

System Strength Mitigation Requirement and Access Standards Workshop

ERC0424: Security Framework Enhancements Rule Change Request

20 August 2026

*This presentation represents the preliminary views of the AEMC project team
and should not be taken to represent the views of the Commission.*

Australian Energy Market Commission

AEMC

The AEMC acknowledges and shows respect for the Traditional Custodians of the many different lands across Australia on which we live and work. The AEMC office is located on the land of the Gadigal people of the Eora Nation. We pay respect to all Elders past and present, and the enduring connection of Aboriginal and Torres Strait Islander peoples to Country.

ACKNOWLEDGEMENT OF COUNTRY



Agenda for today's workshop

1	Welcome and housekeeping	10 mins
2	Workshop focus and objectives	5 mins
3	Background to the system strength framework	10 mins
4	Discussion: Issues and range of reform options	55 mins
5	Wrap up and next steps	10 mins

This presentation represents the preliminary views of the AEMC project team and should not be taken to represent the views of the Commission.

CONSENT TO USE OF PERSONAL INFORMATION

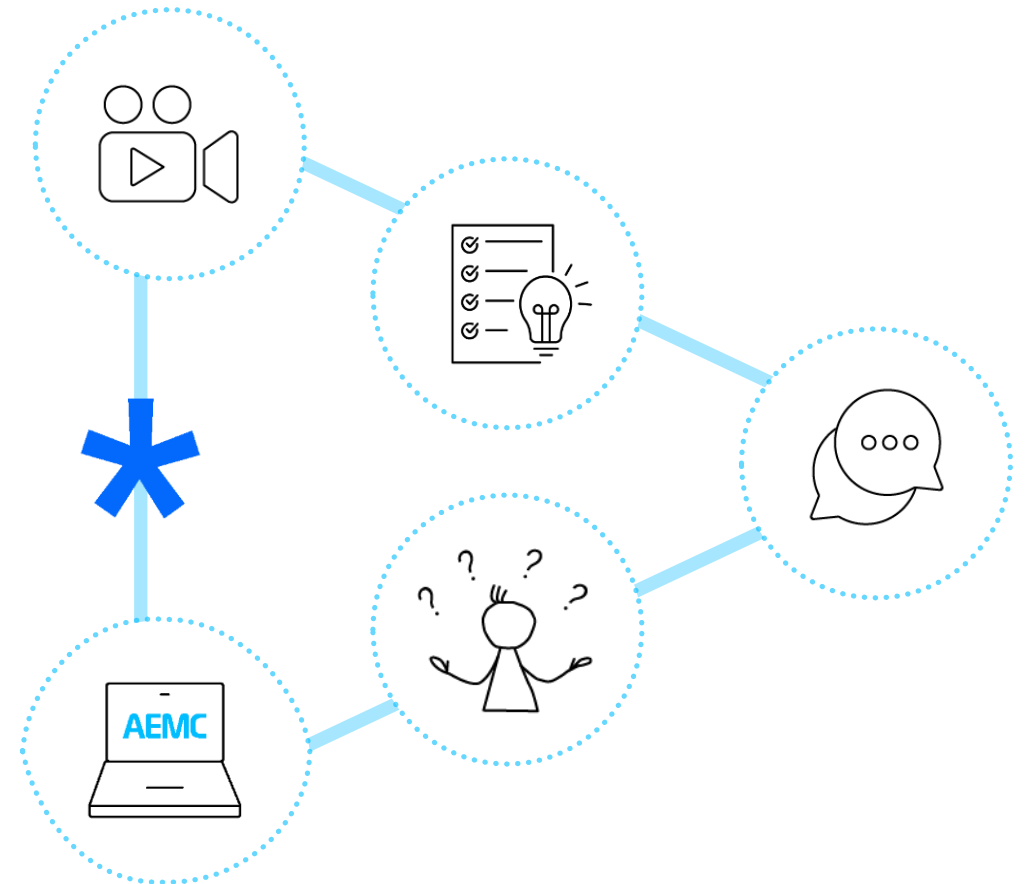


By participating in this workshop, **you give your consent** to our collection, use and disclosure of the personal information you provide to us during this workshop (like your name) for the purpose of completing our consultation and publishing our draft and final determinations and reports on this rule change or review.

This may include **publishing a recording or transcript of the workshop, including your questions or comments.** We will not publish any participant questions or comments that we consider inappropriate, including offensive or defamatory language.

Please read our [privacy policy](#) for more information.

We may publish a transcript or recording of this workshop, which may include your questions or comments



COMPETITION PROTOCOL

KEY PRINCIPLES



The AEMC is committed to complying with all applicable laws, including the ***Competition and Consumer Act 2010*** (CCA), during this forum. Breaching the CCA can lead to serious penalties for individuals involved in any breach (including large financial penalties and imprisonment for key individuals involved). This protocol governs the way in which discussions will proceed at this forum, and each attendee agrees to adhere to this protocol in order to comply with the CCA.

Each attendee must make an independent and unilateral decision about their commercial positions and approach in relation to the matters under discussion in this forum.

Attendees must not discuss, or reach or give effect to any agreement or understanding which relates to:

- **pricing** for the products and/or services that any attendee supplies or will supply, or the terms on which those products and/or services will be supplied (including discounts, rebates, price methodologies etc)
- **targeting (or not targeting) customers** of a particular kind, or in particular areas
- **tender processes** and whether (or how) they will participate
- any decision by attendees:
 - about the purchase or supply of any products or services that other attendees also buy or sell
 - to not engage with persons or the terms upon which they will engage with such persons (i.e. boycotting); or
 - to deny any person's access to any products, services or inputs they require
- **sharing competitively sensitive information** such as non-publicly available pricing or strategic information including details of customers, suppliers (or the terms on which they do business), volumes, future capacity etc
- **breaching confidentiality obligations** that each attendee owes to third parties.

COMPETITION PROTOCOL

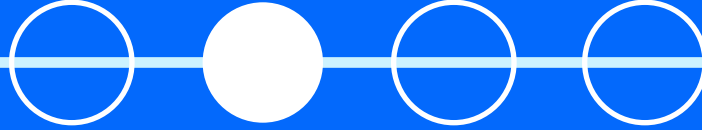
COMMUNICATION AND MEETING GUIDELINES



Attendees must ensure that all communications (including emails and verbal discussions) adhere to the ***Key Principles***.

This forum will be conducted in accordance with the following rules:

- The agenda for this forum does not include anything that could contravene the Key Principles set out in this protocol.
- We will read and minute the below *competition health warning*:
 - Attendees at this forum must not enter into any discussion, activity or conduct that may infringe, on their part or on the part of other attendees, any applicable competition laws. For example, attendees must not discuss, communicate or exchange any commercially sensitive information, including information relating to prices, marketing and advertising strategy, costs and revenues, terms and conditions with third parties, terms of supply or access.
 - Participating in this forum is subject to you having read and understood the protocol including the Key Principles.
- We will keep accurate minutes of the forum, including details of attendees.
- If something comes up during the forum that could risk contravening any competition laws, attendees should:
 - Object immediately and ask for the discussion to be stopped.
 - Ensure the minutes record that the discussion was objected to and stopped.
 - Raise concerns about anything that occurred in the forum with their respective legal counsel immediately afterwards.
- All attendees understand that any competitively sensitive matters must be subject to legal review before any commitment/agreement can be given.
- Any decision about whether, and on what terms, to engage with customers and suppliers is an independent and unilateral decision of each attendee.



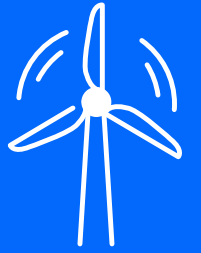
Workshop focus and objectives

Workshop focus

The AEMC is currently considering two rule change requests (now consolidated):

- **Security framework enhancements** (AEMO), submitted in November 2025
- **Clarity and transparency of security frameworks** (AEC/CEC), submitted in January 2026.

The rule change requests raise a wide range of issues and proposed solutions to promote the timely and efficient delivery of system strength services.



Today, we would like to focus on **the system strength mitigation requirement and access standards.**

We will consider:

- issues experienced by those implementing these frameworks since our Efficient management of system strength on the power system rule change in 2021.
- issues that may be experienced in future with the influx of large inverter-based loads, originally canvassed in our Improving the NEM access standards – Package 2 rule changes.

Workshop objectives

We are seeking:

1



Your views on issues with the NER frameworks related to the mitigation requirement and access standards.

2

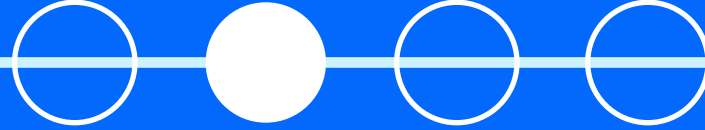


Your views on the benefits, costs, and risks of reform to these parts of the frameworks.

3



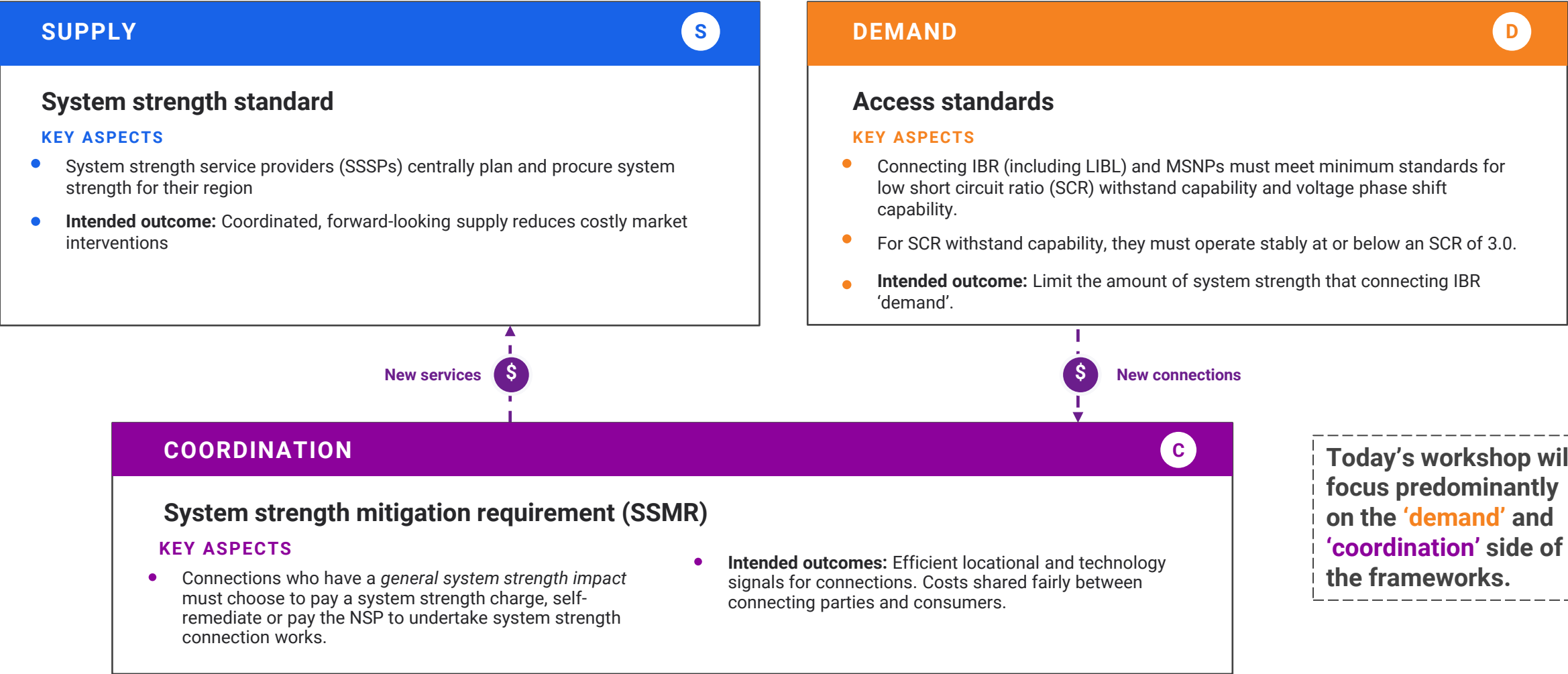
A shared view of the key issues and priority areas for further investigation by the AEMC through this rule change package.



Background to the system strength framework

Three pillars of the NEM system strength framework

Our *Efficient management of system strength on the power system* rule change in 2021 evolved the system strength frameworks in the NEM.



Today's workshop will focus predominantly on the 'demand' and 'coordination' side of the frameworks.

General system strength impact, AFL and SCR withstand

General system strength impact is defined in Chapter 10 of the Rules:

*In relation to a new connection or an alteration to a connected plant, the amount equal to its **adverse system strength impact** as well as any additional amount by which it **reduces the available fault level** at the connection point for the new connection or connected plant, assessed in accordance with the system strength impact assessment guidelines.*

Available fault level (AFL) and **SCR withstand** are key terms used in calculations for the ‘demand’ (access standards) and ‘coordination’ (SSMR) sides of the system strength frameworks under the Rules. They are intended as proxies for the system strength impacts of connecting plant.



AEMO currently uses a modified calculation approach for AFL in the System Strength Impact Assessment Guidelines (SSIAG):

$$\Delta\text{AFL} = - (\text{SCR}_{\text{withstand}} - \alpha) \times \text{Prated}$$

where:*

- $\text{SCR}_{\text{withstand}}$ = is assumed to be 3.0 if there is no model of the 4.6.6 Connection available. If a model is available, the proposed withstand SCR is to be used.
- Prated = rated active power, rated power transfer capability or maximum demand for the system strength connection point.
- α = Stability coefficient which is a constant value of 1.2, reflecting assumed limitations in the network immediately beyond the 4.6.6 Connection.

**From section 3 of AEMO's SSIAG.*

The system strength mitigation requirement (SSMR)

Connection enquiry stage

The relevant network service provider (NSP) undertakes **preliminary impact assessment** to estimate **general system strength impact**, and calculates a plant's system strength locational factor (SSL) and system strength quantity (SSQ) for the system strength charge.

Connection application stage

Connecting IBR with a general system strength impact makes an election under the SSMR

OR

NSP undertakes full impact assessment

1

Self-Remediate or pay for system strength connection works

The connecting party remediates its general system strength impact by either implementing a system strength remediation scheme or entering into an agreement with the NSP to undertake system strength connection works.

2

Pay the System Strength Charge

The connecting party pays the system strength charge to 'use network-provided services'. The charge is intended to reflect an estimate of the forward-looking cost the IBR would impose on the SSSP due to its general system strength impact.

The system strength charge

$$\text{System strength charge (SSC)} = \text{SSUP} \times \text{SSL} \times \text{SSQ}$$

An annual charge for the regulatory year, paid in monthly instalments

SSUP

System strength unit price

- Determined by the SSSP for the relevant system strength node (SSN)
- Set for the five-year system strength charging period
- Changes only by indexation during the charging period

SSL

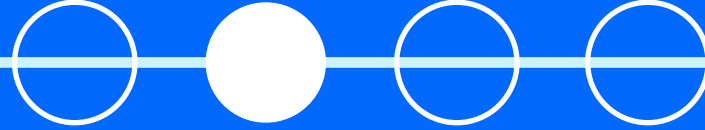
System strength locational factor

- Determined by AEMO in the SSIAG
- Intended to represent the electrical distance from the connection point to the nearest SSN in the region

SSQ

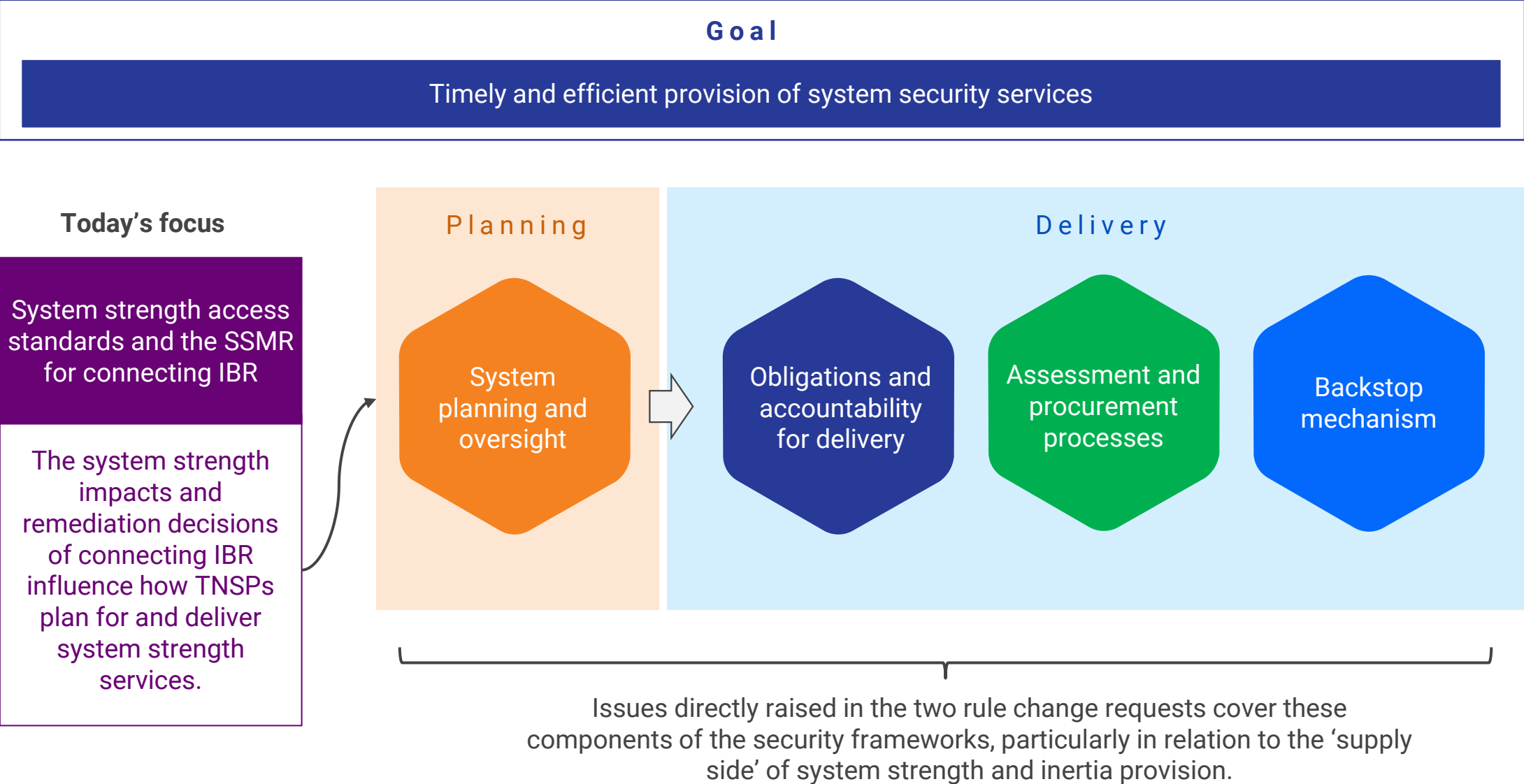
System strength quantity

- Determined by AEMO in the SSIAG and represents the reduction in 'available fault level'
- Based on the connecting party's SCR withstand capability and its rated power (determined using preliminary system strength impact assessment)
- Intended to be broadly equivalent to the 'general system strength impact' the party would otherwise need to remediate



Discussion: Issues and range of reform options

Relation to issues raised in the rule change requests



What we consider success looks like

Reforms through the AEMC's process are progressed based on several NEO criteria. The following criteria have been chosen for the *Security framework enhancements* rule change package:

AEMC assessment criteria	Safety, security and reliability - Future proof, resilient and able to maintain system security through the transition
	Market efficiency - Promotes efficient operation and use of generation facilities, load, networks and other service capability
	Innovation and flexibility - Supports innovation and delivers the benefits of innovation to consumers
	Implementation – Able to be implemented in a timely manner and avoids unreasonable impacts to participant certainty.

... with these assessment criteria in mind, any reforms to improve the demand and coordination side of the frameworks will focus on promoting:

1. **Timely provision of security services**
2. **Efficient investment in security services**
3. **Certainty for market participants**

Issues raised in consultation by stakeholders

Raised through:

- [Security framework enhancements](#)
- [Access standards Package 2](#)
- [CEC system strength report \(2024\)](#)

1. Timing and irrevocable nature of the SSMR nomination ●

Stakeholder issue: Under Rule 5.3.4B(b1), the election to pay the system strength charge must be made before a full impact assessment is undertaken. This means applicants do not have sufficient information on remediation options, costs and system impacts, which may lead to inefficient decisions to self-remediate.

Stakeholder proposed solution: Allow for flexibility in the timing and election to pay the system strength charge. A connecting applicant could confirm or change its election to pay the charge immediately before executing the connection agreement or ahead of the NER 5.3.7(g) letter.

2. Flexibility in system strength remediation in front or behind the connection point ● ●

Stakeholder issue: System strength remediation works are provided by a proponent and must be behind the connection point, while system strength connection works are provided by the NSP and must be in front of the connection point. There may be cost-savings available from allowing for multiple proponents to jointly fund/contract with assets in front of the connection point.

Stakeholder proposed solution: No NER changes to address this issue have been proposed. AEMO is currently reviewing this issue as part of its SSIAG amendments. We note that this issue is related to issue 1 as flexibility in the timing for electing to pay the charge may help inform better decisions on remediation options.

Issues raised in consultation by stakeholders

Raised through:

-  [Security framework enhancements](#)
-  [Access standards Package 2](#)
-  [CEC system strength report \(2024\)](#)

3. Resetting of SSUPs

Stakeholder issue: Unit prices are set for each five-year charging period and cannot be revised down within the charging period to reflect changing system conditions. In addition, project investors view the 5-year charging periods as a material financial risk, having limited ability to hedge against any increases over the lifetime of the project. This may lead to inefficient decisions to self-remediate.

Stakeholder proposed solution: Allow for unit price revisions within and between charging periods, but only downward revisions.

4. Calculation of the SSUP across nodes in a region

Stakeholder issue: Currently, significant variances can occur in the SSUP across nodes in a region, which may create an incentive to locate closer to a particular node, even if this does not align with other factors such as planning requirements, land availability, community acceptance or resource availability. This can distort incentives to utilise system strength services at the relevant node.

Stakeholder proposed solution: Limit variation between lowest and highest SSUPs across nodes in a region.

Issues raised in consultation by stakeholders

Raised through:

- [Security framework enhancements](#)
- [Access standards Package 2](#)
- [CEC system strength report \(2024\)](#)

5. SCR access standards/application of the framework to loads ● ●

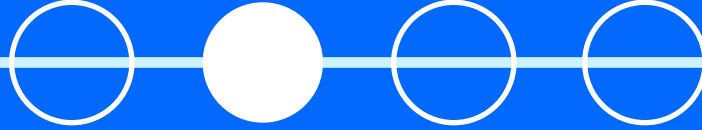
Stakeholder issue: Under the Rules, the withstand SCR access standard is applied in connection and system strength assessments as a proxy for a plant's system strength impacts. The access standard and the preliminary impact assessment methodology were developed primarily for Schedule 5.2 plant (large IBR generators), and cannot be meaningfully applied to loads. This may reduce the effectiveness of the system strength framework.

Stakeholder proposed solution: Reconsider the application of the SCR access standards and/or SSMR to loads, e.g. by reducing the onerousness of the SCR withstand access standard, changing the preliminary impact assessment methodology, and/or changing whether loads remediate general system strength impacts and are liable to pay the charge, or just adverse system strength impacts.

Discussion: Issues raised in consultation

- 1. Timing and irrevocable nature of the SSMR nomination**
- 2. Flexibility in system strength remediation in front or behind the connection point**
- 3. Resetting of SSUPs**
- 4. Calculation of the SSUP across nodes in a region**
- 5. SCR access standards/application of the framework to loads**

Questions for discussion: What is your view of the issues raised? Are there alternative solutions that should be considered? What are the costs, risks and benefits of reform?



Wrap up and next steps

This engagement will inform our draft determination

Through the [Security framework enhancements](#) rule change package, we have the opportunity to consider the core issues raised in [AEMO's Security framework enhancements](#) rule change request and the [AEC & CEC's Clarity and transparency of security frameworks](#) rule change request, as well as issues identified during the consultation process.

Submissions to the [Security framework enhancements consultation paper](#) provided us with valuable information to inform our thinking on the core issues, as well as raising some additional issues that fit within the scope of the rule change package.

We have used stakeholder workshops to improve our understanding of three additional issues:



1. **Retuning:** this workshop, held on **16 July 2026**, sought stakeholder views on the potential role of plant retuning to address system strength issues. Workshop materials are available [here](#) and a summary is available [here](#).
2. **System strength procurement:** this workshop, held on **22 July 2026** sought stakeholder views on opportunities to improve standardisation and transparency in the system strength procurement process. Workshop materials are available [here](#) and a summary is available [here](#).
3. **System strength access standards and mitigation requirement:** in this workshop, held today, **20 August 2026**, we have sought stakeholder views on the system strength access standards and the SSMR for connecting IBR (including issues raised as part of the [Improving the NEM access standards- package 2](#) rule change process). Materials from this workshop will also be published on our project page [here](#).

We are considering potential reforms to the framework as a holistic package, with solutions proportional to the issues.

Next steps for *Security framework enhancements* rule change requests

