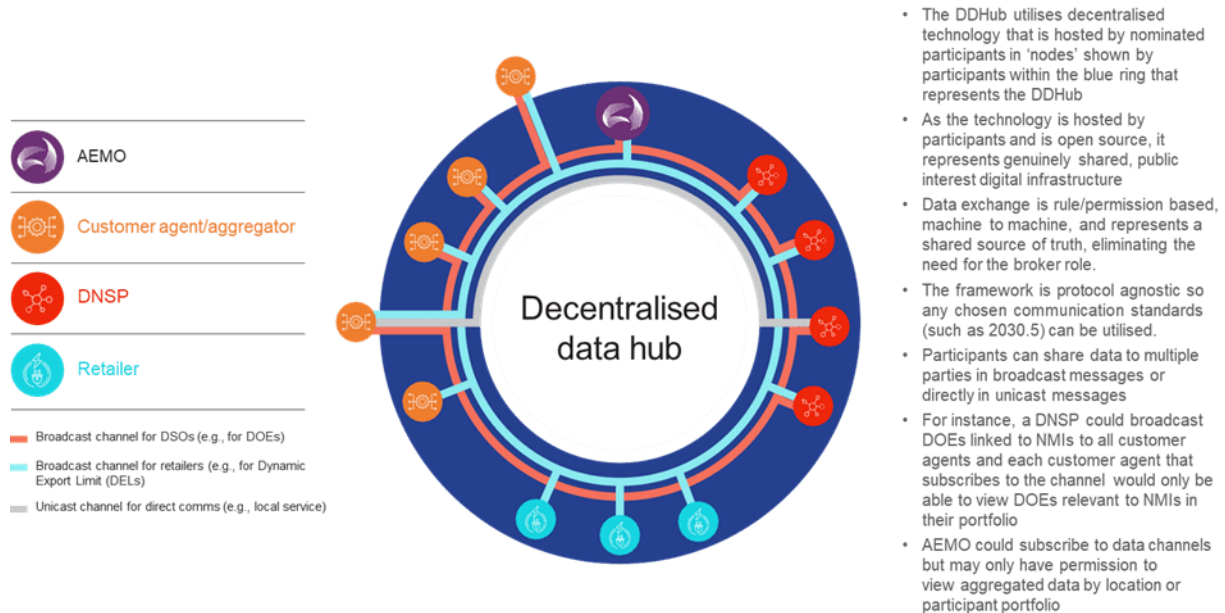


Figure 12 - Decentralised Data Hub (DDH)

Data exchanged between entities/machines is based on each underlying protocol's structure and design requirements, stored using public nodes, and governed by the rules and permissions set forth by the protocol to establish a single source of truth across a shared digital infrastructure. The result is that all network participants can join, interact, and transact over the public environment with all records being stored in a public way using decentralised nodes.

### Private vs public decentralised networks

Decentralised networks can also be privatised where the model becomes permissioned and closed to allow a single entity or a consortium (of industry stakeholders) to dictate network and data parameters. However, this deployment method can remove the core characteristics of a decentralised network being decentralised, accessible, public, and fair, while retaining the node and network architecture. This becomes a trade-off based on the permissioned model on who can join, transact and what characteristics are most important to the controlling entity or consortium.

As such, depending on the holistic architecture of the solution, several architectural choices can be made to achieve a mix of the benefits from consortium systems like scalability and that of distributed systems such as its security.

In the context of this report, the definition of 'decentralised' is utilising a public DLT using a shared public digital infrastructure. We do not prescribe whether the network be permissioned or permissionless for this assessment although it is expected that an energy industry DDH would be private and permissioned due to the critical nature of the infrastructure. The below table provides a comparison of the different distributed ledger types:

			Read	Write	Commit	Example
Distributed Ledger Types <sup>15</sup>	Public	Public permissionless (anonymous)	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned (identity)	Open to anyone	Authorised participants	All or subset of authorised participants	Corda
	Private	Consortium (identity)	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger (Project EDGE)
		Enterprise Private permissioned (identity)	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger between parent company and subsidiaries

► Table 2: DLT types across public and private (source: EY, 2022)

Examples: All network participants can join, interact, and transact over public shared infrastructure utilising shared digital infrastructure, for example, the Ethereum Blockchain. These participants all abide by a standardised governance framework and the rules of the network. Hive Power<sup>16</sup> located in Switzerland has developed a public blockchain enabled smart meter solution to verify quantities of energy produced. Developed on the Ethereum platform, this solution implements smart contracts which can be utilised by prosumers to engage in decentralised energy trading.

### 3.3 Assessment Approach

The challenge of architecting a fit-for-purpose data exchange solution for DER integration at scale is complex. To achieve a successful outcome, the architecture must align with the existing National Electricity Objective (NEO), which focuses on efficiency in the long-term interests of consumers.<sup>17</sup> Project EDGE has also developed data exchange principles and research principles that, when combined, represent Industry Success Criteria.

#### 3.3.1 Assessment Framework

The assessment framework has been broken into three distinct components to provide an end-to-end assessment methodology. The three components and their purpose are as follows:

##### 1. Success Criteria: Industry Alignment

Provides traceability and alignment back to the NEO, Project EDGE principles, and its research plan<sup>18</sup>. In doing so, the assessment framework can build upon the lessons learnt to date and relevant industry insights as part of the ongoing assessment of a digitised, decentralised power system and market.

##### 2. Assessment Criteria

<sup>15</sup> Küfeoğlu et al., 2022

<sup>16</sup> Hive Power. Available: <https://www.hivepower.tech/projects>

<sup>17</sup> AEMC. Applying the energy market objectives. Available: [https://www.aemc.gov.au/sites/default/files/2019-07/Applying%20the%20energy%20market%20objectives\\_4.pdf](https://www.aemc.gov.au/sites/default/files/2019-07/Applying%20the%20energy%20market%20objectives_4.pdf)

<sup>18</sup> Project EDGE Research Plan, 2022

Four thematic groupings of technical non-functional requirements, design principles, and governance that are critical to delivering an electricity market that has the long-term interests of consumers at its core.

### 3. Assessment Rating

The assessment rating utilises a 3 point scale defined as 1 unlikely, 2 neutral and 3 likely. The most appropriate scale point is selected to provide a measure of theoretical suitability.

Assessment Framework: Data Exchange Options		
Success Criteria: Industry Alignment	Assessment Criteria	Assessment Rating
<p><b>National Electricity Objective (NEO)</b></p> <p>To promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to:</p> <ul style="list-style-type: none"> <li>Price, quality, safety and reliability and security of supply of electricity</li> <li>The reliability, safety and security of the national electricity system.</li> </ul>	<p><b>Scalable, Stable &amp; Resilient</b> 1</p> <p>Ability for the integration approach to handle ad-hoc load (peaks and troughs incl. instability) without impacting the performance, stability and reliability of the national energy system</p>	<p>Each data exchange option will be assessed against the each of the four assessment criteria.</p> <p>The assessment rating will be measured utilising Likert scale response anchors of:</p> <p><b>Unlikely, Neutral, Likely</b></p> <p>in respect to the likelihood of the approach being suitable in achieving the purpose of the assessment criteria and the intentions of the success criteria.</p>
<p><b>Project EDGE: Data Exchange Principles</b></p> <ul style="list-style-type: none"> <li>Reduce cost, and complexity of data exchange</li> <li>Agree and implement standards</li> <li>Decouple actors and avoid hidden coupling</li> <li>Reduce barriers to entry</li> <li>Consistent user experience across regions</li> <li>Ensure data privacy, security and quality</li> </ul>	<p><b>Interoperable, Modular &amp; Flexible</b> 2</p> <p>Ability for the integration approach to support connection and communication across a diverse heterogeneous energy network (devices, systems and networks) in a coordinated and structured manner.</p>	
<p><b>Project EDGE: Research Plan</b></p> <ul style="list-style-type: none"> <li>Wholesale market participation enabled at scale</li> <li>Distribution network limits in wholesale dispatch considered</li> <li>Efficient and scalable trade of local network services enabled</li> <li>Efficient, scalable and secure data exchange enabled</li> <li>Integrated technology</li> </ul>	<p><b>Secure, Trustworthy &amp; Auditable</b> 3</p> <p>Ability for the integration approach to enable privacy-preserving energy scheduling that can be trusted to ensure the integrity of the national energy system in a transparent, integral and where required, confidential way. This includes mitigations against and considerations for cyber attacks across the future distributed national energy system</p>	
	<p><b>Standardised, Accessible &amp; Fair</b> 4</p> <p>Ability for the integration approach to enforce standardised communication protocols across the network while supporting the long term interests of consumers through ensuring market accessibility (low barrier to entry) and equitable governance and operations</p>	
		<p>Point to Point Data Exchange</p> <p>Centralised Data Exchange</p> <p>Decentralised Data Exchange</p>

Figure 13: Assessment Framework

Source: EY (2022)

## 3.4 Theoretical Assessment

This assessment determines how closely each integration hub option aligns to the assessment criteria listed in figure 13 above. The expected result of this assessment, determines which integration hub has the most positive outcome and therefore which holds long-term value.

A matrix is used to structure the assessment, grouped by the four assessment criteria. In each subsection, the three integration hub options are assessed against the key elements describing each assessment criteria, and assigned a score as follows: 1 is unlikely, 2 is neutral and 3 is likely. A score of 1 indicates minimal alignment and hence is unlikely to be used, while a score of 3 indicates close alignment and is more likely to be chosen as the preferred integration option.

Section 3.4.5, provides qualitative discussion points from the perspective of the stakeholders which have been identified.

### 3.4.1 Criteria 1 – Scalable, Stable & Resilient

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABILITY REFLECTS THE ABILITY OF THE INTEGRATION</b>	Point-to-point integration hubs are typically not scalable as the number of nodes within the environment	A centralised integration hub is more scalable when compared to a point-to-point integration approach. This is	Decentralised integration approaches require balance in three areas, being decentralisation, security, and

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>APPROACH TO ADAPT TO INCREASED DEMAND OVER SHORT AND EXTENDED PERIODS OF TIME, AS WELL AS THE EASE TO SUPPORT THIS ADDITIONAL WORKLOAD</b>	are directly proportional to the number of entities that can utilise the network. Every node will have a differing governing system and capability. As each new node will need to be manually connected to other required nodes with potentially different architecture designs makes this a time-consuming process.	due to a construction of a centralised hub, acting as a governing body whose purpose is to standardise, enforce, and provide a central information source for other ecosystem parties to use. This addresses the pitfalls of a point-to-point integration approach as all standards for capability, communication and availability can be enforced by a single entity.	scalability, and in many instances these systems skew towards decentralisation and security leaving scalability somewhat limited. However, decentralised integration hubs are still highly scalable when combined with layer 2 solutions (blockchain protocol specific to application performance).
<b>STABILITY REFLECTS THE CAPACITY OF THE INTEGRATION APPROACH TO MAINTAIN ITS STATE DURING AN ARRAY OF EVER-CHANGING EVENTS THAT MAY BE UNDESIRABLE</b>	Stability of the ecosystem relies on the availability of each node present; however, each node is subject to differing standards by their governing body, ultimately resulting in an ecosystem that contains varying availability standards and capabilities. This may then result in specific point-to-point communication links being unavailable while the rest of the ecosystem is unaffected.	While the stability of the centralised ecosystem is improved when compared to a point-to-point integration approach due to the reliance on a single central hub, it also creates a point of weakness. If this central hub is affected by any unforeseen or undesirable event, the wider ecosystem becomes unavailable.	A decentralised integration approach is the most stable integration approach due to the architecture having no single point of failure through the use of multiple decentralised nodes maintaining the network in a transparent and immutable manner. Even when a portion of these nodes go offline the decentralised network can continue to operate in an effective manner.
<b>RESILIENCY ECHOES THE CAPABILITY OF THE DATA INTEGRATION HUB TO RECOVER TO ITS ORIGINAL STATE FROM AN UNFORESEEN EVENT</b>	Resiliency of a point-to-point integration hub is complex and difficult to administer due to the number of varying architecture types, governing bodies, communication methods, capabilities, capacity, and willingness to participate. Recovering from system outages may take significantly longer than expected as many different groups will need to be organised and galvanised into finding a solution.	The restoration of a centralised integration hub is also easier to complete and administer due to the smaller number of entities, systems, hardware, and communication channels that need to be created and consulted with. However, in a similar situation to the stability of a centralised integration approach, the resiliency can be adversely affected by the design of the solution such as a single point of failure. This would lead due to data corruption or loss.	As described above, and shown in public blockchains, the availability of these systems is outstanding, with some networks not experiencing any downtime since their launch. In the event of downtime, the resiliency of these systems is exceptional due to the integrated mechanism for data storage and access that can easily be restored.
<b>SCORE</b>	<b>1</b>	<b>2</b>	<b>3</b>

### 3.4.2 Criteria 2 – Interoperable, Modular & Flexible

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISE D
<b>INTEROPERABILITY CORRESPONDS TO THE CAPABILITY OF THE INTEGRATION APPROACH TO BE USED IN A RECIPROCAL MANNER BETWEEN TWO PARTIES WITHIN THE ECOSYSTEM</b>	The interoperability of a point-to-point hub is very limiting as each node within the ecosystem needs to establish a communication channel with other required nodes existing in the same ecosystem. While there can be bi-directional communication between two nodes it is unlikely to form between multiple nodes limiting the exchange of information. Although agreeing a standard data model and communication protocol can make the point-to-point solution more replicable, there may be small differences in how each party implements a standard that can reduce interoperability, and scalability of the approach.	A centralised integration hub provides improved interoperability compared to a point-to-point integration hub as all nodes within the ecosystem can readily share and use information using the central hub while also maintaining their own personal data.	Decentralised networks forego interoperability, modularity, and flexibility of the underlying network infrastructure, protocols, consensus, and other mechanisms in favour of enabling a global network operated in a standardised, secure, and consistent manner.  Unlike current web applications, distributed ledger technologies have the opposite value proposition whereby value is captured by the fact that the underlying protocol is difficult to change in favour of providing a standardised and interoperable ecosystem for all users and network participants.
<b>MODULARITY OF THE INTEGRATION APPROACH IS DETERMINED BY ITS ABILITY TO FACILITATE NEW PROJECTS AND SYSTEMS BY PROVIDING A STANDARDISED PLATFORM TO BUILD UPON</b>	A point-to-point integration hub does not provide a modular framework to build from by design. Every node operates under a fixed contract agreement. This makes it difficult for new players to build their platform, communicate with established nodes, and provide relevant data to the network.	A centralised hub provides the ability for newcomers to leverage a standardised, well documented, and accessible framework in which to build their product, hence a centralised integration hub provides additional modularity than a point-to-point method.	Once decentralised technologies are implemented and accepted by the community, they become very interoperable, and modular. Decentralised applications enable different users to design and develop specific applications to meet their needs, whilst using the standardised underlying components to enable interoperability.
<b>FLEXIBILITY IS PORTRAYED AS THE CAPABILITY TO SUPPORT A WIDE RANGE OF PROJECTS AND SYSTEMS WHICH MAY REQUIRE DIFFERING DESIGN CHOICES</b>	The point-to-point integration approach offers flexibility to the ecosystem and newcomers which can be a desirable attribute. However, where any entity can design and implement its system, differences between systems lead to inefficiencies at a system wide level as the number of solutions proliferates.	A centralised hub can support a wide range of use cases, but flexibility is somewhat limited through standardisation and changes proposed to the ecosystem needs to be reviewed, approved, and finally implemented by the governing body which can take some time.	Public decentralised infrastructure is highly flexible as any party can design, implement, and maintain their system or project in line with the feature set provided by the decentralised ecosystem. However, private or permissioned approaches may face similar delays to reviewing/approving changes as centralised approaches depending on the Governance framework.
<b>SCORE</b>	<b>1</b>	<b>2</b>	<b>2</b>

### 3.4.3 Criteria 3 – Secure, Trustworthy & Auditable

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SECURITY ALIGNS TO THE PRECAUTIONS THAT HAVE BEEN TAKEN BY THE INTEGRATION METHOD HUB TO GUARD AGAINST ATTACK, SABOTAGE, AND VULNERABILITIES</b>	Security of a point-to-point integration hub is difficult to manage and govern as several entities, technologies, designs, capabilities, and monitoring method exists. This leads to poor communication channels between entities, blurred lines of ownership and responsibility, and heightened attack landscape resulting in additional security threats. In addition, in the event of a security breach, coordination across several environments and entities will be difficult to conduct which may increase the risk of further compromise or damaging effects.	As a centralised integration model removes the number of entities, standards, designs, and technologies the attack surface is decreased when compared to point-to-point integration hub. In addition, the single governing entity has far more control over how security is implemented, maintained, and monitored which is likely to result in a more effective security operations, particularly if it is considered national critical infrastructure. However, consolidation of governance and control leads to a central point of weakness where any attack on this central entity or hub can have devastating effects.	As described in Section <b>Error! Reference source not found.</b> a decentralised integration approach operates as a global network with shared and standardised infrastructure reducing the attack surface and the likelihood of vulnerabilities. As all parties utilise the same infrastructure, design, and implementation, their security capabilities and monitoring activities do not work against each other as shown in a point-to-point integration hub, but rather provide additional security layers. This results in a more secure shared environment as any vulnerabilities or attack vectors are more likely to be found and corrected due to more parties being aligned and involved.
<b>TRUSTWORTHINESS IS DICTATED BY THE USERS AND EXTERNAL ENTITIES CONFIDENCE, DEPENDENCE, PRIVACY, AND PERCEIVED INTEGRITY IN THE ECOSYSTEM</b>	The trustworthiness of a point-to-point integration hub is similar to the security aspect, where several entities, technologies, designs, and standards make it difficult to determine the correctness and accuracy of the wider ecosystem. In many cases an entity will trust their own system and perhaps the nodes they directly interact with, however, trust outside of this circle becomes difficult without a large investment of time and effort.	In similar fashion to the consolidation of duties and governance shown above, the trust of the system is also consolidated into a single point. The governing entity and hub need to maintain a trustworthy role and leadership stance, with a level of independence, to ensure that other parties within the ecosystem feel supported and that the data and services provided can be relied upon.	A decentralised integration hub offers the most trustworthy system of all three approaches. In a public DLT platform, no single entity has complete control to view, write, or modify the protocol. In a permissioned platform, any change conducted can be seen and verified by other parties which results in a highly transparent ecosystem. Furthermore, any change or modification is also immutable increasing trust in the platform.
<b>AUDITABILITY RELATES TO HOW EASILY THE ECOSYSTEM CAN BE EXAMINED FOR CORRECTNESS AND ACCURACY BY A 3RD PARTY</b>	As described above the number of entities, designs, technologies, and standards present within a point-to-point integration hub is a significant pitfall and affects the auditability of the ecosystem as well. Due to the large number of differences, audit complexity, time to completion, and cost will increase.	Auditability is significantly easier when compared to a point-to-point model as the number of entities, designs, standards, and technologies is minimised. This reduce the complexity, time and cost of the audit. A standard model also allows for the audit team to make use of automation which can improve audit speed and reliability.	Auditability is excellent as all data, transactions, and events are public within the ecosystem. For permissioned platforms, auditors can be given additional functionality to see all network activity and data increasing their efficiency and therefore reducing the cost of the audit. Standardisation of the protocol, events, data, and transactions also allows for quicker and more streamlined audits to occur as this procedure is unlikely to change significantly.
<b>SCORE</b>	<b>1</b>	<b>2</b>	<b>3</b>



### 3.4.4 Criteria 4 – Standardised, Accessible & Fair

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>STANDARDISATION BEING ALIGNED TO AN AGREED UPON FORMAT, APPROACH, AND DESIGN OF SYSTEMS, DATA, AND COMMUNICATION</b>	As dictated by its architecture design, a point-to-point integration approach cannot be standardised effectively as several entities are present all with varying requirements and perspectives. In some situations, a point-to-point ecosystem can standardise certain elements such as communication methods however, standardisation to the whole ecosystem across a range of areas is challenging.	Standardisation is a core concept and feature of a centralised integration model, and it is much easier to enforce at an ecosystem level. This is due to limiting the governance duties of network participants and passing these duties to the sole governing entity which also controls and manages the central hub. This results in a governing body that can make informed decisions on design, technologies, and standards on behalf of the wider community.	Due to the architecture design of a decentralised integration platform, the underlying protocol is an ecosystem wide standard which is not easily changed or manipulated. The effect of this is that all entities and projects design their systems according to the features available to them which is dictated by the decentralised protocol. Hence all applications, regardless of when they were developed or who they were developed by, maintain the ability to communicate and be effective within the ecosystem.
<b>ACCESSIBILITY RELATES TO THE USABILITY, OBTAINABILITY, AND EASE OF ACCESS TO THE UNDERLYING SYSTEM AND SUPPORTING FEATURES, INCLUDES THE LEVEL OF BACKWARDS COMPATIBILITY THAT IS SUPPORTED FOR PARTICIPANTS THAT UPGRADE THEIR SYSTEMS AT DIFFERENT TIMES</b>	Accessibility of a point-to-point integration approach from an understanding, documentation, research, and skill availability viewpoint is readily attainable as they have been used in industry for several years. However, failure to standardise on ecosystem features such as communication will make this more complex for relevant parties.	Accessibility of a centralised integration is high as typically there is better, more complete and accurate specifications, APIs and communication standards. However, onboarding applications and changes to technology standards or applications need to be approved by the governing body which can be a point of limitation due to resource availability. In addition, technical debt may increase over time reducing the competitiveness or effectiveness of the ecosystem.	The open and permissionless nature of public DLT solutions which enable a decentralised data exchange promotes the long-term interests of consumers as the networks are designed to have a low barrier of entry to allow anyone to interact, build upon, and be part of the broader ecosystem. Private decentralised solutions still enable easy access for those that are eligible to use the system, however, adds a layer of governance that may be appropriate. Implementing an open system promotes innovation in an ecosystem and enables more participants to get involved. The use of a public blockchain, such as Ethereum is a good example, it's the most widely used open platform by developers <sup>19</sup> .
<b>FAIRNESS ENSURES THAT THE UNDERLYING INTEGRATION HUB CAN BE UTILISED BY ALL PARTIES, HAS LOW BARRIERS TO ENTRY AND COSTS ARE ALLOCATED FAIRLY TO USERS</b>	The point-to-point integration model is fair among ecosystem participants and newcomers as no favouritism to a specific design choice, database schema, or network standard exists or is enforced. It is equally available and fair to existing entities and newcomers wanting to establish themselves within the ecosystem. However, while large organisations may have the resources to build and manage bespoke integrations, the initial costs would likely prevent smaller players from entering the market.	The fairness of the centralised integration approach is dictated in a similar way to the trustworthiness of the system, as all disputes, favouritism, design choices, and industry alignment are decided by the governing body. Therefore, if the governing body is not acting fairly and in the best interest of users and entities, the ecosystem suffers as a result. With regard to cost allocation, the cost to operate a centralised hub is met by the entity responsible and recovered through those channels. In the case of the e-Hub operated by AEMO, the costs are recovered across all NEM participants, meaning the costs to add new	A decentralised data hub is inherently designed to favour consumer interests fairly and transparently, unlike that of a point-to-point or centralised integration hub. In the event of change proposed by the community, the protocol can be altered, but this change is ultimately proposed and accepted by the community rather than a single governing entity.  In the case of a private, permissioned decentralised hub a governing body/committee would determine the ongoing changes and development of the system, which is a similar governance model to the centralised approach.

<sup>19</sup> Consensys, 2022

ASSESSMENT ELEMENT	POINT-TO-POINT	CENTRALISED	DECENTRALISED
		DER use cases that only apply to DER customers would be cross subsidised by non-DER customers, thereby reducing its fairness in this case.	<p>With regard to cost recovery, in a decentralised approach the infrastructure and associated costs are decentralised to participants. As a result, their costs to host the infrastructure can be allocated more directly to the customers that benefit from it. In the case of the DDH, the costs can be allocated directly to DER customers through network or retail tariffs arrangements, creating a fairer cost recovery process than a centralised approach.</p> <p>A standardised DLT solution in a decentralised environment offers improved technical change management. For example, changes to the data transmission are completed at the network layer as opposed to the application layer.</p>
SCORE	1	2	3

### 3.4.5 Data Exchange Options by Stakeholder Assessment Matrix

Table 2 below, is a matrix that includes qualitative discussion for all assessment criteria for each integration option from the perspective of identified stakeholders. The assessment criteria can be found on the Y axis, with the three competing approaches along the X axis. This is then further broken down into each stakeholder's viewpoint with specific commentary being included to provide a qualitative user story.

CONSUMERS			
	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABLE, STABLE &amp; RESILIENT</b>	<ul style="list-style-type: none"> <li>A point-to-point integration approach may work sufficiently for DNSP DOE use cases, but it will not support other use cases as DER scales, such as retailers sending signals to agents/OEMs to manage negative price exposure. Therefore, consumers will not receive offers from Retailers that could incentivise them to allow retailers to manage their exports.</li> <li>An unstable ecosystem may mean that there are material differences in the customer experience between regions if some regions experience more system downtime than others.</li> </ul>	<ul style="list-style-type: none"> <li>A centralised integration hub (such as the eHub) may support new DER use cases, but a centralised hub may not be suitable for the scale of data throughput required as DER proliferates</li> <li>Stability is improved compared to a point-to-point integration approach however, any significant event that impacts the central governing body or hub is likely to be significant and adversely affect the wider ecosystem</li> <li>The operator is able to spend more resources on maintaining high availability systems to deliver greater resilience for consumers (although this can also create a single point of failure risk)</li> </ul>	<ul style="list-style-type: none"> <li>A decentralised integration approach will be able to scale to the required range for both onboarding and throughput as throughput can be improved via scaling solutions, and onboarding is conducted in a public and standardised way by aggregators and consumers</li> <li>This ecosystem can withstand significant interruption and still service consumers due to the shared multi node architecture, giving consumers confidence in the system's stability</li> <li>Decentralised integration approaches offer the most resilient system by removing a single point of failure risk.</li> </ul>
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>	<ul style="list-style-type: none"> <li>Point-to-point integration approaches add unnecessary costs to consumers (indirectly) due to the number of communication connections required</li> <li>Flexibility of consumer choice is likely to be hindered as aggregators need to connect to so many varying systems, creating a barrier to entry for aggregators and making it difficult to develop simple and consistent offers to consumers to allow them to use their DER to deliver wholesale and local services</li> </ul>	<ul style="list-style-type: none"> <li>Standardised formats for data exchange increase the interoperability between ecosystem participants, for example, between aggregators/agents and DNSPs or retailers</li> <li>Standardisation enables many more participants to interact with each other – for example, retailers could connect with hundreds of customer agents/OEMs, which would be difficult point-to-point</li> <li>Consumers benefit from greater choice of offers from aggregators and retailers on how their DER can be utilised.</li> </ul>	<ul style="list-style-type: none"> <li>Like centralised approaches, interoperability standards can be implemented within the ecosystem, creating system efficiencies that reduce overall costs for consumers.</li> <li>The protocol provides the modular building blocks for network participants that may be a more efficient way to grow the system as DER proliferates (centralised approaches can also be modular)</li> </ul>
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>	<ul style="list-style-type: none"> <li>Security appears as a black box to consumers as they cannot verify or attest to the systems durability or availability</li> <li>Consumers are unable to view ecosystem activity and therefore cannot attest to the trustworthiness of the integration hub</li> <li>Consumers are unable to provide verification over their own estate as information is unavailable and privatised so heavy reliance is placed on node providers</li> </ul>	<ul style="list-style-type: none"> <li>Consolidation of infrastructure and standards reduces the DER attack vectors and increases security, although having all use cases flow through a single hub raises a single point of failure and redundancy risk that could have a greater impact on consumers in the unlikely event of attack/failure.</li> <li>The centralised governing body can invest more in security and be more easily held accountable to ecosystem disruption and failure to resolve and prevent malicious attack</li> <li>Centralised systems can have more frequent audits providing consumers with confidence in cyber security of system</li> </ul>	<ul style="list-style-type: none"> <li>Security of the ecosystem is opened to consumers through open-source technology which allows for additional eyes and skills to verify and resolve potential threat vectors</li> <li>All ecosystem participants from node operators to consumers can view network history, data, and current transactions to increase the trustworthiness of the system</li> </ul>
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>	<ul style="list-style-type: none"> <li>A point-to-point integration hub may limit the amount of uses cases for DER data exchange – for example, retailers will struggle to integrate with tens or hundreds of customer agents/OEMs</li> <li>This will limit choice of retail offers made to consumers</li> <li>Higher barriers to the ecosystem (for instance needing resources to integrate with many different systems) inherently makes the ecosystem unfair, (for example, as smaller retailers will not be able to integrate with many PV OEMs to send zero export limits that manage negative price exposure)</li> </ul>	<ul style="list-style-type: none"> <li>Standardisation of ecosystem parameters expands the number of participants that can share data and control signals</li> <li>Accessibility can still be restricted if newer standards are proposed but take the governing body time to implement.</li> <li>A centralised integration model is fair amongst participants but can skew towards unfair if the cost recovery is spread across all participants (for example, non DER owning consumers)</li> </ul>	<ul style="list-style-type: none"> <li>A decentralised integration approach provides the most standardised framework and therefore should provide the most support for varying participants</li> <li>Accessibility is high as the use of decentralised identities and verifiable credentials enable easier customer switching between portfolios.</li> <li>A decentralised approach could more easily allocate the costs of the infrastructure to DER consumers (for example, if DNSPs hosted the infrastructure and allocated costs to DER consumers through network tariffs)</li> </ul>
AGGREGATORS			
	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABLE, STABLE &amp; RESILIENT</b>	<ul style="list-style-type: none"> <li>Point-to-point integration approaches mean aggregators/OEMs need to integrate directly with every DNSP and every retailer/other participant who wants to send control signal to</li> </ul>	<ul style="list-style-type: none"> <li>A centralised integration approach provides additional certainty and comfort to aggregators that their direct network will not be interrupted unnecessarily or unpredictably</li> </ul>	<ul style="list-style-type: none"> <li>Like the centralised model, a decentralised integration model offers the aggregators a single integration platform that is readily</li> </ul>

AGGREGATORS			
	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>	DER, which is not scalable at 100 GW scale (due to the lifecycle management complexity in number of DER devices)	<ul style="list-style-type: none"> <li>▶ Aggregators are provided with a stabilised and standardised platform in which to work from, which increases productivity due to reduced downtime and automation availability</li> <li>▶ Aggregators are more certain of where their information and their consumers information are held making backup and restoration procedures easier to execute</li> </ul>	available and scalable to meet their growing needs with lower cost/effort
	<ul style="list-style-type: none"> <li>▶ The stability of the directly linked ecosystem is determined by multiple parties where any downtime of supporting nodes also affects your own which affects your DER portfolio and consumers</li> <li>▶ Backup and recovery of all critical information is difficult to obtain as it may be spread across a range of nodes, data schemas, and standards resulting in an inefficient system</li> </ul>	<ul style="list-style-type: none"> <li>▶ Easier communication across the ecosystem allows aggregators/agents to communicate more effectively with DNSPs and retailers, saving time and money</li> <li>▶ Providing frameworks and standards to the ecosystem means that newcomers have modular building blocks in which to utilise and progress projects</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aggregators are provided with a highly resilient system where their data is stored and maintained by multiple nodes in a private way ensuring that data is always available and accurate</li> </ul>
	<ul style="list-style-type: none"> <li>▶ Agreeing data model/communication standards may improve interoperability but implementation may still have small differences and they may not apply to all use cases</li> <li>▶ Reduced modularity means aggregators need to interact with many systems to modify and update their DER</li> <li>▶ Flexibility is provided to aggregators in how they construct their portfolio due to reduced standards, but may leave the aggregator with technical debt</li> </ul>	<ul style="list-style-type: none"> <li>▶ All stakeholders are aligned to improve the security of the globally shared protocol further aligning efforts which reduce the risks of vulnerabilities</li> <li>▶ As the underlying protocol is immutable and transparent aggregators can ensure that the platform remains trustworthy and identify malicious behaviour</li> <li>▶ As the decentralised integration model is public and visible to all, any aggregator can conduct an audit and even share results to other stakeholders for further analysis</li> </ul>	
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>	<ul style="list-style-type: none"> <li>▶ Aggregators do not have the certainty that the nodes they interact with have the same security capability, skills, and monitoring activities that they do</li> <li>▶ Trust between aggregators and their direct communication channels is limited and non-existent between unknown nodes and services</li> <li>▶ Aggregators can only audit their own infrastructure, data, and communication channels</li> </ul>	<ul style="list-style-type: none"> <li>▶ Centralised integration approaches improve ecosystem security as goals, procedures, hardware, and operations are aligned to work together</li> <li>▶ The centralised hub absorbs the trust for all aggregators and provides a trusted service, however failure to be transparent or trustworthy will affect the aggregator and their consumers</li> <li>▶ Aggregators can continue to audit their own direct systems and can obtain an audit from the centralised entity but do not know the status of other stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aggregators have increased accessibility to the wider ecosystem improving their insights, productivity, and ability to respond to events</li> <li>▶ Aggregators can more easily communicate with any party also connected to the decentralised hub, without needing to go through a central data broker, resulting in an ecosystem that supports stakeholder wide fairness</li> </ul>
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>	<ul style="list-style-type: none"> <li>▶ Lack of standardisation in the ecosystem makes it difficult for aggregators to perform daily duties outside of their direct systems</li> <li>▶ The need to integrate with many systems (potentially with differing standards) consumes significant investment to support and acts as a barrier to entry</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aggregators can more easily perform duties due to standardisation on input and output</li> <li>▶ New aggregators can more easily establish a foothold within the ecosystem and establish a DER portfolio adding to the accessibility of the wider ecosystem</li> <li>▶ A centralised integration approach established the central governing body as a mediator between disputes increasing the effectiveness of the ecosystem</li> </ul>	

DNSP'S / DSO'S			
	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABLE, STABLE &amp; RESILIENT</b>	<ul style="list-style-type: none"> <li>▶ Point-to-point solutions may be scalable for each DNSP from their own perspective as the onus is on aggregators/agents to connect to the DNSP systems</li> <li>▶ The need to maintain high availability and highly cyber secure systems adds cost and resources to DNSP budgets, and duplication across DNSPs add cost to the overall system.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Having a central authority managing the data integration hub allows DNSPs to focus resources on network operations, but DNSPs would lose autonomy of systems to communicate with aggregators/agents</li> <li>▶ DNSPs could be part of industry committee to govern the centralised hub but changes could take time to be designed, approved and implemented that may impact DNSP operations and their ability to respond to opportunities.</li> </ul>	<ul style="list-style-type: none"> <li>▶ A global protocol allows the DNSP to include all known and online DER installations or DER portfolios into the network optimisation and reporting</li> <li>▶ A decentralised integration model may enable DNSPs to more easily be given access/permissions to more data (including on a commercial basis) that can help them operate their networks</li> <li>▶ As the decentralised integration hub is the most resilient the DNSP can continue to provide DOE and pricing to local services regardless of other events</li> </ul>
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>	<ul style="list-style-type: none"> <li>▶ From a DNSP perspective the need for interoperability and flexibility is lower than for aggregators/agents (who need to interact with each DNSP and retailer)</li> </ul>	<ul style="list-style-type: none"> <li>▶ DNSPs can utilise the interoperability of a centralised hub to gain additional insights by utilising additional data sources, such as visibility of planned curtailment of customer PV exports in response to</li> </ul>	<ul style="list-style-type: none"> <li>▶ A decentralised integration approach can bring a level of autonomy back to DNSPs about how they support the decentralised infrastructure and can enable DNSPs to develop their own</li> </ul>

DNSP'S / DSO'S			
POINT-TO-POINT	CENTRALISED	DECENTRALISED	
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>	<p>forecast negative prices. This will enable DNSPs to factor this into the calculation of DOEs for other customers.</p> <ul style="list-style-type: none"> <li>▶ DNSP's will have flexibility to join and use the centralised hub as and when they need to, without having to develop their own systems in advance of their anticipated need.</li> <li>▶ Centralised integration models collate data and communication making operational processes easier to design, administer, and maintain</li> <li>▶ Change management complexity relating to backwards compatibility for technology, data standard changes</li> </ul>	<p>innovative decentralised applications, for example, for their own Local Service Exchange</p> <ul style="list-style-type: none"> <li>▶ Improved change management relating to backwards compatibility for technology, data standard changes. This is completed in an abstract way at a protocol level via a soft or hard fork.</li> </ul>	
	<p>Under this approach DNSPs have greater autonomy over how they develop and maintain their systems and can react faster to make changes if required.</p> <p>Change management complexity relating to backwards compatibility for technology, data standard changes.</p>	<p>In a centralised integration model security vulnerabilities are lessened and therefore the chance of breach is decreased which will allow DNSPs to continue to operate in an efficient way</p> <p>DNSPs will be able to reduce their cyber threats as the risk is transferred to the centralised hub, enabling the DNSP to focus resources on core competencies Centralised ecosystems will provide some comfort in DNSP reporting, tools, and audits; however, this ultimately heavily relies on the governing body and central hub</p>	<p>Decentralised ecosystems will allow DNSPs to perform their duties regardless of what network events occurs due to the improve resiliency and availability</p> <p>Decentralised ecosystems will provide additional trust than centralised integration approaches as data is transparent and immutable</p> <p>DNSPs will be able to more easily perform audits of the tools, reports, and forecasts as correct and accurate information is readily available</p>
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>	<p>Replication of systems, capabilities and resources across DNSPs will reduce efficiency and fairness of overall system for consumers</p> <p>DNSPs would have easy access to their own systems, however, would not have any visibility of signals that retailers may send to aggregators/agents to reduce exports during negative price periods. This may mean that DNSPs impose unnecessarily lower exports on other customers, reducing the fairness and efficiency of network utilisation.</p>	<p>New DNSPs will find it easier to get up to speed on each aggregators systems and reporting requirements due to standardisation, however, this will need to be repeated for each aggregator</p> <p>A centralised ecosystem should establish a baseline assessment and reporting system to ensure that DNSPs do not favour certain sections of the network</p> <p>Even with a centralised asset register it is likely that DNSPs would maintain their own customer asset register and portfolio management tool, particularly if using an independently developed Local Services capability</p>	<p>As the decentralised integration option provides standardisation across the ecosystem the DNSPs can develop automation tools to increase their effectiveness and productivity</p> <p>A decentralised ecosystem will remove the potential biasness as all aggregators and DER portfolios can be reported on in a holistic manner</p> <p>A decentralised hub and asset registry could enable a single source of truth of customer assets, VPP portfolios and aggregator switching so that DNSPs do not need to maintain their own separate records (for example, DER Registers)</p>
ALL OF SYSTEM			
POINT-TO-POINT	CENTRALISED	DECENTRALISED	
<b>SCALABLE, STABLE &amp; RESILIENT</b>	<p>Construction of a centralised governing body allows for enforcement of standards across availability, communication, and security increasing the scalability of the ecosystem</p> <p>A well designed, implemented, and available centralised hub to take the brunt of the ecosystems communication increase stability however introduces a central point of weakness</p> <p>Resiliency is improved as communication and data storage is consolidated to a single point making backup and recovery procedures more straightforward</p>	<p>A shared DLT platform once implemented and accepted by the community will provide scalability as dictated by the protocols TPS (Transactions per Second) and number of nodes deployed</p> <p>The DLT protocol can continue to operate effectively if one or several nodes in the ecosystem are unavailable making it extremely stable</p> <p>Resiliency of the protocol is aligned to the transparent, immutable, and censorship resistant model where data and communication can easily be restored</p>	
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>	<p>Point-to-point integration models are limited in their interoperability as each communication channel to other network participants need to be manually created and communication between multiple nodes (at least 3) is rare</p> <p>Due to the large variation in standards, design, and architecture choices does not make the ecosystem modular</p> <p>Flexibility is available but this is a biproduct of no enforcement of standardisation, architecture, design, and communication</p>	<p>Improved interoperability is available in a centralised integration hub as the central hub takes on a leadership and standardisation role</p> <p>With increased standardisation also provides modularity to the ecosystem as newcomers find it easier to integrate and maintain their systems and applications</p> <p>Flexibility is somewhat limited as long processing times can be present due to the capability and availability of the governing body and the centralised hub</p>	<p>DLT platforms forego interoperability, modularity, and flexibility of the underlying infrastructure, protocols, and consensus in favour of enabling a global, distributed, standardised, and secure ecosystem</p> <p>Once established and accepted the DLT platform becomes interoperable, modular, and flexible within the bounds of the agreed upon rules</p>

ALL OF SYSTEM			
	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>	<ul style="list-style-type: none"> <li>▶ The threat landscape of a point-to-point ecosystem is immense as each new addition of an architecture, design, or communication method increases attack vectors</li> <li>▶ Trust extends to only nodes in close proximity that are interacted with directly, nodes outside of this circle are unknown and cannot be trusted</li> <li>▶ Audit complexity, price, and time to completion is high as the number of varying entities and nodes differences is also likely to be high</li> </ul>	<ul style="list-style-type: none"> <li>▶ Centralised integration models remove the number of nodes, standards, architecture choices, and communication methods which in turn reduces the threat landscape</li> <li>▶ Consolidation of governance, data, and standards increases the trustworthiness of the ecosystem but also creates a single point of corruption and collusion</li> <li>▶ Centralised data and governance reduce audit complexity, price, and time to completion and in addition allows for audit automation</li> </ul>	<ul style="list-style-type: none"> <li>▶ Changes can be made to the protocol to increase flexibility, interoperability, and modularity and is governed by the community consensus</li> <li>▶</li> <li>▶ Security of a decentralised system is exceptional as all interacting parties can combine their capability, availability, and skill sets to investigate vulnerabilities and patch accordingly</li> <li>▶ Due to the immutability, transparency, and censorship resistant model, a decentralised integration hub provides the most trustworthy ecosystem</li> <li>▶ Auditability of a decentralised integration model is excellent as all data, transactions, and events can be publicly reviewed for accuracy and validation</li> <li>▶</li> </ul>
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>	<ul style="list-style-type: none"> <li>▶ As many varying entities and nodes are present with differing technical implementations makes standardisation challenging across the ecosystem</li> <li>▶ Skill availability, documentation, and research is readily attainable for architects however technical debt will be accumulated by each party present</li> <li>▶ A point-to-point integration ecosystem is fair among participants and newcomers as no favouritism exists to a specific design choice, standard or data schema. However, this may create an unruly ecosystem which is impossible to manage and maintain</li> </ul>	<ul style="list-style-type: none"> <li>▶ Centralised integration approaches improve standardisation as a single governing entity is in control which can dictate and enforce ecosystem parameters</li> <li>▶ Accessibility of these integration models is high as a more complete knowledge base, API, and communication standards exists making it easier for newcomers to get started</li> <li>▶ Fairness of the ecosystem is controlled by the governing body, where if the governing body is acting in the best interest of participants, then the system is fair, however, if it does not then the entire ecosystem suffers</li> </ul>	<ul style="list-style-type: none"> <li>▶ Due to the underlying design of the protocol and the network, the decentralised ecosystem is standardised for all ecosystem participants</li> <li>▶ The open and permissionless nature of the DLT platform works in unison with participant long-term interests which decreases barrier to entry</li> <li>▶ A decentralised integration hub inherently favours consumer interests fairly and transparently where all changes and governed by the community</li> </ul>

Table 2: Data Exchange Options – Theoretical Assessment by Stakeholder Source: EY (2022)

### 3.5 Assessment Summary

The below table summarises the findings and discussion contained in Section 3.4. The four assessment criteria have been given numerical weights between 1 and 3 to indicate the likelihood of their architecture suitability. For a more detailed description of this scale, please refer to Section 3.3 - Assessment Approach.

The table below contains the scores for each data exchange option categorised by assessment criteria, as well as rating which indicates the total suitability of the architecture design.

	POINT-TO-POINT	CENTRALISED	DECENTRALISED
<b>SCALABLE, STABLE &amp; RESILIENT</b>			
<b>ASSESSMENT RATING</b>	1 Unlikely	2 Neutral	3 Likely
<b>INTEROPERABLE, MODULAR &amp; FLEXIBLE</b>			
<b>ASSESSMENT RATING</b>	1 Unlikely	2 Neutral	2 Neutral
<b>SECURE, TRUSTWORTHY &amp; AUDITABLE</b>			
<b>ASSESSMENT RATING</b>	1 Unlikely	2 Neutral	3 Likely
<b>STANDARDISED, ACCESSIBLE &amp; FAIR</b>			
<b>ASSESSMENT RATING</b>	1 Unlikely	2 Neutral	3 Likely
<b>AVERAGE</b>			
	<b>Point-to-point</b>	<b>Centralised</b>	<b>Decentralised</b>
<b>INTEGRATION HUB AVERAGE</b>	1 Unlikely	2 Neutral	2.75 Likely

Table 3: Assessment Summary  
Source: EY (2022)

As shown in the table above, a decentralised integration approach is assessed as the most suitable architecture design for an integration approach to comply with the four assessment criteria, being Scalable, Stable & Resilient (1), Interoperable, Modular & Flexible (2), Secure, Trustworthy & Auditable (3), Standardised, Accessible & Fair (4).

The decentralised approach also aligns with the long-term efficiency focus of the National Electricity Objective<sup>20</sup>, and enables more accurate allocation of costs onto DER consumers.

<sup>20</sup> AEMC. Applying the Energy Market Objectives. Available: [https://www.aemc.gov.au/sites/default/files/2019-07/Applying%20the%20energy%20market%20objectives\\_4.pdf](https://www.aemc.gov.au/sites/default/files/2019-07/Applying%20the%20energy%20market%20objectives_4.pdf)

### 3.6 Transition to Decentralised Energy System and Technology

The foundation for this report considers how data exchange approaches should evolve in line with an ever-increasing penetration of distributed energy resources (DER). The move towards DER is a move towards decentralisation, placing the focus on customers/prosumers.

Decentralised technology components such as decentralised identities and DLT is a shift in supporting business and technology decentralisation, aligned to the proliferation of DER.

Using decentralised technologies requires a shift in mindset, in essence the focus is to move away from centralisation and therefore control and management under traditional arrangements are rewired to support this outcome. Table 4 highlights a small subset of global projects and companies that have developed open and closed decentralised solutions for energy applications.

#	Company & project	Scope	Platform	Location
1	Alliander & Spectral Energy (Jouliette at De Ceuvel)	Decentralised energy trading	MultiChain	Netherlands
2	Bankymoon	Metering, billing & security	Ethereum	South Africa
3	Blockchain Futures Lab	General purpose initiatives & consortia	N/A	US
4	Car eWallet	Electric e-mobility	Hyperledger Fabric	Germany
5	CarbonX	Green certificates & carbon trading	Ethereum	Canada
6	CGI & Eneco	Metering, billing & security	Tendermint	Netherlands
7	DAISEE	IoT, smart devices, automation & asset management	Ethereum	France
8	Electron	Grid management	Energy Web (Ethereum-based)	UK
9	eMotorwerks	Electric e-mobility	Ethereum	US
10	Endesa Energia (Blockchain Lab)	General purpose initiatives & consortia	n/a	Spain
11	Energy Web Foundation	General purpose initiatives & consortia	Energy Web (Ethereum-based)	Switzerland
12	Grid Singularity	Grid management	Energy Web (Ethereum-based)	Austria
13	Hive Power	Decentralised energy trading	Ethereum	Switzerland
14	LO3 Energy	Micro Grids, Decentralised energy trading	Tendermint, Proprietary	US
15	Poseidon	Green certificates & carbon trading	Stellar	Switzerland
16	Power Ledger	Decentralised energy trading, IoT, Green Certificates, Electric mobility. Grid Management	Solana (Ethereum Bridge)	Australia
17	Wien Energie	Decentralised energy trading	Interbit	Austria

Table 4: DLT Energy Projects

Source: Table adapted from EY (2022)

The potential use of DLT within the energy sector is growing, as are the range of decentralised technology components and supported functions. Examining the feasibility requires the understanding



of DLT concepts. The UK Government Office for Science<sup>21</sup> states that the real potential of this technology can be fully realised only when combined with smart contracts.

A transition towards decentralised technologies being used in DER data exchange may start simple, for a few use cases, and add new functions and features as confidence grows in the technology maturity. Figure 14 highlights decentralised technology concepts (with brief descriptions) that may be considered in a transition towards decentralisation that adds progressive levels of sophistication over time.










Core Concept	Design considerations
 <p><b>1. Contract Automation &amp; Compliance</b> "Smart Contracts"</p>	<ul style="list-style-type: none"> <li>• Today, the use of Smart Contracts is constrained by confidence and acceptance that agreements can be codified and run under privacy on chain.</li> </ul>
 <p><b>2. Digital Twin Network Visualisation</b> "Tokenization"</p>	<ul style="list-style-type: none"> <li>• Implementation of NFT's for mobile and fixed network Digital Assets Twins has not been considered.</li> <li>• Flow of meta-data and reliable supply chain dependencies used to visualise network supply chain</li> </ul>
 <p><b>3. Self Sovereign Decentralised Identity</b> "DID"</p>	<ul style="list-style-type: none"> <li>• Decentralised Identity, a W3C standard utilised by Organisations today.</li> <li>• Aligned to Consumer Data Reporting (CDR) legislation, data is owned by originator.</li> <li>• Proven in Project Edge PILOT and confidence the solution works.</li> </ul>
 <p><b>4. Pubic, Private, Hybrid DLT</b> "Open or Closed DLT"</p>	<ul style="list-style-type: none"> <li>• Proven Public chain in Project Edge PILOT and confidence the solution works.</li> <li>• Supports open innovation</li> <li>• Public based infrastructure supports scaling of the solution</li> </ul>
 <p><b>5. Shared Decentralised Transactions</b> "Transactions"</p>	<ul style="list-style-type: none"> <li>• Immutable data verification on chain.</li> <li>• Strong focus on trust an immutability relating to data exchange.</li> <li>• The use of Identity data utilising a DLT has been considered</li> </ul>
 <p><b>6. Decentralised Governance</b> "DAO"</p>	<ul style="list-style-type: none"> <li>• Industry focused governance structure (e.g. value chain aligned)</li> <li>• De-centralised decision making for ecosystem improvements</li> <li>• Not considered.</li> </ul>
 <p><b>7. Decentralised Self Custody</b> "Digital Wallets"</p>	<ul style="list-style-type: none"> <li>• Non-transparent token management to transparent ownership token management.</li> <li>• Long term alignment of new purpose and values</li> <li>• Not considered.</li> </ul>
 <p><b>8. Open Industry Innovation</b> "DaPP"</p>	<ul style="list-style-type: none"> <li>• Allow industry participants to innovate and develop solutions based on open decentralised market data. The outcome based on Decentralised Applications (DaPP)</li> <li>• Not considered.</li> </ul>
 <p><b>9. Near Realtime Data Exchange</b> "Light Weight DLT Protocols"</p>	<ul style="list-style-type: none"> <li>• Movement away from 5min market resolution to lower thresholds.</li> <li>• Performance directs the DLT protocol solution.</li> <li>• Not considered.</li> </ul>

Figure 14: DLT Core Concepts

Source: EY (2022)

<sup>21</sup> UK Government Department for Science. Available: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf)

## 4. Cyber Security Threat Assessment

The objective of this assessment was to identify potential cyber security risks and impacts on the DER marketplace platform deployed by AEMO in accordance with the high-level architecture options listed in Section 3.2.3.

### 4.1 AEMO Risk Assessment Method

The risk ratings used in this report reflect the recommended priority to address the risks identified as part of the Cyber Security Threat and Risk Assessment and walkthroughs with relevant stakeholders. The rating is provided based on probability of the risk being exploited and significance of impact associated with each issue and is in accordance with the AEMO risk rating guidelines defined in Appendix B

### 4.2 Key Risks

A total of 12 cyber security risks (two (2) critical-rated, six (6) high-rated and four (4) medium-rated) were identified during the assessment. Some of the risks identified as part of this review are attributable to key themes such as:

1. Vulnerabilities and weaknesses in the multiple software ecosystems leveraged in the DER ecosystem could lead to unauthorised access to disclosure of sensitive information - Given the nature of the (DER) marketplace, weaknesses and vulnerabilities in the software/application eco-systems leveraged across the marketplace could negatively impact the confidentiality, integrity, and availability-of information resources in the marketplace. Therefore, secure application development processes should be leveraged wherever possible, and appropriate application security controls should be developed and administered for all key software components across the DER ecosystem.
2. Lack of appropriate management of Supply Chain risks could lead to data disclosure or unavailability of key DER resources - Each entity across the DER Marketplace would have their own supply chains based on their business requirements. Such supply chains provide a threat actor with opportunities to perform malicious activities targeting specific DER Marketplace entities. Cyber Security requirements should be established for key suppliers according to industry better practices and information sources should be monitored to identify and address supply chain threats and risks.
3. Lack of asset and entity classification processes could lead to inappropriate application of security controls thereby increasing the impact of a potential cyber attack- Multiple entities across the DER Marketplace have critical assets. In an event of a security incident affecting these critical assets, lack of appropriate security controls could lead to significant impact to the confidentiality or availability of the affected DER marketplace entity. Each entity across the DER Marketplace should perform a Business Impact Analysis (BIA) to understand the criticality of their assets and thereby implement appropriate controls to ensure critical assets have the right level of protection against cyber-attacks.
4. Weaknesses in Security Operations could lead to cyber-attacks not being identified or having greater impact: The DER marketplace is designed to have bi-directional flow of information with each single entity having significant amount of customer and operational data at a given point in time. Due to the interconnected-ness of the marketplace, a compromise of a single entity could have significant impacts across the DER marketplace. Lack of consolidated visibility over malicious activity and security incidents across the DER Marketplace, could lead to such activity going unnoticed for a long period of time which could affect the confidentiality and availability of data across the DER Marketplace.
5. Attacks due to weak transmission and communication protocols: Protocols facilitate the communication and transmission between DER devices, aggregators, DNSPs, DSOs and other entities across the DER Marketplace. Secure communication and transmission channels should be established for communications and transmissions between these entities. At the time of writing, there are multiple protocols which could be used across the DER Marketplace such as IEEE 2030.5, Modbus, LoraWAN, IEEE 1815. Such protocols have

inherent weaknesses, for example, Modbus has known vulnerabilities which could lead to a Denial of Service attack. Integrity of communications should also be considered between devices and entities across the DER marketplace and independent verification processes should be implemented to ensure integrity.

6. **Compromise of DER Marketplace entities & Critical Assets:** Each entity across the DER Marketplace has a key role and has critical assets which could lead to significant loss of services in an event where an DER Marketplace entity or a critical asset at an entity were compromised. For example, a DNSP would not be able to supply energy requirements if their infrastructure went offline. DER Marketplace entities should have appropriate monitoring and alerting processes, Incident Response plans and Disaster Recovery processes. Redundant technologies should be implemented for critical assets and processes. The Department of Energy's (DOE) Cyber-Information Engineering (CIE) framework<sup>22</sup> provides guidance on building Cyber Security practices into the design life cycle of engineered systems to impacts of a Cyber incident. The framework emphasises on "Assume Compromise" thereby driving requirements for appropriate detection, isolation and mitigation of Cyber risks. Each entity across the DER Marketplace should also have an asset classification framework. Having an asset classification framework enables consistent application of risk management processes as well as security controls across critical and high-value assets. The SOCI Act (Security of Critical Infrastructure Act 2018) mandates recording and reporting of critical and high-value assets.

## 4.2.1 Long term considerations

Although the scope of Project EDGE was limited to considering DER data exchange between key industry (actors, aggregators, DNSPs and AEMO) for specific use cases such as the exchange of dynamic operating envelopes, the critical risks identified above relate to the full supply chain for data exchange that includes aggregator/customer agent to device communications.

It is important that this threat assessment looks beyond the confined scope of Project EDGE to consider DER cyber threats, and mitigating controls from a holistic lens. As a result, the consideration of mitigating controls includes measures that can be applied to the entire supply chain.

Project EDGE has tested some of the key concepts of a decentralised approach to DER integration, such as decentralised identities (DIDs) and a decentralised data hub, to automatically assign DOEs sent by DNSPs (assigned at the NMI level) to the right aggregator without the need for a centralised broker, but the full potential of a decentralised approach has not been comprehensively and practically examined due to the scope restriction outlined above.

A more comprehensive application of DIDs across the DER Marketplace could deliver a range of further benefits for the industry and consumers that have been considered in the mitigating controls element of this assessment, including:

- i) **Secure integration with the DER ecosystem:** Devices and entities with a DID could automatically upload their standing data and credentials to an updated DER Register as they first connect to the internet, saving time, effort and errors in manually uploading data.
- ii) **End to end visibility and auditability across the DER ecosystem:** DIDs and Verifiable Credentials (VCs) at each level of the supply chain (for example, device and aggregator / retailer level) enables greater integrity checking and isolation of operation via revocation of VCs in an event of a security incident.
- iii) **Secure interoperability across the DER ecosystem:** An extended capability of DIDs and VCs can enable any retailer/aggregator to send control signals to compatible devices if they have the correct VCs, customer consent and are connected to an industry data hub. This would give

---

<sup>22</sup> United States Department of Energy. Available: [https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022\\_0.pdf](https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf)

customers freedom to switch between providers and enable aggregators to easily coordinate numerous different device types within their portfolio.

- iv) **Compliance with industry standards:** DIDs and VCs can provide a medium for traceability of settings and firmware upgrades for compliance to industry standards (for example, AS 4777.2.2020 or CSIP-AUS).

### 4.3 Summary of Risks

The details of the risks identified as part of the Cyber Security Threat Assessment are summarised in the table below:

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.1	Vulnerabilities in DER marketplace software leading to confidentiality, integrity and availability based attacks	<p>The DER marketplace uses multiple software ecosystems which works cohesively to provide an efficient DER marketplace. Given the nature of the distributed environment, weaknesses in the software/applications could have serious implications which could affect the DER marketplace as a whole.</p> <p>Software across the DER marketplace could consist of application software, firmware, third-party applications etc.</p>	Critical	<ul style="list-style-type: none"> <li>▶ Ensure appropriate security processes are in place across the SDLC process, for example:                             <ul style="list-style-type: none"> <li>○ Perform security code reviews (SASTs &amp; SCM) against application software</li> <li>○ Perform Penetration Tests against DER Marketplace applications</li> </ul> </li> <li>▶ Ensure application developers have gone through appropriate level of secure coding training programs</li> <li>▶ Perform integrity checks against any code before runtime (proprietary &amp; custom code). For example, secure boot mechanisms, signature verifications prior to software installations and vendor signed software</li> <li>▶ Enable secure configuration checks periodically across all software components</li> <li>▶ Perform security scans on application and infrastructure environments to secure application and infrastructure workflows</li> </ul>	<p>Cyber Security Program Management-C2F: MIL-2 and SP-2</p> <p>Cyber Security Program Management-4A: MIL-2 and SP-2</p> <p>Supply Chain and External Dependencies Management-2E: MIL-2 and SP-2</p>	Low/Medium

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.2	Malware and Ransomware attacks	<p>A successful malware or ransomware attack could have significant impact over the DER Marketplace. For example, a successful ransomware attack against an Aggregator could disrupt day-to-day operations (disruption in the flow of bids &amp; offers, disruption on onboarding new customers). The ransomware attack could also have a financial as well as reputational impact for the Aggregator.</p> <p>Also, due to the inter-connectedness of the DER marketplace, a malware or ransomware attack could propagate across different entities in the DER Marketplace having significant impact on the overall availability of the environment.</p>	Critical	<ul style="list-style-type: none"> <li>▶ Implement appropriate anti-malware and ransomware controls across all entities in the DER Marketplace</li> <li>▶ Incident management and Disaster Recovery processes should be in place to minimise impact of a successful malware/ransomware attack. Processes should include appropriate out-of-band isolation, triage and response mechanisms ensuring minimal disruption to ongoing operations of the DER Marketplace.</li> <li>▶ Perform table-top exercises to simulate a malware/ransomware attack to understand any process or knowledge gaps in the Incident Management and Disaster Recovery process</li> <li>▶ Implement appropriate Backup procedures and test/verify backups periodically</li> </ul>	<p>Event and Incident Response, Continuity of Operations-3B: MIL-1 and SP-1</p> <p>Threat and Vulnerability Management-1D: MIL-2 and SP-2</p> <p>Event and Incident Response, Continuity of Operations-3M: MIL-3 and SP-3</p>	Low/Medium
4.3.3	Attacks due to weak transmission and communication protocols	<p>Protocols facilitate the communication and transmission between DER devices, aggregators, DNSPs, DSOs and other entities across the DER Marketplace. Secure communication and transmission channels should be established for communications and transmissions between these entities. At the time of writing, there are multiple protocols which could be used across the DER Marketplace such as IEEE 2030.5, Modbus, LoraWAN, IEEE 1815. Such protocols have inherent weaknesses, for example, Modbus has known vulnerabilities which could lead to a Denial of Service attack.</p>	High	<ul style="list-style-type: none"> <li>▶ Leverage well-known protocols which have security mechanisms inbuilt such as authentication, authorisation, integrity checks for messages, etc. to enable secure communication channels between DER marketplace entities</li> <li>▶ Enable Transport-Layer Security wherever possible across communications between entities</li> <li>▶ Implement independent verification processes to ensure integrity of communications</li> </ul>	Information Sharing and Communications-1F: MIL-2 and SP-2	Low/Medium

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.4	Attacks due to weak initial DER device configurations	During the trial, it was identified that the D DER devices will have a private key configured on them which allows them to generate DLT credentials (Decentralised Identifiers (DIDs) & Verifiable Credentials (VCs)) to participate in the DER marketplace. Security checks and processes need to be in place at DER device manufacturing organisations to ensure appropriate management of these private keys and PKI systems. Compromise of any such manufacturing organisations or device manufacturing systems/processes and related supply chains could lead to compromise of private keys which could severely affect the DER marketplace.	High	<ul style="list-style-type: none"> <li>▶ AEMO should provide security configuration guidelines for organisations, so all devices have a consistent baseline configuration process, which also has security configuration baselines.</li> <li>▶ Appropriate third-party risk management processes should be in place with organisations developing DER devices. Such processes should also focus on incident response &amp; mitigation capabilities in an event wherein a compromise does occur along with breach notification requirements.</li> </ul>	<p>Asset, Change and Configuration Management-2A: MIL-1 and SP-1</p> <p>Asset, Change and Configuration Management-2B: MIL-1 and SP-1</p> <p>Asset, Change and Configuration Management-2C: MIL-2 and SP-2</p>	Low/Medium
4.3.5	Data exposure and unauthorised access attacks	<p>As part of the trial, all DER marketplace data is stored on databases (MongoDB, SQL Server) and other Pxise components (Azure environment). In discussions with AEMO stakeholders, no encryption at rest controls were identified across these databases and Pxise components. Apart from this information, participant identities (DIDs and VCs) are stored on the EWF DLT, which has encryption at rest.</p> <p>In further discussions with AEMO, it was identified that Encryption in transit (TLS/SSL) is not configured or configured consistently across the Azure environment across Pxise assets. This could lead to disclosure of sensitive information such as usernames &amp; passwords as well as other critical application data.</p> <p>Encryption at rest is to be designed to prevent unauthorised access to data in an event where the threat-actor has underlying physical access to data-stores.</p>	High	<ul style="list-style-type: none"> <li>▶ Ensure DER marketplace data is encrypted at rest at all datastores across all entities (Aggregator, DNSP/DSO and MO). Encryption algorithms should be industry best practice and should align with business and security requirements</li> <li>▶ Configure Transport Layer Security (TLS 1.2 and above) across communication channels in the DER Marketplace</li> </ul>	<p>Identity and Access Management-2A: MIL-1 and SP-1</p> <p>Information Sharing and Communications-1F: MIL-2 and SP-2</p>	Low/Medium

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.6	Blockchain-based attack	<p>During the Project EDGE trial, Blockchain technology was being considered as the core backend system to store DER marketplace identities (DIDs and VCs). Few examples of Blockchain related attacks are listed below:</p> <p>Denial of Service attacks using spam transactions could be used to disrupt legitimate identity transactions thereby rendering the DER marketplace unavailable for a period of time.</p> <p>Eclipse attacks are attacks in which an attacker can restrict/control communications to specific nodes on the P2P network. By doing so, an attacker could restrict certain communications to a node, or even send malicious information to a node.</p> <p>Sybil attacks redirect the inbound and outbound connections of an operational node from legitimate nodes to the threat actor's nodes to obtain information about the bids/offers that take place on it or to manipulate a bid/offer to make someone believe that it has been successfully executed, when in fact it has been manipulated. MitM based attacks.</p> <p>Note: Eclipse and Sybil attacks would have a larger impact once additional DER marketplace data is stored on the DLT. During the time of this assessment only DIDs and VCs were stored on the DLT.</p>	High	<p>To prevent DoS based attacks:</p> <ul style="list-style-type: none"> <li>▶ Filtering transactions allows block creators the choice of which transactions are included in their blocks. By being able to identify and discard potential spam transactions, this can prevent the possibility of transaction flooding on the network</li> <li>▶ Ensuring appropriate resources have been configured - storage, processing, network bandwidth</li> </ul> <p>To prevent Eclipse based attacks:</p> <ul style="list-style-type: none"> <li>▶ Use validation and chain of trust systems</li> <li>▶ Use consensus protocol that implies a cost per identity or access to network resources</li> <li>▶ Create a reputation system where users with more time on the network have more power</li> </ul> <p>To prevent Sybil based attacks:</p> <ul style="list-style-type: none"> <li>▶ Have a reliable node selection process to ensure the network has well-identified and related nodes</li> <li>▶ Increase amount of node connections</li> </ul>	<p>Supply Chain and External Dependencies Management-2A: MIL-1 and SP-1</p> <p>Supply Chain and External Dependencies Management-2J: MIL-3 and SP-3</p>	Low/Medium



Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.7	Supply Chain attacks	<p>Each entity across the DER Marketplace would have their own supply chains based on their business requirements. Such supply chains provide a threat actor with opportunities to perform malicious activities targeting a specific DER Marketplace entity. For example, a misconfigured device, or backdoor enabled software application.</p> <p>Each entity should have appropriate Third-Party Risk Management (TPRM) processes which align with their business and risk management requirements. Such processes would allow for appropriate level of controls and processes providing visibility across actions and processes in the supply chain.</p>	High	<ul style="list-style-type: none"> <li>▶ Implement a Third-Party Risk Management framework which aligns with business requirements. The AESCSF framework could be leveraged to understand the security posture levels of entities across the DER marketplace.</li> <li>▶ Ensure security controls and processes are in place which align with the criticality of third-parties/supply chains</li> <li>▶ If feasible, AEMO should provide guidance to all DER Marketplace entities on managing their Third-Party/Supply chain risk</li> </ul>	<p>Supply Chain and External Dependencies Management-2A: MIL-1 and SP-1</p> <p>Supply Chain and External Dependencies Management-2E: MIL-2 and SP-2</p> <p>Supply Chain and External Dependencies Management-2N: MIL-3 and SP-3</p>	Low/Medium
4.3.8	Compromise of Critical Assets	<p>Each entity across the DER Marketplace has critical assets which could lead to significant loss of services in an event where they were compromised. For example, a DNSP would not be able to supply energy requirements if their infrastructure went offline.</p> <p>Each entity across the DER Marketplace should have an asset classification framework. Having an asset classification framework enables consistent application of risk management processes as well as security controls across critical and high-value assets.</p> <p>The SOCI Act (Security of Critical Infrastructure Act 2018) mandates recording and reporting of critical and high-value assets.</p>	High	<ul style="list-style-type: none"> <li>▶ Implement a consolidated asset classification framework across the DER Marketplace or at an DER Marketplace entity level</li> <li>▶ Ensure risk management processes and security processes are aligned with the classification of assets</li> <li>▶ Security controls should also be applied in alignment with the criticality of assets, ensuring optimisation of available resources</li> <li>▶ Periodic review of the classification of assets should be performed to align with changing business and regulatory requirements</li> </ul>	<p>Asset, Change and Configuration Management-1D: MIL-2 and SP-2</p> <p>Cyber Security Program Management-1C: MIL-2 and SP-2</p> <p>Event and Incident Response, Continuity of Operations-2D: MIL-2 and SP-2</p>	Low/Medium

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.9	Insider attacks/Internal threats	Due to the nature of the DER marketplace, different entities will have their own employee onboarding programs in-place. Such programs may or may not be aligned with industry requirements. Lack of appropriate background checks and specific technical controls in place to identify intended/accidental malicious behaviour could lead to significant impact across the DER Marketplace. Impact could range from disclosure of customer/sensitive PII data or disclosure of Bids and Offers information which could lead to financial as well as reputational damage.	Medium	<ul style="list-style-type: none"> <li>▶ Ensure appropriate onboarding and background/verification checks are performed for all entities across the DER Marketplace</li> <li>▶ Ensure appropriate alerting, incident management and response procedures are implemented across all DER Marketplace entities</li> <li>▶ Have appropriate security awareness training for all employees across the organisation</li> <li>▶ If feasible, AEMO should provide guidance on security awareness training, technical controls, data security &amp; privacy and incident management processes to other DER Marketplace entities</li> <li>▶ Implement appropriate UAM controls (5.2.10)</li> </ul>	<p>Threat and Vulnerability Management-1D: MIL-2 and SP-2</p> <p>Workforce Management-2E: MIL-3 and SP-3</p> <p>Workforce Management-2F: MIL-3 and SP-3</p>	Low
4.3.10	Lack of appropriate User Access Management processes could lead to disclosure of DER Marketplace data	<p>DER Marketplace entity access management (DIDs and VCs) is performed at the DLT (based on Project EDGE). Based on architectural decisions, this DLT can be hosted at the Aggregator (Decentralised) or at the Market Operator (Centralised).</p> <p>User Access Management (UAM) review across the entity organisations was not part of the scope of Project EDGE. Weaknesses in UAM policies and processes within an entity's infrastructure could lead to disclosure of sensitive information or disruption to day-to-day operations.</p> <p>Also, due to the interconnected-ness of the DER Marketplace, some user accounts may be shared across entities. User account compromises at one entity could lead to unauthorised access to other entities too.</p>	Medium	<ul style="list-style-type: none"> <li>▶ Ensure appropriate UAM/IAM programs, processes and tools are implemented across each DER Marketplace entity organisation.</li> <li>▶ AEMO should provide guidance on UAM/IAM program expectations</li> <li>▶ Ensure appropriate alerting, incident management and response procedures are implemented across all DER Marketplace entities</li> <li>▶ If feasible, employ a single RBAC user access management model which can be leveraged by all entities/users across the DER Marketplace</li> </ul>	<p>Identity and Access Management-2B: MIL-1 and SP-1</p> <p>Identity and Access Management-1G: MIL-3 and SP-1</p> <p>Identity and Access Management-2D: MIL-2 and SP-2</p>	Low

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
4.3.11	Weaknesses in Security Operations could lead to cyber-attacks not being identified or having greater impact	The DER marketplace is designed to have bi-directional flow of information with each single entity having significant amount of customer and operational data at a given point in time. Due to the interconnected-ness of the marketplace, a compromise of a single entity could have significant impacts across the DER marketplace. Lack of consolidated visibility over malicious activity and security incidents across the DER Marketplace, could lead to such activity going unnoticed for a long period of time which could affect the confidentiality and availability of data across the DER Marketplace.	Medium	<ul style="list-style-type: none"> <li>▶ Establish infrastructure and processes which provide a consolidated view of alerts, incidents and security issues for entities across the DER Marketplace</li> <li>▶ Each entity should have their dedicated processes to manage security incidents. AEMO should have visibility and provide guidance in such cases</li> <li>▶ Establish a centralised governance structure, along with Incident Response plans and procedures enabling timely triage and remediation of security incidents and malicious activity across the DER Marketplace</li> </ul>	<p>Event and Incident Response, Continuity of Operations-1B: MIL-1 and SP-1</p> <p>Event and Incident Response, Continuity of Operations-2B: MIL-1 and SP-1</p> <p>Event and Incident Response, Continuity of Operations-1E: MIL-2 and SP-1</p>	Low

Finding #	Finding Description	Risk Description	Severity Level	Proposed Mitigating Controls	AESCSF Mapping	Residual Risk Rating
5.2.12	Threat actors targeting weak onboarding and registration processes to gain access to the DER Marketplace	<p>Before joining the DER marketplace, each participant (consumer, prosumer, aggregator, DSO/DNSP) needs to go through the registration and onboarding process to generate blockchain identities and public key infrastructure (PKI) certificates for participating in the DER Marketplace. However, during the time of assessment, the implementation strategy of the DER Marketplace DLT (Centralised vs Decentralised) was not finalised.</p> <p>Access to the DER marketplace should only be provided after appropriate checks against the new participant has taken place. Without such processes, a malicious participant could be in a position to initiate malicious actions against other entities across the DER Marketplace. These malicious actions could include:</p> <ol style="list-style-type: none"> <li>1) Gain access to sensitive customer information and PII (Aggregator)</li> <li>2) Disrupt operations severely affecting the energy distribution across the DER Marketplace (DNSP/DSO and AEMO)</li> <li>3) Have the ability to perform a range of malicious attacks at a point in time, or in the future</li> <li>4) Capture information on the DER Marketplace and leverage such information for financial gain or to cause reputational damage to the Market operator (AEMO)</li> </ol>	Medium	<ul style="list-style-type: none"> <li>▶ Ensure registration &amp; onboarding processes align with business and regulatory requirements</li> <li>▶ Background checks (based on type of participant) should be performed before access has been given to the DER marketplace</li> <li>▶ DER marketplace entities should have appropriate checks and onboarding processes for their third-party suppliers to ensure supply chain attacks are at a minimum (4.2.7)</li> </ul>	<p>Supply Chain and External Dependencies Management-2N: MIL-3 and SP-3</p> <p>Workforce Management-2F: MIL-3 and SP-3</p>	Low

Table 5: Detailed Summary of Risks

The detailed description of the impact and the recommendations for all risks identified during the assessment can be found in Sections 4.4.2 of this report.

## 4.4 Detailed Risks

The below sections provide the details of the identified risks from the different phases of the assessment. The general format in documenting each finding is explained in the format provided below:

### 4.4.1 Detailed Risk Format

<b>Threat Agent</b>	Class of actors that could cause a failure scenario to occur, for example, External – malicious	<b>Likelihood</b>	Probability of a threat event realising
<b>Risk Rating</b>	Critical/High/Medium/Low	<b>Consequence</b>	The possible consequence if the risk is realised
<b>Threat objectives</b>	Objectives of a threat actor, for example, Gain access to customer PII		
<b>Threat scenarios</b>	A scenario of a threat agent trying to achieve an objective		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	NESCOR <sup>23</sup> Failure scenarios mapped with the Risk		
<b>Risk Statement</b>	Description of the risk		
<b>Applicability</b>	Applicability of the threat & threat actor to all the entities in the marketplace		
<b>Observations</b>	Observations from Project EDGE aligned with the risk		
<b>AESCSF Mapping</b>	Mapping of the threat to the Australian Energy Sector Cyber Security Framework, where applicable. The purpose of this framework is to enable participants to assess, evaluate and improve their cyber security capability and maturity.		
<b>OWASP Mapping</b>	Mapping of the threat to the OWASP Top 10, where applicable		
<b>Proposed mitigating controls</b>	Controls proposed to manage risk, for example, Multi-Factor authentication		
<b>Integration type affected</b>	The integration scenario the Risk is applicable to, for example, Centralised vs Decentralised		
<b>Residual Risk rating</b>	Risk rating after considering implementation of proposed Mitigating controls		

Table 6: Detailed Risk Format

<sup>23</sup> National Electric Sector Cybersecurity Organization Resource (NESCOR) Failure scenarios document used to map specific Failure Scenarios with the identified Risk. The document can be found at - <https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf>

## 4.4.2 Risks

### 4.4.2.1 Vulnerabilities in DER marketplace software leading to confidentiality, integrity and availability based attacks

<b>Threat Agent</b>	External - malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Possible
<b>Risk Rating</b>	<b>Critical</b>	<b>Consequence</b>	Extreme
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Leverage software weaknesses to gain access to sensitive data</li> <li>▶ Compromise user accounts to gain persistent access across the DER Marketplace</li> <li>▶ Cause disruption and affect the availability of entities across the marketplace</li> <li>▶ Perform unauthorised and malicious actions through application software with an intent of causing financial or operational damage</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor or disgruntled employee may exploit software used by an entity of the DER marketplace to gain control of the entity environment thereby gaining access to sensitive entity data</li> <li>▶ A threat actor or a disgruntled employee may leverage application software weaknesses to gain access to entity environments and disrupt operations at a DNSP/DSO environment</li> <li>▶ An insider may accidentally gain access to sensitive data due to lack of secure authentication and authorisation controls across software applications across the DER Marketplace</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>AMI.1 Authorised Employee Issues Unauthorised Mass Remote Disconnect</b> An employee within the utility having valid authorisation, issues a "remote disconnect" command. The employee may be bribed, disgruntled, or socially engineered</li> <li>▶ <b>DER. 16 DER SCADA System Issues Invalid Commands</b> A threat actor breaches a DER SCADA system and causes the DER SCADA system to issue an invalid command to all DER systems. Since DER systems may react differently to invalid commands, the power system experiences immediate and rapid fluctuations as some DER systems shut down, while others go into default mode with no volt-var support, still others revert to full output, and a few become islanded microgrids</li> <li>▶ <b>DER. 19 Threat Actor gains Access to Utility DERMS via application software</b> A threat actor leveraging an application software to which they have full access, to the utility's Distributed Energy Resources Management System (DERMS). The threat agent is able to modify the DER commands, schedules, and requests sent to other DER systems, making these settings beneficial to their own DER systems, and consequently less beneficial to other DER systems</li> </ul>		
<b>Risk Statement</b>	<p>The DER marketplace uses multiple software ecosystems which works cohesively to provide an efficient DER marketplace. Given the nature of the distributed environment, weaknesses in the software/applications could have serious implications which could affect the DER marketplace as a whole.</p> <p>Software across the DER marketplace could consist of application software, firmware, third-party applications etc.</p>		
<b>Applicability</b>	<p>AEMO/Market Operator - Yes Aggregator - Yes DNSP/DSO - Yes</p> <p>Due to the interconnected-ness of the DER Marketplace, a successful compromise at a single entity in the DER Marketplace could lead to downstream attacks to other entities in the Marketplace. For example, in Project EDGE, EWF leveraged containerised instances of software which was installed at the Aggregator and the MO. Successful attacks against a single entity in this case, could potentially lead to compromise on the other entity too.</p>		
<b>Observations</b>	<p>As part of the Project EDGE trial, EWF was leveraged as the DLT &amp; software solution. In discussions with EWF, it was identified that there weren't appropriate security processes</p>		

	in place. However, EWF did mention that they would be performing security assurance processes after the Project EDGE trial.
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ Cyber Security Program Management-2F: MIL-2 and SP-2</li> <li>▶ If the organisation develops or procures software, secure software development practices are sponsored as an element of the Cyber Security program.</li> <li>▶ Cyber Security Program Management-4A: MIL-2 and SP-2</li> <li>▶ Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices.</li> <li>▶ Supply Chain and External Dependencies Management-2E: MIL-2 and SP-2</li> <li>▶ Cyber Security requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate.</li> </ul>
<b>OWASP Mapping</b>	<p>A01:2021 - Broken Access Control</p> <p>A04:2021 - Insecure Design</p> <p>A05:2021 - Security Misconfiguration</p> <p>A07:2021 - Identification and Authentication Failures</p> <p>A08:2021 - Software and Data Integrity Failures</p>
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Ensure appropriate security processes are in place across the SDLC process, for example: <ul style="list-style-type: none"> <li>○ Perform security code reviews (SASTs &amp; SCM) against application software</li> <li>○ Perform Penetration Tests against DER Marketplace applications</li> </ul> </li> <li>▶ Ensure application developers have gone through appropriate level of secure coding training programs</li> <li>▶ Perform integrity checks against any code before runtime (proprietary &amp; custom code)</li> <li>▶ Enable secure configuration checks periodically across all software components</li> <li>▶ Perform security scans on containerised services and applications to secure containerised workflows</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	<p>Centralised Hub - High</p> <p>Decentralised Hub - Low</p> <p>Point to Point - Low</p>
<b>Residual Risk rating</b>	Low/Medium

Table 7: Vulnerabilities in DER marketplace software leading to confidentiality, integrity and availability based attacks

#### 4.4.2.2 Malware and Ransomware attacks

<b>Threat Agent</b>	External – malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Likely
<b>Risk Rating</b>	<b>Critical</b>	<b>Consequence</b>	Major
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Gain access to the DER Marketplace to perform malicious activities at present or have the capability to perform malicious activities in the future</li> <li>▶ Disruption of operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> <li>▶ Perform malicious changes across devices or applications across the DER Marketplace with an intention of causing disruption to operations</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor may deliver malware/ransomware in the software or firmware of a component of the DER marketplace and inter-connected devices, or in the operating environment of the DER marketplace and inter-connected device</li> </ul>		

	<p>control systems, to gain control of the environment and inter-connected devices remotely, exfiltrate data and/or encrypt data</p> <ul style="list-style-type: none"> <li>▶ A deranged or disgruntled employee may use their legitimate access to operational systems to encrypt and/or exfiltrate data in secret</li> <li>▶ An insider may accidentally deliver malware/ransomware in the software or firmware of a component of the DER marketplace and inter-connected devices, or in the operating environment of the DER marketplace and inter-connected device control systems, to gain control of the environment and inter-connected devices remotely, exfiltrate data and/or encrypt data</li> </ul>
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>DER.3 Malware Introduced in DER System During Deployment.</b></li> <li>▶ A threat agent, possibly a disgruntled employee, makes malicious software changes to equipment software or firmware. This malware causes large numbers of DER systems to ignore certain critical commands from the utility</li> <li>▶ <b>DER.13 Custom Malware Gives Threat Agent Control of Utility Server (DSO), Aggregator Platform or Market Platform [CMS/BMS].</b></li> </ul> <p>A threat agent compromises the operating system/operating environment platform of a CMS/BMS and installs malware. The malware leverages automated machine-to-machine authentication mechanisms and/or compromises stored cryptographic authentication keys to allow it to impersonate the authorised CMS/BMS software. This gives the threat agent complete control over all of the CMS/BMS resources and remote resources controlled or managed by the CMS/BMS</p> <ul style="list-style-type: none"> <li>▶ <b>DR.5 Non-specific Malware Compromises Aggregator Platform [DRAS], DER/CMS [Customer DR System] or Utility Server [DSO]</b></li> </ul> <p>The DRAS or customer DR system is infected by non-specific common malware. This malware may consume system resources, thus slowing other system processes or may attempt to compromise typical components such as databases. This could cause the DRAS to fail to send DR messages when needed or to disclose customer information in its database. It could cause the customer system not to execute the contractual terms of the DR service although it receives legitimate DR messages</p>
<b>Risk Statement</b>	<p>A successful malware or ransomware attack could have significant impact over the DER Marketplace. For example, a successful ransomware attack against an Aggregator could disrupt day-to-day operations (disruption in the flow of bids &amp; offers, disruption on onboarding new customers). The ransomware attack could also have a financial as well as reputational impact for the Aggregator.</p> <p>Also, due to the inter-connectedness of the DER marketplace, a malware or ransomware attack could propagate across different entities in the DER Marketplace having significant impact on the overall availability of the environment.</p>
<b>Applicability</b>	<p>AEMO/Market Operator - Yes  Aggregator - Yes  DNSP/DSO - Yes</p> <p>All entities in the DER marketplace would be susceptible to an attack in the form of malware and ransomware. Each entity should be responsible for having appropriate anti-malware tools and processes (Incident response, backups, etc.) to minimise the damage from a malware or ransomware attack.</p>
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Event and Incident Response, Continuity of Operations-3B: MIL-1 and SP-1</b></li> </ul> <p>Responses to escalated Cyber Security events and incidents are implemented, at least in an ad hoc manner, to limit impact to the function and restore normal operations.</p> <ul style="list-style-type: none"> <li>▶ <b>Threat and Vulnerability Management-1D: MIL-2 and SP-2</b></li> </ul> <p>A threat profile for the function is established that includes characterisation of likely intent, capability, and target of threats to the function.</p> <ul style="list-style-type: none"> <li>▶ <b>Event and Incident Response, Continuity of Operations-3M: MIL-3 and SP-3</b></li> </ul> <p>Cyber Security event and incident response plans are aligned with the function's risk criteria and threat profile.</p>
<b>OWASP Mapping</b>	<p>A05:2021 - Security Misconfiguration  A06:2021 - Vulnerable and Outdated Components</p>



	A09:2021 - Security Logging and Monitoring Failures
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Implement appropriate anti-malware and ransomware controls across all entities in the DER Marketplace</li> <li>▶ Incident management and Disaster Recovery processes should be in place to minimise impact of a successful malware/ransomware attack</li> <li>▶ Perform table-top exercises to simulate a malware/ransomware attack to understand any process or knowledge gaps in the Incident Management and Disaster Recovery process</li> <li>▶ Implement appropriate Backup procedures and test/verify backups periodically</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub - High Decentralised Hub - High Point to Point - Low
<b>Residual Risk rating</b>	Low/Medium

Table 8: Malware and Ransomware attacks

#### 4.4.2.3 Attacks due to weak transmission and communication protocols

<b>Threat Agent</b>	External – malicious Internal – malicious	<b>Likelihood</b>	Possible
<b>Risk Rating</b>	High	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or corporate data</li> <li>▶ Capture sensitive information such as username and passwords</li> <li>▶ Capture/ Modify sensitive financial details such as Bids &amp; Offers (Boffers)</li> <li>▶ Capture/ Modify operational information such as Dynamic Operating Envelopes (DOEs)</li> <li>▶ Communicate with DER devices across the DER Marketplace</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor may exploit communication protocol weaknesses to mount a man-in-the-middle (MitM) attack, to redirect communication through a compromised node to enable monitoring and modification of communication</li> <li>▶ A malicious insider could capture communications between devices and use such information for financial/personal gain, or to cause reputational damage to the DER Marketplace entity</li> <li>▶ A threat actor could monitor communications between DER marketplace entities/devices and use the knowledge gained to perform additional attacks against the DER Marketplace</li> <li>▶ A threat actor or malicious insider could leverage lack of authentication/authorisation controls in communication &amp; transmission protocols to perform unauthorised actions on DER devices</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>DER.4 Confidential DER Generation Information Stolen To Harm Customer</b> A utility is monitoring the energy and ancillary services provided by an industrial or commercial customer's DER system. The communication protocol that transports this information is intercepted and a threat agent gains access to the private generation data from the DER system because the protocol provides either no confidentiality or inadequate confidentiality. This private data is used to harm the customer</li> <li>▶ <b>DR.2 Private Information is Publicly Disclose on Communications Channel</b> A threat agent eavesdrop on traffic on the network. This could leak private information to the threat agent</li> <li>▶ <b>AMI.24 Weak Cryptography Exposes Device Communication</b> A vendor implements weak cryptography that is easy to crack, allowing access to and modification of configuration or data on that interface</li> </ul>		
<b>Risk Statement</b>	Protocols facilitate the communication and transmission between DER devices, aggregators, DNSPs, DSOs and other entities across the DER Marketplace. Secure communication and transmission channels should be established for communications and transmissions between these entities. At the time of writing, there are multiple protocols which could be used across the DER Marketplace such as IEEE 2030.5, Modbus, LoraWAN, IEEE 1815. Such protocols have inherent weaknesses, for example, Modbus		

	has known vulnerabilities which could lead to a Denial-of-Service attack. Integrity of communications should also be considered between devices and entities across the DER marketplace and independent verification processes should be implemented to ensure integrity.
<b>Applicability</b>	AEMO/Market Operator - No - The nature of the communications between the Aggregator/DNSP/DSO to AEMO would be TCP/IP with the ability to have TLS configured. Aggregator - Yes DNSP/DSO - Yes  At the point of assessment, although Project EDGE leveraged Mutual TLS between Energy Web (Aggregator/Mondo) and AEMO, communication and transmission protocols between DER devices and other entities was yet to be determined.  Due to the interconnected-ness of the DER marketplace, there is high potential that insecure communication between DER devices and the Aggregator would still have an impact to AEMO.
<b>Observations</b>	<ul style="list-style-type: none"> <li>▶ As part of the Project EDGE trial, Mutual TLS was configured between the Aggregator (Mondo/EFW scenario) and AEMO.</li> <li>▶ For the e-hub implementation, HTTPS is used.</li> <li>▶ IEEE 2030.5 is being considered for DER marketplace communications, but still needs to be confirmed.</li> </ul>
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Information Sharing and Communications-1F: MIL-2 and SP-2</b>  Provisions are established and maintained to enable secure sharing of sensitive or classified information.</li> </ul>
<b>OWASP Mapping</b>	A02:2021 - Cryptographic Failures A04:2021 - Insecure Design A07:2021 - Identification and Authentication Failures
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Leverage well-known protocols which have security mechanisms inbuilt such as authentication, authorisation, integrity checks for messages, etc. to enable secure communication channels between DER marketplace entities</li> <li>▶ Enable Transport-Layer Security wherever possible across communications between entities</li> <li>▶ Implement independent verification processes to ensure integrity of communications</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub - High Decentralised Hub - Low Point to Point - High
<b>Residual Risk rating</b>	Low/Medium

Table 9: Attacks due to weak transmission and communication protocols

#### 4.4.2.4 Attacks due to weak initial DER device configurations

<b>Threat Agent</b>	External – malicious Supply chain - compromised Internal – malicious	<b>Likelihood</b>	Possible
<b>Risk Rating</b>	High	<b>Consequence</b>	High
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or corporate data</li> <li>▶ Compromise devices in the supply chain to gain an initial foothold in the DER Marketplace</li> <li>▶ Monitor communications between DER devices and entities in the DER marketplace</li> <li>▶ Manipulate communications between DER devices and entities in the DER marketplace for financial gain or to cause reputational damage</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ Threat actors in the supply chain could perform a Man-in-the-Middle type of attack to gain access to private keys stored on DER devices</li> <li>▶ A supply chain entity may get compromised which may lead to knowledge of the private key by the threat actor and subsequent compromise of the system</li> </ul>		

	<ul style="list-style-type: none"> <li>▶ A malicious insider with administrative access to DER devices could manage to export PKI information from a DER device</li> </ul>
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>AMI.4 Overused Key Captured Enables Usage Data Manipulation</b> Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. A threat agent is able to acquire the secret encryption key after monitoring communications. Usage data is then manipulated to over/understate energy usage or to under/overstate energy production from DERs</li> <li>▶ <b>AMI.5 Mass Meter Rekeying Required when Common Key Compromised</b> Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. Key compromise occurs in the field due to the ability to extract the secret key when in physical possession of a meter, or during distribution of keys to meters</li> <li>▶ <b>AMI.16 Compromised Headend Allows Impersonation of CA</b> The private key for the certificate authority (CA) used to set up a Public Key Infrastructure (PKI) at the headend is compromised, which allows a threat agent to impersonate the CA</li> <li>▶ <b>Supply Chain Attacks Weaken Trust in Equipment</b> An adversary replaces a legitimate device with a maliciously altered device and introduces the device into the supply chain without directly compromising a manufacturing entity. This can be done by buying a legitimate device, buying, or creating a malicious device and returning the malicious device in place of the legitimate device as an exchange</li> </ul>
<b>Risk Statement</b>	During the trial, it was identified that the DER devices will have a private key configured on them which allows them to generate DLT credentials (DIDs & VCs) to participate in the DER marketplace. Security checks and processes need to be in place at DER device manufacturing organisations to ensure appropriate management of these private keys and PKI systems. Compromise of any such manufacturing organisations or device manufacturing systems/processes and related supply chains could lead to compromise of private keys which could severely affect the DER marketplace.
<b>Applicability</b>	<p>AEMO/Market Operator – No  Aggregator - Yes  DNSP/DSO - No</p> <p>Based on discussions with AEMO, AEMO advises market entities to change the private key across devices after initial delivery. This reduces the risk overall, however in such a scenario, entities would need to have mature PKI infrastructure setups.</p> <p>Given the nature of the risk, the impact of a successful attack would affect the Aggregator strongly. Therefore, an Aggregator should have strong Third-Party Risk Management procedures to ensure risks associated with device manufacturing and related supply chains are appropriately managed.</p>
<b>Observations</b>	<ul style="list-style-type: none"> <li>▶ Device manufacturing and initial configuration was not part of the Project EDGE trial.</li> <li>▶ In discussions with AEMO, it was identified that there was a process in which AEMO recommends the consumer/prosumer to change the private key after the DER device is delivered to the consumer.</li> </ul>
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Asset, Change and Configuration Management-2A: MIL-1 and SP-1</b> Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly.</li> <li>▶ <b>Asset, Change and Configuration Management-2B: MIL-1 and SP-1</b> Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment.</li> <li>▶ <b>Asset, Change and Configuration Management-2C: MIL-2 and SP-2</b> The design of configuration baselines includes Cyber Security objectives.</li> </ul>
<b>OWASP Mapping</b>	<p>A02:2021 - Cryptographic Failures  A04:2021 - Insecure Design</p>
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ AEMO should ensure appropriate security review of organisations developing DER devices and should provide guidance on initial configuration of such devices, so all devices have a consistent initial configuration process (which also has security config baselines &amp; security governance)</li> </ul>

	<ul style="list-style-type: none"> <li>▶ Appropriate third-party risk management processes should be in place with organisations developing DER devices. Such processes should also focus on incident response &amp; mitigation capabilities in an event wherein a compromise does occur</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub - High Decentralised Hub - Low Point to Point - Medium
<b>Residual Risk rating</b>	Low/Medium

Table 10: Attacks due to weak initial DER device configurations

#### 4.4.2.5 Data exposure and unauthorised access attacks

<b>Threat Agent</b>	External – malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Likely
<b>Risk Rating</b>	<b>High</b>	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain access to sensitive customer information or Bid/Offers information for financial gain or to cause reputational damage to AEMO</li> <li>▶ Gain access to information which could be used to gain an unfair advantage in the DER Marketplace</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor may exploit configuration weaknesses within systems to gain unauthorised access to stored data, to modify and/or exfiltrate data</li> <li>▶ A non-malicious insider could accidentally gain access to information which they should not have access to</li> <li>▶ A disgruntled employee may access unencrypted data across the data stores for financial gain or cause reputational damage</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>DER.24 Aggregator Misuses Confidential/Private Information</b> An aggregator that manages a group of DER systems normally receives commands on what energy levels and ancillary services that group of DER systems should provide. A threat agent accesses confidential or private information in the DER database on customers who own DER systems, and uses that information to "market" to those customers</li> <li>▶ <b>DR.2 Private Information is Publicly Disclosed on DRAS Communications Channel</b> A threat agent eavesdrops on traffic on the network between a DRAS and a customer system. This could leak private information to the threat agent. This might be the easiest attack that the agent can launch while not being detected by utilities</li> </ul>		
<b>Risk Statement</b>	<p>As part of the trial, all DER marketplace data is stored on databases (MongoDB, SQL Server) and other Pxise components (Azure environment). In discussions with AEMO stakeholders, no encryption at rest controls were identified across these databases and Pxise components. Apart from this information, participant identities (DIDs and VCs) are stored on the EWF DLT, which has encryption at rest.</p> <p>In further discussions with AEMO, it was identified that Encryption in transit (TLS/SSL) is not configured or configured consistently across the Azure environment across Pxise assets. This could lead to disclosure of sensitive information such as usernames &amp; passwords as well as other critical application data.</p> <p>Encryption at rest is designed to prevent unauthorised access to data in an event where the threat-actor has underlying physical access to data-stores.</p>		
<b>Applicability</b>	<p>AEMO/Market Operator - Yes Aggregator - Yes DNSP/DSO - No</p> <p>Based on discussions with AEMO, the DNSP/DSO will not have customer sensitive data as the DNSP/DSO is an operational network (demand &amp; supply of energy itself). At the point of assessment, no sensitive data was to be stored at the DNSP/DSO.</p>		
<b>Observations</b>	<ul style="list-style-type: none"> <li>▶ No data at rest encryption controls were able to be observed across AEMO's Azure Environment.</li> <li>▶ For encryption in transit, TLS 1.2 was documented as required as part of the EDGE Symphony SAD document (Section 9.2).</li> <li>▶ However, TLS 1.2 is not universal across the architecture and data-in-transit still poses a significant risk.</li> </ul>		
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Identity and Access Management-2A: MIL-1 and SP-1</b> Access requirements, including those for remote access, are determined.</li> <li>▶ <b>Information Sharing and Communications-1F: MIL-2 and SP-2</b> Provisions are established and maintained to enable secure sharing of sensitive or classified information.</li> </ul>		
<b>OWASP Mapping</b>	<p>A02:2021 - Cryptographic Failures A06:2021 - Vulnerable and Outdated Components</p>		

<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Ensure DER marketplace data is encrypted at rest at all datastores across all entities (Aggregator, DNSP/DSO and MO). Encryption algorithms should be industry best practice and should align with business and security requirements</li> <li>▶ Configure Transport Layer Security (TLS 1.2 and above) across communication channels in the DER Marketplace</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub - High Decentralised Hub - Low Point to Point - Medium
<b>Residual Risk rating</b>	Low/Medium

Table 11: Data exposure and unauthorised access attacks

#### 4.4.2.6 Blockchain-based attack

<b>Threat Agent</b>	External – malicious Internal – malicious	<b>Likelihood</b>	Possible
<b>Risk Rating</b>	High	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Disruption of operations on the Distributed Ledger (DLT)</li> <li>▶ Spoofing of identities in the DER Marketplace</li> <li>▶ Modify financial data (Bids/Offers)</li> </ul>		
<b>Threat scenarios</b>	A threat actor may exploit inherent weaknesses in the blockchain DLT, to launch a Denial-of-Service attack to disrupt the activities on the Project Edge network, causing unavailability of the network		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	No failure scenarios identified		
<b>Risk Statement</b>	<p>During the Project EDGE trial, Blockchain technology was being considered as the core backend system to store DER marketplace identities (DIDs and VCs). Few examples of Blockchain related attacks are listed below:</p> <p>Denial of Service attacks using spam transactions could be used to disrupt legitimate identity transactions thereby rendering the DER marketplace unavailable for a period of time</p> <p>Eclipse attacks are attacks in which an attacker can restrict/control communications to specific nodes on the P2P network. By doing so, an attacker could restrict certain communications to a node, or even send malicious information to a node.</p> <p>Sybil attacks redirect the inbound and outbound connections of an operational node from legitimate nodes to the threat actor's nodes to obtain information about the bids/offers that take place on it or to manipulate a bid/offer to make someone believe that it has been successfully executed, when in fact it has been manipulated. MitM based attacks.</p> <p>Note: Eclipse and Sybil attacks would have a larger impact once additional DER marketplace data is stored on the DLT. During the time of this assessment only DIDs and VCs were stored on the DLT.</p>		
<b>Applicability</b>	AEMO/Market Operator - Yes - in a Centralised architecture environment Aggregator - Yes - In a decentralised Architecture environment DNSP/DSO - No Blockchain based DLT will be leveraged for storing DER Marketplace identities across the DER marketplace. Based on the outcomes of architectural decisions (centralised vs decentralised hub), the DLT could be managed by the Aggregator or the MO.		
<b>Observations</b>	Energy Web employs Proof-of-Authority as its consensus protocol.		
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Supply Chain and External Dependencies Management-2A: MIL-1 and SP-1</b> Significant Cyber Security risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner.</li> <li>▶ <b>Supply Chain and External Dependencies Management-2J: MIL-3 and SP-3</b> Cyber Security risks due to external dependencies are managed according to the organisation's risk management criteria and process.</li> </ul>		
<b>OWASP Mapping</b>	A07:2021 - Identification and Authentication Failures		
<b>Proposed mitigating controls</b>	To prevent DoS based attacks:		

	<ul style="list-style-type: none"> <li>▶ Filtering transactions allows block creators the choice of which transactions are included in their blocks. By being able to identify and discard potential spam transactions, this can prevent the possibility of transaction flooding on the network</li> <li>▶ Ensuring appropriate resources have been configured - storage, processing, network bandwidth</li> </ul> <p>To prevent Eclipse based attacks:</p> <ul style="list-style-type: none"> <li>▶ Use validation and chain of trust systems</li> <li>▶ Use consensus protocol that implies a cost per identity or access to network resources</li> <li>▶ Create a reputation system where users with more time on the network have more power</li> </ul> <p>To prevent Sybil based attacks:</p> <ul style="list-style-type: none"> <li>▶ Have a reliable node selection process to ensure the network has well-identified and related nodes</li> <li>▶ Increase amount of node connections</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub – N/A Decentralised Hub – Medium/High Point to Point – N/A
<b>Residual Risk rating</b>	Low/Medium

Table 12: Blockchain-based attack

#### 4.4.2.7 Supply Chain attacks

<b>Threat Agent</b>	External – malicious Supply chain – compromised	<b>Likelihood</b>	Possible
<b>Risk Rating</b>	High	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Gain access to the DER Marketplace to perform malicious activities at present or have the capability to perform malicious activities in the future</li> <li>▶ Disruption of the operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> <li>▶ Perform malicious changes across devices or applications across the DER Marketplace with an intention of causing disruption to operations</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor may add malware during either the manufacturing, shipping, or installation stages to perform unauthorised actions</li> <li>▶ A supply chain entity may get compromised which may lead to malicious configurations or software delivered from the compromised entity</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>DGM.8 Supply Chain Vulnerabilities Used to Compromise Equipment</b> Lifecycle attacks against equipment during development, production, shipping, and maintenance can introduce deliberate errors that will result in failure under special conditions</li> <li>▶ <b>G.4 Supply Chain Attacks Weaken Trust in Equipment</b> A threat actor replaces a legitimate device with a maliciously altered device and introduces the device into the supply chain without directly compromising a manufacturing entity. This can be done by buying a legitimate device, buying, or creating a malicious device and returning the malicious device in place of the legitimate device as an exchange. Alteration may be a modification or deletion of existing functions or addition of unexpected functions</li> </ul>		
<b>Risk Statement</b>	Each entity across the DER Marketplace would have their own supply chains based on their business requirements. Such supply chains provide a threat actor with opportunities to perform malicious activities targeting a specific DER Marketplace entity. For example, a misconfigured device, or backdoor enabled software application.		

	Each entity should have appropriate Third-Party Risk Management (TPRM) processes which align with their business and risk management requirements. Such processes would allow for appropriate level of controls and processes providing visibility across actions and processes in the supply chain.
<b>Applicability</b>	AEMO/Market Operator - Yes Aggregator - Yes DNSP/DSO - Yes Each entity across the DER Marketplace has their own supply chains. Each entity should be responsible for having appropriate Third-Party risk management processes based on business and security requirements.
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Supply Chain and External Dependencies Management-2A: MIL-1 and SP-1</b> Significant Cyber Security risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner.</li> <li>▶ <b>Supply Chain and External Dependencies Management-2E: MIL-2 and SP-2</b> Cyber Security requirements, are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate.</li> <li>▶ <b>Supply Chain and External Dependencies Management-2N: MIL-3 and SP-3</b> Information sources are monitored to identify and avoid supply chain threats (for example, counterfeit parts, software, and services)</li> </ul>
<b>OWASP Mapping</b>	Not applicable - OWASP Top 10 does not apply to this risk, as application vulnerabilities do not fall under this specific risk.
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Implement a Third-Party Risk Management framework which aligns with business requirements</li> <li>▶ Ensure security controls and processes are in place which align with the criticality of third-parties/supply chains</li> <li>▶ If feasible, AEMO should provide guidance to all DER Marketplace entities on managing their Third-Party/Supply chain risk</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub - High Decentralised Hub – Medium/High Point to Point - High
<b>Residual Risk rating</b>	Low/Medium

Table 13: Supply Chain attacks

#### 4.4.2.8 Compromise of DER Marketplace entities & Critical Assets

<b>Threat Agent</b>	External – malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Likely
<b>Risk Rating</b>	High	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Disruption to DER Marketplace operations and services</li> <li>▶ Disruption to grid and bulk grid stability</li> <li>▶ Compromise of marketplace/consumer data</li> <li>▶ Reputational damage from the exploitation of an asset or entity of high criticality</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor may exploit an asset/application of high/critical importance of the DER marketplace, to cause significant impact on the day-to-day operations of the DER Marketplace</li> <li>▶ A disgruntled employee may exploit their legitimate access to the system to expose an asset/application of high/critical importance in DER marketplace, to cause significant impact on the functional operation of the network</li> </ul>		



	<ul style="list-style-type: none"> <li>▶ A threat actor could leverage weaknesses (software vulnerabilities, security misconfigurations, accidental exposure) across critical assets to gain unauthorised access to the DER Marketplace</li> <li>▶ Malicious nation state actors could specifically target critical operational assets or DER Marketplace entities to gain access to the DER Marketplace to cause financial and reputational harm</li> </ul>
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	No failure scenarios identified
<b>Risk Statement</b>	<p>Each entity across the DER Marketplace has a key role and has critical assets which could lead to significant loss of services in an event where an DER Marketplace entity or a critical asset at an entity were compromised. For example, a DNSP would not be able to supply energy requirements if their infrastructure went offline.</p> <p>DER Marketplace entities should have appropriate monitoring and alerting processes, Incident Response plans and Disaster Recovery processes. Redundant technologies should be implemented for critical assets and processes. The Department of Energy's (DOE) Cyber-Information Engineering (CIE) framework provides guidance on building Cyber Security practices into the design life cycle of engineered systems to impacts of a Cyber incident. The framework emphasises on "Assume Compromise" thereby driving requirements for appropriate detection, isolation, and mitigation of Cyber risks.</p> <p>Each entity across the DER Marketplace should also have an asset classification framework. Having an asset classification framework enables consistent application of risk management processes as well as security controls across critical and high-value assets. The SOCI Act (Security of Critical Infrastructure Act 2018) mandates recording and reporting of critical and high-value assets.</p>
<b>Applicability</b>	<p>AEMO/Market Operator - Yes</p> <p>Aggregator - Yes</p> <p>DNSP/DSO - Yes</p> <p>All entities in the DER marketplace have assets that are critical to their operation.</p>
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Asset, Change and Configuration Management-1D: MIL-2 and SP-2</b> Inventoried assets are prioritised based on their importance to the delivery of the function.</li> <li>▶ <b>Cyber Security Program Management-1C: MIL-2 and SP-2</b> The Cyber Security program strategy and priorities are documented and aligned with the organisation's strategic objectives and risk to critical infrastructure.</li> <li>▶ <b>Event and Incident Response, Continuity of Operations-2D: MIL-2 and SP-2</b> Criteria for Cyber Security event escalation, including Cyber Security incident criteria, are established based on the potential impact to the function.</li> </ul>
<b>OWASP Mapping</b>	Not applicable - OWASP Top 10 does not apply to this risk, as application vulnerabilities do not fall under this specific risk.
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ DER Marketplace entities should develop information security programs based on DOE's CIE framework alongside other known frameworks such as NIST</li> <li>▶ Appropriate detection, isolation and redundant technologies should be implemented across key DER Marketplace entities and critical assets</li> <li>▶ Implement a consolidated asset classification framework across the DER Marketplace or at an DER Marketplace entity level</li> <li>▶ Ensure risk management processes and security processes are aligned with the classification of assets</li> <li>▶ Security controls should also be applied in alignment with the criticality of assets, ensuring optimisation of available resources</li> <li>▶ Periodic review of the classification of assets should be performed to align with changing business and regulatory requirements</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	<p>Centralised Hub - High</p> <p>Decentralised Hub - Medium</p> <p>Point to Point – Medium/High</p>
<b>Residual Risk rating</b>	Low/Medium

Table 14: Compromise of Critical Assets

#### 4.4.2.9 Insider attacks/Internal threats

<b>Threat Agent</b>	Internal – malicious Internal - non-malicious	<b>Likelihood</b>	Unlikely
<b>Risk Rating</b>	<b>Medium</b>	<b>Consequence</b>	Major
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Disruption of the operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> <li>▶ Perform malicious changes across devices or applications across the DER Marketplace with an intention of causing disruption to operations</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A disgruntled employee may leverage their access to capture sensitive information for financial gain or use their access to disrupt day-to-day operations</li> <li>▶ A user may accidentally click on a phishing link which could lead to an external threat gaining access to DER marketplace data or applications</li> <li>▶ A threat actor may use vishing to gain information from an active user from the DER marketplace and use that information to conduct further attacks against the DER Marketplace</li> <li>▶ An IT employee can deploy a software patch which wasn't tested appropriately thereby causing disruption in day-to-day operations</li> <li>▶ An internal employee could install a software on their endpoint device which could be malicious/ransomware. Such software could disrupt operational activities and cause availability issues across the DER Marketplace</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<p><b>Generics.1 Malicious and Non-malicious Insiders Pose Range of Threats</b>            Authorised personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems and/or control networks</p>		
<b>Risk Statement</b>	<p>Due to the nature of the DER marketplace, different entities will have their own employee onboarding programs in-place. Such programs may or may not be aligned with industry requirements. Lack of appropriate background checks and specific technical controls in place to identify intended/accidental malicious behaviour could lead to significant impact across the DER Marketplace. Impact could range from disclosure of customer/sensitive PII data or disclosure of Bids and Offers information which could lead to financial as well as reputational damage.</p>		
<b>Applicability</b>	<p>AEMO/Market Operator - Yes            Aggregator - Yes            DNSP/DSO – Yes</p>		
<b>Observations</b>	<p>Reviewing onboarding and background checks wasn't in-scope for Project EDGE.</p>		
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Threat and Vulnerability Management-1D: MIL-2 and SP-2</b>                A threat profile for the function is established that includes characterisation of likely intent, capability, and target of threats to the function.</li> <li>▶ <b>Workforce Management-2E: MIL-3 and SP-3</b>                Risk designations are assigned to all positions that have access to the assets required for delivery of the function.</li> <li>▶ <b>Workforce Management-2F: MIL-3 and SP-3</b>                Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation.</li> </ul>		
<b>OWASP Mapping</b>	<p>Not applicable - OWASP Top 10 does not apply to this risk, as application vulnerabilities do not fall under this specific risk.</p>		
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Ensure appropriate onboarding and background/verification checks are performed for all entities across the DER Marketplace</li> <li>▶ Ensure appropriate alerting, incident management and response procedures are implemented across all DER Marketplace entities</li> <li>▶ Have appropriate security awareness training for all employees across the organisation</li> </ul>		

	<ul style="list-style-type: none"> <li>▶ If feasible, AEMO should provide guidance on security awareness training, technical controls, and incident management processes to other DER Marketplace entities</li> <li>▶ Implement appropriate UAM controls (4.2.10)</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	<p>Centralised Hub - High</p> <p>Decentralised Hub - Low</p> <p>Point to Point – Low/Medium</p>
<b>Residual Risk rating</b>	Low

Table 15: Insider attacks/Internal threats

#### 4.4.2.10 Lack of appropriate User Access Management processes could lead to disclosure of DER Marketplace data

<b>Threat Agent</b>	External - malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Unlikely
<b>Risk Rating</b>	<b>Medium</b>	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Disruption of the operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> <li>▶ Perform malicious changes across devices or applications across the DER Marketplace with an intention of causing disruption to operations</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor or a disgruntled employee may exploit inadequate identity access management rules (i.e., failure to deactivate old accounts), to perform unauthorised/unintended actions</li> <li>▶ Weak password policies could allow a threat actor to gain unauthorised access to DER Marketplace devices or applications</li> <li>▶ Weak access permissions or generic permissions across many multiple roles could allow accidental changes to DER devices or applications</li> <li>▶ Lack of Multi-Factor authentication could lead to changes to critical configurations on DER devices or applications across the DER Marketplace</li> <li>▶ Shared user accounts could be leveraged to access DER devices and applications across the DER Marketplace. Disclosure of such accounts could lead to unauthorised access</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>DGM.13 Poor Account Management Compromise</b> After a maintenance employee retires, computer service personnel forgot to deactivate the employees account on the network. A week later, a threat agent uses the employee's credentials to access the network</li> <li>▶ <b>AMI.10 Unauthorised Pricing Information Impacts Utility Revenue</b> The threat agent sends out unauthorised pricing information, such as Time-of-Use (TOU) pricing. This may result in either a loss or increase in utility revenue until the invalid price is recognised</li> <li>▶ <b>AMI.23 Meter Authentication Credentials are Compromised and Posted on Internet</b> A utility deploys all AMI devices with the same authentication credentials granting privileged access via the local infra-red port, and the credentials are compromised and posted on the Internet</li> <li>▶ <b>DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System</b> A threat agent performs reconnaissance of utility communications, electrical infrastructure, and ancillary systems to identify critical feeders and electrical equipment</li> <li>▶ <b>DGM.5 Remote Access Used to Compromise DMS</b> A threat agent compromises distribution management system (DMS) functionality through remote access modification of executable programs and libraries, rendering the DMS inoperable</li> </ul>		
<b>Risk Statement</b>	<p>DER Marketplace entity access management (DIDs and VCs) is performed at the DLT (based on Project EDGE). Based on architectural decisions, this DLT can be hosted at the Aggregator (Decentralised) or at the Market Operator (Centralised).</p> <p>User Access Management (UAM) review across the entity organisations was not part of the scope of Project EDGE. Weaknesses in UAM policies and processes within an entity's infrastructure could lead to disclosure of sensitive information or disruption to day-to-day operations.</p> <p>Also, due to the interconnected-ness of the DER Marketplace, some user accounts may be shared across entities. User account compromises at one entity could lead to unauthorised access to other entities too.</p>		

<b>Applicability</b>	<p>AEMO/Market Operator - Yes</p> <p>Aggregator - Yes/Potentially</p> <p>DNSP/DSO - Yes</p> <p>Blockchain based DLT will be leveraged for storing DER Marketplace identities across the environment. Each entity will have their own set of Digital Identifiers (DID) and Verifiable Credentials (VC)</p> <p>User identities for management of DER devices and applications is dependent on each entity.</p> <p>AEMO is responsible for developing and managing appropriate User Access Management (UAM) policies and processes across AEMO's infrastructure only. Other entities are responsible for their UAM policies and processes. AEMO can choose to provide guidance to entities to enable consistency using RBAC models across the Marketplace.</p>
<b>Observations</b>	<ul style="list-style-type: none"> <li>▶ Project EDGE was focused on the Entity ID management - DIDs and VCs on the DLT</li> <li>▶ User Access Management review for entity organisations wasn't in scope of the trial</li> <li>▶ AEMO does use jump hosts for privileged access to the Project EDGE environment. User management is done by Azure AD</li> </ul>
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Identity and Access Management-2B: MIL-1 and SP-1</b></li> </ul> <p>Access is granted to identities, at least in an ad hoc manner, based on requirements.</p> <ul style="list-style-type: none"> <li>▶ <b>Identity and Access Management-1G: MIL-3 and SP-1</b></li> </ul> <p>Requirements for credentials are informed by the organisation's risk criteria (for example, multifactor credentials for higher risk access)</p> <ul style="list-style-type: none"> <li>▶ <b>Identity and Access Management-2D: MIL-2 and SP-2</b></li> </ul> <p>Access requirements incorporate least privilege and separation of duties principles.</p>
<b>OWASP Mapping</b>	<p>A01:2021 - Broken Access Control</p> <p>A04:2021 - Insecure Design</p> <p>A07:2021 - Identification and Authentication Failures</p>
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Ensure appropriate UAM/IAM programs, processes and tools are implemented across each DER Marketplace entity organisation.</li> <li>▶ AEMO should provide guidance on UAM/IAM program expectations</li> <li>▶ Ensure appropriate alerting, incident management and response procedures are implemented across all DER Marketplace entities</li> <li>▶ If feasible, employ a single RBAC user access management model which can be leveraged by all entities/users across the DER Marketplace</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	<p>Centralised Hub - High</p> <p>Decentralised Hub - Low</p> <p>Point to Point – Medium/High</p>
<b>Residual Risk rating</b>	Low

Table 16: Lack of appropriate User Access Management processes could lead to disclosure of DER Marketplace data

#### 4.4.2.11 Weaknesses in Security Operations could lead to cyber-attacks not being identified or having greater impact

<b>Threat Agent</b>	External – malicious Internal - malicious Internal - non-malicious	<b>Likelihood</b>	Unlikely
<b>Risk Rating</b>	<b>Medium</b>	<b>Consequence</b>	Moderate
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Gain access to the DER Marketplace to perform malicious activities at present or have the capability to perform malicious activities in the future</li> <li>▶ Disruption of the operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Capture sensitive customer or operational data and distribute such data to competing parties or to other nation state actors for financial gain or to cause reputational damage</li> <li>▶ Perform malicious changes across devices or applications across the DER Marketplace with an intention of causing disruption to operations</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ Ongoing or newly initiated cyber-attacks against the DER Marketplace or a specific DER Marketplace entity</li> <li>▶ A malicious entity performing unauthorised or malicious actions on a specific device or application across the DER Marketplace</li> <li>▶ A non-malicious entity performing an accidental change on a device or an application</li> <li>▶ Introducing malicious software across the DER Marketplace, for example, a malicious USB drive, downloaded file from the Internet, browsing malicious websites</li> <li>▶ Malicious network activity across the DER Marketplace. For example, host/port scans initiated across the DER Marketplace</li> <li>▶ Cyber-attacks originating from one DER Marketplace entity targeting other DER Marketplace entities</li> </ul>		
<b>Rationale – Mapped with NESCOR Threat Scenarios</b>	<ul style="list-style-type: none"> <li>▶ <b>AMI.18 Unauthorised Devices Create DoS and Prevent Valid DR Messages</b> Unauthorised devices gain access to a home area network (HAN). The devices can then be used to create a Denial-of-Service (DoS) condition so that DR messages cannot reach end customer devices</li> <li>▶ <b>AMI.25 Known but Unpatched Vulnerabilities Exposes Infrastructure</b> A threat agent is able to gain access to the system by exploiting a known vulnerability that has not yet been patched</li> <li>▶ <b>ET.15 Malware Causes Discharge of EV to the Grid</b> A threat agent compromises the Vehicle-to-Grid (V2G) protocol that allows bi-directional flows of electricity. The threat agent may hack a protocol translation module directly or insert malware in the charging station management system</li> <li>▶ <b>Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats</b> Authorised personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks</li> <li>▶ <b>DGM.4 Malicious Code Injected into Substation Equipment via Remote Access</b> A threat agent uploads malicious code into substation equipment via remote engineering access, either through an IP network WAN or dialup to a linesharing switch (LSS)</li> </ul>		
<b>Risk Statement</b>	The DER marketplace is designed to have bi-directional flow of information with each single entity having significant amount of customer and operational data at a given point in time. Due to the interconnected-ness of the marketplace, a compromise of a single entity could have significant impacts across the DER marketplace. Lack of consolidated visibility over malicious activity and security incidents across the DER Marketplace, could lead to such activity going unnoticed for a long period of time which could affect the confidentiality and availability of data across the DER Marketplace.		
<b>Applicability</b>	AEMO/Market Operator - Yes		

	<p>Aggregator - Yes DNSP/DSO - Yes</p> <p>At the point of assessment, no integrated security operations environment was observed in Project EDGE. A consolidated view of security operations and events across the DER marketplace enable consistent incident triage and response across the DER marketplace enabling timely remediation.</p> <p>Based on discussions with AEMO, DNSPs and DSOs have their own operational environment and therefore not the responsibility of the Market Operator (AEMO). However, given the interconnected-ness of the DER Marketplace, it is recommended to have consolidated visibility across the entire environment. The overall ownership and responsibility of this consolidated environment wasn't discussed during the time of the assessment.</p>
<b>Observations</b>	Review of Security operational activities wasn't in scope for Project EDGE
<b>AESCSF Mapping</b>	<ul style="list-style-type: none"> <li>▶ <b>Event and Incident Response, Continuity of Operations-1B: MIL-1 and SP-1</b></li> </ul> <p>Detected Cyber Security events are reported, at least in an ad hoc manner.</p> <ul style="list-style-type: none"> <li>▶ <b>Event and Incident Response, Continuity of Operations-2B: MIL-1 and SP-1</b></li> </ul> <p>Cyber Security events are analysed, at least in an ad hoc manner, to support escalation and the declaration of Cyber Security incidents.</p> <ul style="list-style-type: none"> <li>▶ <b>Event and Incident Response, Continuity of Operations-1E: MIL-2 and SP-1</b></li> </ul> <p>There is a repository where Cyber Security events are logged based on the established criteria.</p>
<b>OWASP Mapping</b>	A09:2021 - Security Logging and Monitoring Failures
<b>Proposed mitigating controls</b>	<ul style="list-style-type: none"> <li>▶ Establish infrastructure and processes which provide a consolidated view of alerts, incidents, and security issues for entities across the DER Marketplace</li> <li>▶ Each entity should have their dedicated processes to manage security incidents. AEMO should have visibility and provide guidance in such cases</li> <li>▶ Establish a centralised governance structure, along with Incident Response plans and procedures enabling timely triage and remediation of security incidents and malicious activity across the DER Marketplace</li> </ul>
<b>Impact on the DER Marketplace based on Data Exchange model</b>	<p>Centralised Hub - High Decentralised Hub - High Point to Point - High</p>
<b>Residual Risk rating</b>	Low

Table 17: Weaknesses in Security Operations could lead to cyber-attacks not being identified or having greater impact

#### 4.4.2.12 Threat actors targeting weak onboarding and registration processes to gain access to the DER Marketplace

<b>Threat Agent</b>	External - malicious	<b>Likelihood</b>	Rare
<b>Risk Rating</b>	Medium	<b>Consequence</b>	Major
<b>Threat objectives</b>	<ul style="list-style-type: none"> <li>▶ Gain unauthorised access to customer and/or operational data for financial gain</li> <li>▶ Disruption of the operations severely affecting the availability of energy across the DER marketplace</li> <li>▶ Gain access to the DER Marketplace to perform malicious activities at present or have the capability to perform malicious activities in the future.</li> </ul>		
<b>Threat scenarios</b>	<ul style="list-style-type: none"> <li>▶ A threat actor could falsify information about themselves/third-parties to gain access to the DER Marketplace</li> <li>▶ A threat actor bypasses onboarding steps or processes during registration which could give them access to the DER Marketplace</li> <li>▶ A threat actor could impersonate valid credentials of another entity and gain access to the DER Marketplace</li> <li>▶ A threat actor could leverage weak onboarding processes to gain access to the DER Marketplace</li> </ul>		

<p><b>Rationale – Mapped with NESCOR Threat Scenarios</b></p>	<ul style="list-style-type: none"> <li>▶ <b>Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats</b>            Authorised personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks</li> <li>▶ <b>DER.2 DER's Rogue Wireless Connection Exposes the DER System to Threat Agents via the Internet</b>            An industrial or large commercial DER system is configured for local operational access through a wireless network, but is erroneously connected to the company's wireless corporate network, thus exposing the DER system to the Internet</li> <li>▶ <b>DER.21 DER System Registration Information Stolen</b>            A threat agent accesses the systems and steals the customer DER registration information, using it for industrial espionage or other purposes, causing confidentiality impacts to these utility customers</li> </ul>
<p><b>Risk Statement</b></p>	<p>Before joining the DER marketplace, each participant (consumer, prosumer, aggregator, DSO/DNSP) needs to go through the registration and onboarding process to generate blockchain identities and public key infrastructure (PKI) certificates for participating the DER Marketplace. However, during the time of assessment, the implementation strategy of the DER Marketplace DLT (Centralised vs Decentralised) was not finalised.</p> <p>Access to the DER marketplace should only be provided after appropriate checks against the new participant has taken place. Without such processes, a malicious participant could be in a position to initiate malicious actions against other entities across the DER Marketplace. These malicious actions could include:</p> <ol style="list-style-type: none"> <li>1) Gain access to sensitive customer information and PII (Aggregator)</li> <li>2) Disrupt operations severely affecting the energy distribution across the DER Marketplace (DNSP/DSO and AEMO)</li> <li>3) Have the ability to perform a range of malicious attacks at a point in time, or in the future</li> <li>4) Capture information on the DER Marketplace and leverage such information for financial gain or to cause reputational damage to the Market operator (AEMO)</li> </ol>
<p><b>Applicability</b></p>	<p>AEMO/Market Operator - Yes            Aggregator - Yes            DNSP/DSO - Yes</p> <p>Review of onboarding and registration processes wasn't part of Project EDGE. However, in discussions with AEMO, it was identified that AEMO performs appropriate checks for new entities participating in the DER Marketplace. These checks ensure entities claim who they are and have the appropriate controls and processes before participation in the DER Marketplace.</p>
<p><b>Observations</b></p>	<ul style="list-style-type: none"> <li>▶ Onboarding processes for the different entities across the DER marketplace was not in scope as part of the trial. The trial had established participants - Mondo (Aggregator) &amp; AusNet (DNSP/DSO)</li> <li>▶ It was identified that there are checks and balances in place against risks arising from onboarding and registration processes</li> </ul>
<p><b>AESCSF Mapping</b></p>	<ul style="list-style-type: none"> <li>▶ <b>Supply Chain and External Dependencies Management-2N: MIL-3 and SP-3</b>            Information sources are monitored to identify and avoid supply chain threats (for example, counterfeit parts, software, and services).</li> <li>▶ <b>Workforce Management-2F: MIL-3 and SP-3</b>            Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation.</li> </ul>
<p><b>OWASP Mapping</b></p>	<p>Not applicable - OWASP Top 10 does not apply to this risk, as application vulnerabilities do not fall under this specific risk.</p>
<p><b>Proposed mitigating controls</b></p>	<ul style="list-style-type: none"> <li>▶ Ensure registration &amp; onboarding processes align with business and regulatory requirements</li> <li>▶ Background checks (based on type of participant) should be performed before access has been given to the DER marketplace</li> <li>▶ DER marketplace entities should have appropriate checks and onboarding processes for their third-party suppliers to ensure supply chain attacks are at a minimum (4.2.7)</li> </ul>



<b>Impact on the DER Marketplace based on Data Exchange model</b>	Centralised Hub – Medium/High Decentralised Hub - Medium/High Point to Point - Low
<b>Residual Risk rating</b>	Low

*Table 18: Threat actors targeting weak onboarding and registration processes to gain access to the DER Marketplace*

## 5. Data Exchange Resilience and Compensatory Controls

This section outlines an assessment of the required levels of DER data exchange resilience and compensatory control considerations across the integration options to deliver resilient and scalable DER data exchange. The approaches assessed within this report are:

- ▶ Point-to-point integration
- ▶ Centralised Hub (CH)
- ▶ Decentralised Data Hub (DDH)

The definitions for each integration option can be found in Section **Error! Reference source not found**.3.2.3 of this document.

### 5.1 Definitions and scope

According to Integrated Service Plan 2020, power system resilience is *the “ability of the system to limit the extent, severity, and duration of system degradation following an extreme event”*. Maintaining power system resilience has long been embedded in energy system planning.

For this report, data exchange resilience has been defined as the ability to withstand and recover from incidents or other causes of interruption to DER data exchange. Specifically, this report will consider resilience of the conceptual approaches to data exchange as a measure of their respective ability to limit the extent, severity, and duration of an outage due to the below factors:

- ▶ Redundancy and Failover/Failsafe
- ▶ Complexity
- ▶ Scalability

Compensatory control is considered as the process considerations that define the behaviour of DER in the event of a communication failure. Each conceptual approach to data exchange has been considered for its capability to monitor and enact compensatory control for each of the below compensatory control triggers:

- ▶ Low/Bad Data quality
- ▶ Latency and slow response times
- ▶ Trust of market participants

Compensatory control will also consider the resilience requirements for data exchange as well as the post-conditions on triggering a compensatory control. For detail on the circumstances and actions on the occurrence of a threat please see [Section 4- Cyber Threat Assessment](#) of this document

#### 5.1.1 Out of Scope

This theoretical assessment of data exchange resilience and compensatory controls does not evaluate the following:

- ▶ Resilience of the energy network as defined by but not limited to:
  - Maintaining frequency control
  - Voltage Stability

- Black Restart capability needs
- ▶ Cyber-attack resilience of data exchange options is covered in the previous section
- ▶ Communications between smart appliances, inverter controls and the grid and other switching controls
- ▶ Operational data processing and management by the DNSP's network control system
- ▶ Telemetry of operational data and transmission of commands to and from AEMO control centres that normally utilise secure private networks, and
- ▶ The systems and processes used to register and qualify DER assets.

## 5.1.2 Assumptions

The assessment of de-centralised datahub options will consider two use cases for distributed computing discussed in the Project EDGE solution architecture. At the time of this report, these two cases have matured in regards to the solution architecture and business process requirements so that they could be assessed for resilience and compensatory control requirements

- ▶ Use Case 1: Distributed Identity Management (Diagram Below):

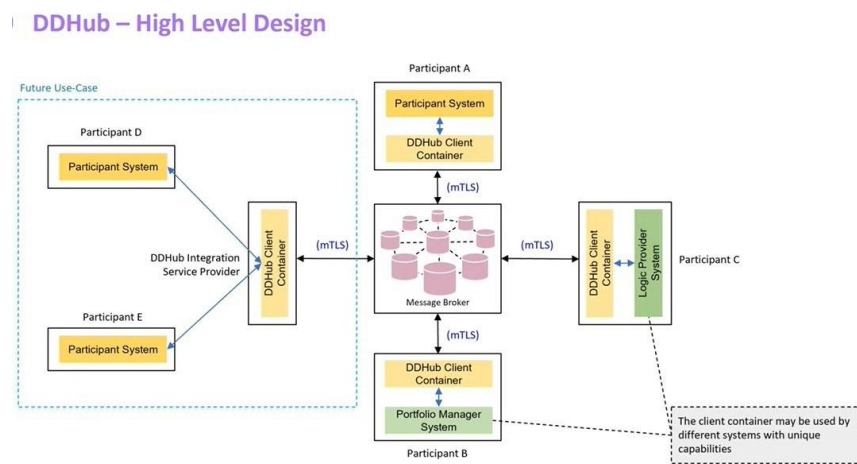


Figure 15: Distributed Identity Management

- ▶ Use Case 2: Dynamic Operating Envelope (DoE) Passthrough (Diagram Below) where:
  1. A DNSP submits a DoE to the datahub (publish)
  2. Decentralised workers receive DoE (subscribe)
  3. Workers return NMIs partitioned by their managing Aggregator
  4. Aggregators receive their relevant Operating Envelopes
  5. AEMO receives a copy of the partitioned Operating Envelopes

## DOE Passthrough - Overview

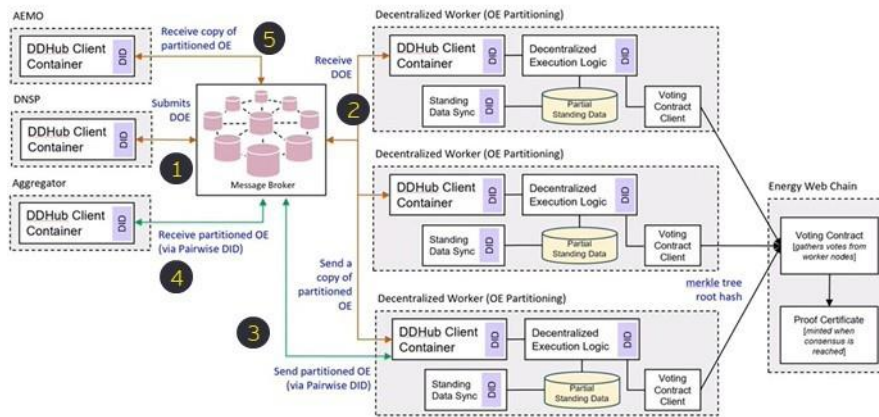


Figure 16: Dynamic Operating Envelope (DoE) Passthrough

## 5.2 Assessment Approach

### 5.2.1 Assessment Framework

The assessment framework considers three elements – principal alignment, resilience, and compensatory controls. Each of which are summarised described in the following points and illustrated in figure 17.

#### 1. Alignment to Data Exchanges Principles

This assessment considers the Project EDGE data exchange design principles to highlight key capability requirements that are critical to delivering a resilient and reliable data exchange, as well as any related compensatory controls to ensure the secure delivery of energy to consumers. Where an alignment to data exchange principles has been identified it has been documented as part of the assessment 'notes'. For reference the data exchange design principles have been documented below.

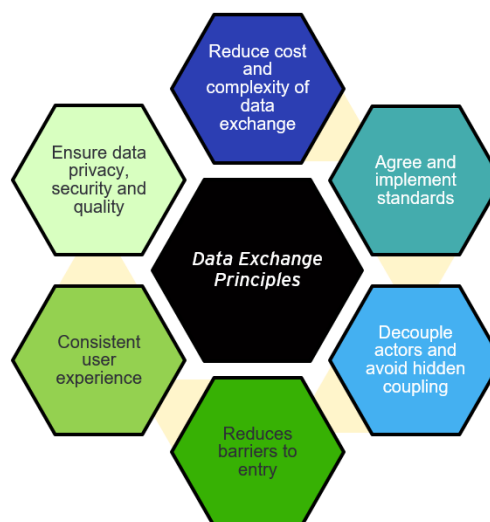


Figure 17 - Project EDGE Data Exchange Design Principles<sup>24</sup>

<sup>24</sup> Project EDGE Research Plan. Available: <https://aemo.com.au/-/media/files/initiatives/der/2022/master-research-plan-edge.pdf?la=en>

## 2. Data Exchange Resilience

The resilience of each data exchange conceptual approach will be assessed their respective ability to limit the extent, severity, and duration of an outage due to the below factors:

- ▶ Redundancy and Failover/Failsafe
- ▶ Complexity
- ▶ Scalability

## 3. Compensatory Controls

Data exchange conceptual approaches are considered for their capability to enact compensatory controls to ensure the safe, reliable, and secure supply of electricity.

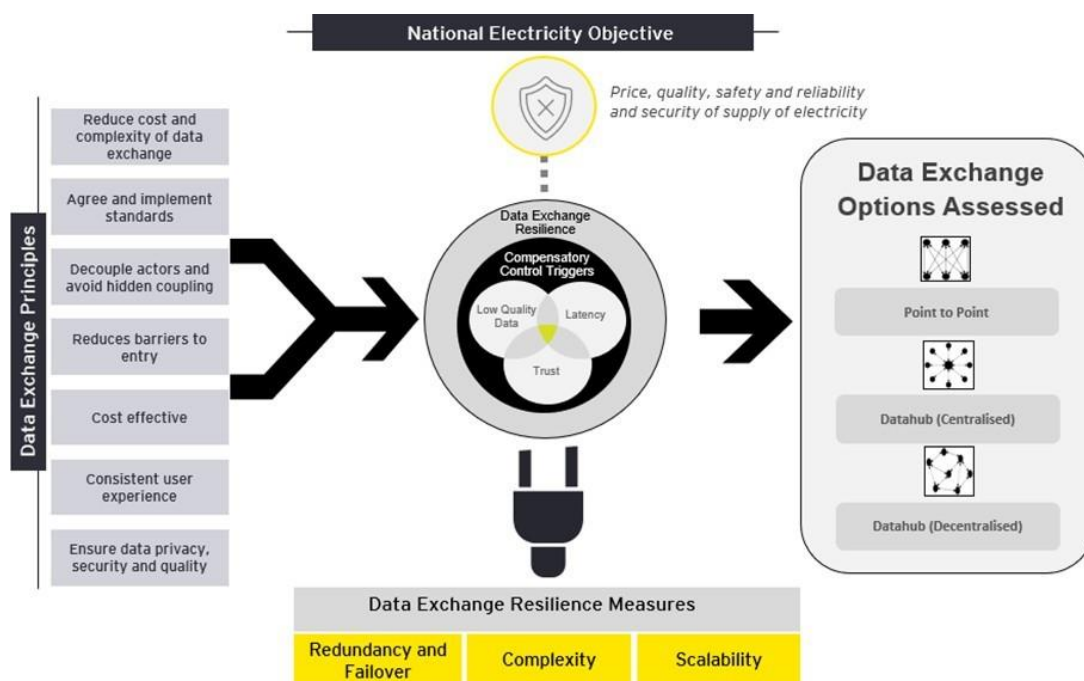


Figure 18: Resilience and Compensatory Controls Assessment Approach

## 5.3 Data Exchange Resilience

### 5.3.1 Introduction

According to the Integrated Service Plan (ISP) 2020, power system resilience is the ability of the system to limit the extent, severity, and duration of system degradation following an extreme event. Maintaining power system resilience has long been embedded in energy system planning.

For this assessment, data exchange resilience has been defined as the ability to withstand and recover from incidents or other causes of interruption to DER data exchange. Specifically, this assessment will consider resilience of the conceptual approaches to data exchange as a measure of their respective ability to limit the extent, severity, and duration of an outage due to the below factors:

- ▶ Scalability, that is, their ability to ensure only trusted participation and their scalability<sup>25</sup>. For example, the AEMO’s ISP 2022 “step-change” scenario that envisages over 100 GW of DER by 2050 including VPPs and vehicle-to-grid (V2G) services..
- ▶ Redundancy in the event of data exchange Failure and Failover/failsafe in order to prevent data loss
- ▶ Complexity of the data exchange conceptual approach to enable recovery from incidents.

Compensatory control is considered as the processes that define the behaviour of DER in the event of a communication failure. The below triggers for compensatory control have been considered as well as each conceptual approach to data exchanges capability to monitor and enact compensatory control:

- ▶ Low/Bad Data quality
- ▶ Latency and slow response times
- ▶ Trust of market participants

Together, these possible triggers provide a measure for resilience of each data exchange option, that is, the information availability, stability of data exchange ecosystem as well as the scalability of data exchange options.

## 5.3.2 Data Exchange Resilience Assessment

### Data Exchange Scalability

Each data exchange approach has been considered for their respective abilities to facilitate data exchange as the energy network reaches greater levels of DER penetration i.e., data exchange scalability. A conceptual data exchange approach that is not scalable may have an additional risk of incident and failure when required to manage the exchange of DER data at this scale, in near real-time and ensure power system resilience through seasonal variations in output.

---

<sup>25</sup> Scalability reflects the ability to adapt to increased demand over short and extended periods of time.

Data Scalability		
Data Exchange Approach	Assessment Outcomes	Notes
Point to Point	Low Fit	<p>Initially, point to point accelerates solution development because there is no need for a Data Hub. However, as new participants join the marketplace, they are required to tightly coupled, where systems are strongly associated so that changes to one component will impact the capability and performance of another.</p> <p>Point-to-point integration methods are typically not as scalable because the number of nodes within the environment are directly proportional to the number of entities that can utilise the network, and hence each may have a differing governing system and capability. As each new node will need to be manually connected to other required nodes with potentially different architecture designs makes this a time-consuming process.</p> <p>Additionally, each interface has to be updated and agreed by both parties if new versions or new features are to be included.</p>
Data Hub (centralised)	Medium Fit	<p>The data hub option allows for granular scaling of solution. When workloads peak additional compute can add centrally to relieve peak. Similarly, compute could shrink on demand.</p> <p>As it is participant independent, a data hub allows for the rapid onboarding of new participants, additions of new processes as well as maintaining data integrity across multiple participants</p> <p>A centralised integration method is more scalable than point to point approach. This is due to a characteristic of a centralised hub, acting as a governing body whose purpose is to standardise, enforce, and provide a central information source for other ecosystem parties to use. This highlights the pitfalls of a point-to-point integration approach as all standards for capability, communication and availability can be enforced by a single entity.</p> <p>For a centralised hub approach, only the data hub and one party need to update/change an interface which doesn't require all parties to update. An independent body, like the Information Exchange Committee (IEC) can manage the creation of new (standardised communications) which may be introduced by different parties through the hub. This may require all parties to upgrade or use these new features.</p> <p><b>Project EDGE principle: Decouple actors and avoid hidden coupling</b></p> <p><b>Project EDGE principle: Reduce cost and complexity of data exchange</b></p> <p><b>Project EDGE principle: Reduces barriers to entry</b></p>
Data Hub (de-centralised)	High Fit	<p>The distributed computing of the de-centralised Data Hub approach enables the greatest scalability of each of the options considered, as decentralised resources can be leveraged to grow and shrink the distributed computing requirements on demand. Additionally, these resources may be recruited at less cost than would be required for a software and/or hardware refresh of a centralised approach.</p> <p>As the need for DER Data exchange grows to a "step-change" level defined in the ISP 2022, the "shared-asset" approach to the decentralised data exchange may have broader scalability benefits.</p> <p>A decentralised approach may enable broader ownership of the digital infrastructure (rather than a centralised approach) enabling greater trust and transparency to potentially foster greater levels of innovation and collaboration, to add functionality to the infrastructure as DER scales</p> <p><b>Project EDGE principle: Decouple actors and avoid hidden coupling</b></p> <p><b>Project EDGE principle: Reduce cost and complexity of data exchange</b></p> <p><b>Project EDGE principle: Reduces barriers to entry</b></p>

--	--	--

Table 19: Data Exchange Scalability

### Data Exchange Redundancy and Failover

Data redundancy refers to the practice of keeping data in two or more places. Data redundancy ensures an organisation can provide continued operations or services in the event something happens to its data -- for example, in the case of data corruption or data loss. For DER data exchange, data redundancy is essential for the partitioning of NMI to Aggregator relationships in the event of data exchange failover to secondary systems of control.

Data Redundancy		
Data Exchange Option	Assessment Outcomes	Notes
Point to Point	Low Fit	<p>Point to point data exchange relies on participants maintaining separate databases, siloing DER data and reducing the visibility of the latest and most accurate data set.</p> <p>Point-to-point integration method is complex and difficult to administer due to the number of varying architecture types, governing bodies, communication methods, capabilities, capacity, and willingness to participate.</p> <p>Recovering from system outages may take significantly longer than expected, as many different groups need to be organised and galvanised to find a solution.</p>
Data Hub (centralised)	Medium Fit	<p>Allows for buffering of exchanged data until they can be processed by the data recipient. In the instance of single participant failure, the data hub can persist data so that it can be processed when the data recipient is available again. In this sense, the datahub provides a delivery guarantee.</p> <p>The restoration of a centralised integration method is simpler than a point-to-point approach due to the smaller number of entities, systems, hardware, and reduced number communication channels that need to be created, coordinated and consulted with.</p>
Data Hub (de-centralised)	High Fit	<p>A decentralised integration approach is the most stable integration approach due to the architecture having no single point of failure using multiple decentralised nodes, maintaining the network in a transparent, immutable, and censorship-resistant manner. Even when a portion of these nodes go offline, the decentralised network can continue to operate in an effective manner.</p>

Table 20: Data Exchange Redundancy and Failover

### Data Exchange Complexity

Data Complexity - Highly complex data is defined as data with multiple related elements or where specific components are not known in advance. For example, where DoEs are provided by a DSO containing only NMIs and require mapping to Aggregators across potentially millions of customers.



Data Complexity		
Data Exchange Option	Assessment Outcomes	Notes
Point to Point	Low Fit	<p>Point to point integration is initially less complex than other options but each participant must be tightly coupled to the participants they need to interact with. Participant DNSPs must also store and maintain the mapping for partitions of dynamic operating envelopes by representative aggregators.</p> <p>Tight coupling allows for simpler and faster integration as well as reduced difficulty in error handling. However, the interoperability of a point-to-point approach is limited as each node within the ecosystem needs to establish a communication channel with other required nodes that exist in the same ecosystem. While there can be bi-directional communication between two nodes it is more complex to form between multiple nodes limiting the exchange of information.</p> <p>A data model "standard" and communication protocol can make the point-to-point solution more replicable, but there may be small differences in how each party implements a standard that can reduce the interoperability and scalability of the approach.</p>
Data Hub (centralised)	High Fit	<p>Although the adoption of a data hub adds a new layer of integration that does not exist in point-to-point, maintenance and renewal of centralised approach will become less complex than point to point with scale as new integrations are added.</p> <p>Loose coupling (which is where systems are weakly associated so that changes to one component have the least impact on the capability and performance of another), introduces another layer of integration that may be required to translate, reformat and restructure data.</p> <p>However, a centralised integration approach provides improved interoperability as all nodes within the ecosystem can readily share and use information using the central hub while also maintaining their own personal data.</p> <p>A centralised hub provides the ability for newcomers to leverage a standardised, well documented, and accessible framework in which to build their product. Hence a centralised integration method provides more modularity than a point-to-point method.</p> <p>The centralised hub enables participants to exchange information and maintain their own personal data in a standardised, secure, and consistent manner.</p> <p><b>Project EDGE principle: Decouple actors and avoid hidden coupling</b></p> <p><b>Project EDGE principle: Reduces barriers to entry</b></p>

Data Hub (de-centralised)	High Fit	<p>Initially, the de-centralised data hub is a more complex data exchange approach than centralised and point-to-point.</p> <p>However it maintains the principles of loose coupling, introduces standardised approaches and distributed identities that reduce complexity as DER scales as less interfaces will need to be maintained.</p> <p>With distributed identity management, the decentralised approach may reduce barriers to entry and reduce the costs for network operators in identifying new connections to enrol, qualify and register every asset that provides services to the electricity grid. Additionally, participants will maintain their own personal data in a standardised, secure, and consistent manner. Backed by distributed identity management, the decentralised approach may become less complex than a centralised hub at scale with a reduced manual workload.</p> <p>Decentralised networks also eliminate the need for a centralised interface broker. Using digital identities, highly complex data can be exchanged and processed in an automated way without the need for a centralised hub as a broker.</p> <p><b>Project EDGE principle: Decouple actors and avoid hidden coupling</b></p> <p><b>Project EDGE principle: Reduce cost and complexity of data exchange</b></p> <p><b>Project EDGE principle: Reduces barriers to entry</b></p>
---------------------------	----------	---

Table 21: Data Exchange Complexity

## 5.4 Compensatory Controls

### 5.4.1 Overview

Compensatory control addresses the processes that define the behaviour of DER as well as the considerations for communication redundancy requirements in the event of a communication failure, loss of trust in one or many market participants, low-quality data, and/or high latency of messaging.

Increased penetration of DER will likely decrease the control that DNSPs have over the energy resources in power grids and DER deployments, and present additional risks due to the number of devices and access points that operate outside the typical DNSP’s scope. Compensatory control should act as the “fail-safe” to address these risks, and enable high levels of renewable penetration and maintain system security. To aid network planning, control and operations compensatory control parameters should be defined at the time of DER registration in the marketplace and, in the future, considered with how to best manage the quality, safety and reliability and security of the supply of electricity.

This analysis of compensatory control considers AS/NZS 4777.2, an existing engineering standard for behaviour and expected performance of inverters at low voltages (such as households or small-scale commercial), as well as IEEE 2030.5, a standard for communication between smart grid and consumers. There are compensatory controls built into the AS/NZS 4777.2.2020 that define the conditions in which inverters should stay connected and generating power to the electricity grid, or disconnect to support power system security and prevent major events. These conditions, including speed of isolation and islanding, will likely be triggered in a power outage or loss of supply to the connected device. The IEEE 2030.5 defines the behaviour and expected outcome in the case of loss of communication, i.e., the loss of DER data exchange.

An example of an engineering control for communication networks is found AEMO’s standard for Power System Data Communication 2022<sup>26</sup>, where power system data exchange must be capable of remaining operational for up to 10 hours following loss of external AC supply. A similar requirement may be proposed for telemetry of data between the individual remote monitoring and control

<sup>26</sup> AEMO, 2022. Available: <https://aemo.com.au/consultations/current-and-closed-consultations/review-of-power-system-data-communication-standard>

equipment and Intervening Facilities. This requirement may also apply to the Intervening Facilities themselves. Variations to these requirements may be required for smaller participants connecting directly to AEMO, subject to individual and regional significance. With this consideration, compensatory control should be able to be triggered even without external AC supply, for example, in the event of a network outage.

A compensatory control should be enforced by the controlled device and monitored by their representative aggregator. If a compensatory control is triggered, and the controlled device does not comply, an agreed import/export limit a notification could be sent to the DNSP's network control system allowing the relevant circuit breaker to be opened to disconnect load/generation/storage (as applicable). In the case of DER, as part of Project EDGE, this may result in the disconnection of unrelated but networked customers (The cost burden of these kinds of outages should be considered in further stakeholder analysis and research).

As part of network planning, DNSP's should identify, either individual or networked, DER that play an important role in the reliability and security of supply of electricity and targeted protection and control processes should be implemented for these DER.

### 5.4.2 SA Power Networks' Example of Compensatory Control

An example of an implementation of compensatory control is found in ARENA's Flexible Exports program, where SA Power Networks (SAPN) have adopted the IEEE 2030.5 (Smart Energy Profile 2.0), a standard for communication between smart grid and consumers. This standard is built using Internet of Things (IoT) concepts and gives consumers a variety of means to manage their energy usage and generation. Information exchanged using the standard includes pricing, demand response, and energy usage, and enables the integration of devices such as smart thermostats, meters, plug-in EVs, smart inverters, and smart appliances.

To ensure system security, SAPN has utilised IEEE2030.5's "DefaultDERControl" control mode as a failsafe to revert DER to minimal export on the loss of communications. IEEE2030.5 defines "DefaultDERControl" as the *control mode information to be used if no active DERControl is found*. Note that this form of compensatory control is for loss of communications; if the DER has been compromised by a cyber-attack, this function for compensatory control would not apply.

SAPN are using this standard to communicate flexible export limit (or dynamic operating envelope) schedules to customer agents.<sup>27</sup> These schedules typically run for a 24-hour rolling window, and devices regularly receive new export limit schedules from the SAPN system. If devices lose communications (for example, internet), then it is expected that the device will continue operating using the most recently downloaded schedule.

The DefaultDERControl setting is configurable and can be changed based on prevailing circumstances, and devices would have this setting updated the next time they download it.

Currently, SAPN's DefaultDERControl setting curtails export limits based on a 1-hour scale decaying confidence schedule. Where after two hours without communication, the controlled device will revert to minimal export, failsafe mode (diagram below).

---

<sup>27</sup> SAPN, 2020. Flexible Exports program. Available: <https://www.sapowernetworks.com.au/industry/flexible-exports/>

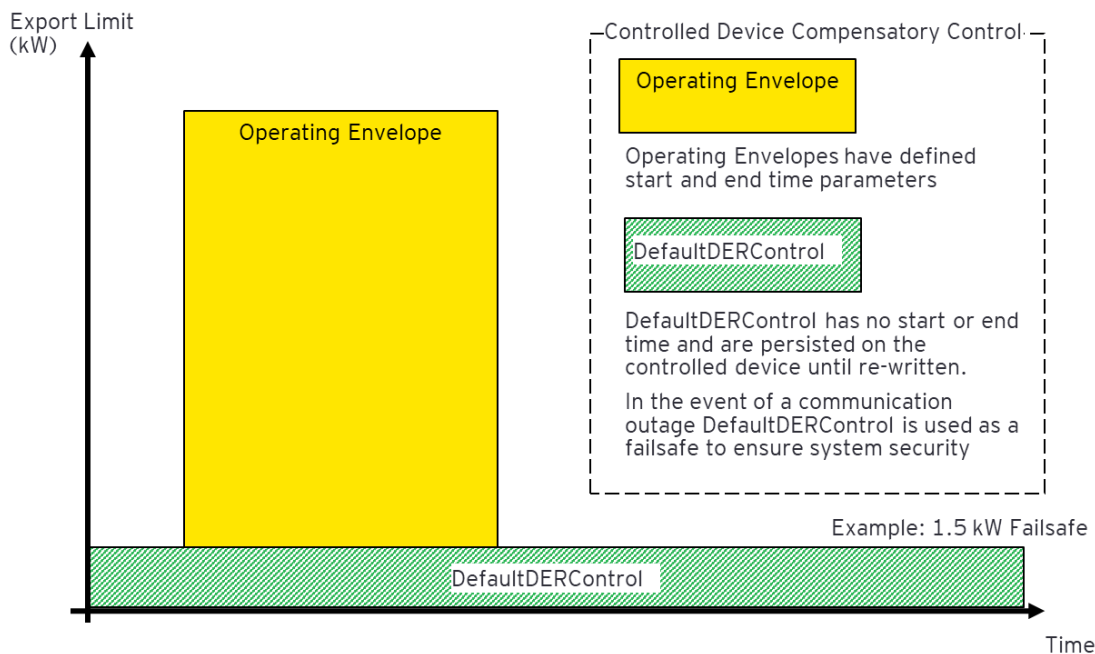


Figure 19: Compensatory Control Overview

This procedure implements effective controls to curtail DER export with an extended loss of communication, ensuring system security with the existing level of DER penetration. Currently, if there is an extended communication network outage, SAPN provide AEMO a static view of the expected loss of generation for that outage (for example, 2 hours after the communication outage)

It is important to consider that, with greater penetration of DER, this procedure may need to be further developed. SA Power Networks is currently assessing how the DefaultDERControl procedures can be updated with greater levels of DER penetration. This may include the development of an operational procedure between SAPN and AEMO control rooms, or dynamic communication between SAPN and AEMO to agree different DefaultDERControl settings to apply under different seasons or operating conditions.

### 5.4.3 Triggers for compensatory control

Beyond a total loss of communication between market participants and controlled devices, other possible pre-conditions that would trigger compensatory controls are considered along with the data exchange’s capability to monitor and enact compensatory control in the case of these triggers occurring. The below triggers represent the most significant risks to data exchange resilience:

- ▶ Low/Bad Data quality
- ▶ Latency and slow response times
- ▶ Loss of trust in one or many market participants

#### 5.4.3.1 Loss of communication

A total loss of communication to one or more market participants can represent a risk to system reliability and security. While resilient and redundant communications should be considered as a key risk mitigation, a loss of communication should be considered a trigger for compensatory control. Without communication to a device, to ensure compliance with import/export limitations, the DNSP cannot effectively manage system resilience and security of supply.

**Date Exchange Compensatory Control Consideration – Loss of Communication**

Point to Point
<p>Point to point data exchange limits the impact on single party loss of communications. Compensatory control can be limited to only the impacted party where;</p> <ul style="list-style-type: none"> <li>• in the case of the DNSP losing communication, DER could revert to their failsafe protocol and;</li> <li>• a single aggregator loses communications to part of its fleet, alternative-controlled devices may allow for corrective control to improve system stability and mitigate any impacts to the security of supply</li> </ul>
Datahub (Centralised)
<p>The datahub is a potential single point of failure, unless architected with multi-site redundancy. Incidents that impact the availability of the datahub may result in a complete failure of the DER energy market across the NEM. The DER datahub must be designed for high availability compensatory controls to ensure the security of the supply throughout data exchange failure.</p>
Datahub (De-centralised)
<p>Distributed computing reduces the reliance on a single party (centralised data hub). In the event of loss of communication participants may either revert to failsafe protocol and/or allow for corrective control to improve system stability and mitigate any impacts to security of supply dependent on their role.</p>

#### 5.4.3.2 Data Quality

Quality data can be defined as the validity, accuracy, consistency, completeness, appropriateness, and timeliness of data being exchanged (see figure below for further detail). A lack of quality data due to actors operating in silos and data being inconsistent across the internal and external ecosystems of DER market participants, may be a limiting factor in the successful roll out of a DER marketplace.

According to the Power System Data Communication Standard 2022<sup>28</sup>, the provision of poor data quality has similar effects on operations of AEMO's systems as the failure to receive data at all. For this reason, the provision of quality data is to be considered in the same way as an outage or failure of data exchange. It is recommended that a DER Data Exchange Data Quality Framework is established to provide a guide to stakeholder groups for implementing data quality controls and addressing data quality issues.

Compensatory control provides a failsafe if high-severity data quality issues are identified that would impact system security as defined by an agreed data quality standard.

<sup>28</sup> AEMO, 2022. Available: <https://aemo.com.au/consultations/current-and-closed-consultations/review-of-power-system-data-communication-standard>



Figure 20: Example Data Quality Measures  
 Source: EY Data Quality Framework (2022)

Date Exchange Compensatory Control Consideration – Data Quality
Point to Point
<p>Point-to-point data exchange, even with the alignment with an agreed common standard, requires each DNSP to develop physical data standards, derived from agreed standards, that may add complexity to customer agents operating across multiple DNSPs. Additionally, small differences in data standards may introduce issues of data validity as well as appropriateness of data across DNSPs. These issues create additional cost to industry that could be passed onto the aggregator’s customers, and may also create entry barriers because of technical and cost burden. For example, where a participant’s data is known to be corrupted, incurred or poorly structured, workarounds may be required.</p> <p>For ongoing measurement of data quality, this option would require additional data-sharing agreements between individual participants.</p>
Datahub (Centralised)
<p>Effective monitoring of data quality requires a centralised governance control framework best suited to the datahub option for data exchange. A datahub allows for establishing standards for data quality measures such as accuracy and timeliness of data exchanged that can be monitored centrally. The datahub approach allows for the isolation of participants from one another, decoupling, allowing for increased flexibility, better visibility, reduced overall industry administration costs and reduced interdependencies between participants.</p> <p>Additionally, a datahub allows individuals to follow a different protocol or upgrade pathway. This means that not all users of the datahub are required to use the same protocol or be on the same protocol version (for example, provision of backwards compatibility).</p>
Datahub (De-centralised)
De-centralised datahub provides the benefit of a governance control framework while potentially leveraging distributed computing for the validation of records, without the need for a

single authoritative source or data store. When adopting the distributed hub conceptual architecture approach, participants will have the ability to reduce reliance on manual interventions for monitoring, aggregating and sharing data.

### 5.4.3.3 Latency

High levels of latency may introduce unacceptable risks to power system security and, therefore, should be considered as a trigger for compensatory control. Latency refers to the time it takes for data to be transmitted between DER marketplace participants. Failure to provide data within agreed tolerances of timeliness, (that is, the degree that data represents reality from the required point in time), can create significant issues for real time operational applications and processes dependent upon analysis of the exchanged data.

<b>Data Exchange Compensatory Control Consideration – Latency</b>
Point to Point
In general, the point-to-point data exchange will have the lowest overall latency due to the most direct method of communication being utilised.
Datahub (Centralised)
<p>A datahub acts as an intermediary where all DER market data and network data will flow through, creating an additional component in data exchange that must be maintained, as well as additional messages flowing from source to datahub then datahub to target. A datahub provides additional operational complexity in terms of additional messages flowing end to end, albeit complexity it is reduced as DER scales through standardisation of data exchange.</p> <p>As an intermediary, the centralised data hub may impose higher levels of latency than point to point communications. Communications may be required to queue, dependent on the integration pattern, in order to be processed and, in the case of operating envelope, partition.</p>
Datahub (De-centralised)
De-centralised datahub reduces latency over a centralised datahub approach because processing power is evenly distributed across many nodes. The de-centralised approach also provides higher capacity computing, distributing the overall workload, for example, when leveraging the decentralised approach for operating envelope partitioning aggregators received their NMI to operating envelope instructions from a collective of trusted “workers” rather than AEMO. The highly complex and time sensitive partitioning of NMI to Aggregator relationships is not dependent on a single centralised hub and can be distributed across many nodes.

### 5.4.3.4 Loss of Trust

As the energy system increases dependency on DER for grid operations, there is a strong need for trustworthy market participants, particularly aggregators representing DER devices. To protect the security of supply, any DER data exchange should implement processes and protocols to ensure trusted data exchange.

<b>Data Exchange Trust</b>
Point to Point
As an example, the trustworthiness of a point-to-point integration, where several entities share technologies, designs, and standards, makes it difficult to determine the correctness and

accuracy of the wider ecosystem where other point-to-point integrations sharing the same or similar information have different technologies, designs and/or interpretations of standards. In many cases, an entity will trust their own system and perhaps the nodes they directly interact with. However, outside of this initial circle of trust becomes difficult without a large investment of time and effort. This lack of implicit trust may impact the onboarding of new point-to-point integrations and increase overall cost.

#### Datahub (Centralised)

In a centralised datahub, the trust of the system is consolidated into a single point. The governing entity maintains a trustworthy role and leadership stance, with a level of independence, to ensure that other parties within the ecosystem feel supported and that the data and services provided can be relied upon.

#### Datahub (De-centralised)

A decentralised integration removes the need for a centralised datahub broker/hub, both in terms of operations and hosting. A decentralised approach utilises several technologies such as distributed ledgers and digital identities to enable all market participants to work simultaneously in a trusted environment.

A decentralised integration approach offers the most trustworthy system of all three approaches. In a public DLT platform, no single entity has complete control to view, write, or modify the protocol. As part of the decentralised approach, any change can be seen and verified by other parties, resulting in a highly transparent ecosystem. Furthermore, any change or modification is also immutable, increasing trust in the platform.

Additionally, auditability of a decentralised integration approach is excellent as all data, transactions, and events are traceable, either publicly within an open ecosystem or by the governing authority in a permissioned/private ecosystem.

## 5.5 Summary of Resilience and Compensatory Control Assessment

Each of the three data exchange approaches has been assessed for their resilience, and their ability to monitor triggers for compensatory control as well as enact compensatory control. The pre-conditions and post-condition considerations for the enactment of compensatory control have also been defined.

When considering the Project EDGE principles for data exchange and the requirements for compensatory control, this assessment finds point-to-point data exchange to be a low fit for ensuring safe, reliable and secure DER data exchange at scale. Tight coupling of market participants, limited resilience and inability to monitor triggers for compensatory control at scale reduce the point-to-point's approach suitability as a grid-scale solution for DER data exchange.

A Decentralised Data Hub (DDH) conceptual data exchange option was found to be the best fit to intended resilience goals. The DDH approach best enabled trusted participation and distributed identity management, while ensuring loose coupling (a data exchange design principle) and the decentralised node approach for use cases such as Dynamic Operating Envelope (DOE) partitioning should enable the scalability of data exchange for a future full NEM level roll-out and market participation.

The Centralised Hub (CH) conceptual data exchange options shared many of the high fit results of the DDH including loose coupling and a low barrier to entry however was found to have a medium fit for scalability without the decentralised worker approach to use cases such as DOE partitioning. A key advantage of blockchain-based solutions is that they reduce the amount of human involvement required to create and execute, thereby lowering transaction cost while raising the assurance of execution and enforcement processes. By automating a transaction in a fully verifiable framework (the



blockchain) the transactions can have legal validity even at high frequency – a key enabler for network management required as part of the energy transition.

Further work is required to understand the threshold/scale at which a decentralised approach becomes more efficient than a centralised approach, which could be considered in the Industry Data Exchange project as part of the NEM 2025 program.

With regard to compensatory controls, SA Power Networks (SAPN) have adapted IEEE2030.5's "DefaultDERControl" as a failsafe to revert DER to minimal export on the loss of communications. This approach can be applied under either of the three data exchange mechanisms assessed and is not a differentiating factor in the assessment. It is recommended that AEMO work with DNSPs so that:

- ▶ A consistent approach to DER compensatory controls is adopted across DNSPs, so that DOEs can still be applied even when communications are lost.
- ▶ An operational procedure between DNSPs and AEMO control rooms is developed, as DER penetration gain further scale, to communicate the settings applied and impact of an extended communication outage on aggregated DER operations.
- ▶ To agree upon different DefaultDERControl settings to apply under different seasons or operating conditions, if appropriate.

The DDH conceptual data exchange option was also found to have the best fit to mitigate the risk of a compensatory requiring through efficient management of low/bad data quality, low risk of latency due to decentralised worker processing as well as inherent trust being built into the blockchain based data exchange.

The CH conceptual data exchange option shared benefits of the DDH approach for low/bad data quality management but may be at risk of higher latency as DER data exchange begins to scale to a level defined in the ISP 2022 "step change" scenario. Whereas the Point to Point option was found to be less effective for data quality management.

## 6. Risk, benefits and feasibility of implementing decentralised data hub for DER

The assessment thus far has indicated that decentralised technologies can theoretically deliver a range of benefits that may be in the long-term interests of consumers, in the context of the scale required to support over 100 GW of DER in a high DER future.

An MIT Technology Review<sup>1</sup> states that there will be an evolutionary change from a centralised world to a disintermediated and decentralised world, achieved through emerging technologies like DLT blockchains. In a decentralised world, individuals and organisations have greater autonomy and control over their data and assets, and do not need to rely on intermediaries or central authorities to facilitate transactions or access information. Decentralisation also enables greater transparency and accountability, as the distributed nature of the network makes it difficult for any one actor to manipulate or control the system.

Furthermore, the City of Manchester<sup>29</sup> in the UK has developed a set of principles and guidelines to deliver cooperative Shared Digital Infrastructure under the alignment of the UK's Digital Spine directive. One of the key principles developed indicates "innovating digital-tech businesses are better able to roll-out services on shared infrastructure".

This section moves beyond conceptual theory and, given the relatively low level of maturity for decentralised technologies in the energy industry globally, seeks to explore the feasibility of implementing a decentralised data hub for DER with the NEM. The basis of assessment is theoretical, exploring future adoption without any identified time horizon.

Feasibility can be defined as the possibility or likelihood of something being done or accomplished.<sup>30</sup> In this context, this section explores the risks, benefits and feasibility of a shared digital infrastructure for DER industry participants using decentralised technologies/components and is structured as follows:

- ▶ Practical considerations of implementing shared DER data exchange infrastructure
- ▶ Risks and mitigating actions to consider
- ▶ Potential longer-term benefits of transitioning to decentralised infrastructure
- ▶ Feasibility of making the transition

The risk assessment methodology used for the analysis is included within the appendix C.

---

<sup>29</sup> Manchester City Council et al., 2021

<sup>30</sup> Dictionary.com. Available: <https://www.dictionary.com/browse/feasibility>

## 6.1 Practical considerations of a decentralised data hub for DER

Implementing a new decentralised data hub (DDH) would need to consider a number of practical considerations to establish the feasibility of implementation, including but not limited to:

- ▶ **Establishment:** what will the first applications/use cases be for the new DDH, at what scale and who will use it? Should use of the DDH be voluntary or mandated through regulatory change (either in the National Electricity Rules or state-based regulation)? If a DDH is first established as a small initiative for specific use cases / participants, then regulatory change may not be necessary. For example, if DNSPs in a region decide to collaborate to enable the communication of DOEs to customer agents using shared digital infrastructure, instead of each developing their capability, so that customer agents can subscribe to their DOEs through a single integration.
  - If the DDH sees more participants utilising it across a growing number of use cases, then it may support a case for regulatory change. This approach is consistent with a phased implementation of a DDH being more feasible to establish.
- ▶ **Governance & legal:** how should the establishment and operation of a DDH be governed?
  - For decentralised infrastructure, this includes whether the infrastructure should be public (completely open for all to access) or permissioned (requiring authorised access). It is envisaged that a DDH for the energy industry would be permissioned as it is critical infrastructure, in which case it would require a Governance structure that may be similar to a centralised model. For instance, the Information Exchange Committee that Governs the eHub is comprised of industry representatives and Chaired by AEMO. A DDH could equally be governed by a similar, but separate, committee of industry and (potentially) other representatives.
  - Legal aspects, including how privacy is ensured through the allocation and enforcement of permissioned based access to data, including the access of 'hosting' participants to access data flowing through the system.
- ▶ **Ownership and cost recovery:** who would ultimately own a DDH, and how should its establishment and operational costs be recovered?
  - A centralised model, for example the eHub, could involve AEMO establishing and operating the hub and passing costs onto all consumers through NEM participant fees, as is done through the eHub.
  - A decentralised model could see the hosting/operation of DDH infrastructure decentralised to participants who may be able to recover costs from DER customers specifically. This approach would need to be explored in more detail and consulted on.
- ▶ **Stakeholder engagement and education:** even with a small implementation of a DDH for a small number of use cases, there would need to be clear information sharing about the benefits of this approach, the practical experience, and the steps participants need to take to implement this approach. This is important for both:
  - Participants directly involved in the DDH to facilitate a seamless implementation experience, and mitigate the risk of implementation errors eroding trust in the new infrastructure.
  - Broader industry stakeholders who may be interested to learn if this approach would suit their use cases.

The following section outlines a number of more technical risks and mitigating actions to support a feasible establishment of a new DDH. These have been categorised into four topics:

- ▶ Scalability, Stability and Resiliency
- ▶ Governance, Cost and Ownership
- ▶ Data Privacy, Security, and Quality
- ▶ Change Management

## 6.2 Risk Analysis

The implementation of a DDH presents challenges to the participating stakeholders. This includes consideration of the practical elements outlined above along with operating risks and technical considerations such as the level of enterprise-grade maturity of the technology components for use in critical energy infrastructure.

Identification and management of risks are an important facet to reduce the likelihood of a risk occurring and its impact should it occur. The identification of potential risks has been captured within this report along with actions to determine how to manage each risk. The risk register matrix captured in the Table below, outlines risks as well as approaches for possible risk mitigations.

The selection of an appropriate risk management framework included evaluating AEMO’s Corporate risk management framework. Unfortunately, this risk management framework is oriented towards internal AEMO goals and objectives. Therefore, the selection of an appropriate generic risk management framework is ISO 31000:2009. This framework contains risk management principles and guidelines to support implementation of a decentralised model for shared DER infrastructure. The application of this framework was used in the analysis and captured within section 6.2.1.

The table below is an aggregated view for all 15 risks after the initial risk assessment process.

Likelihood	Impact		
	Minor	Serious	Major
Likely	Low	Significant 2	High 1
Possible	Low	Moderate	Significant 12
Unlikely	Low	Moderate	Moderate

Table 22: Summarised Initial Risk Rating

Source: EY (2022)

The table below is an aggregated view for all 15 risks after the risk mitigation assessment process.

Likelihood	Impact		
	Minor	Serious	Major
Likely	Low	Significant	High
Possible	Low	Moderate	Significant
Unlikely	Low 1	Moderate 4	Moderate 9

Table 23: Summarised Residual Mitigation Risk Rating

Source: EY (2022)

## 6.2.1 Risks Assessment Matrix

The Table below is a list of 14 (non-exhaustive) risks based on theoretical implementation of the Decentralised Data Hub (DDH). Refer to Appendix C, elaborating the definitions for the table below such as categories of risk, impact and likelihood among other definitions.

#	Risk Categories	Risk Title	Risk Description	Impacted Stakeholder	Impact	Likelihood	Risk Rating	Possible Mitigation	Residual Risk Rating (if mitigations were addressed)
1	Governance, Cost and Ownership	Unauthorised Access due to poor Identity and Access Lifecycle Management (IDAM)	Insufficient planning and determination of roles and responsibilities prior and during implementation	Aggregators, DNSPs, DSOs	3	3	High	An oversight board should be established with clear roles and responsibilities in place to carry out agreed upon action plans within timelines. Example, meeting on a regular basis to determine roles and responsibilities of each of the participants and the organisational structure of the project, having several levels of review prior to implementing or changing critical areas of the project etc.  Consideration of Digital Governance via the use of a Decentralised Autonomous Organisation (DAO).	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Major = 3  Rating = Moderate
	Governance, Cost and Ownership	Alignment with industry identify and access management (IDAM) approaches	AEMO's implementation of NEM 2025 includes developing an industry wide approach to IDAM at the wholesale/retail level. Inconsistencies between this and DDH IDAM may lead to inefficiencies	Aggregators, DNSPs, DSOs	2	3	Significant	Ensure that design teams for NEM 2025 IDAM, IDX and the DDH engage to align as many design components as possible for their respective IDAM approaches. Explore the merits of applying decentralised identity concepts in broader applications than the DDH.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Major = 3  Rating = Moderate
2	Governance, Cost and Ownership, Change Management	Instability due to poor Change Management practices	Lack of planning and oversight prior to testing and implementation. Improperly designed governance causing difficulties in establishing the DDH and unclear roles and responsibilities for its functioning.	All	3	2	Significant	The Governance structure and oversight board should ensure sufficient resources are applied to change management and stakeholder engagement / education so that stakeholders understand how to establish/integrate with the DDH and what their role/responsibilities are. The Information Exchange Committee for the eHub is a good example of industry oversight.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Serious = 2  Rating = Moderate
3	Governance, Cost and Ownership	Limited adoption due to poor community establishment and communication	Insufficient communication of benefits of a distributed DER marketplace to stakeholders leading to insufficient network participation causing wastage of resources and loss of revenue	Agents, Prosumers	3	2	Significant	Implement use cases in a phased manner to gauge interest and participation prior to proceeding. Conduct cost benefit analysis for each phase. Design and implement each phase in open and transparent approach that clearly articulates the benefits and practical steps required for participants to engage with a DDH. Ensure sufficient education material is available to communicate benefits to end consumers.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Minor = 2  Rating = Low

#	Risk Categories	Risk Title	Risk Description	Impacted Stakeholder	Impact	Likelihood	Risk Rating	Possible Mitigation	Residual Risk Rating (if mitigations were addressed)
4	Governance, Cost and Ownership  Scalability, Stability and Resiliency	Limited or no establishment of a technology governance model	Lack of standardised framework adopted prior to scaling leading to inability to operate the business and cope with demand ultimately leading to breakdown in controls and loss of data, revenue and possible cyber exploitations	All	3	2	Significant	External and internal collaboration and frequent consultation and benchmark exercises can be performed to be made aware of and keep up with industry trends. A strong relationship between Business and IT like CAB meetings, change approval process, user acceptance testing prior to implementations etc is also needed to understand the significance of and effectively implement a standard framework.	<b>Likelihood</b> Unlikely = 1  <b>Impact</b> Serious = 2  Rating = Moderate
5	Data privacy, security and quality  Scalability, Stability and Resiliency	Instability of shared Infrastructure due to small participant numbers	Limited nodes on network causing a potentially vulnerability (sybil or 51% attack) of the shared DER marketplace to facilitate better energy distribution for all participants.	All	3	2	Significant	Incentivise the addition of nodes plus add appropriate intrusion protection and detection controls should be in place, configured correctly and monitored for failure and anomalies. Example, stateful inspection of firewalls rules, regular penetration and vulnerability testing, monitoring of user activity via a security operations centre, incident planning etc.	<b>Likelihood</b> Unlikely = 1  <b>Impact</b> Serious = 3  Rating = Moderate
6	Data privacy, security and quality  Scalability, Stability and Resiliency	Malicious staff administrator actor attack	Compromised credentials administering the blockchain network causing interference with energy allocation and delivery (unbalanced power generation and load). Note: more applicable towards private blockchains	All	3	2	Significant	Appropriate intrusion protection and detection controls should be in place, configured correctly and monitored for failure and anomalies. Example, stateful inspection of firewalls rules, regular penetration and vulnerability testing, monitoring of user activity via a security operations centre, incident planning etc.	<b>Likelihood</b> Unlikely = 1  <b>Impact</b> Major = 3  Rating = Moderate
7	Data privacy, security and quality	Compromised Key Management due to poor responsibility	Participants losing their own data (keys), in a decentralised network, causing permanent loss of their data and temporary loss of access to the network.  Note: Assuming they opt to share their data and the provider has no backup.	All	3	2	Significant	A regularly tested key management policy and procedure should be in place along with knowledgeable personnel managing this process. Highly secure key recovery procedures should also be in place depending on the model implemented.  Implementation of a Multi-sig approval to support change management  Implementation of various change management practises to increase awareness and education.	<b>Likelihood</b> Unlikely = 1  <b>Impact</b> Major = 3  Rating = Moderate

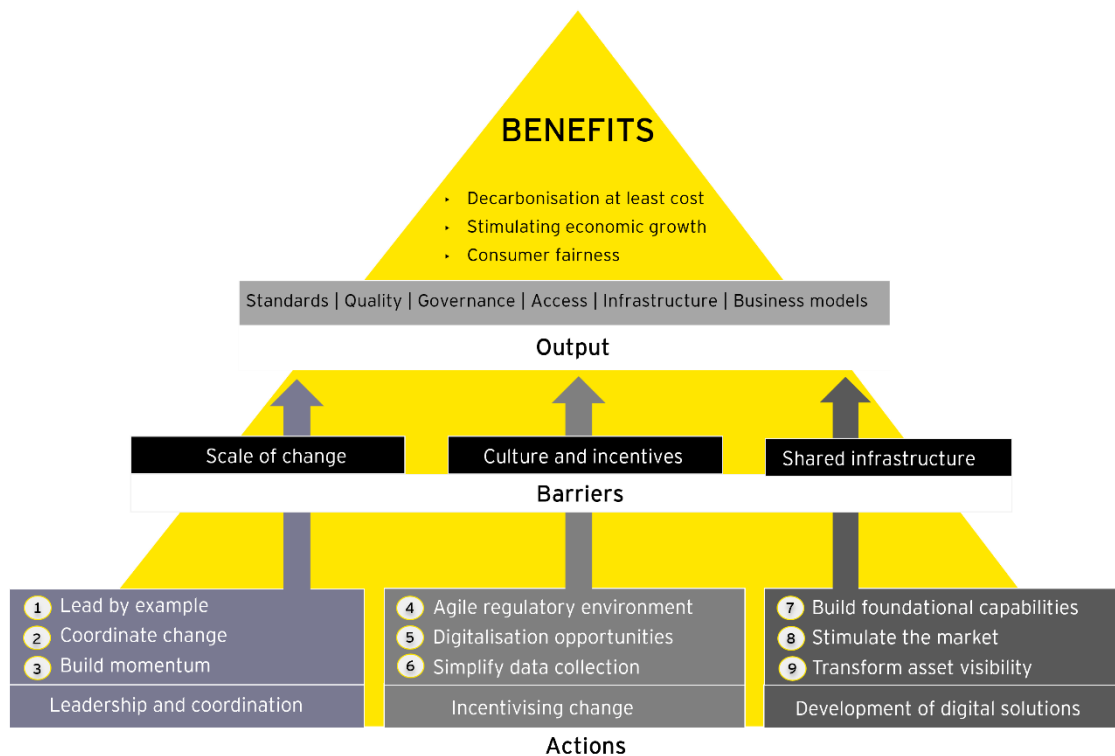
#	Risk Categories	Risk Title	Risk Description	Impacted Stakeholder	Impact	Likelihood	Risk Rating	Possible Mitigation	Residual Risk Rating (if mitigations were addressed)
8	Data privacy, security and quality Scalability, Stability and Resiliency	Data breach due to uncontrolled data management practices	Failed or compromised network control centres or hubs that manage data collection and analysis which could lead to widespread data leakage, unequal distribution of benefits, misinformation and be used to manipulate or bring down the network.	All	3	2	Significant	Appropriate intrusion protection and detection controls should be in place, configured correctly and monitored for failure and anomalies. Example, stateful inspection of firewalls rules, regular penetration and vulnerability testing, monitoring of user activity via a security operations centre, incident planning etc. Robust cyber security and data privacy practices should be crucial to the stability and success of the project which means significant investment should be made into the uplift of existing security policies and procedures as well as hiring specialised skillset to manage these procedures.	<b>Likelihood</b> Unlikely = 1 <b>Impact</b> Major = 3 Rating = Moderate
9	Data privacy, security and quality	Custody breach due to limited centralised non-repudiation	Unauthorised transaction signing/approval process due to stolen devices, cyber-attacks, inaccurate provisioning, causing unequal distribution of energy, possible failure of the network due to overload and inaccurate presentation of information	All	3	2	Significant	Strengthen physical access controls and transaction signer process via approvals. Also have in place regular event logging and monitoring of the network along with a responsive incident response team.	<b>Likelihood</b> Unlikely = 1 <b>Impact</b> Major = 3 Rating = Moderate
10	Data privacy, security and quality Scalability, Stability and Resiliency	Compromised private/protected data on DDH	Compromise of private / protected data held by systems on the network (database, SaaS system, APIs etc)	All	3	2	Significant	Effective change management controls (testing, approvals, segregation of duties), automated checks in the SDLC process and access provisioning controls to systems. Ensure obligations for private / protected data are met in DDH design for access and storage of data. Appropriate intrusion protection and detection controls should be in place, configured correctly and monitored for failure and anomalies. Example, stateful inspection of firewalls rules, regular penetration and vulnerability testing, monitoring of user activity via a security operations centre, incident planning etc.	<b>Likelihood</b> Unlikely = 1 <b>Impact</b> Major = 3 Rating = Moderate
11	Data privacy, security and quality Scalability, Stability and Resiliency	Inability to recover chain at specific block/checkpoint	Manual error, attack or failure of the network, broken down internal processes and controls leading to loss or inability to backup network/data dependencies	All	2	2	Moderate	Backup and recovery procedures should be regularly tested, BCP plan should be in place.	<b>Likelihood</b> Unlikely = 1 <b>Impact</b> Serious = 2 Rating = Moderate

#	Risk Categories	Risk Title	Risk Description	Impacted Stakeholder	Impact	Likelihood	Risk Rating	Possible Mitigation	Residual Risk Rating (if mitigations were addressed)
12	Data privacy, security and quality	Inability to service to customers due to limited quality reviews that are transparent	Inaccurate onboarding of customers leading to inability to provide services as required	Agents, Prosumers	2	3	Significant	A good policy and procedure should be in place to onboard customers. This should include AML/KYC checks, approvals for special services, correct system/device configuration, testing integration into the network etc.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Serious = 2  Rating = Moderate
13	Change Management	Unmanaged configuration settings	Inappropriate and inaccurate configuration settings amongst dependent systems on the network leading to service disruption and loss of data and revenue	All	3	2	Significant	Upfront change management controls (testing, approvals, segregation of duties), automated checks in the SDLC process and regular monitoring and review.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Major = 3  Rating = Moderate
14	Change Management	Unauthorised implemented changes	Unauthorised changes promoted to production leading to service disruption and loss of data and revenue	All	3	2	Significant	Upfront change management controls (testing, approvals, segregation of duties), automated checks in the SDLC process and regular monitoring and review.	<u>Likelihood</u> Unlikely = 1  <u>Impact</u> Major = 3  Rating = Moderate

Table 24: Risk Assessment Matrix

Source: EY (2022)





## 6.3 Benefits Assessment Approach

As outlined in section 3, decentralised digital infrastructure is theoretically more suitable to facilitate DER data exchange at scale than other integration approaches, which may deliver efficiency gains and better user experiences as DER proliferates.

### 6.3.1 Assumptions

There are certain assumptions for evaluating the benefits of a decentralised data hub and we draw a similar strategy to that of the UK's digitalisation of the energy sector<sup>31</sup>. This strategy focuses primarily on the assumption that prosumers opt-in to share their personalised energy consumption/DER information.

Decentralised technology components such as Self Sovereign Identities (SSI) at different levels of the value chain can enable consumers and participants granular level control over sharing and access to data, based on customer consent and appropriate permissions established in the Governance process.

In a decentralised model, technology like Zero-Knowledge Proofs can also provide privacy when sensitive data is transacted with on-chain, however, this technology is a relatively newer concept that is being implemented in the DLT space.

### 6.3.2 Benefits Summary

The figure below represents a summary of actions and barriers to benefits that can be achieved from a decentralised data hub for DER. Identifying potential barriers to benefits being achieved can indicate priority actions that can alleviate those barriers and enhance the likelihood of achieving the benefits.

Based on actions and barriers, benefits are then given a rating below to approximately understand the value over centralisation and point to point models.

<sup>31</sup> Government of UK, Department for Business, Energy & Industrial Strategy, OfgemDataServices., 2021

Figure 21: Benefits Delivery Diagram  
 Source: EY (2022)

The table below provides a matrix of the benefit rating by combining the impact and achievability for each benefit.

		Achievability		
Impact		Possible	Very Likely	Almost Certain
		1	2	3
High	3	Low	Significant	High
Moderate	2	Low	Moderate	Significant
Low	1	Low	Moderate	Moderate

Table 25: Benefits Impact and Achievability Matrix  
 Source: EY (2022)

### 6.3.3 Benefits Register

Table 26 below is a list of theoretical benefits of the Decentralised Data Hub (DDH) separated into the different benefit ratings identified.

#	Benefit Category	Benefit Title	Benefit Description	Impacted Stakeholder	Impact	Achievability	Benefit Value	Possible Barriers
<b>High</b>								
1	Data security	Heightened security	If there is a full transition to a decentralized model of operation, then all this model's security benefits will be realised through the use of foundational components. The security provides a high level of data protection to its users via data encryption through the use of private keys and transactional accounts that will be pseudo-anonymous. The use of a decentralised hub, which has several distributed nodes, as well as using a consensus mechanism on a blockchain, establishes trust and speedy transaction processing.	Prosumers, agents	3	3	Increased revenue due to high participation	<p>Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability.</p> <p>Care should be taken around integrating any centralised components into the model (example, databases for storage of critical data etc) as these could defeat this benefit.</p> <p>Participants should be convinced of this decentralised solution more than the current model, in order to sign up.</p>
2	Participant experience	Innovation potential through development of decentralised applications (dapps)	Enables participants to create decentralised applications (dapps) that use the underlying identity and messaging infrastructure, but are personalised for whatever application is required, such as DNSPs creating local services applications.	All	3	3	Enables participants to have autonomy over developing dapps that suit their needs and design, whilst also enabling other participants to interact with those applications through consistent identify and messaging infrastructure.	If there is low participation, there is a lower requirement/benefit from developing dapps
3	Use of Data	Higher Environment, Sustainability, Governance (ESG) impact	Shared DER infrastructure means that improved data quality and data sharing will also enable much better planning and operation of our energy infrastructure. For example, more widespread and efficient use of DOEs will enable distribution network to host more rooftop PV, accelerating the decarbonisation of the grid.	All	3	3	Greater contribution to society's climate change goals and a reputational win which prosumers will see value in contributing to	Regulation or lack of standardised frameworks to adopt in implementation, will slow the roll out of DOEs and restrict the PV hosting capacity of distribution networks.
4	Infrastructure stability	More efficient management of distributed energy	A stable system will enable market participants to interact under desired parameters. Therefore a performant supply chain enables the market work effectively/efficiently.	All	3	3	More efficient allocation of resources, as more resources are able to respond to negative price signals (balancing supply and demand), and	Low participation from customer agents, retailers and DNSPs would reduce the available benefits for consumers, particularly as retailers are unlikely to be able to connect to every customer agent / PV manufacturer without a data hub being in place

#	Benefit Category	Benefit Title	Benefit Description	Impacted Stakeholder	Impact	Achievability	Benefit Value	Possible Barriers
							responsiveness to operating envelopes at scale will ensure distribution network limits are not breached.	
5	Participant experience	Innovation through Ecosystem development/ evolution	A highly engaged community of participants will support the evolution of the ecosystem. Therefore enriching features that have high value to all participants.	All	3	3	Increased revenue streams and participation  Increased innovators supporting that will build out a more active community and therefore add continuous improvements	Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability. There could be overprotective and bespoke data sharing agreements.  Care should be taken around integrating any centralised components into the model (example, web 2 databases for storage of critical data etc) as these could defeat this benefit.  Participants should be convinced of this decentralised solution more than the current model, in order to sign up. Development of a value driver tree may result in identifying and communicating clear value to mitigate this barrier.  Benefits of data sharing are not realised due to lack of understanding on what data is collected and secure and for what purpose, leading to hoarding of data for personalised use
6	Participant experience	Service diversity	Enabling agents to deliver multiple services whilst minimising market participation complexity.	Prosumers	3	3	Increased revenue streams and participation	Regulation or lack of standardised frameworks for the services that can be provided as well as poor articulation of agent benefit, could lead to disincentivising agent participation.
7	Cost and Ownership	Data Movement	Decentralised data hub model reduces cost and complexity of data exchange and provides an economically efficient and scalable approach for the DER marketplace.	Prosumers	3	3	Reduced cost of data management providing increased insights for forecasting and planning in a scalable manner	Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability. There could be overprotective and bespoke data sharing agreements.  Care should be taken around integrating any centralised components into the model (example, web 2 databases for storage of critical data etc) as these could defeat this benefit.  Lack of a standardised frameworks or regulatory support leads to delayed implementation of a decentralised data hub model which leads to further lack of interest from participants as other

#	Benefit Category	Benefit Title	Benefit Description	Impacted Stakeholder	Impact	Achievability	Benefit Value	Possible Barriers
								private solutions develop to gain participant market share.
8	Roles and responsibilities	Change in capabilities of participants	As more of the business logic is done via smart contracts (automated pieces of code on the blockchain), roles and responsibilities of various participants can be extended. For example, DNSP investment to develop DNSP capabilities improve the economic efficiency of the DER Marketplace.	All	3	3	Gives back time to the participants to do more value adding activities	<p>Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability. There could be overprotective and bespoke data sharing agreements.</p> <p>Care should be taken around integrating any centralised components into the model (example, web 2 databases for storage of critical data etc) as these could defeat this benefit.</p> <p>Benefits of data sharing are not realised due to lack of understanding on what data is collected for what purpose, leading to hoarding of data for personalised use</p>
9	Participant experience	Adjacent but aligned use cases, for example, EVs	Sharing of standing and operational data from electric vehicle charge points, similar to the National Charge Link concept, could be highly efficient in a decentralised DER data hub particularly since those charge points would need to receive dynamic operating envelopes from DNSPs in future.	All	3	3	Efficient use of digital infrastructure that enables consistent visibility of data across energy and electric vehicles for participants that have the right permissions	<p>Coordinating the development of digital infrastructure to serve both electricity and transport industries cannot be achieved by the leadership of one sector alone.</p> <p>A champion that operates across both sectors, such as State/Federal Government, is required to coordinate the assessment and implementation of digital infrastructure to serve both industries.</p>
<b>Significant</b>								
10	Network scalability	Ease of participant onboarding	Seamless onboarding of new participants creates a great user experience and ambassadors encouraging others to join and transact. Therefore increasing volume of users and transactions.	Market Operator	2	3	Increased revenue due to high participation	<p>Infrastructure integration with participants can be a challenge due to capacity management of the network as well as configuration set up.</p> <p>Further users may not be convinced of the model based on communication received and hesitate to onboard or share data. Furthermore, the interface for easy onboarding would have to be built and integrated into the main IT landscape incurring cost and effort.</p>
11	Operational resiliency	Higher resiliency of a decentralised network	Uninterrupted services - For the components of the network that are truly decentralised, there would not be a single point of failure due to the distributed nature of set up and integration leading to more	All	3	2	Network resiliency delivering better market outcomes	Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability.

#	Benefit Category	Benefit Title	Benefit Description	Impacted Stakeholder	Impact	Achievability	Benefit Value	Possible Barriers
			resiliency to maintenance down times, cyber-attacks or network/system failure.  Additionally, network reliability can be managed through the provision of local network services from customer owned assets.					Care should be taken around integrating any centralised components into the model (example, web 2 databases for storage of critical data etc) as these could defeat this benefit.
12	Participant experience	Elimination of information asymmetry	A decentralised model would be accessible, public and fair enabling eliminating information asymmetry for all participants.  This concept also extends to the code of the blockchain. If a truly decentralised model is adopted, then the code can be open source which can be contributed to by the public as well. Products like Linux operate this way which benefit from public improvement protocols while they heavily control the changes that actually get implemented in production.	All	2	3	Transparency over value provided and received that will be visible to all relevant parties and hence easy to verify. This presents as a fair and equitable market to all participants.  Open-source technology leads to a collaboration of public ideas that could increase in additional features available to the participants and inculcates a sense of belonging to an ecosystem with shared values.	Either a change in design authorised from governing parties which would lead to more adoption of centralisation or too much centralised control over the administration of the network, making it a centralised vulnerability. There could be overprotective and bespoke data sharing agreements.  Care should be taken around integrating any centralised components into the model (example, web 2 databases for storage of critical data etc) as these could defeat this benefit.  Participants should be convinced of this decentralised solution more than the current model, in order to sign up.  Benefits of data sharing are not realised due to lack of understanding on what data is collected for what purpose, leading to hoarding of data for personalised use
<b>Moderate</b>								
13	Data privacy and security, Participant experience	Ownership of identity	DLTs enable the use of digital IDs which enables participants to manage their own data independently, privately and securely	Prosumers	2	2	This puts data in the hands of the participants in a way that allows participants to provide consent on the use of owned data.	Enforcing this technology in this model might be unfavourable to participants by giving them no choice but to adopt a digital identity. Additionally, this part of the technology is still evolving due to its sensitive nature, as a compromise to this data would not mean a compromise of identity in real life.
14	Use of Data	Near real-time integration	Seamless flow of data once integrated with all systems leading to real-time information flow avoiding wastage in time and discrepancy resolution. Further, DNSPs can leverage this data for better service procurement from DER agents and providing better services to customers	All	2	2	Reduced latency of data to enable better decision making.	Data collection regulation or lack of standardised frameworks to adopt during data analysis, lack of incentives for clean energy and reporting.  Integration challenges with various systems to provide accurate data

Table 26: Benefits Register

Source: EY (2022)

Project EDGE

Benefits, Risk & Feasibility Assessment for Shared DER Infrastructure

### 6.3.4 Broader considerations to achieve benefits

Given AEMO's experience with testing decentralised technologies in Project EDGE, AEMO will need to provide leadership and coordination by adopting a collaborative approach with regulatory bodies and industry stakeholders to broaden their understanding of decentralised approaches.

This will help to further explore the feasibility of a decentralised data hub that works for participants, as well as developing a shared vision and an agreed approach for getting there. This includes continuous time-measured monitoring of progress and benefits realisation to make sure efforts are aligned and delivering value.

It is also important to consider broader industry processes relating to data exchange, including AEMO's Industry Data Exchange (IDX) and Identity and Access Management (IDAM) projects.<sup>32</sup> These projects address wholesale and retail interactions with AEMO; achieving consistency between these processes and the DDH will enable a consistent user experience for DER aggregators as they scale up to interact in wholesale markets.

#### 6.3.4.1 Linkage to Consumer Data Right

With the upcoming defined rules around the ownership of data set out in the Treasury Laws Amendment Act 2019 called Consumer Data Right (Energy Sector) Designation 2020, there will be more responsibility and ownership required over consumer data energy consumption. This sets out classes of information held, who is permitted to hold this information and who is required to transfer it at the customer's request. Therefore, quality of data is now required to be standardised and access to it will not be subject to competitive pressures.

This elevates the importance of approaches that provide consumers and businesses with greater controls over their data and how it is shared, which is a core characteristic of decentralised approaches, including self-sovereign identities.

The data holding ownership will require consideration and should be taken into account as a part of the decentralisation model's next steps.

#### 6.3.4.2 Stakeholder engagement and resources

Achieving the benefits of implementing DDH will require buy-in and engagement from industry that will only be achieved if the benefits are effectively articulated and communicated to industry so that stakeholders are involved in the implementation journey.

Given that decentralised technology is a relatively new concept in the energy industry, effective education materials should be developed and made available so that:

- ▶ Existing energy professionals can upskill on this new integration technology.
- ▶ Technology professionals from outside the energy industry can learn the context and application for a DDH in the energy industry.

Any skill shortages for an implementation to be achieved should be determined in advance and an action plan formulated. For example, skills required to run a complex distributed network utilising modern data collection, data analysis and digital control systems may be in short supply.

---

<sup>32</sup> AEMO 2022. NEM 2025 Implementation Roadmap. Available: <https://aemo.com.au/initiatives/major-programs/nem-reform-implementation-roadmap>

## 7. Conclusion

The first conclusion from this theoretical assessment is that point-to-point data integration approaches are not efficient at the 100 GW of DER scale envisaged in the 2022 Integrated System Plan.

A DER data hub (either centralised or decentralised) integration approach has consistently rated more beneficial for consumers than point-to-point approaches, for instance in terms of efficiency, scalability and security.

An independent cost benefit analysis (CBA) on Project EDGE has evaluated that a DER Data Hub would deliver significant customer benefits when compared to a point-to-point data exchange approach<sup>33</sup>. The practical trial has also demonstrated, at small scale, how a DDH could work to facilitate emerging DER use cases across many industry actors.

If a DER data hub approach is recognised as a more efficient and scalable way to facilitate data exchange across numerous use cases, then the following realistic options may be considered:

- ▶ Centralised approach: adding DER data exchange use cases (such as the Dynamic Operating Envelopes) to the existing eHub, Shared Market Protocol and consideration of how that should evolve towards a target state following the Industry Data Exchange project.
- ▶ Decentralised approach: establishing an alternative decentralised data hub for DER use cases that can operate in parallel, and separately, to the eHub. In order to enable consistent user experiences for stakeholders that need to interact with each system (for example, a retailer or DNSP), consistent approaches should be prioritised for elements such as Identity and Access Management. This, and consideration of how these two approaches could converge over time, should be explored further in the Industry Data Exchange project.

There is also a spectrum of technology choices available, between conventional centralised to fully decentralised technologies including, for example, conventional technology choices deployed in containers to mitigate single point of failure risks.

While current volumes of DER data exchange is relatively small, there is less distinction between centralised and decentralised options, but there may come a tipping point where the advantages of decentralised approaches may outweigh the costs and complexities of transitioning towards decentralised technologies.

A key question relates to the timing of those net benefits, and whether there is sufficient confidence in those benefits to advance a pathway of decentralisation before the tipping point in order to reduce the costs and complexities of the transition. This would also need to be considered in the context of broader developments in the electricity industry system architecture.

A balanced approach may involve implementing a phase 1 DER Data Hub in a centralised model, but using technology that gives optionality to support a smooth transition to a decentralised approach when appropriate in future. The detailed design for a phase 1 implementation should consider the option value that technology solutions can provide for future development.

This assessment finds that implementing a decentralised model for a DER data hub is theoretically feasible, which is supported by the practical demonstration of the decentralised model at small scale in Project EDGE. It is considered worthwhile to invest time, effort and resources to explore an implementation in more detail given the potential consumer benefits outlined in this report.

However, to realise the potential consumer benefits the industry must navigate the following key challenges:

- ▶ Broader stakeholder education is required, in simple and digestible formats, regarding the long-term benefits to consumers of developing a Decentralised Data Hub (DDH). AEMO's

---

<sup>33</sup> Deloitte Access Economics, 2023. Project EDGE Cost Benefit Analysis. Available: <https://aemo.com.au/en/initiatives/major-programs/nem-distributed-energy-resources-der-program/der-demonstrations/project-edge>



experience of decentralised technologies in Project EDGE means it is best placed to champion this approach.

- ▶ Decentralised technologies in the energy industry have not yet developed the enterprise grade maturity of other technologies such as the enterprise service bus. A gradual, phased implementation of a DDH is considered the best way to develop and demonstrate the maturity required for industry stakeholders to adopt a DDH at scale.
- ▶ More certainty is required on standardised frameworks to be used, including decentralised identities and communication protocols, which will prepare the industry for rapid scalability given the continued growth of DER, including a rapid uptake of EVs.
- ▶ More consideration is needed on how a decentralised approach for DER data exchange may interact and/or integrate with broader data exchange initiatives, such as Industry Data Exchange (IDX) and Identity and Access Management (IDAM) projects<sup>34</sup>.

Notwithstanding these challenges, there is an opportunity to evolve and standardise DER data exchange using a DDH. The actual transition, however, does not need to be done in a single 'big bang' approach.

A phased implementation of a decentralised data hub is considered the most appropriate approach, starting with a small number of use cases and participants. A successful small-scale implementation may pave the way to add further use cases and scale the solution as rapidly as required by industry, noting that economies of scale may not be achieved until later phases.

A conceptual roadmap of how use cases could be added in phases is outlined below, but this would need to be consulted on extensively.

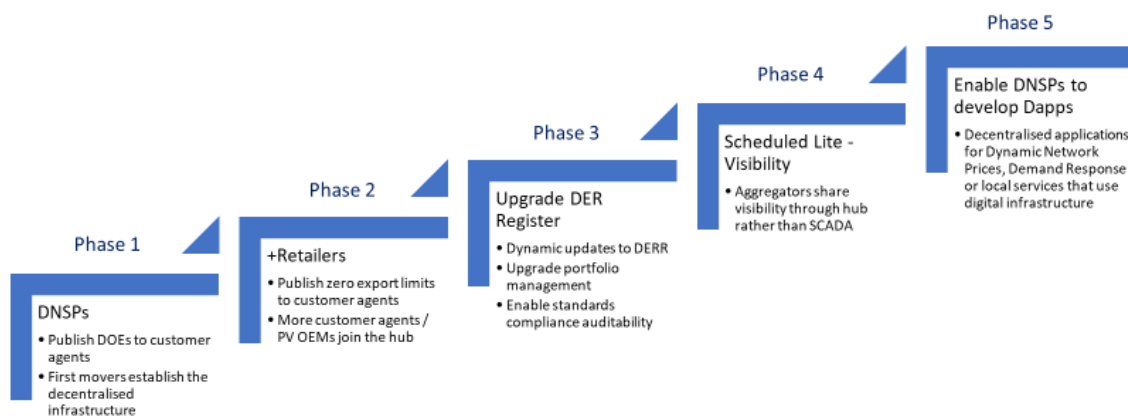


Figure 22: Conceptual roadmap for phased implementation of DER data hub

In considering the case for the first small-scale implementations, it is important to consider the potential long-term benefits of decentralisation taking all stakeholder impacts into account collectively rather than considering individual use cases on a stand-alone basis.

It is equally important not to lose sight of the scale of effort required to develop a detailed design and business case for implementation. There are layers of detail that have not been considered to date. Hence further research and small-scale implementations will be required to explore ways in which various frameworks and models can support the successful delivery through a decentralised transition.

<sup>34</sup> AEMO 2022. NEM 2025 Implementation Roadmap. Available: <https://aemo.com.au/initiatives/major-programs/nem-reform-implementation-roadmap>

Finally, Australia is not alone in exploring these concepts. Potential applications for decentralised technologies are being explored across many sectors around the world, and particularly in energy.

The UK Government is considering industry data hub across both energy and EV chargepoint data:

- ▶ An Energy Digitalisation Taskforce made ambitious recommendations for the UK Government to “create a radically different energy system, driven by open-source software and open standards,” facilitated through the deployment of a “Digital Spine” (including an Energy Asset Register and Energy Data Catalogue) that would create a network of connected nodes to share data across the energy sector.<sup>35</sup>
- ▶ The Department of Transport is establishing an EV Chargepoint Data Hub with a vision for “all chargepoint operators in the UK share their chargepoint data to a central location, creating a single source of truth”, which will ultimately enable better experiences for consumers to locate a reliable and available charge points. This is similar to the National Charge Link concept proposed in Australia by RACE for 2030.

Both UK initiatives are similar concepts to the data exchange hub that Project EDGE is examining, and each warrants more detailed investigations to validate whether this public interest digital infrastructure, potentially operating across the electricity and transport sectors, is in the long-term interests of consumers.

### 7.1.1 Next steps

This independent theoretical assessment and the independent CBA on Project EDGE have identified that a DER Data Hub is more aligned to the long-term interest of consumers than a point-to-point approach for DER related data exchange in a high DER future<sup>36</sup>. The practical field trial has also demonstrated, at small scale, how a DDH could work to facilitate emerging DER use cases across many industry actors.

To advance practical considerations on how to implement a production grade DER Data Hub, next steps may include the following:

- ▶ Identify appropriate use cases and voluntary participants for a phase 1 implementation.
- ▶ Develop detailed design for a minimum viable product (for phase 1 implementation), that includes Enterprise and Solution Architecture (conceptual and logical).
  - Detailed design should determine whether to adopt centralised, decentralised or hybrid technology solutions considering the option value of solutions that can enable a transition to alternative approaches as needed in future.
  - It should also examine governance, ownership and cost recovery models, and requirements for stakeholder engagement and education.
- ▶ Design a more detailed implementation roadmap on which use cases could be added and when.
- ▶ Link with other activities, such as the development of Public Key Infrastructure for DER or the exploration of an EV charge point data hub like the National Charge Link<sup>37</sup> proposal, to identify opportunities to integrate initiatives to deliver more efficient outcomes.

These activities could all be progressed within the broader context of the Industry Data Exchange and DER Data Hub and Registry Services projects in the NEM 2025 Program - Operational Technology Uplift initiatives<sup>38</sup>, and through engagement with industry stakeholders.

---

<sup>35</sup> UK Energy Digitalisation Taskforce. Available: <https://es.catapult.org.uk/report/delivering-a-digitalised-energy-system/>

<sup>36</sup> Deloitte Access Economics, 2023. Project EDGE Cost Benefit Analysis. Available: <https://aemo.com.au/en/initiatives/major-programs/nem-distributed-energy-resources-der-program/der-demonstrations/project-edge>

<sup>37</sup> RACE for 2030. National Charge Link. Available: [https://issuu.com/racefor2030/docs/national\\_charge\\_link](https://issuu.com/racefor2030/docs/national_charge_link)

<sup>38</sup> AEMO 2022. NEM 2025 Implementation Roadmap. Available: <https://aemo.com.au/initiatives/major-programs/nem-reform-implementation-roadmap>

## 8. References

- Accelerating the energy transition with Web 3 technologies, MIT Tech Review Insights, 2022. Available online: <https://www.thetechnologyreview.com/2022/11/021062403/accelerating-the-energy-transition-with-web3-technologies/>
- AEMO. 2022. Shared Market Protocol (SMP) Technical Guide. Available online: [https://www.aemo.com.au/-/media/Files/Electricity/NEM/Retail\\_and\\_Metering/B2B/2018/B2B-SMP-Technical-Guide.pdf](https://www.aemo.com.au/-/media/Files/Electricity/NEM/Retail_and_Metering/B2B/2018/B2B-SMP-Technical-Guide.pdf)
- AEMO. 2022. *Solution Architecture Document*. Available online: <https://nougroupp.sharepoint.com/sites/TS13559-InsightsandAlignment/Shared%20Documents/Insights%20and%20Cyber/01.%20RFI%20and%20Response/01.%20Architecture%20Viewpoint/EDGE%20Symphony%20-%20AEMO%20SAD.pdf?CT=1664513756984&OR=ItemsView>
- NESCOR Failure Scenarios Document:  
<https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf>
- Andoni, Merlinda., Robu, Valentin., Flynn, David., Abram, Simone., Geach, Dale., Jenkins, David., McCallum , Peter., and Peacock, Andrew. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. 100(2019): 143-174. <https://doi.org/10.1016/j.rser.2018.10.014>.
- Abeysekera, R. 2005. Effects of system integration in an organization. Available online: <https://www.diva-portal.org/smash/get/diva2:20658/FULLTEXT01.pdf> (accessed 10 September 2022)
- AEMC. 2022. *National Energy Objectives*. Available online: [https://www.aemc.gov.au/regulation/neo#:~:text=The%20National%20Electricity%20Objective%20\(NEO\)&ext=%E2%80%9Cto%20promote%20efficient%20investment%20in,security%20of%20supply%20of%20electricity](https://www.aemc.gov.au/regulation/neo#:~:text=The%20National%20Electricity%20Objective%20(NEO)&ext=%E2%80%9Cto%20promote%20efficient%20investment%20in,security%20of%20supply%20of%20electricity) (Accessed 10 September 2022).
- AEMO. 2022. *Shared Market Protocol (SMP) Technical Guide*. Available online: [https://www.aemo.com.au/-/media/Files/Electricity/NEM/Retail\\_and\\_Metering/B2B/2018/B2B-SMP-Technical-Guide.pdf](https://www.aemo.com.au/-/media/Files/Electricity/NEM/Retail_and_Metering/B2B/2018/B2B-SMP-Technical-Guide.pdf)
- AEMO. 2022. *Solution Architecture Document*. Available online: <https://nougroupp.sharepoint.com/sites/TS13559-InsightsandAlignment/Shared%20Documents/Insights%20and%20Cyber/01.%20RFI%20and%20Response/01.%20Architecture%20Viewpoint/EDGE%20Symphony%20-%20AEMO%20SAD.pdf?CT=1664513756984&OR=ItemsView>
- AEMO. 2018. *Project EDGE Research Plan*. Available online: <https://aemo.com.au/-/media/files/initiatives/der/2022/master-research-plan-edge.pdf?la=en> (accessed 10 September 2022).
- Cantillo-Luna, S., Moreno-Chuquen, R., Chamorro, H., Sood, V., Badsha, S. and Konstantinou, C., 2022. Blockchain for Distributed Energy Resources Management and Integration. *IEEE Access*, 10, pp.68598-68617.
- Consensys. 2022. *Ethereum Has 4x More Developers Than Any Other Crypto Ecosystem*. Available online: <https://consensys.net/blog/developers/ethereum-has-4x-more-developers-than-any-other-crypto-ecosystem>
- European Union Blockchain Observatory & Forum. 2022. *Blockchain Applications in the Energy Sector*. European Union Blockchain Observatory & Forum. Available online: [https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF-Thematic\\_Report\\_Energy\\_Sector\\_0.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF-Thematic_Report_Energy_Sector_0.pdf) (accessed 10 September 2022).
- Gangwal, A., Ravali Gangavalli, H., & Thirupathi, A. 2022. *A Survey of Layer-Two Blockchain Protocols*. International Institute of Information Technology. Available online: <https://arxiv.org/pdf/2204.08032.pdf> (accessed 10 September 2022).
- Gourisetti, S., Cali, Ü., Choo, K., Escobar, E., Gorog, C., & Lee, A. et al. 2021. Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications. *Sustainable Energy, Grids And Networks*, 28, 100553. doi: 10.1016/j.segan.2021.100553 (accessed on 10 September 2022).
- Government of UK, Department for Business, Energy & Industrial Strategy, OfgemDataServices., 2021. Available online: <https://www.gov.uk/government/organisations/department-for-business-energy-and-industrial-strategy>

- Guan, J., & Barker, R. M. 2002. The Strategic Imperative For An Integrated Enterprise. *International Business & Economics Research Journal (IBER)*, 1(6). <https://doi.org/10.19030/iber.v1i6.3940>
- Hive Power. 2022. Grids made Smart. <https://www.hivepower.tech>
- Hohpe, G., & Woolf, B. 2003. *ENTERPRISE INTEGRATION PATTERNS; DESIGNING, BUILDING, AND DEPLOYING MESSAGING SOLUTIONS*. READING: ADDISON-WESLEY.
- Küfeoğlu, S., Açıkgöz, E., Taşcı, Y., Arslan, T., Priesmann, J. and Praktknjo, A., 2022. Designing the Business Ecosystem of a Decentralised Energy Datahub. *Energies*, 15(2), p.650.
- Manchester City Council. 2021. Manchester City Council. Cooperative Network Infrastructure. The. Available online: <https://democracy.manchester.gov.uk/documents/s26075/Appendix%203%20-%20Digital%20infrastructure%20planning%20design%20guide.pdf>
- Mollah, M., Zhao, J., Niyato, D., Lam, K., Zhang, X., Ghias, A., Koh, L. and Yang, L., 2021. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet of Things Journal*, 8(1), pp.18-43.
- Modern Messaging for Distributed Systems, L Magnoni 2015 J.Phys.:Conf.Ser.608 012038. Available online: <https://iopscience.iop.org/article/10.1088/1742-6596/608/1/012038>
- Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed 10 September 2022).
- Risimic, D. 2007. AN INTEGRATION STRATEGY FOR LARGE ENTERPRISES. Available online: <http://www.doiserbia.nb.rs/img/doi/0354-0243/2007/0354-02430702209R.pdf> (accessed 10 September 2022).
- Security aspects of distributed ledger technologies. (2020). Retrieved 10 September 2022, from <https://figi.itu.int/wp-content/uploads/2021/04/Security-Aspects-of-Distributed-Ledger-Technologies-1.pdf>
- Smart Energy International, Digital Identities – building block for an automated energy system, 2022. Available online: <https://www.smart-energy.com/digitalisation/digital-identities-building-block-for-an-automated-energy-system/>
- Strusanu, Davide., and Hougbonon, Georges. 2020. Accelerating Digital Connectivity Through Infrastructure Sharing. Available online: <https://www.ifc.org/wps/wcm/connect/2d3c4eff-12a8-4b0b-b55d-9113a950ed33/EMCompass-Note-79-Digital-Infrastructure-Sharing.pdf?MOD=AJPERES&CVID=n2dwWtn>
- Strusanu, Davide., and Hougbonon, Georges. 2020. Accelerating Digital Connectivity Through Infrastructure Sharing. Available online: <https://www.ifc.org/wps/wcm/connect/2d3c4eff-12a8-4b0b-b55d-9113a950ed33/EMCompass-Note-79-Digital-Infrastructure-Sharing.pdf?MOD=AJPERES&CVID=n2dwWtn>
- Tilson, David., Lyytinen, Kalle., and Sorensen, Carsten. 2010. Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research. Available online. [https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F220079905\\_Digital\\_Infrastructures\\_The\\_Missing\\_IS\\_Research\\_Agenda&data=05%7C01%7CRick.Ros%40au.ey.com%7Cf668d041993f45ea9d7608dabf23ae38%7C5b973f9977df4bebb27daa0c70b8482c%7C0%7C0%7C638032457290883264%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLjBtIl6lk1haWwiLCJXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=vaxfwM51OoMLTz3dAQ44d0ItMx2IfA9A11u9BzzEOVU%3D&reserved=0](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F220079905_Digital_Infrastructures_The_Missing_IS_Research_Agenda&data=05%7C01%7CRick.Ros%40au.ey.com%7Cf668d041993f45ea9d7608dabf23ae38%7C5b973f9977df4bebb27daa0c70b8482c%7C0%7C0%7C638032457290883264%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLjBtIl6lk1haWwiLCJXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=vaxfwM51OoMLTz3dAQ44d0ItMx2IfA9A11u9BzzEOVU%3D&reserved=0)
- Walport M. Distributed ledger technology: beyond blockchain. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/g-s-16-1-distributed-ledger-technology.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/g-s-16-1-distributed-ledger-technology.pdf)
- Watt, G., 2022. *Integrating distributed energy resources in the electricity grid: Energy EVP discussion paper*. Available online: <https://www.engineersaustralia.org.au/sites/default/files/2022-03/Integrating-DER-in-the-grid-Discussion-Paper.pdf> (accessed 10 September 2022).
- Wing Lam and V. Shankaraman, "An enterprise integration methodology," in *IT Professional*, vol. 6, no. 2, pp. 40-48, March-April 2004, doi: 10.1109/MITP.2004.1278864

## Appendix A DER Data Exchange Detailed Problem Statements

This section contains DER data exchange problem statements highlighting the responsibilities for each market participant role for the future DER marketplace. Table 27 highlights collated use cases into categories for each DER marketplace role. There are 13 identified use cases, approximately one third relates specifically to asset register management or portfolio management.

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
<b>STANDING DATA - INVERTER SETTINGS</b>				
DERR05	OEM	If required I need to update the DER Register inverter, standards compliance and other protection settings as they change which is often given the scale of DER penetration and activation	have a simple automated way to update the DER Register with these changes	reduce my compliance burden and operational costs.
DERR08	OEM	If required, I cannot update the DER Register with updated inverter settings of DER devices following a firmware upgrade.	I want to write and update inverter settings of a DER device following a firmware upgrade	fulfill my obligation to reflect accurate settings about DER device functionalities in the DER Register which is used by the market, service and standards compliance authorities and participants as an up-to-date and enduring single source of truth
DERR09	Aggregator	<b>Cannot update market on inverter settings</b> If required, as the customer's DER representative, I cannot update Market system and network operators with updated inverter settings of DER devices in my VPP portfolio following a firmware upgrade.	I want to write and update inverter settings of a DER device following a firmware upgrade	fulfil my obligation to reflect accurate settings about DER device functionalities in the DER Register which is used by the market, service and standards compliance authorities and participants as an up-to-date and enduring single source of truth

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
<b>DERR03</b>	DNSP	<p><b>Inaccurate DER Configurations</b>  The DER Register does not necessarily reflect the "as-is" configured state of the connected DER, as settings can be changed after the installation, and this can have a consequential impact on network DER hosting capacity assessments and dynamic operating envelope calculations</p>	view inverter settings of registered DER (within appropriate permissions)	adapt network DER connection assessments and DOE calculations to accurately reflect the existing installed DER status
<b>DERR01</b>	Market and System Operator	<p><b>Unknown DER standard non-compliance</b>  I cannot confirm whether inverters connecting to the network and integrating with the grid are compliant with the specified service requirements and standards. This inhibits the MSO's ability to plan for power system disturbances, increasing costs to the power system relating to need for greater operating reserve.</p>	view inverter standard compliance and performance threshold settings of registered DER in aggregate at a region level and initiate changes (within appropriate permissions)	reliably identify whether inverter settings are compliant with standards and service requirements (for example, droop settings for FCAS and fault ride-through settings)
<b>DERR01.1</b>	DNSP	<p>Many installed inverter-based DER connecting to the network do not have the mandated standard AS4777 settings applied and this adversely impacts local network voltage management. Other than analysing historical smart meter data (where that exists), I have no way of</p>	view inverter settings of registered DER and initiate changes (within appropriate permissions)	adapt network DER connection assessments and DOE calculations to accurately reflect the existing installed DER status

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
		knowing whether the installed system is compliant		
<b>STANDING DATA - PORTFOLIO MANAGEMENT</b>				
<b>DERR07</b>	Hypothetical Test Certification Authority	If required, I need to record certifications provided to an aggregator that can be viewable by multiple authorised participants	I want to verify that a portfolio can deliver a particular service after comparing device and NMI data	the Market and System Operator and DNSP have confidence registered aggregator portfolios can deliver the services they are registered to provide
<b>IAM01</b>	Market and System Operator	I do not have a scalable registration process to certify and re-certify portfolios of DER assets as their its composition frequently changes with device upgrades and customer churn across many aggregator portfolios	facilitate aggregators' ability to provide me with portfolio updates close to the event time and the ability to process these updates in a short amount of time with minimal manual processing	enable aggregators of DER to participate in providing wholesale services (energy, FCAS) with the confidence that I can identify whether they can perform those services at any time as their portfolio composition changes in line with the nature of DER
<b>PMS02</b>	Market and System Operator, DNSP, and aggregator	<b>Duplicate Portfolio Management Systems</b> - Each party maintaining a different portfolio management system (AEMO for wholesale, DNSP for local services, aggregator internal) is inefficient and raises risk of errors and	Have a designated source of truth that is up-to-date and that multiple entities can access and update within appropriate permissions	rely on the aggregator portfolio information in my business operations

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
PMS03	Aggregator	disputes and is not scalable for a high DER future <b>Duplicated VPP Portfolio</b> registration updates - The MSO and DNSPs need up-to-date information about the sites and DER devices within my portfolio and there is no single mechanism to update all participants. This adds to my compliance burden and cost to serve customers.	Have a simple, standardised way of sharing my DER portfolio information	Through standardisation, reduce my compliance and operational costs and recruit more customers by sharing greater financial value with them.
PMS04	Aggregator	<b>Current AEMO Portfolio</b> management system for Wholesale Demand Response is not suitable for the scale and frequency of updates forecast for VPP fleets (small scale and mobile DER)	Hold up-to-date, and traceable information about the status of my portfolio including smaller scale DER and have a standard method to provide updates to both the MSO and DNSPs	Reduce my operational costs and recruit more customers by sharing greater financial value with them.
PMS07	Aggregator	<b>Speed to market</b> I cannot seamlessly monetise new DER in my portfolio across one or more actors (wholesale (AEMO) and local (DNSP) services) because it takes a long time to register my assets to provide a service after they are installed or recruited to my VPP	register my devices to provide services (wholesale and local) as soon as possible after they sign up to my VPP program.	maximise the service revenue opportunities available to my portfolio customers
<b>STANDING DATA - EVS</b>				



ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
EVMR01	Aggregator	<b>EV market registration at static location</b> my ability to utilise EVs to provide services as part of my portfolio is limited as they are only recognised at one designated location.	provide grid services whenever and wherever my EV may be connected to the grid	maximise revenue opportunities for my EV customer portfolio
EVMR02	Aggregator	<b>Fractured settlement of EV V2G services</b> when utilising an EV to provide V2G services across multiple locations, I do not have an efficient way to reconcile my settlement records against AEMO or other counterparties such as DNSPs.	have EVs in my portfolio recognised by AEMO and DNSPs where and when they are providing services	simply reconcile market and local services settlement with individual EVs (and their owners) after they have provided services
EVMR03	Market and System Operator	<b>Invisible EV/EV Supply Equipment</b> I have no visibility of EV ownership or EVSE installations to coordinate system and market operations as there is no appropriate asset register.	I want to access a dynamic EV Mobility Register that allows entities with appropriate access permissions to record location and characteristics of Electric Vehicle Supply Equipment (EVSE) (standing data) and dynamic data on charging operations	to inform up-to-date network modelling and forecasting and support research on EV charging behaviours as well as market settlement.
EVMR03.1	DNSP	<b>Invisible EV/EV Supply Equipment</b> I have no visibility of EV ownership or EVSE installations to manage emerging network loading conditions, network DER	I want to access a dynamic EV Mobility Register that allows entities with appropriate access permissions to record location and	better manage emerging network loading conditions, adapt network DER hosting capacity assessment to factor in the EV loads, and to improve the accuracy of calculating DOEs.

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
		hosting capacity assessment, and in future the calculation of DOEs.	characteristics of Electric Vehicle Supply Equipment (EVSE) (standing data) and dynamic data on charging operations	
EVMR05	Consumer	I can't see where all the public / private EV chargers are, and whether they are online/working, whether there is a booking, whether they are operating at their rated capacity	access and view data about EV charger location, operation, and availability across the entire national charging infrastructure network	have an efficient, simple and seamless experience when I utilise my EV and need to charge it regardless of the charge point service provider, distribution network, and wherever I am
EVMR06	Consumer	I need to register with multiple public charging networks or mobility services providers if I want to charge across different public charging networks	have simple options, including a single method of access and payment, to use any public charge point wherever I am regardless of the provider or distribution network	roam across different charging networks and states without concern about accessibility and charging technology available
<b>STANDING DATA - DER REGISTER</b>				
DERR04	Aggregator	The DER Register does not allow me to use it to prospect new VPP customers as only summary data is available.	search for and access records relating to DER installed and location	run targeted marketing campaigns to sign up VPP customers
PMS01	Market and System Operator	The information in the DER Register is not up to date (compliance requirement means 20 day delay) and therefore can be out of sync with aggregator/retailer portfolio standing data (NMI &	have the DER Register updated more frequently and these changes reflected in my portfolio management	maintain an accurate up to date relationship between the DER Register device data and aggregator portfolios

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
		Devices) registered with AEMO and so has limited trust as a source of truth because the aggregator assets that underpin the services I rely on will change after install, decommission or upgrade.	system, potentially intra-day	
PMS02.1	DNSP	I do not know what the operational state of the DER is with respect to connection, energisation and faults.	be able to access data on this that I can trust	determine if and when I can include those DER in DOE calculations or load control problems
<b>MARKET OPERATIONS</b>				
DDH01	Market and System Operator	I may be required by the AEMC, under the rules and in line with the NEO, to facilitate B2B transactions between multiple market participants that emerge from DER integration (for example, DOEs, LSE, Retailer Dynamic Export Limits), similar to my current role under Chapter 7 in relation to the B2B e-Hub	interact with participants in a standardised way, with appropriate authorisations, for a range of new and future DER use cases	fulfill my role under the rules to execute traceable and secure B2B transactions whose effect on wholesale market outcomes is known and accommodated
OPS01	Market and System Operator	where I need to provide market directions to aggregations of DER, I do not know the distribution network limits within which they can draw or inject power	have visibility of each Aggregator's assigned DOEs	account for distribution network limits in forming market directions for the aggregator DUID as well as other resources
OPS02	Market and System Operator	where I need to provide market directions to aggregations of DER, I do not know the capacity of that portfolio to draw or inject power on an operational timescale (on the day)	have visibility of each Aggregator's forecast generation and load from DER and close to real time updates on stored battery energy	account for DER portfolio capacity in forming market directions for the aggregator DUID as well as other resources

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
<b>LOCAL NETWORK SERVICES - EASE OF CONTRACTING</b>				
DDH04	DNSP	the current bespoke, bilateral agreements used to procure non-network alternatives to traditional network investment have significant costs and cannot easily scale	contract based on standardised and replicable terms	efficiently execute contracts and procure services at scale
DDH09	Aggregator	I need to enter into multiple, separate, and bespoke contractual bilateral service agreements with DNSPs to provide 'similar but different' local network services across the NEM. This complexity means its difficult, and potentially not scalable or economic, for me to develop consistent consumer offers to utilise their DER to deliver network services	Be able to access a single market interface to discover and bid on local network support opportunities across the NEM	Maximise service revenue opportunities for my customers, minimise market operational costs, and so make local services economic for my portfolio
<b>LOCAL SERVICES EXCHANGE</b>				
DDH02	Market and System Operator	<b>Invisible off-market capacity commitments</b> I do not have visibility of flexible capacity committed to off-market services such as those between aggregators and DNSPs to incorporate into my operational planning and market solve (for example, observe DNSP procured 300MW of peak demand support under a TNI on a given day)	receive both forecast as well as actual data of capacity committed to off-market services	take this into account to better balance supply and demand to run an efficient market, plan contingency reserves, RERT and other interventions

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
DDH03	DNSP	<p><b>Poor service provider discoverability</b> Currently, my processes to discover and contract with DER aggregators for local network support is highly manual and has access to a limited pool of providers</p>	Participate in a mechanism to reduce transaction costs and make it easy for as many DER service providers as possible to participate, but maintain autonomy over the specific detailed design and procurement of services in my network	Retain control over which services I want to procure and how, but also access the largest pool possible of ready aggregators that can provide firm, cost-effective DER-based non-network solutions to manage network reliability and stability, and to defer/displace network augmentation expenditure.
DDH05	DNSP	I do not have a scalable registration process to certify and re-certify portfolios of DER assets as their composition frequently changes with device upgrades and customer churn across many aggregator portfolios	Have efficient access (minimising risk of reconciliation errors) to a data source that accurately reflects the composition of DER aggregator portfolios at any given time, which can also record sub-portfolios that I can register to deliver local services	Have an accurate record of DER portfolios that can deliver local services that is consistent with information held regarding the same portfolios delivering wholesale services
DDH06	DNSP	a firm network support service I have contracted and am relying on, may be eroded by DER churn or availability and I have no visibility of this so that I can trust that my network limits will not be breached.	Have efficient access (minimising risk of reconciliation errors) to a data source that accurately reflects the composition of DER aggregator portfolios at any given time, which can also record sub-portfolios that I can register to deliver local services	Have an accurate record of DER portfolios that can deliver local services that is consistent with information held regarding the same portfolios delivering wholesale services

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
DDH08	DNSP	I don't have an efficient way to receive telemetry data or other service verification data from aggregators to validate services performed for the purposes of settlement, if required	simply and scalably receive telemetry/service verification data to calculate service performance and payment	efficiently determine service compliance and payment
DDH11	Aggregator	Each DNSP I contract with for local network support services has different requirements and mechanisms for me to provide local service verification data, which increases my cost to serve.	Standardised approach and efficient mechanism for transmitting service verification data (static and performance data) with DNSPs for local service verification and off-market settlement calculations	minimise operational costs in delivering local network services across multiple DNSP boundaries
DDH15	Aggregator	<b>Ease of Integration (Local Services)</b> I need to integrate into multiple, separate, and bespoke data exchange systems with DNSPs to deliver 'similar but different' local network services across the NEM in addition to integrating with AEMO to provide wholesale market services. This complexity means it's difficult, and potentially not scalable or economic, for me to deliver these services using my portfolio or participate in new B2B services as they arise.	Be able to access a market interface to discover and bid on local network support opportunities and wholesale market services across the NEM via one integration point	Maximise service revenue opportunities for my customers, minimise market operational costs, and so make local services economic for my portfolio
LS01	DNSP	If the AEMC deem it more efficient for consumers to	retain autonomy over the specific detailed	procure the right services, at the right amount, at the right time, and I

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
		standardise the definition and trade of local services, I need flexibility in governance arrangements to procure local services that meet my needs	design of services so that they meet my local needs, how I procure them and Governance of local services rather than have these dictated to me	can control who I want to procure them from. This will enable me to efficiently manage my network in the long term interests of consumers
<b>INTEGRATION</b>				
DDH10	Aggregator	<b>Ease of Integration (DOEs)</b> I need to integrate into multiple, separate, and bespoke data exchange systems with each DNSP to know which Dynamic Operating Envelopes (DOEs) to apply in operating my portfolio in addition to integrating with AEMO to provide wholesale market services. This adds to my compliance burden and cost to serve customers	Be able to access all DOEs that relate to my portfolio across different DNSP jurisdictions in the NEM via one integration point	minimise my operational costs and cost to serve customers
DDH12	Data Hub administrator	<b>Backward Compatibility</b> Market systems cannot be improved quickly if all registered hub users are not able to adopt schema updates at the same time	Have backwards compatibility in the Data Hub which means I am able to support multiple different schemas for the same transaction at the same time	support multiple (backward compatible) versions of messages from different participants for a period to give them time to upgrade
DDH13	Retailer	<b>Ease of Integration (Retailer Zero Exports)</b> I need to integrate into multiple, separate, and bespoke data exchange	Be able to broadcast my zero exports need to multiple providers via a single market interface	Access many potential zero export limit providers including new ones that emerge through a single integration point, lowering my cost of

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
		<p>systems with Aggregators and customer agents to request 'zero exports' at my retail sites during negative spot market prices to avoid paying for these (up to \$1,000/MWh). This is in addition to integrating with AEMO to provide wholesale market services. This adds to my cost of managing risk and cost to serve customers</p>		<p>managing spot price risk and serving customers.</p>
DDH14	Aggregator	<p><b>Poor service opportunity access</b> To provide non-market business-to-business services (for example, to DNSPs and Retails) I need to integrate into multiple, separate, and bespoke data exchange systems with each of these service providers in addition to integrating with AEMO to provide wholesale market services. This provides barriers to me providing more services and limits the value I can share with my customers</p>	<p>Access many potential business-to-business service opportunities (with DNSPs, Retailers and others) and new ones that emerge through a single integration point.</p>	<p>minimise my administration overhead and barriers to accessing non-market revenue opportunities to recruit more customers by sharing greater financial value with them.</p>
PMS06	Aggregator	<p><b>Portfolio update standardisation</b> The MSO and DNSPs want up to date information about my portfolio and I have no standardised way to transmit this data to these entities.</p>	<p>Hold up-to-date, and traceable information about the status of my portfolio and have a standard method to provide updates to both the MSO and DNSPs</p>	<p>minimise my compliance costs and recruit more customers by sharing greater financial value with them.</p>



ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
<b>IDENTITY AND ACCESS MANAGEMENT (IDAM)</b>				
IAM02	Data Hub administrator	It is not efficient for one party to administer all data exchange permissions as DER use cases and number of participants reach a very high scale.	Provide and edit permissions of actors regarding their use of the Data Hub infrastructure in line with their own role including the ability to provision and edit permissions of other actors. <i>For example, AEMO provide DNSPs ability to provision and edit aggregator permissions relating to use of an LSE within their jurisdiction.</i>	Delegate responsibility of governing role based permissions to those best able to manage the risk
IAM03	DNSP and Aggregator	<b>Duplicated Identity Verification Processes</b> I need to participate in multiple, separate and bespoke organisation identity verification processes with DNSPs to deliver 'similar but different' local network services across the NEM as well as AEMO to provide wholesale market services and any other entity for additional B2B services. This adds to my compliance burden and cost to serve customers	have a single process to verify my organisation identity that can be used across all energy market actors	minimise my administration overhead and barriers to accessing non-market revenue opportunities to recruit more customers by sharing greater financial value with them.
<b>CYBER SECURITY</b>				

ID	AS THE	I HAVE A PROBLEM THAT	THEREFORE, I WANT TO	SO THAT I CAN
CYB01	Market and System Operator, DNSP, and aggregator	<p><b>Maintain cyber security in a decentralising power system</b></p> <p>We need to maintain a secure and reliable communication infrastructure that extends to DER devices directly and/or via aggregators.</p>	<p>Have a highly controlled and auditable data exchange arrangement that is maintained to the required level of security and reliability standards as may apply to essential services or critical national infrastructure.</p>	<p>Transact DER services safely and securely with lower (acceptable) risk of malicious or accidental misuse of distributed devices.</p>

Table 27: DER Data Exchange Problem Statements  
Source: AEMO (2022)

# Appendix B AEMO Risk Rating Guidelines

AEMO Corporate Risk Matrix		CONSEQUENCE					LIKELIHOOD	ANNUAL PROBABILITY	QUALITATIVE DESCRIPTION
		Immaterial	Minor	Moderate	Major	Extreme			
LIKELIHOOD	Almost Certain	Medium	Medium	High	Critical	Critical	Almost Certain	>90%	Will occur in most circumstances; statistical record of several occurrences
	Likely	Low	Medium	High	Critical	Critical	Likely	51% - 90%	Can be expected to occur in most circumstances; statistical record of multiple occurrences
	Possible	Low	Medium	High	High	Critical	Possible	11% - 50%	May occur, but not expected in most circumstances; statistical record of a few occurrence
	Unlikely	Low	Low	Medium	Medium	High	Unlikely	1% - 10%	Conceivable but unlikely to occur in any given year; statistical record of at least one occurrence
	Rare	Low	Low	Medium	Medium	High	Rare	<1%	Will only occur in exceptional circumstances; no history of occurrence
Consequence	Reputation and Stakeholders	Financial (AEMO)	People* (Health & Safety, Workforce)		Environment	Market & System Impact*	Legal & Compliance		
<b>Extreme</b>	Significant long-term damage to stakeholder and public confidence and relationships. Continued adverse media exposure. Significant financial impact drives participant(s) towards insolvency.	> \$25M	Health & Safety Single fatality, severe permanent injury or multiple notifiable injuries, or life-threatening exposure to a health risk. Workforce Workforce impact across AEMO causing an inability to deliver core functions and/or strategy implementation over a sustained period.	Permanent long-term environmental harm. e.g. major pollution incident causing significant damage or potential to health or the environment; and/or Fines and prosecution likely.	Loss of supply to a state(s) for any duration (e.g. system black). Market suspension market(s) for a prolonged period.	Corporate fine >\$1M. Imprisonment and/or disqualification to Officer or Director. Government inquiry on AEMO's functions. Litigation involving Class Actions.			
<b>Major</b>	Significant short-term damage to stakeholder confidence and relationships. Some loss of public confidence. Short term adverse media exposure. Significant financial impact on participant(s).	\$5M - \$25M	Health & Safety Injury or illness requiring > 5 days hospitalisation or medical treatment (incapacity beyond 3 months). Workforce Workforce impact causing an inability to deliver some core functions and/or strategy implementation.	Long term or serious environmental damage (extensive rectification activity required); and/or Multiple complaints received; and/or Potential for prosecution	Loss of supply to a large portion* of a state, for any duration. Market suspension in one jurisdiction or market for a short period.	Corporate fine or civil penalty \$100K to \$1M and/or court enforceable undertaking. Fine for personal liability to Officer or Director. Sustained Regulator scrutiny requiring extensive management effort to address. Litigation involving protracted Court actions possible.			
<b>Moderate</b>	Some damage to stakeholder confidence and relationships. Some adverse media exposure. Adverse financial impact on participant(s).	\$500K - \$5M	Health & Safety Injury or illness requiring < 5 days hospitalisation or medical treatment and/or counselling services or intervention (6 days to 3 months incapacity). Workforce Workforce impact in multiple areas but not impacting delivery of core functions and/or strategy implementation.	Measurable environmental impact (significant rectification required); and/or Will cause complaints; and/or Possible fine.	Localised/minimal loss of supply in a state. Market(s) in administered state or material scheduling error.	Corporate fine or civil penalty <\$100K No personal liability but resignation of an Officer or Director. Targeted Regulator scrutiny or investigation requiring significant management effort to address. Possible dispute resolution process.			

Figure 23: AEMO Risk Rating Guidelines

## Appendix C Risk Assessment Approach

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. The risk management approach is underpinned by the following key principles:

- ▶ is integrated into all parts of the business to achieve common objectives.
- ▶ is structured and comprehensive enough to provide guidance on achieving consistent and comparable results.
- ▶ is customised and proportionate to external and internal context related to its objectives.
- ▶ is inclusive through appropriate and timely involvement of stakeholders to enable their knowledge, views and perceptions to be considered.
- ▶ is dynamic, in that it anticipates, detects, acknowledges and responds to changes and events in an appropriate and timely manner.
- ▶ is based on the best available information.
- ▶ takes human and cultural factors into account; and
- ▶ is continually improved through monitoring, learning and experience.

Risk management is embedded in the business, span across multiple functions for accountability and should enable mitigation of process failure. The risk management process (illustrated in Figure 24 below) should be structured on the platform of making risk management the responsibility of all personnel, with active and committed risk strategies, oversight, comprehensive policies and accountability standards in place at senior management and board level.

In summary, the risk framework should encompass the following:

- ▶ Supports value creation for the stakeholders which revolves around a committed risk assessment process at all levels of operation.
- ▶ Board's commitment to risk management with the embedment of a risk culture.
- ▶ Relevant workshops, frequent risk training, publication of risk knowledge
- ▶ Risk intranet and a transparent risk structure are characteristics of this risk culture; and
- ▶ Assurance to the Board and stakeholders that a stable risk management platform is entrenched and embedded will come from a proper coordinated system of risk identification, measurement and reporting procedures from the bottoms-up corresponding with a tops-down commitment from Board and Senior Management by way of an established risk management policy and framework.

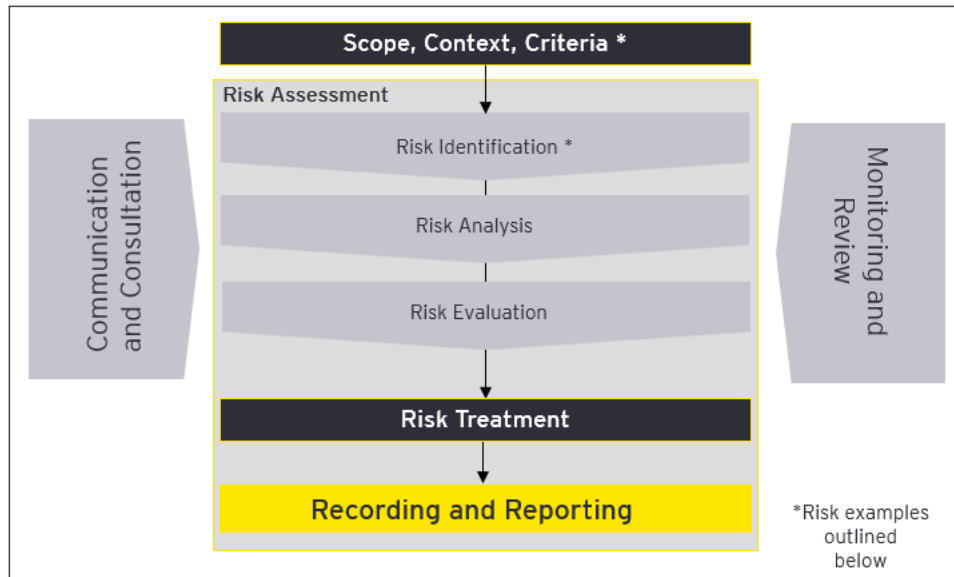


Figure 24: Risk framework  
Source: EY (2022)

A key challenge is the balance for the right mixture of risk aversion and risk taking to maximise long term value creation, by seeking to maximise return for an acceptable level of risk or minimise risk for a target level of profitability in strategic decision-making processes.

Future risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

## Risk Analysis

Risk analysis can consider factors such as:

- ▶ the likelihood of events and impacts;
- ▶ the nature and magnitude of impacts;
- ▶ complexity and connectivity;
- ▶ time-related factors and volatility;
- ▶ the effectiveness of existing controls;
- ▶ sensitivity and confidence levels.

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe Impacts. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk assessment, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide

insight for decisions, where choices are being made, and the options involve different types and levels of risk.

While we have listed and categorised risks below, we have assigned a likelihood of occurrence and defined a risk event. As Project Edge is in exploratory phase, existing controls of AEMO's environment have not been considered. While determining the likelihood of rating, we considered the following factors:

- ▶ the anticipated frequency of the event occurring;
- ▶ the potential working environment of a decentralised model;
- ▶ the procedures and skills currently in place;
- ▶ staff commitment;
- ▶ morale and attitude;
- ▶ complexity and connectivity;
- ▶ time-related factors and volatility;
- ▶ the effectiveness of existing controls; and
- ▶ history of previous events.

It is important to note that the analysis performed below is qualitative, separates minor risks from major risks and provides additional information on the risk assessment.

The table below provides a matrix of the risk rating by combining the Impact and likelihood for each risk.

	Impact			
Likelihood		Minor	Serious	Major
		1	2	3
Likely	3	Low	Significant	High
Possible	2	Low	Moderate	Significant
Unlikely	1	Low	Moderate	Moderate

Table 28: Risk Impact and Likelihood Matrix  
Source: EY (2022)

## Scope, Context and Criteria

As a part of this report, within the DER marketplace, we have analysed the risk point of view for the following stakeholders to adopt a decentralised model for the shared DER marketplace over a point to point or centralised approach:

- ▶ Primary Stakeholders – Agents and DSO's/DNSP's
- ▶ Secondary Stakeholders – Customers/Prosumers and Market Operator

## Risk Criteria:

The risk criteria includes the following elements:

- ▶ the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible).
- ▶ how impact (both positive and negative) and likelihood will be defined and measured.
- ▶ time-related factors.
- ▶ consistency in the use of measurements.
- ▶ how the level of risk is to be determined.
- ▶ how combinations and sequences of multiple risks will be taken into account.
- ▶ AEMO's risk appetite

## Categories of risk

Since risk criteria should reflect the AEMO's values, objectives and resources and be consistent with policies and statements about risk management, we have categorized risks of implementation of a decentralised model in a shared DER infrastructure landscape, under the following themes, that are aligned to AEMO's NEO Objectives, Project Edge Data Exchange Principles and Project Edge Research Plan for all stakeholders:

- ▶ Scalability, Stability and Resiliency
- ▶ Governance, Cost and Ownership
- ▶ Data Privacy, Security, and Quality
- ▶ Change Management

## Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk assessment. Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary. Below is an illustrative example of the assessment process:

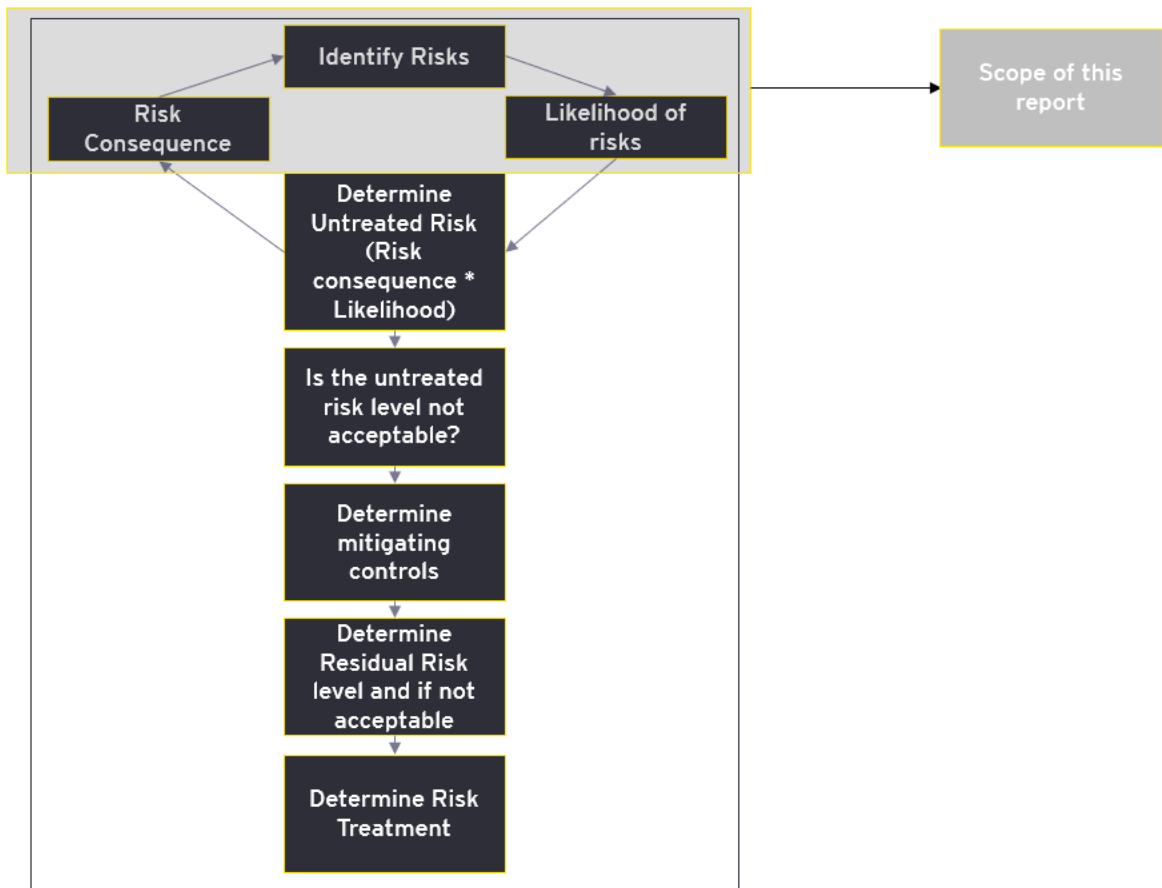


Figure 25: Risk Assessment Process  
Source: EY (2022)

## Risk Identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent an organisation achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks. While not specifically listed further in the report, the below listed factors (and relationships between these factors) have played an important role in the identification of risks. Further, we have limited our set of identified risks based solely on the theoretical knowledge of decentralised model for data exchange within the shared DER marketplace and not AEMO's existing control environment.

- ▶ tangible and intangible sources of risk;
- ▶ causes and events;
- ▶ threats and opportunities;
- ▶ vulnerabilities and capabilities;
- ▶ changes in the external and internal context;
- ▶ indicators of emerging risks;
- ▶ the nature and value of assets and resources;
- ▶ their impact on objectives;



- ▶ limitations of knowledge and reliability of information;
- ▶ time-related factors;
- ▶ biases, assumptions and beliefs of those involved.

AEMO might also consider categorising them into the following for divisional accountability:

- ▶ Strategic risk
- ▶ Financial risk
- ▶ Safety risk
- ▶ Operational risk
- ▶ Regulatory risk
- ▶ Reputational risk etc.

There are no predefined rules for just how specific the risk needs to be. However, as a general rule, it should be specific enough to ensure that the full extent of the risk is understood, and that specific risk treatment can be assigned to that risk. Therefore, under certain circumstances further sub risk categories may be appropriately identified.

## **Risk Causes**

Once a risk has been identified, it is often useful to record any contributing factors that may cause the risk to exist. This involves the identification of the situation(s) or key cause(s), which could result in the risk event occurring. This step in the identification process assists with better risk analysis, where the causes of the risk identified may be linked to one or more key controls as a means to manage or treat the risk, and therefore manage the level of risk exposure.

## **Risk Management Framework for Maintenance**

The Risk Management framework will have to be integrated into significant activities and functions for appropriate monitoring and governance, including decision making for enforcement. Post implementation, periodic gap assessments are usually leading practice with regular remediation plans to address those gaps in the organisation prior to implementation of controls (or remediation sometimes becomes the control implemented).



Figure 26: Risk Management  
Source: EY (2022)

Once risks are assigned a priority level and are untreated as well as residual risks are included in the assessment, risk treatment plans can then be formulated. A risk can be avoided, shared, accepted, reduced in rating or pursued for further action. Risk treatment is undertaken by responding to the risk, bringing it down to an acceptable level, and then retaining the remaining risk.

Communication and consultation occurs throughout the framework to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Additionally, both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or ad hoc. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.

## Appendix D Compensatory Controls supporting material

### Compensatory Control Scenario

To assist in gaining a consensus of understanding for compensatory controls triggers among market participants, a set of scenarios for compensatory control are documented as per the below. This approach provides a re-usable example for the consistent application of compensatory control logic. Scenario diagrams have defined for documentation of the impacted parties in each scenario.

Loss of Data Exchange	
Problem	This compensatory control trigger describes the loss of communication throughout the data exchange, no Boffers, Dynamic Operating Envelopes or Dispatch data exchange is available
Actors	1. DSO/DNSP 2. AEMO 3. Aggregator
Pre-conditions/trigger	1. A Boffer is sent from Aggregator OR; 2. An Operating Envelope is sent from the DSO OR; 3. Dispatch is sent from AEMO  AND No acknowledgement messages are received
Proposed Requirement	All market participants will fall back to most recent period instructions given for operations
Assumptions	1. Capacity available sent as part of previously received Boffer remains constant 2. DSO can operate and control network safely and securely within restrictions of most recently received operating envelope acknowledgement
Post-conditions	1. DSO operates and controls network within restrictions of most recently received operating envelope acknowledgement

Which market participants are involved →

Proposed compensatory control →

Expected Outcomes →

Description of Compensatory Control Trigger →

What needs to occur to trigger compensatory control →

Associated Assumptions →

Figure 27: Compensatory Control Scenario

The following additional scenarios have been considered for data exchange including impacted actors, pre-conditions, requirements and post-conditions.

Scenario
Failure/loss of communication to the aggregator/customer representative
Failure/loss of total communications across the data exchange
Failure to meet the requirements of a market arrangement
Loss of DNSP Communication
Loss of Communication Between Customer Representative and DER

### Summary of Data Exchanged

The below interfaces have been considered for the development of scenarios. They do not represent an exhaustive list of data to be exchanged.

Data name	Sender	Receiver
Boffer	Aggregator	AEMO
bofferAck	AEMO	AEMO
dsoOperatingEnvelop	DSO	AEMO
dsoOperatingEnvelopAck	AEMO	Participant (DSO)
dispatch	AEMO	Participant (Aggregator)
dispatchAck	Aggregator	AEMO

Table 29: Summary of Data Exchanged

### Scenario: Failure/loss of communication to the aggregator/customer representative

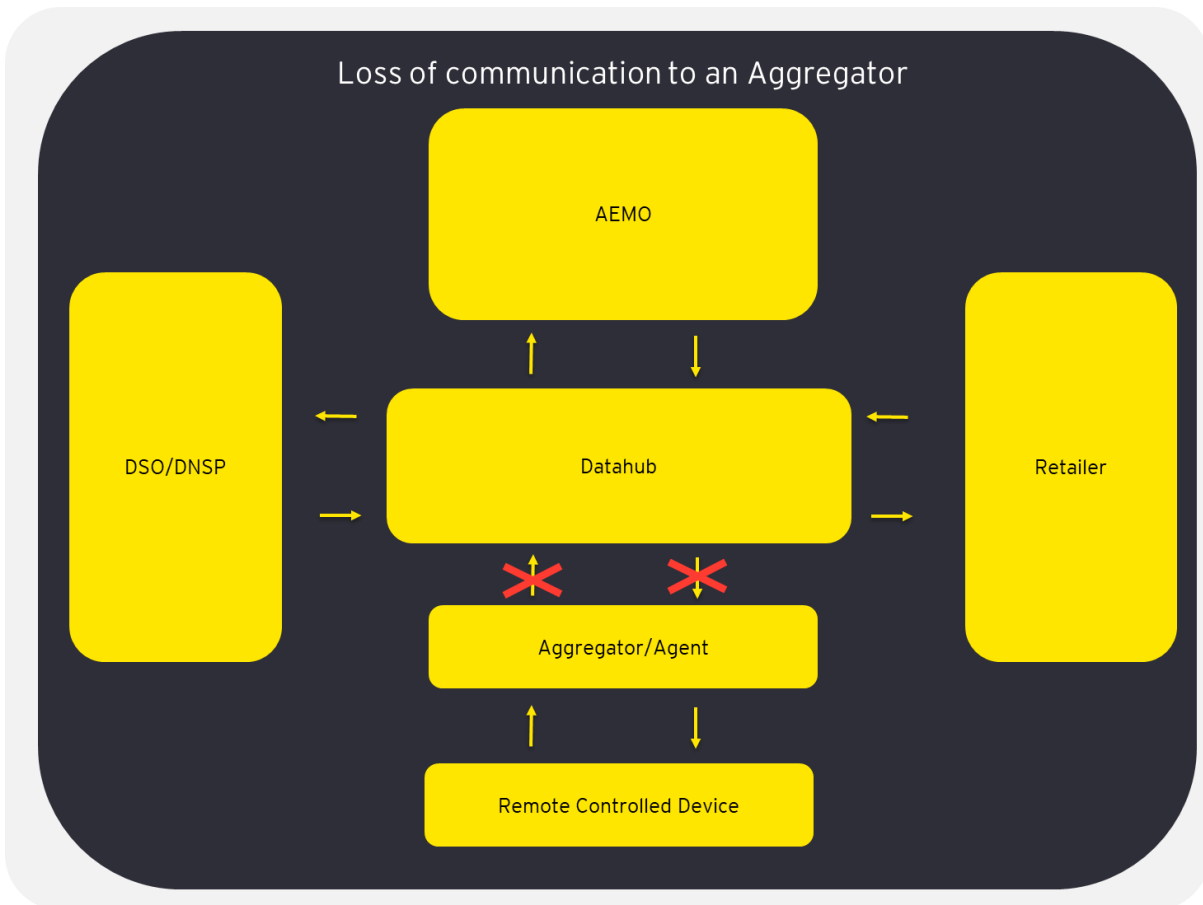


Figure 28: Scenario - Loss of Aggregator

Loss of communication to an Aggregator	
Problem	No data exchange is available between the Aggregator and the data hub
Actors	<ol style="list-style-type: none"> <li>1. AEMO</li> <li>2. Aggregator</li> </ol>
Pre-conditions/ trigger	<ol style="list-style-type: none"> <li>1. No Boffers are received from an aggregator</li> <li>2. No dispatch acknowledgement is received from the Aggregator</li> </ol> <p>OR;</p> <ol style="list-style-type: none"> <li>1. Data received from the aggregator is considered low quality as defined by marketplace data quality framework</li> </ol> <p>OR;</p> <ol style="list-style-type: none"> <li>1. Data received from aggregator does not comply with agreed latency requirements</li> </ol> <p>OR;</p> <ol style="list-style-type: none"> <li>1. Identity of the aggregator cannot be validated, trust is lost</li> </ol>
Proposed Requirement	<ol style="list-style-type: none"> <li>1. To ensure system security, controlled devices should fall back to the most recently received failsafe import/export limit parameter sent.</li> <li>2. Aggregators will not be compensated for any curtailed capacity as a result of imposed failsafe to a communications outage</li> </ol>
Assumptions	<ol style="list-style-type: none"> <li>1. At least one dynamic operating envelope containing a failsafe protocol has been received and acknowledge for each device under the control of the aggregator experiencing an outage</li> <li>2. DNSP can operate and control network safely and securely within restrictions of most recently sent failsafe protocol</li> <li>3. If any controlled devices fail to comply with import/export limits set by the failsafe protocol the DNSP may operate disconnect impacted DER if they are a risk to overall security of supply</li> </ol>
Post-conditions	<ol style="list-style-type: none"> <li>1. DSO operates and controls network within restrictions of most recently acknowledged failsafe protocol of any impacted DER</li> <li>2. The aggregator notifies all market participants of return to service</li> </ol>

Table 30: Scenario - Loss of Aggregator

## Failure/loss of total communications across the data exchange

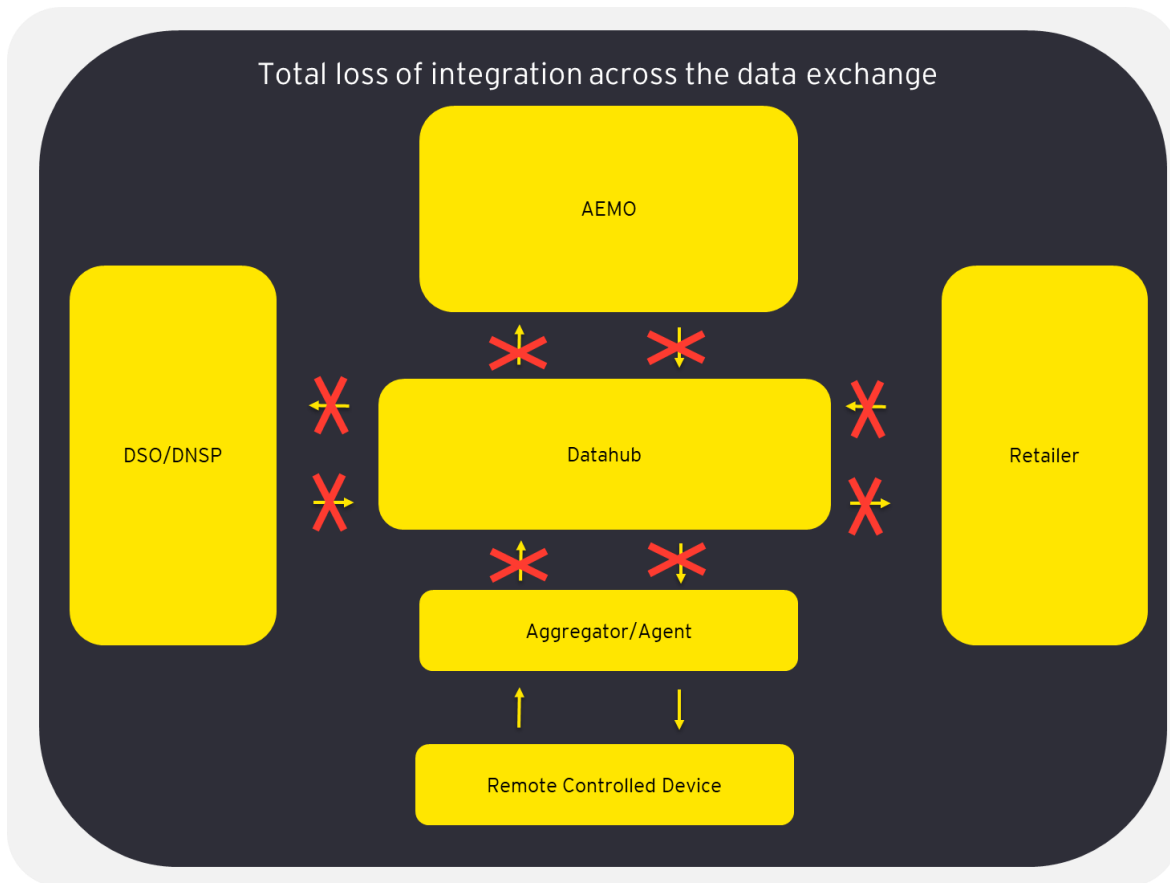


Figure 29: Failure/loss of total communications across the data exchange

Failure/loss of total communications across the data exchange	
Problem	This compensatory control trigger describes the loss of communication throughout the data exchange, no Boffers, Dynamic Operating Envelopes or Dispatch data exchange is available
Actors	<ol style="list-style-type: none"> <li>1. DSO/DNSP</li> <li>2. AEMO</li> <li>3. Aggregator</li> </ol>
Pre-conditions/trigger	<ol style="list-style-type: none"> <li>1. A Boffer is sent from Aggregator OR;</li> <li>2. An Operating Envelope is sent from the DSO OR;</li> <li>3. Dispatch is sent from AEMO</li> </ol> <p>AND No acknowledgement messages are received within the agreed latency window</p>
Proposed Requirement	<ol style="list-style-type: none"> <li>1. To ensure system security, controlled devices should fall back to the most recently received failsafe import/export limit parameter sent. Aggregators will not be compensated for any curtailed capacity as a result of imposed failsafe to a communications outage</li> </ol>
Assumptions	<ol style="list-style-type: none"> <li>1. At least one dynamic operating envelope containing a failsafe protocol has been received and acknowledge for each device under the control of the aggregator experiencing an outage</li> <li>2. DNSP can operate and control network safely and securely within</li> </ol>

Failure/loss of total communications across the data exchange	
	restrictions of most recently sent failsafe protocol 3. If any controlled devices fail to comply with import/export limits set by the failsafe protocol the DNSP may operate disconnect impacted DER if they are a risk to overall security of supply
Post-conditions	1. DNSP operates and controls network within restrictions of most recently acknowledged failsafe protocol of any impacted DER 2. The aggregator notifies all market participants of return to service

Table 31: Failure/loss of total communications across the data exchange

## Failure/loss of communication to a DNSP

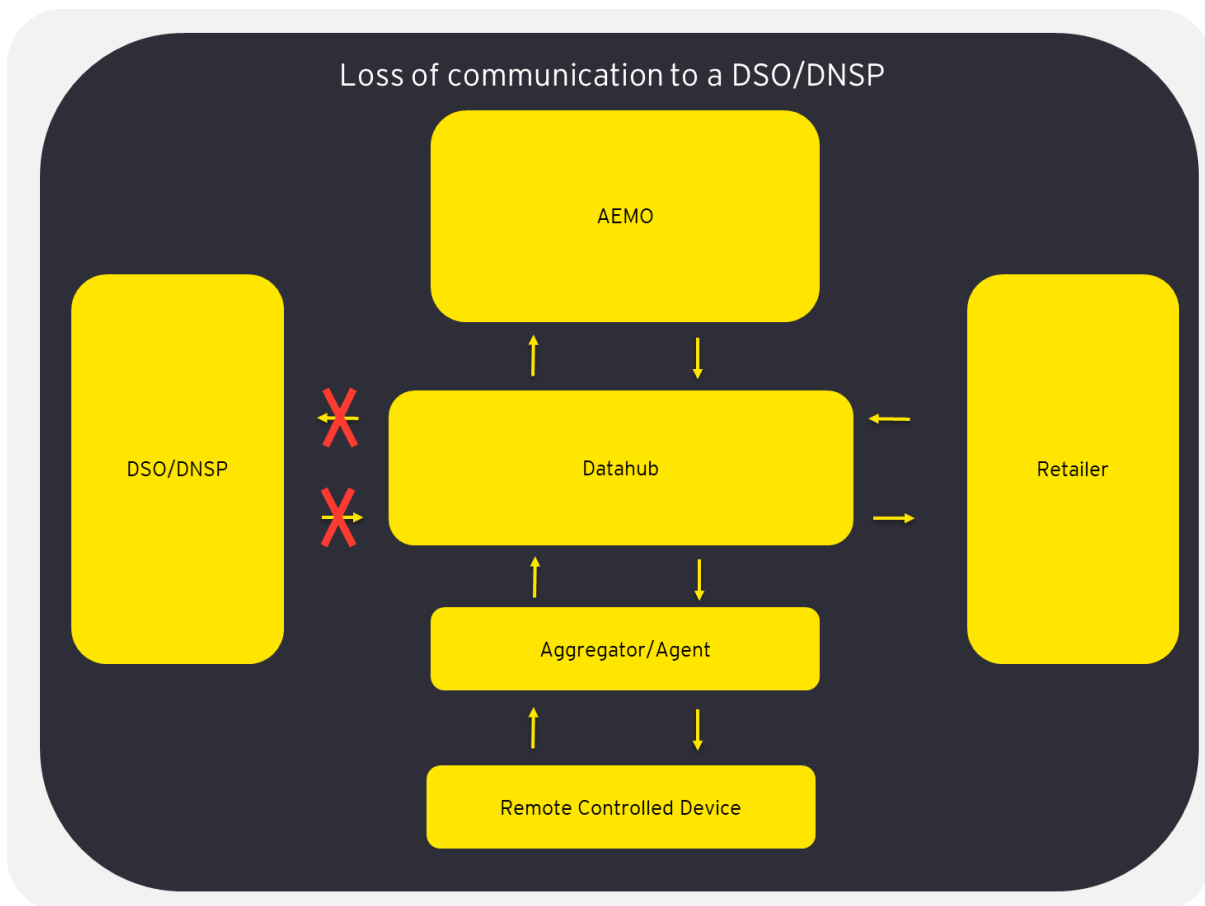


Figure 30: Failure/loss of communication to a DNSP

Loss of DNSP Communication	
Problem	No data exchange is available between the DNSP and AEMO
Actors	1. DSO/DNSP 2. AEMO
Pre-conditions/trigger	1. No initial/first for period Dynamic Operating Envelope information is received from the DNSP OR; 2. Dynamic Operating Envelope revisions for a given period are not received

Loss of DNSP Communication	
	in the requisite latency window
Proposed Requirement	<ol style="list-style-type: none"> <li>To ensure system security, controlled devices should fall back to the most recently received failsafe import/export limit parameter sent.</li> <li>Aggregators will not be compensated for any curtailed capacity as a result of imposed failsafe to a communications outage</li> </ol>
Assumptions	<ol style="list-style-type: none"> <li>At least one dynamic operating envelope containing a failsafe protocol has been received and acknowledge for each device under the control of the aggregator experiencing an outage</li> <li>DNSP can operate and control network safely and securely within restrictions of most recently sent failsafe protocol</li> <li>If any controlled devices fail to comply with import/export limits set by the failsafe protocol the DNSP may operate disconnect impacted DER if they are a risk to overall security of supply</li> </ol>
Post-conditions	<ol style="list-style-type: none"> <li>DNSP operates and controls network within restrictions of most recently acknowledged failsafe protocol of any impacted DER</li> <li>On restoration of communication the DNSP notifies all market participants of return to service via the hub messaging service</li> </ol>

Table 32: Failure/loss of communication to a DNSP

### Failure to meet the requirements of a market arrangement

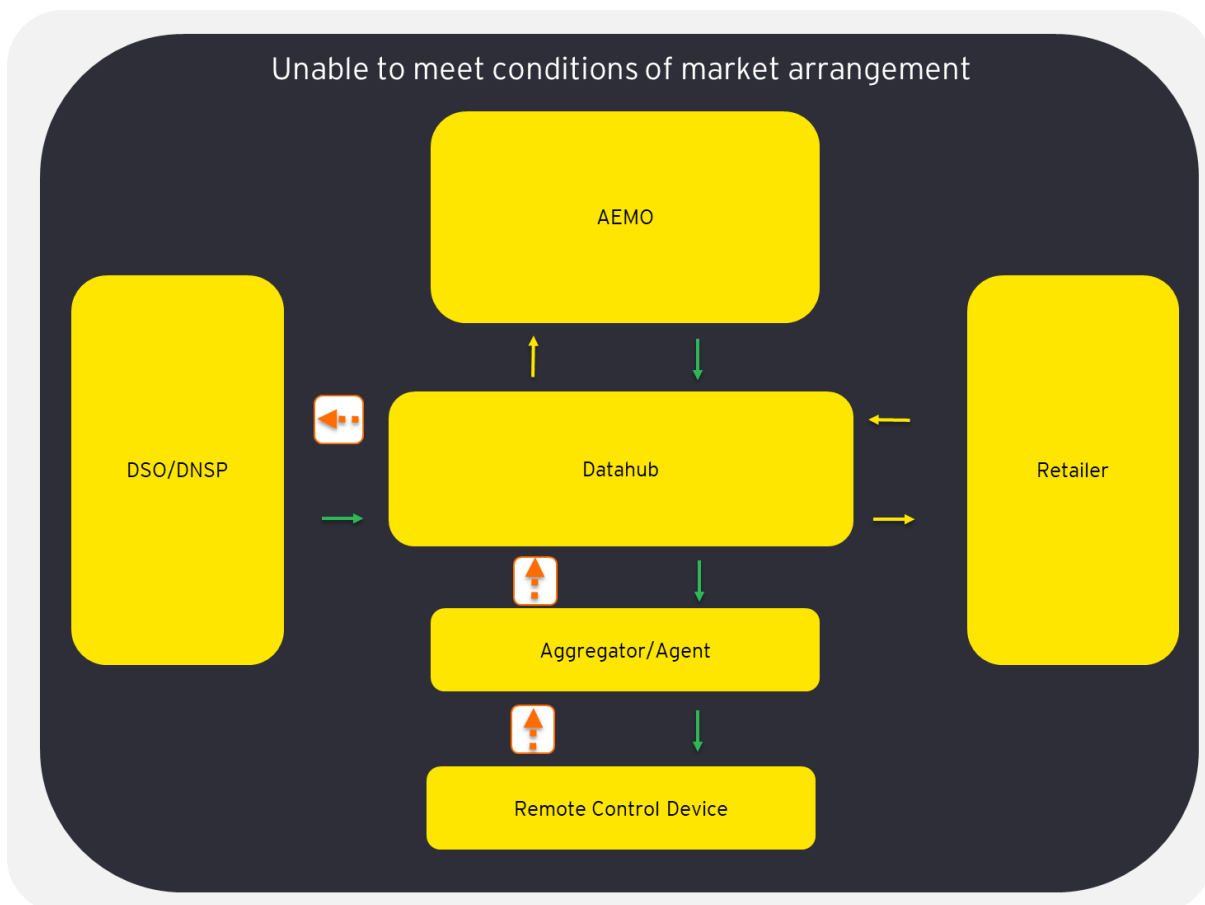


Figure 31: Failure to meet the requirements of a market arrangement



Failure to meet market arrangement	
Problem	The RCD fails to meet the requirements of a dynamic operating envelope
Actors	<ol style="list-style-type: none"> <li>1. Aggregator</li> <li>2. AEMO</li> <li>3. DNSP</li> <li>4. RCD</li> </ol>
Pre-conditions/trigger	<ol style="list-style-type: none"> <li>1. A Boffer has been sent from the RCD's representative, the aggregator</li> <li>2. The DNSP/DSO has sent a Dynamic Operating Envelope to AEMO</li> <li>3. AEMO has sent a Dispatch to the aggregator</li> </ol>
Proposed Requirement	<ol style="list-style-type: none"> <li>1. The Aggregator should notify AEMO and the DNSP of a failure to meet market arrangement as per any pre-determined industry arrangement</li> <li>2. Compensation for failure to meet an agreed market arrangement is documented at the time of Dispatch</li> </ol>
Assumptions	<ol style="list-style-type: none"> <li>1. Conditions of Dispatch define the expected behaviour and market outcomes for a failure to meet a market arrangement</li> <li>2. DNSP can operate and control network safely and securely</li> <li>3. If any controlled devices fail to comply with import/export limits set by the failsafe protocol the DNSP may disconnect impacted DER if they are a risk to overall security of supply</li> </ol>
Post-conditions	<ol style="list-style-type: none"> <li>1. The aggregator notifies AEMO and the DNSP of the failure to meet market arrangement</li> </ol>

Table 33: Failure to meet the requirements of a market arrangement

## Communication Redundancy Requirements

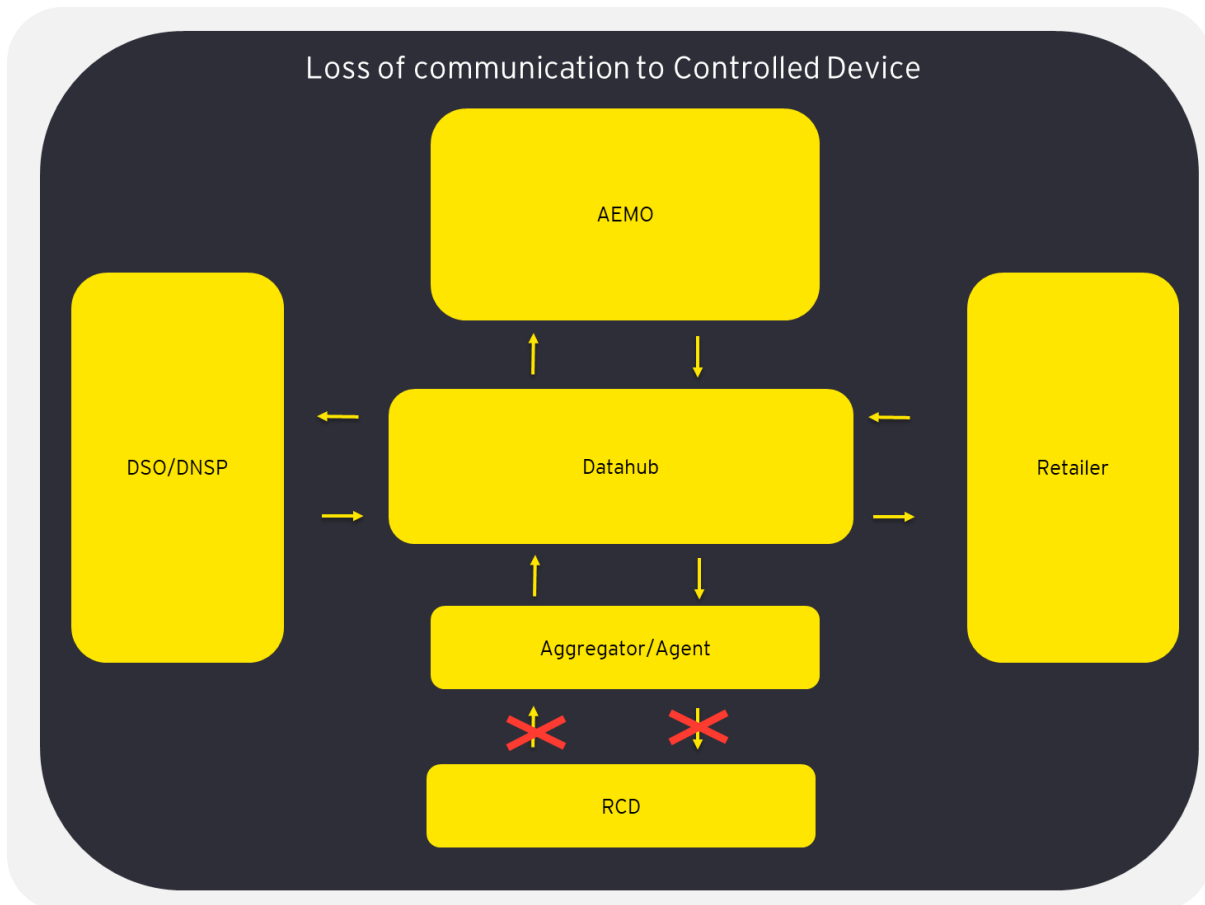


Figure 32: Communication Redundancy Requirements

Loss of Communication Between Customer Representative and DER	
Problem	No communication is possible to the RCD via their representative aggregator or via RCD metering point. For example, a communication outage by the mobile service provider
Actors	<ol style="list-style-type: none"> <li>1. RCD</li> <li>2. Aggregator</li> <li>3. DNSP</li> </ol>
Pre-conditions/trigger	<ol style="list-style-type: none"> <li>1. The aggregator is unable to communicate with the RCD</li> <li>2. To ensure system security, controlled devices should fall back to the most recently received failsafe import/export limit parameter sent.</li> <li>3. Aggregators will not be compensated for any curtailed capacity as a result of imposed failsafe to a communications outage</li> </ol>
Proposed Requirement	<ol style="list-style-type: none"> <li>1. At least one dynamic operating envelope containing a failsafe protocol has been received and acknowledge for each device under the control of the aggregator experiencing an outage</li> <li>2. DNSP can operate and control network safely and securely within restrictions of most recently sent failsafe protocol</li> <li>3. If any controlled devices fail to comply with import/export limits set by the failsafe protocol the DNSP may disconnect impacted DER if they are a risk to overall security of supply</li> </ol>
Assumptions	<ol style="list-style-type: none"> <li>1. DSO operates and controls network within restrictions of most recently</li> </ol>

Loss of Communication Between Customer Representative and DER	
	acknowledged failsafe protocol of any impacted DER

*Table 34: Communication Redundancy Requirements*

## Appendix E Glossary of Terms

Term	Meaning
AEMO	Australian Energy Market Operator – The manager of electricity and gas systems and markets across Australia, helping to ensure Australians have access to affordable, secure and reliable energy.
Centralised / Federated ID	Federated identity allows authorised users to access multiple applications and domains using a single set of credentials.
CH	Centralised Hub
CISP	Cybersecurity Information Sharing Partnership
DD	Decentralised Hub
DDH	Decentralised Data Hub
Decentralised Workers	Resources used in decentralised technology approaches to compute various tasks using distributed computing power.
DER	Distributed Energy Resources – Smaller Generation units such as rooftop solar and batteries that are installed on the customer’s side behind the meter.
DID	Decentralised Identities - A trust framework in which identifiers, such as usernames, can be replaced with IDs that are self-owned, independent, and enable data exchange using distributed ledger technology to protect privacy and secure transactions. The objective is to allow a subject such as an individual or device to create their identity and manage it under their control. (Alternatives are Siloed Identities (Centralised ID, Federated ID)).
Distributed Computing	A methodology that uses multiple distributed computers work together to solve a common problem.
DLT	Distributed Ledger Technology - Distributed ledger technology is a platform that uses ledgers stored on separate, connected devices in a network to ensure data accuracy and security.
DNSP	Distribution Network Service Provider
DOE	Dynamic Operating Envelopes - Operating envelopes are the limits that an electricity customer can import and export to the electricity grid. These limits are agreed between networks, customers and the AER as part of the customer connection or regulatory process. Currently, in most cases, operating envelopes are fixed at conservative levels regardless of the capacity of the network because they are static and need to account for ‘worst case scenario’ conditions. Dynamic operating envelopes are where import and export limits can vary over time and location. Dynamic rather than fixed export limits could enable higher levels of energy exports from customers’ solar and battery systems by allowing higher export limits when there is more hosting capacity on the local network.
DSO	Distribution System Operator

EDGE	Energy Demand Generation Exchange – Project EDGE (Energy Demand and Generation Exchange) is a multi-year project to demonstrate an off-market, proof-of-concept Distributed Energy Resource (DER) Marketplace that efficiently operates DER to provide both wholesale and local network services within the constraints of the distribution network.
e-Hub	Consists of the API Portal and the API Gateway for both electricity and gas.
ESB	Enterprise Service Bus
GW	Giga Watt
IEC	International Electrotechnical Commission
Loose Coupling	Where systems are weakly associated so that changes to one component have the least impact on the capability and performance of another, introduces another layer of integration that may be required to translate, reformat and restructure data.
NEM	National Electricity Market
NEO	National Electricity Objective - The objective to promote efficient investment in, and efficient operation and use of, electricity services for the long-term interests of consumers of electricity with respect to the reliability, safety and security of the national electricity system.
RCD	Remote Control Device
SAPN	South Australia Power Networks
VCs	Verifiable Credentials

## EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform, and operate.

Working across assurance, consulting, law, strategy, tax, and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

© 2023 Ernst & Young, Australia  
All Rights Reserved.

Liability limited by a scheme approved under Professional Standards Legislation.



In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

Ernst & Young is a registered trademark.

Our report may be relied upon by AEMO for the purpose of EDGE Technology and Cybersecurity assessment only pursuant to the terms of our engagement letter dated 8<sup>th</sup> August 2022. We disclaim all responsibility to any other party for any loss or liability that the other party may suffer or incur arising from or relating to or in any way connected with the contents of our report, the provision of our report to the other party or the reliance upon our report by the other party.

[ey.com](https://ey.com)