Industry pain points and benefits survey results

Strategic & Foundational initiatives:
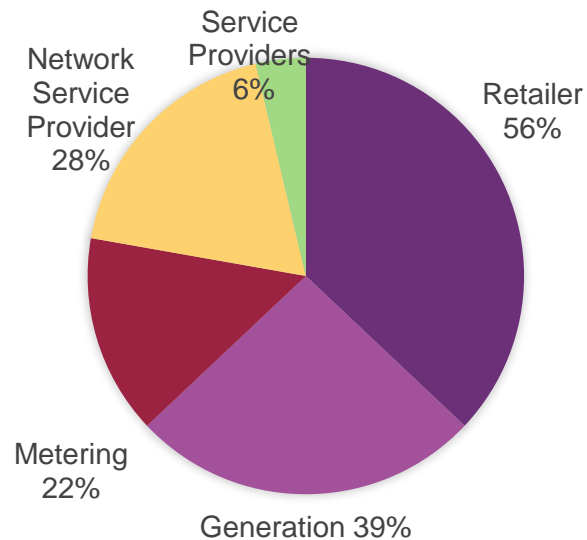- Identify Access Management (IDAM)
- Portal Consolidation (PC)
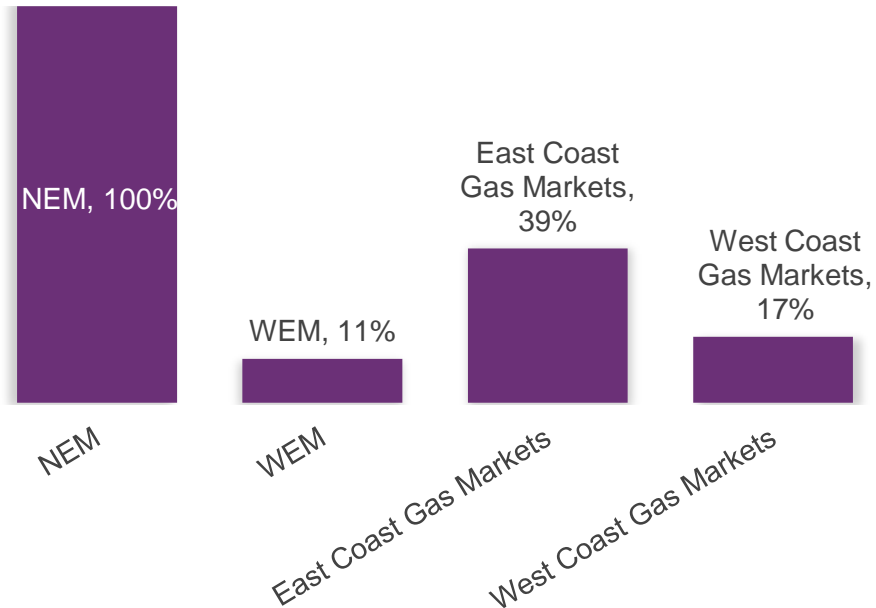
AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Introduction

- This is an artifact from AEMO's [consultation with industry](#) on a target state, transition strategy and business case for Foundational and Strategic initiatives IDAM, IDX and Portal Consolidation.

- On 17 April 2023, the Foundational and Strategic initiatives Focus Group gathered for a Discovery workshop for IDAM and Portal Consolidation, after which AEMO sought to validate, update and prioritise inputs captured through an online survey.

- AEMO received 18 survey responses out of the 36 organisations that have nominated representatives for the consultation. The respondents contributed a broad range of perspectives from the roles and markets in which they operate.

Respondents' role in the Energy Market

Service Providers 6%
Network Service Provider 28%
Retailer 56%
Metering 22%
Generation 39%

Jurisdictional Market in which the respondents operate

NEM, 100%
WEM, 11%
East Coast Gas Markets, 39%
West Coast Gas Markets, 17%

NEM   WEM   East Coast Gas Markets   West Coast Gas Markets

IDAM Summary
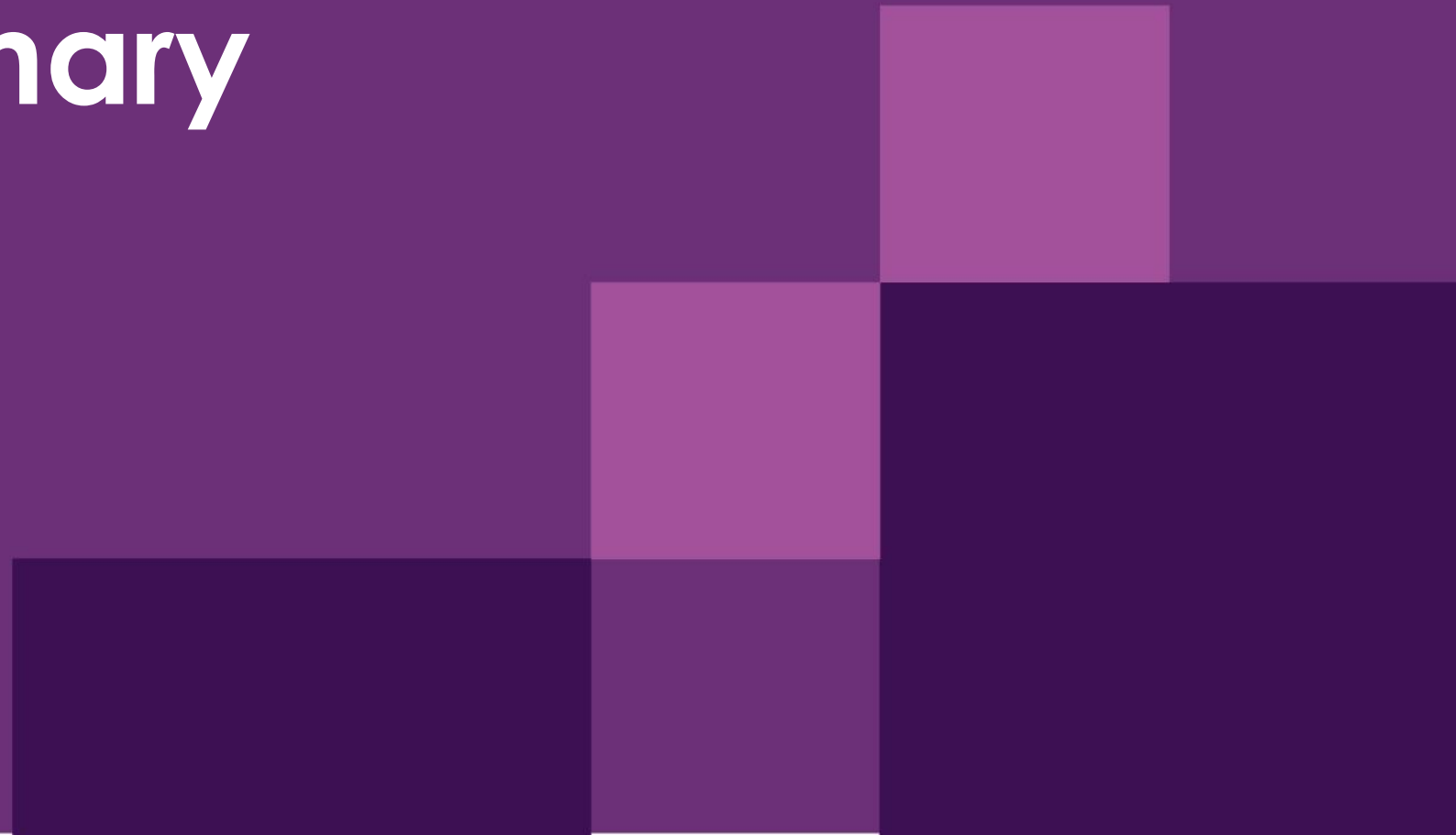
Identity and Access Management Scope

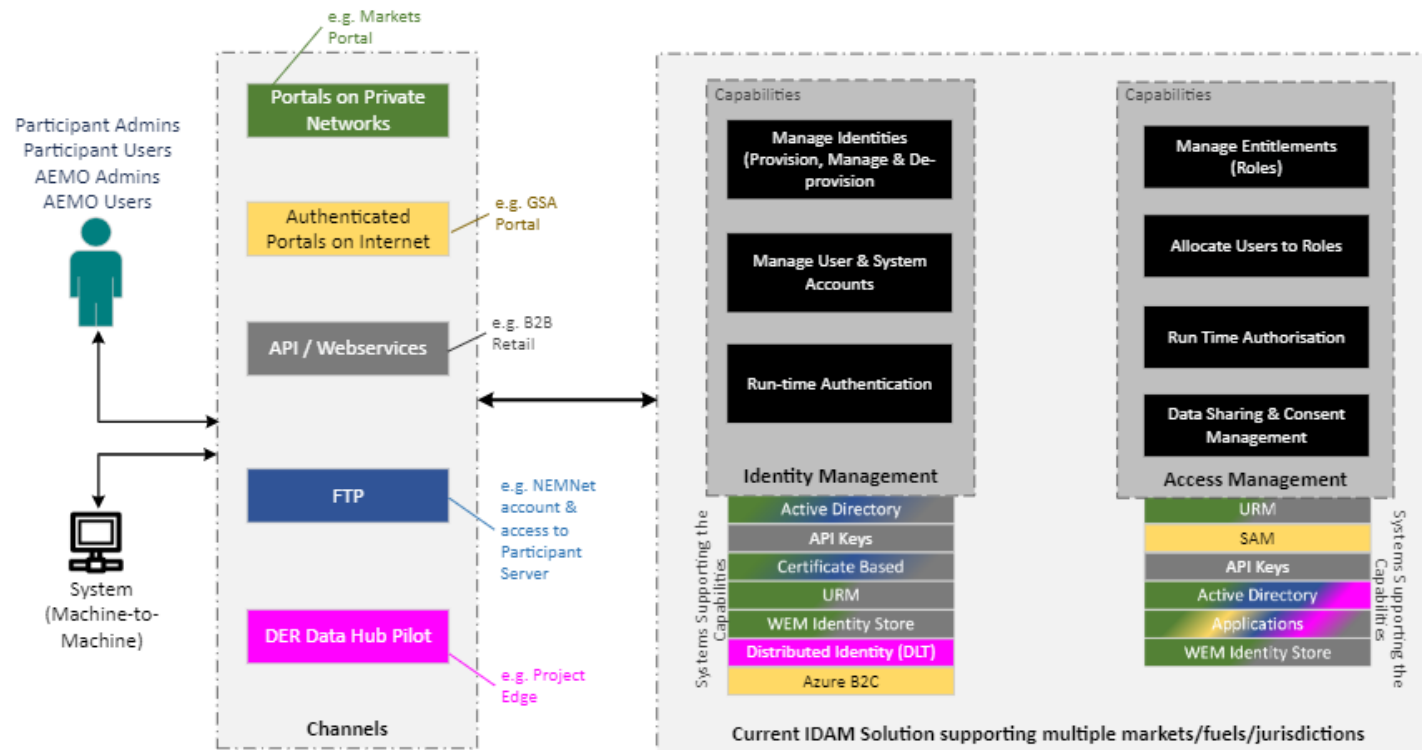*Identity and Access Management: A unified mechanism to authenticate and authorise external identity when accessing AEMO services, consolidating and improving overall cyber security controls.*

Problem Statement:

AEMO's Identity and Access Management (IDAM) services are disparate, requiring users to retain multiple sets of credentials in order to access AEMO business services. The legacy IDAM services do not implement best practices in cyber security controls (e.g., multifactor authentication) and are insufficient to meet new industry obligations introduced under the SOCI Act.

IDAM Current State Context Diagram:

Participant Admins
Participant Users
AEMO Admins
AEMO Users

System (Machine-to-Machine)

Channels

- Portals on Private Networks — e.g. Markets Portal
- Authenticated Portals on Internet — e.g. GSA Portal
- API / Webservices — e.g. B2B Retail
- FTP — e.g. NEMNet account & access to Participant Server
- DER Data Hub Pilot — e.g. Project Edge

Capabilities

Identity Management
- Manage Identities (Provision, Manage & De-provision)
- Manage User & System Accounts
- Run-time Authentication

Systems Supporting the Capabilities:
- Active Directory
- API Keys
- Certificate Based
- URM
- WEM Identity Store
- Distributed Identity (DLT)
- Azure B2C

Capabilities

Access Management
- Manage Entitlements (Roles)
- Allocate Users to Roles
- Run Time Authorisation
- Data Sharing & Consent Management

Systems Supporting the Capabilities:
- URM
- SAM
- API Keys
- Active Directory
- Applications
- WEM Identity Store

Current IDAM Solution supporting multiple markets/fuels/jurisdictions

⚠ Note: Channels & IDAM Stores illustrated in this slide are indicative only and not the finite list

Following areas will be explored during the IDAM feasibility phase.

In Scope	Out of Scope
✓ NEM, WEM and Gas involving AEMO external interactions	× Network layer security

✓ External Identities including:
  - Registered Participants
  - Non-registered Participants
  - Potential Participants
  - Service Providers
	× Control systems communications / interactions

✓ External System Accounts Interactions via all supported channels (current & future)	× Direct device communications /interactions

Key challenges for participants

Below is a summary of the key pain points from Business and Technical focus group discussions, classified into themes according to the challenges they pose to the legacy IDAM services.

Participant Administrator (PA) experience

- Perform **repetitive tasks** e.g., creation of roles, unable to inherit the roles from an existing set
- Inability to set **expiration dates for user access** to automatically revoke access upon expiration
- Lack of **reporting capabilities** to conduct **periodic assessments**
- Inability to **automate user offboarding**, resulting in increased risk of unauthorised access and security risks
- Need to extend PA concept to other markets.
- Lack of **role catalogue** with pre-defined roles.

User experience

- **Multiple credentials** required to access different AEMO systems
- **Lack of integration between the Participant's organisation and AEMO's identity store (Federation)**
- Inadequate **self-service capabilities** e.g. Password reset, consent management, etc
- Inadequate training material, support, and documentation to support the complex user management landscape
- Lack of **designation of account to a specific AEMO environment** such as pre-production or production

Security & compliance

- Lack of the visibility of the **audit trail to monitor significant identity and access management services**
- Need for **Multi-Factor Authentication (MFA)** to **enhance security** by requiring multiple forms of authentication
- Lack of ability **to identify inactive, unused, and suspicious accounts to maintain security**

Management of Service Accounts

- **Multiple user credentials** are required to access AEMO systems
- **Multiple access controls** to access AEMO systems
- **Multiple AuthN patterns** e.g., API keys, Basic Auth and OAuth
- Inadequate capabilities for **managing password changes** e.g., the use of shared credentials across multiple applications necessitating concurrent change
- Lack of **designation of account to a specific AEMO environment** such as pre-production or production

Executive summary

The issue with **managing multiple credentials** for accessing different AEMO systems was highlighted in the survey emphasising the need for a unified IDAM solution

Respondents **supported the concept of Identity Federation** with 66% stating that their organisation can implement federation within 2 years

78% respondents felt their Participant Admins would benefit from a **pre-defined role catalog**

Respondents highlighted that the **ability identify inactive accounts** and the **ability to monitor, identify and address suspicious or unusual activity** is a critical and necessary requirement to maintain security

The **cybersecurity risk** has been identified as one of the drivers of the IDAM initiative with participants highlighting the **need for modern authentication mechanisms** like OAuth and token-based authentication as well as enhanced security controls like **Multi-factor authentication**

Inadequate capabilities for managing **password changes for service accounts** is a key challenge.

The results of the survey clearly demonstrate **the need for the Data Sharing concept to be discussed** in upcoming consultations in order to clarify the concept. This concept will be discussed in the upcoming Technical and Business Focus Target state consultation.

The majority of respondents voted for **NEM** (particularly NEM Wholesale) to be **transitioned firs**t and preferred a phased approach to transition.
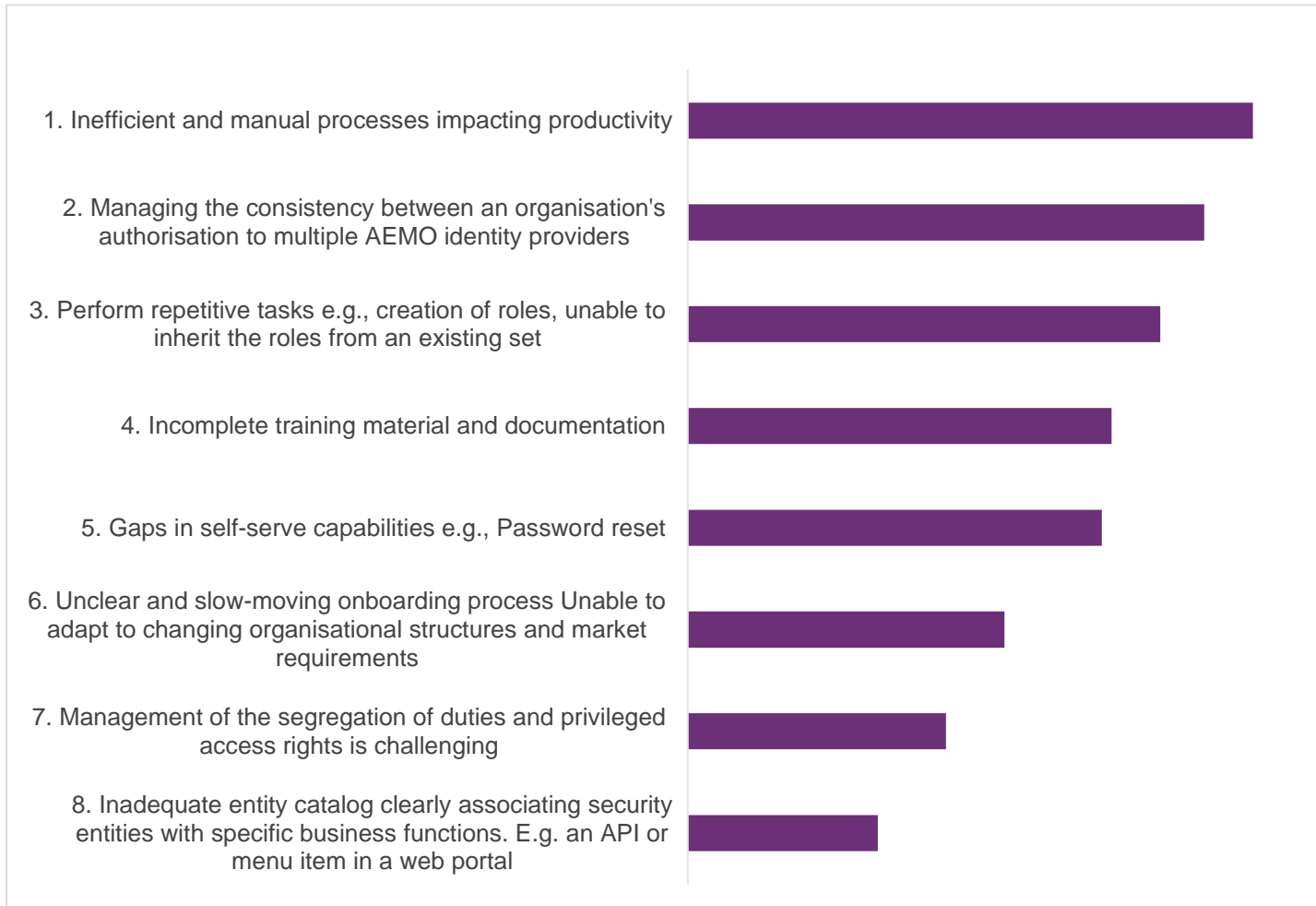
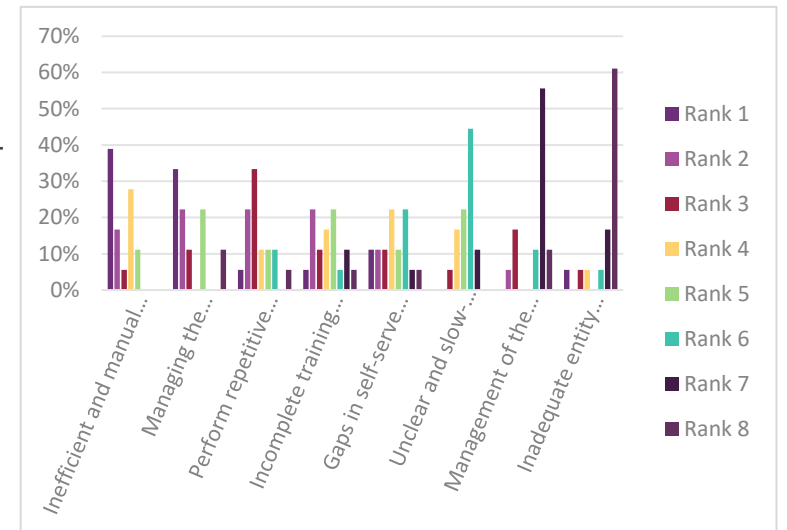# IDAM Participant Pain Points and Priorities

- IDAM pain points
- User Experience
- Management of Service Account
- Reporting, Auditing, Governance and Compliance
- Target State Capabilities

IDAM pain points Ranking

Normalised ranking of key pain points based on the survey response

1. Inefficient and manual processes impacting productivity

2. Managing the consistency between an organisation's authorisation to multiple AEMO identity providers

3. Perform repetitive tasks e.g., creation of roles, unable to inherit the roles from an existing set

4. Incomplete training material and documentation

5. Gaps in self-serve capabilities e.g., Password reset

6. Unclear and slow-moving onboarding process Unable to adapt to changing organisational structures and market requirements

7. Management of the segregation of duties and privileged access rights is challenging

8. Inadequate entity catalog clearly associating security entities with specific business functions. E.g. an API or menu item in a web portal
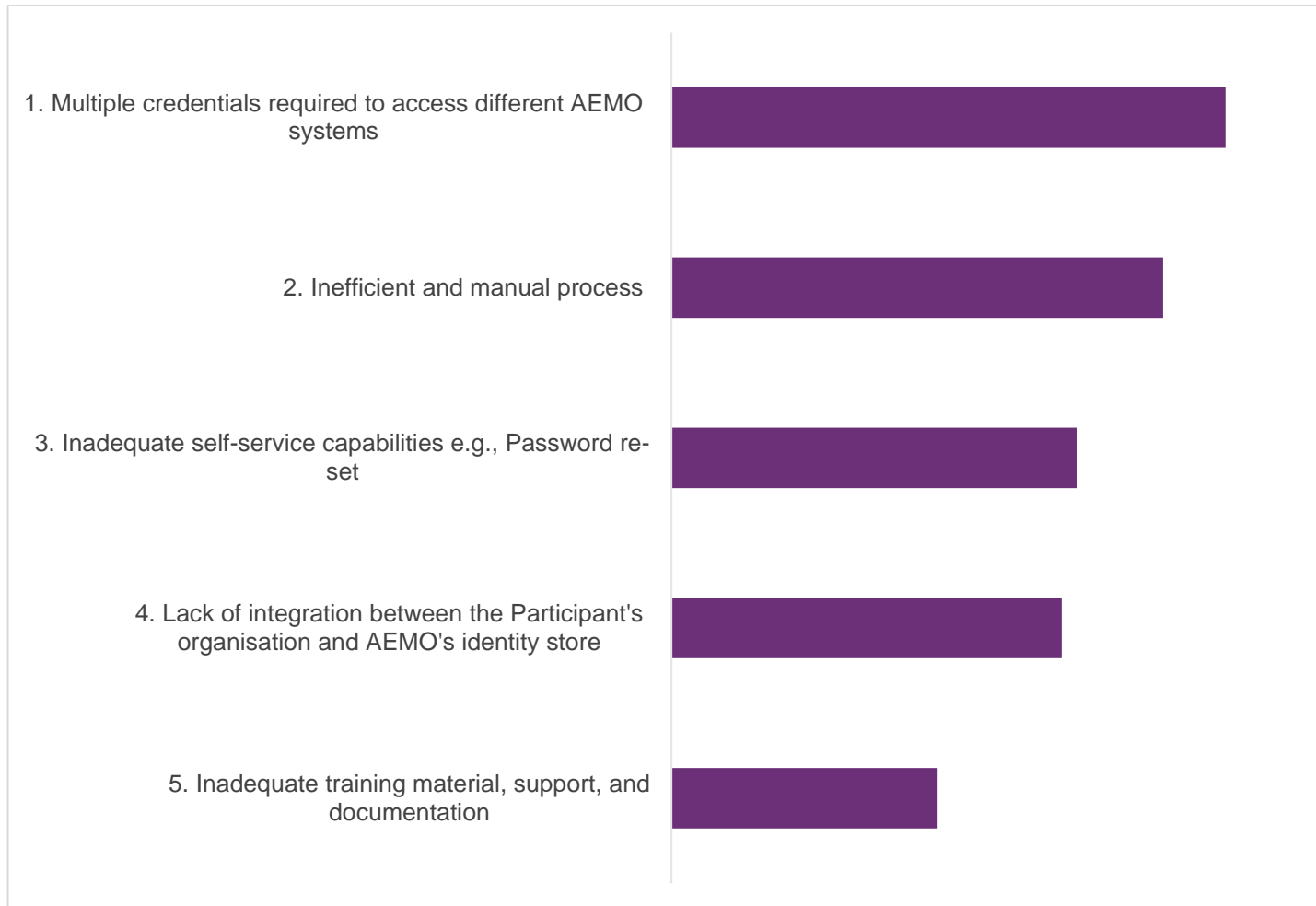
Survey results representing the ranking of the key pain points that contribute to a negative user experience.

User Experience Pain points Ranking

Normalised ranking of key pain points based on the survey response

1. Multiple credentials required to access different AEMO systems

2. Inefficient and manual process

3. Inadequate self-service capabilities e.g., Password re-set

4. Lack of integration between the Participant's organisation and AEMO's identity store

5. Inadequate training material, support, and documentation

Survey results representing the ranking of the key pain points that contribute to a negative user experience.

Legend:
- Rank 1
- Rank 2
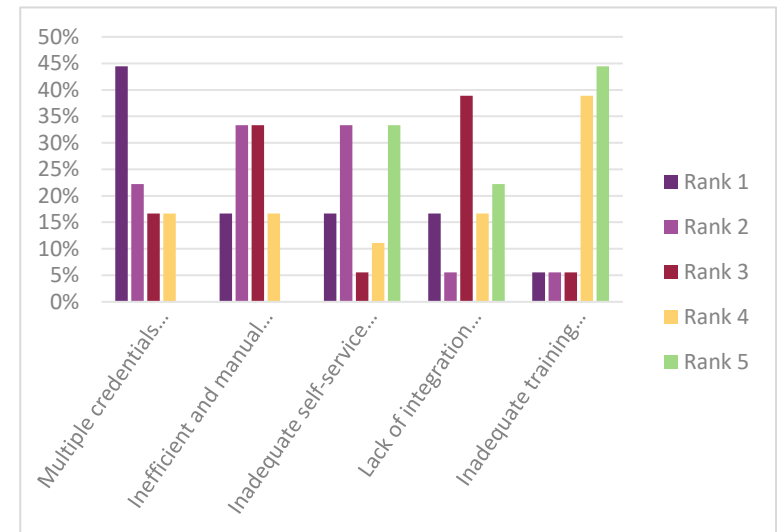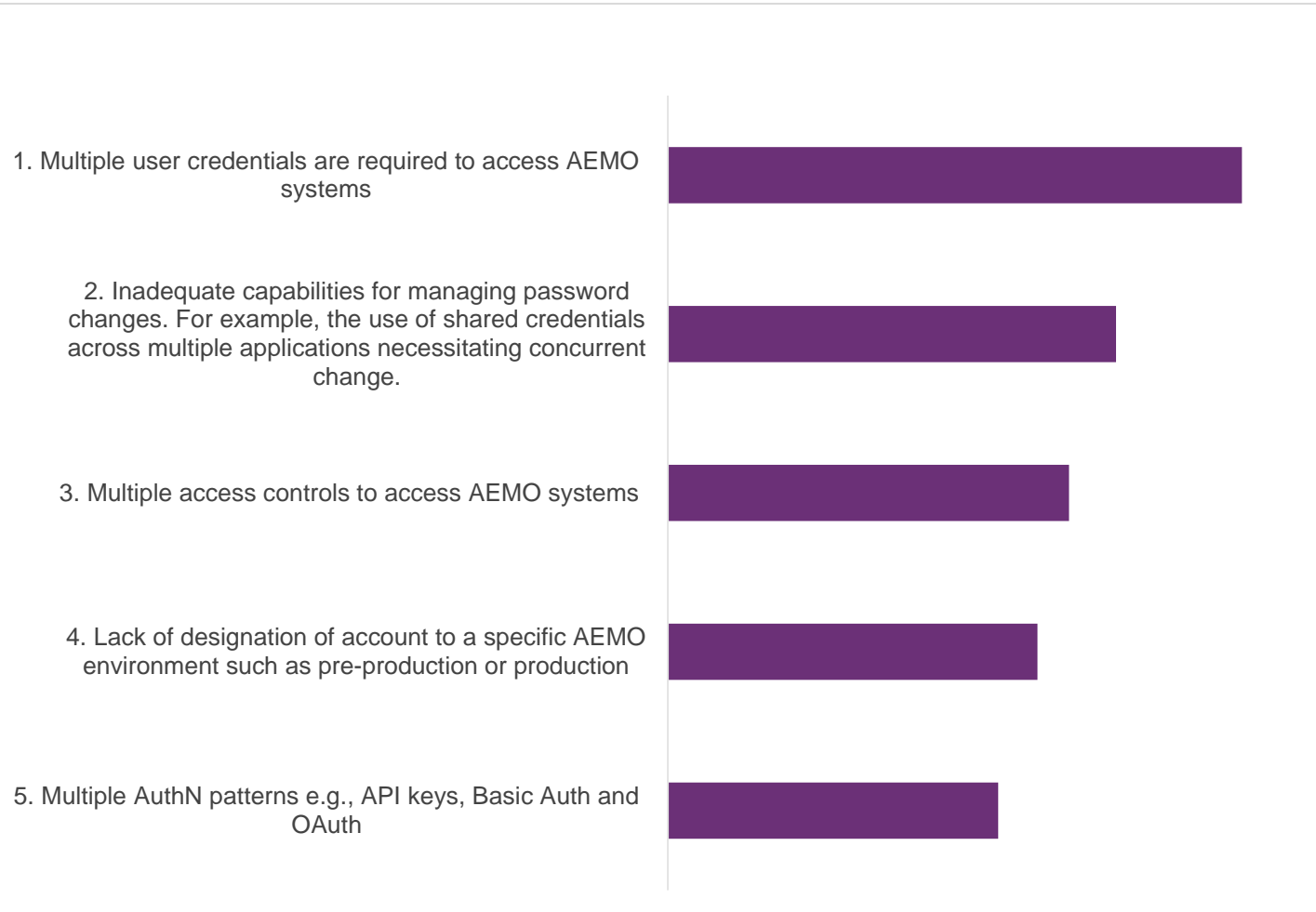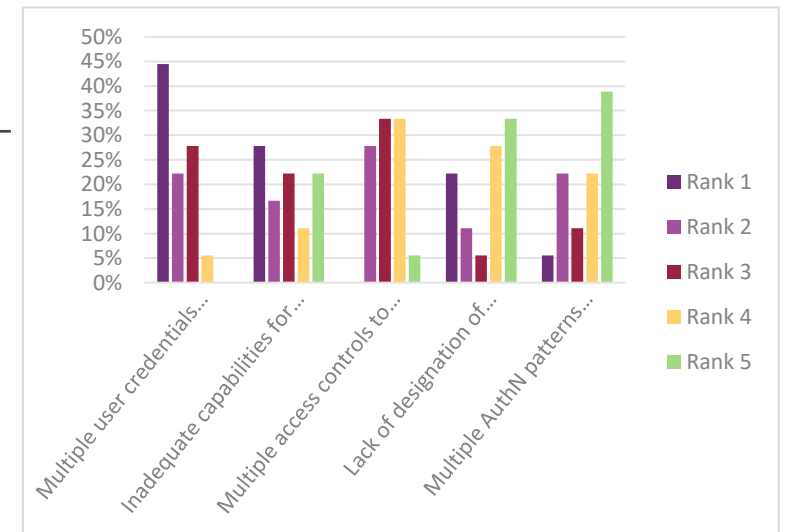- Rank 3
- Rank 4
- Rank 5

Chart categories: Multiple credentials..., Inefficient and manual..., Inadequate self-service..., Lack of integration..., Inadequate training...

Management of Service Accounts

Normalised ranking of key pain points based on the survey response

1. Multiple user credentials are required to access AEMO systems

2. Inadequate capabilities for managing password changes. For example, the use of shared credentials across multiple applications necessitating concurrent change.

3. Multiple access controls to access AEMO systems

4. Lack of designation of account to a specific AEMO environment such as pre-production or production

5. Multiple AuthN patterns e.g., API keys, Basic Auth and OAuth

Survey results representing the ranking of the current key challenges in the management of service accounts.

Legend:
- Rank 1
- Rank 2
- Rank 3
- Rank 4
- Rank 5

X-axis categories:
- Multiple user credentials...
- Inadequate capabilities for ...
- Multiple access controls to ...
- Lack of designation of ...
- Multiple AuthN patterns...

Reporting, Auditing, Governance & Compliance

Normalised ranking of key pain points based on the survey response

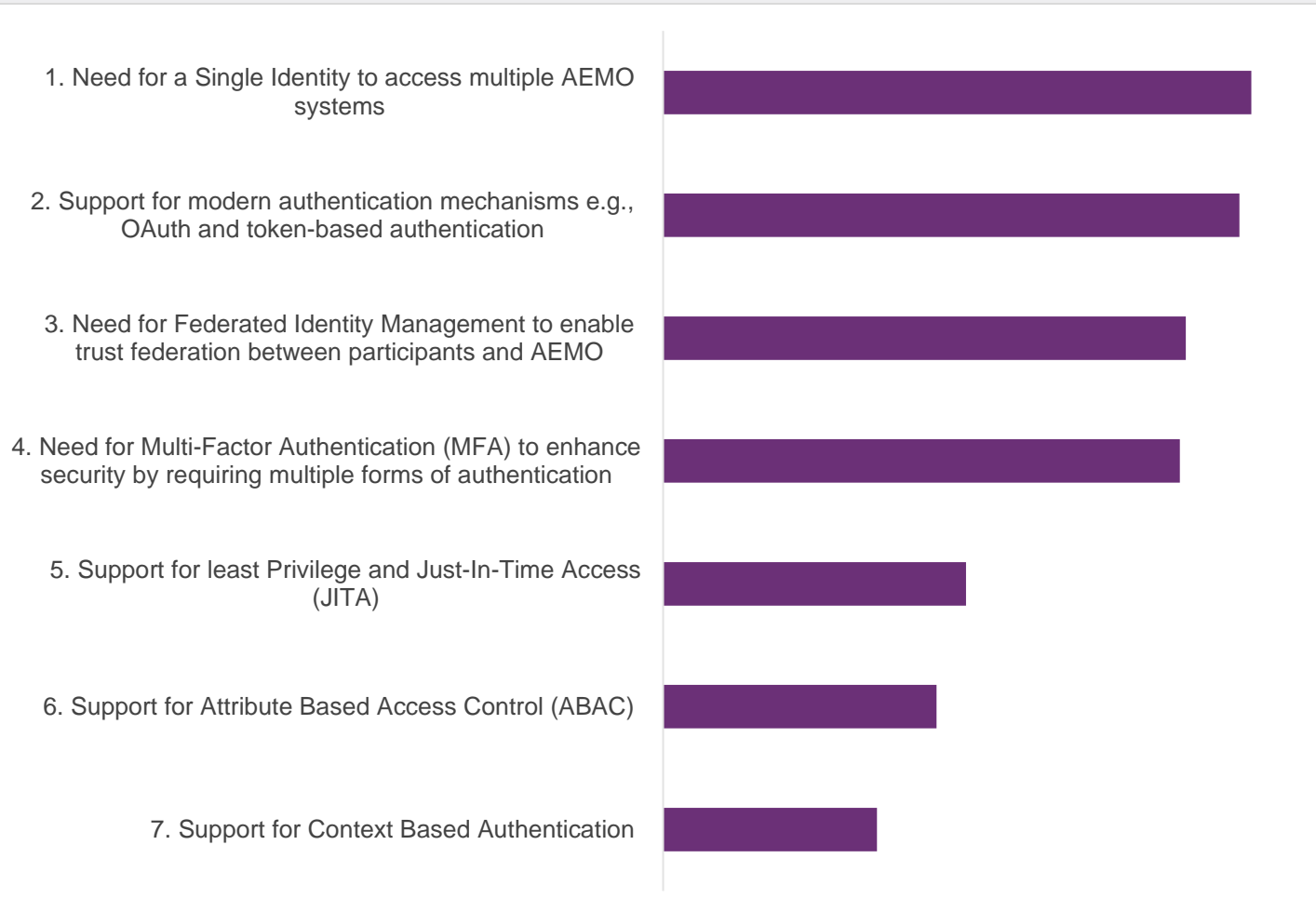1. Lack of ability to Identify inactive, unused, and suspicious accounts

2. Inability to automate user offboarding, resulting in unauthorised access and security risks

3. Inability to set expiration dates for user access to automatically revoke access upon expiration

4. Lack of reporting capabilities to conduct periodic assessments

5. Inefficient and manual process

6. Lack of the visibility of the audit trail to monitor significant identity and access management services

Survey results representing the ranking of the current key challenges in Governance and Compliance

Legend:
- Rank 1
- Rank 2
- Rank 3
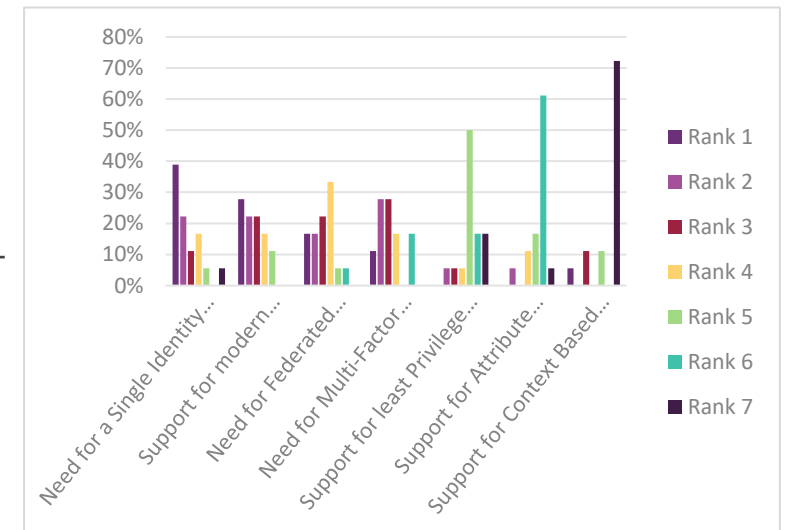- Rank 4
- Rank 5
- Rank 6
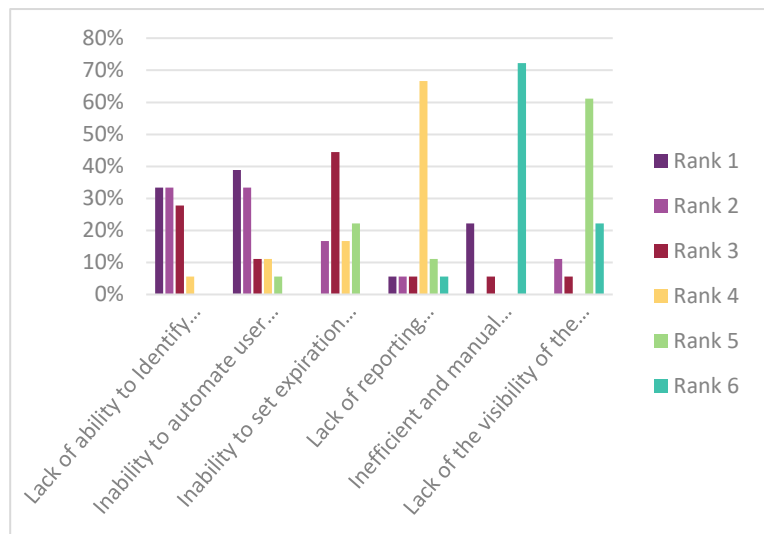
What Target State Capabilities needs to be addressed first

Normalised ranking of capabilities desired in the target state based on the survey results

1. Need for a Single Identity to access multiple AEMO systems

2. Support for modern authentication mechanisms e.g., OAuth and token-based authentication

3. Need for Federated Identity Management to enable trust federation between participants and AEMO

4. Need for Multi-Factor Authentication (MFA) to enhance security by requiring multiple forms of authentication

5. Support for least Privilege and Just-In-Time Access (JITA)

6. Support for Attribute Based Access Control (ABAC)

7. Support for Context Based Authentication

Survey results representing the ranking of the capabilities desired in the target state
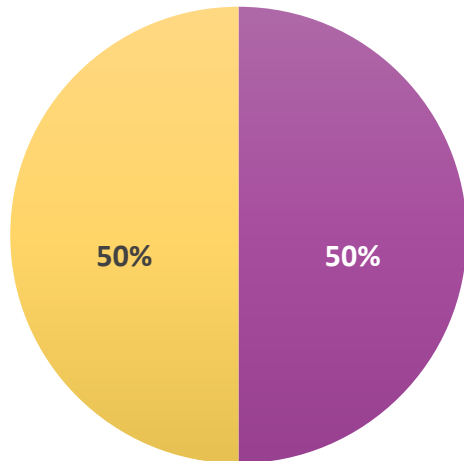

12

Survey Polls

Participant Admin Experience

Q. Do you see a benefit in expanding the concept of Participant Administrator to other markets such as Gas Retail & Wholesale markets?
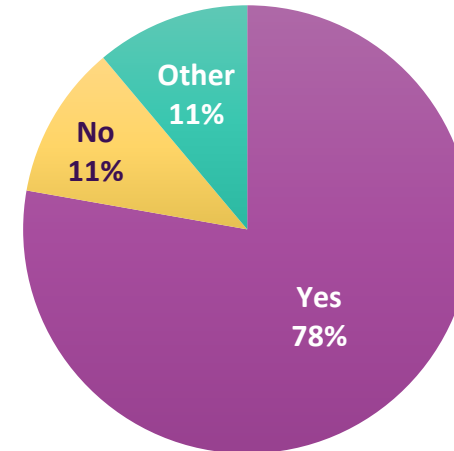
Concept of PA to other Markets

- Yes
- NA/Unspecified

Majority of respondents voted NA/Unspecified currently operate only in a NEM Markets

Q. Would a **pre-defined role catalogue** improve efficiency in establishing role definitions?
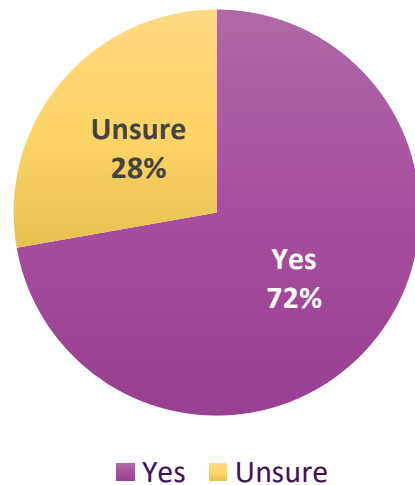
Benefit of a pre-defined role catalog

- Yes
- No
- Other

*Majority of respondents supported a concept of pre-defined role catalogue and voted **YES***

Identity Federation

Q. If AEMO's supporting **Identity federation** would your organisation be interested in using your enterprise identity to access AEMO system?
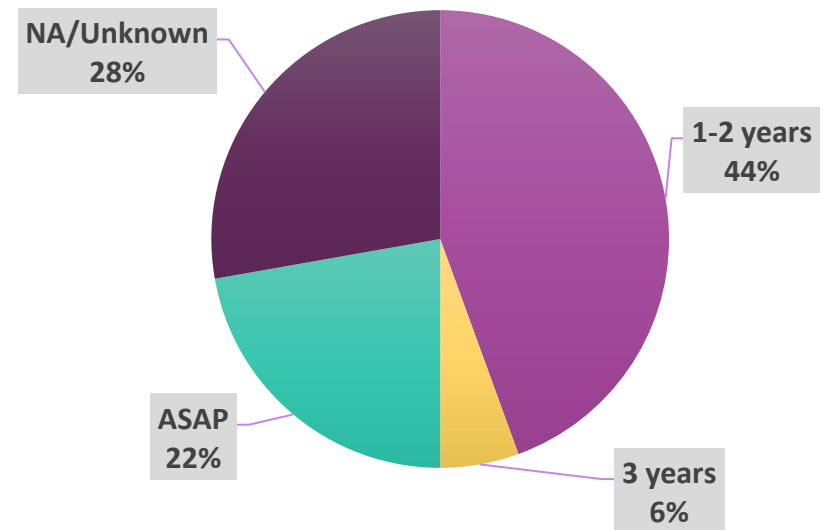
Support for Identity Federation

Yes
72%

Unsure
28%

■ Yes ■ Unsure

*Respondents **supported** the concept of Identity Federation*

Q. How long will it take for your organisation to implement identity federation? (ASAP, 1-2years, 3-5 years)

Timeframe to Implement Federation

NA/Unknown
28%

1-2 years
44%

ASAP
22%

3 years
6%

*12 respondents voted **ASAP-2years**
5 respondents were unsure or the concept was not applicable for them
1 respondent voted 3years*

Data Sharing Capability

Q. Should data sharing capabilities be extended to other markets beyond NEM wholesale?

- Yes

- No

- Unsure and further investigation required

YES ✓ 17%   NO ✗ 6%   Unsure 78%

Q. Should data sharing capabilities be extended to offer asset level granularity, e.g., DUID level, to support power purchase agreements?
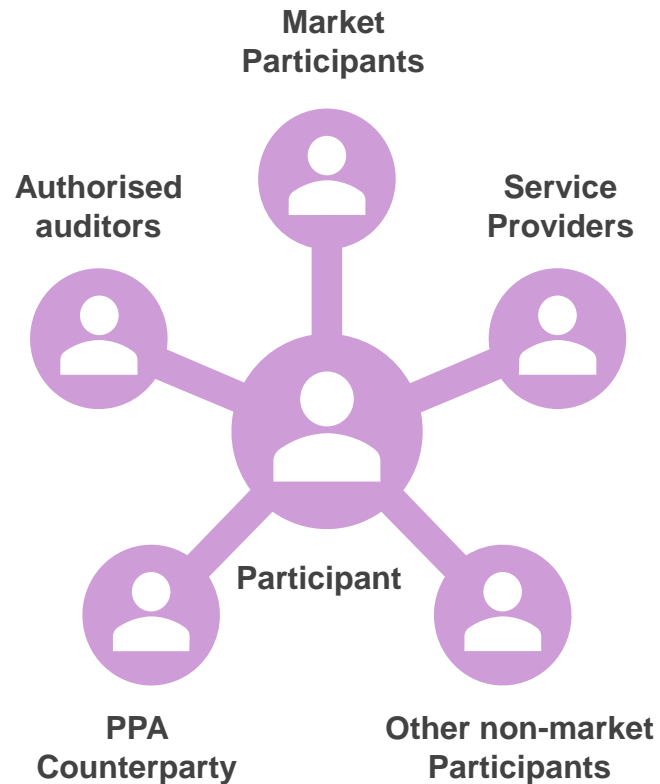
- Yes

- No

- Unsure and Not applicable

YES ✓ 39%   NO ✗ 6%   Unsure 56%

The results of the survey clearly demonstrate the need for the Data Sharing concept to be discussed in upcoming consultations in order to clarify the concept. This concept will be discussed in the upcoming Technical and Business Focus Target state consultation.

Current Data Sharing Scenarios

Who do Participants share their confidential data with?

- Market Participants
- Authorised auditors
- Service Providers
- PPA Counterparty
- Other non-market Participants
- Participant

Participants shared their current scenarios

I Say:
Share Gas Market Data in markets like STTM, DWGM

I Say:
Provide authorised auditors access to data sets for audit of sales for green certificate information
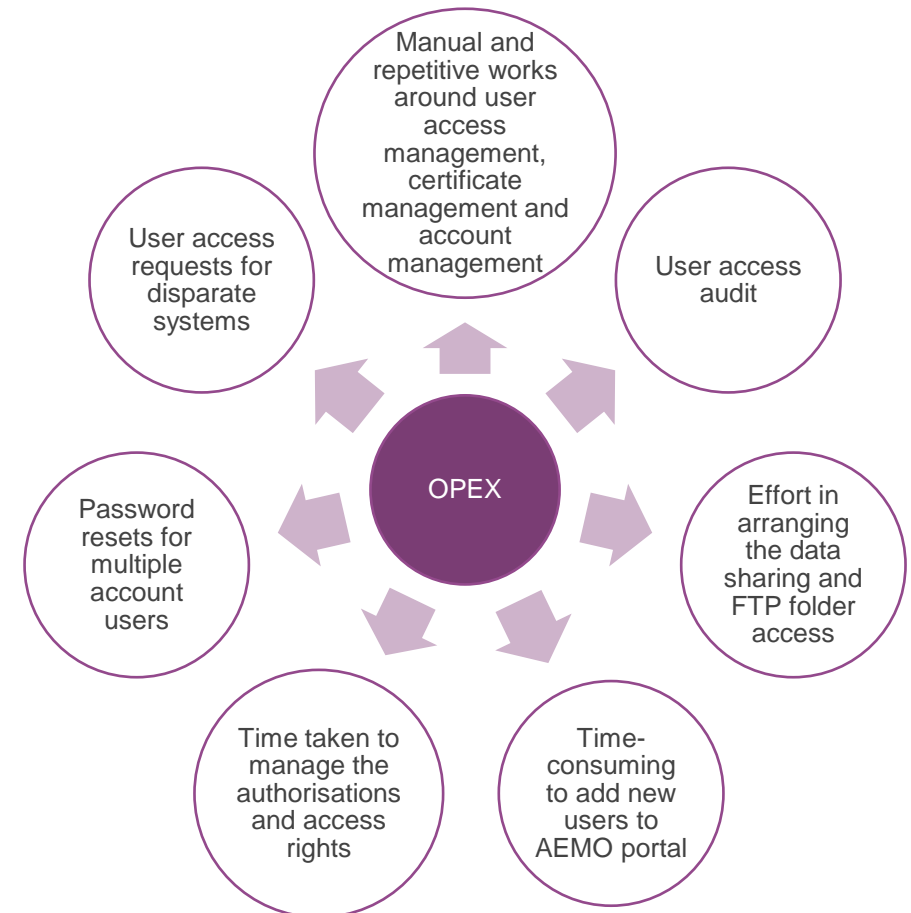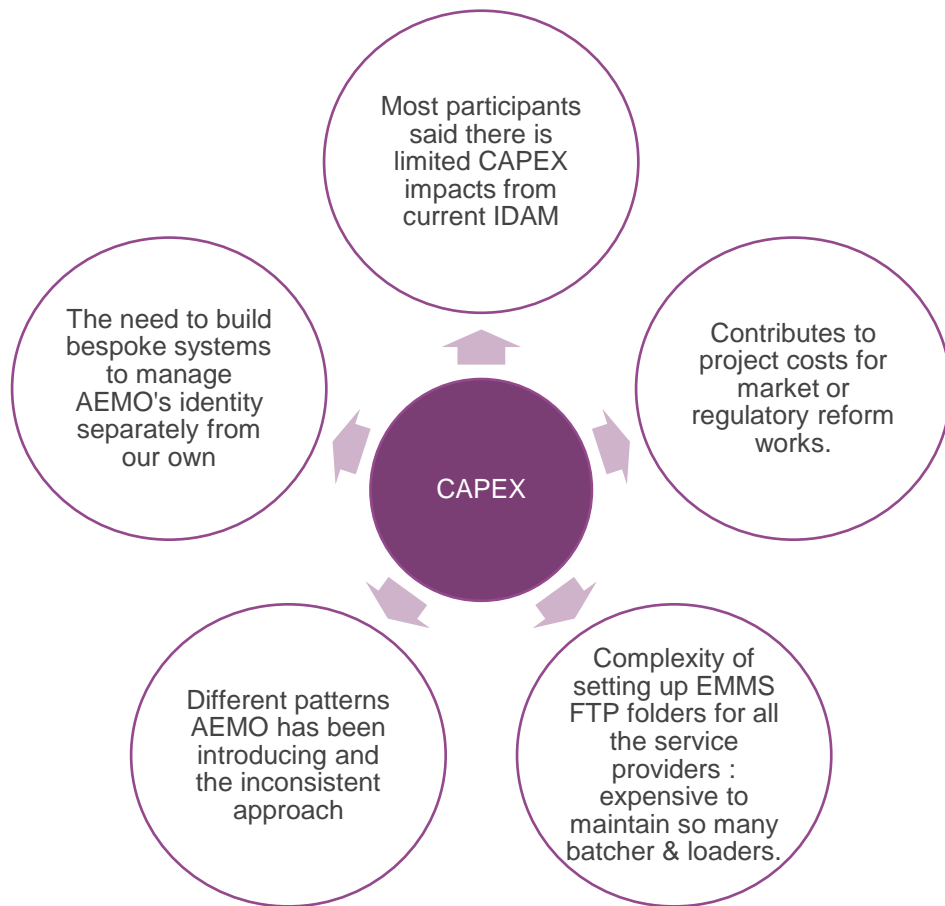
I Say:
For PPAs where the bidding of plant is shared, the ability to provide restricted access to the counterparty

I Say:
Facilitation of meter data sharing i.e. bilateral meter data agreements.

I Say:
The ability to share selected relevant information securely with authorized non-participants

Factors contributing to participant costs

CAPEX

- Most participants said there is limited CAPEX impacts from current IDAM
- Contributes to project costs for market or regulatory reform works.
- Complexity of setting up EMMS FTP folders for all the service providers : expensive to maintain so many batcher & loaders.
- Different patterns AEMO has been introducing and the inconsistent approach
- The need to build bespoke systems to manage AEMO's identity separately from our own

OPEX

- Manual and repetitive works around user access management, certificate management and account management
- User access audit
- Effort in arranging the data sharing and FTP folder access
- Time-consuming to add new users to AEMO portal
- Time taken to manage the authorisations and access rights
- Password resets for multiple account users
- User access requests for disparate systems

Transition Timeframe

What is an appropriate timeframe for the transition period?

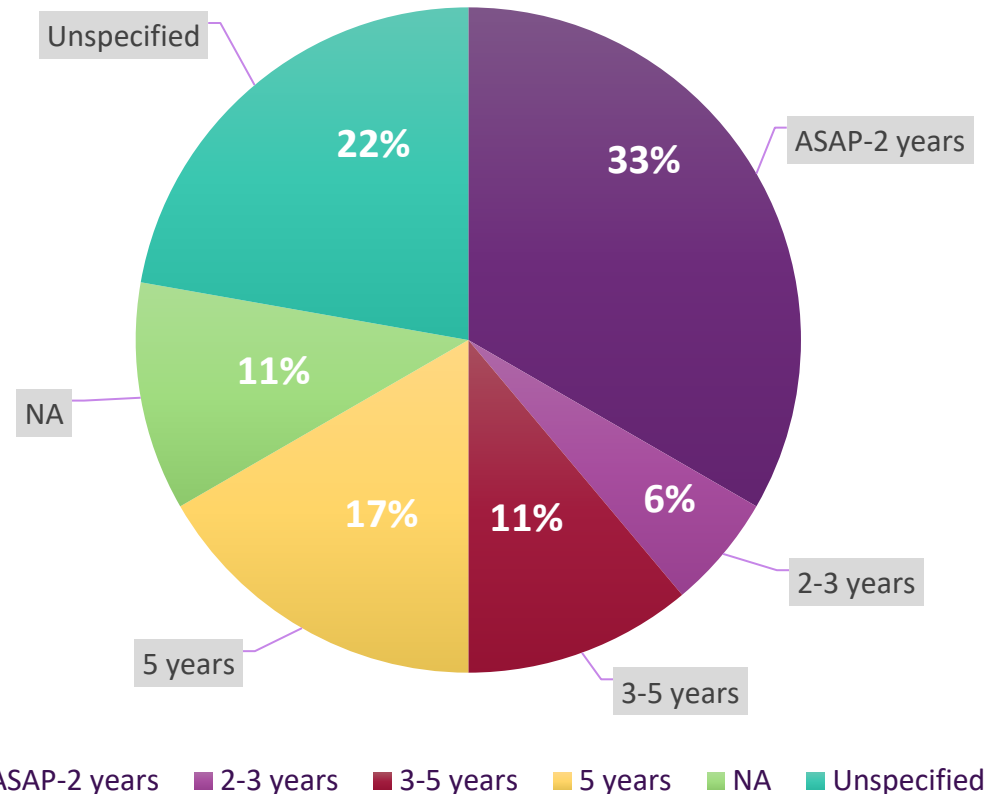**I Say:**
An approach that will be utilised across all AEMO markets

I Say:
Getting it right in one market first before transitioning the other markets would provide benefits.

I Say:
Clear definition of sunset period

I Say:
Backward compatibility should be considered

I Say:
Encourage flexibility to enable organizations to manage that transition

Transition Timeframe

Pie chart "Transition Timeframe":
- 33% ASAP-2 years
- 6% 2-3 years
- 11% 3-5 years
- 17% 5 years
- 11% NA
- 22% Unspecified

Legend: ■ ASAP-2 years ■ 2-3 years ■ 3-5 years ■ 5 years ■ NA ■ Unspecified

What market must be transitioned first?

Market to transition first

NA/Unspecified 28%

NEM 50%

Least impact first 6%

Gas and NEM Wholesale 17%

■ NEM ■ Gas and NEM Wholesale ■ Least impact first ■ NA/Unspecified
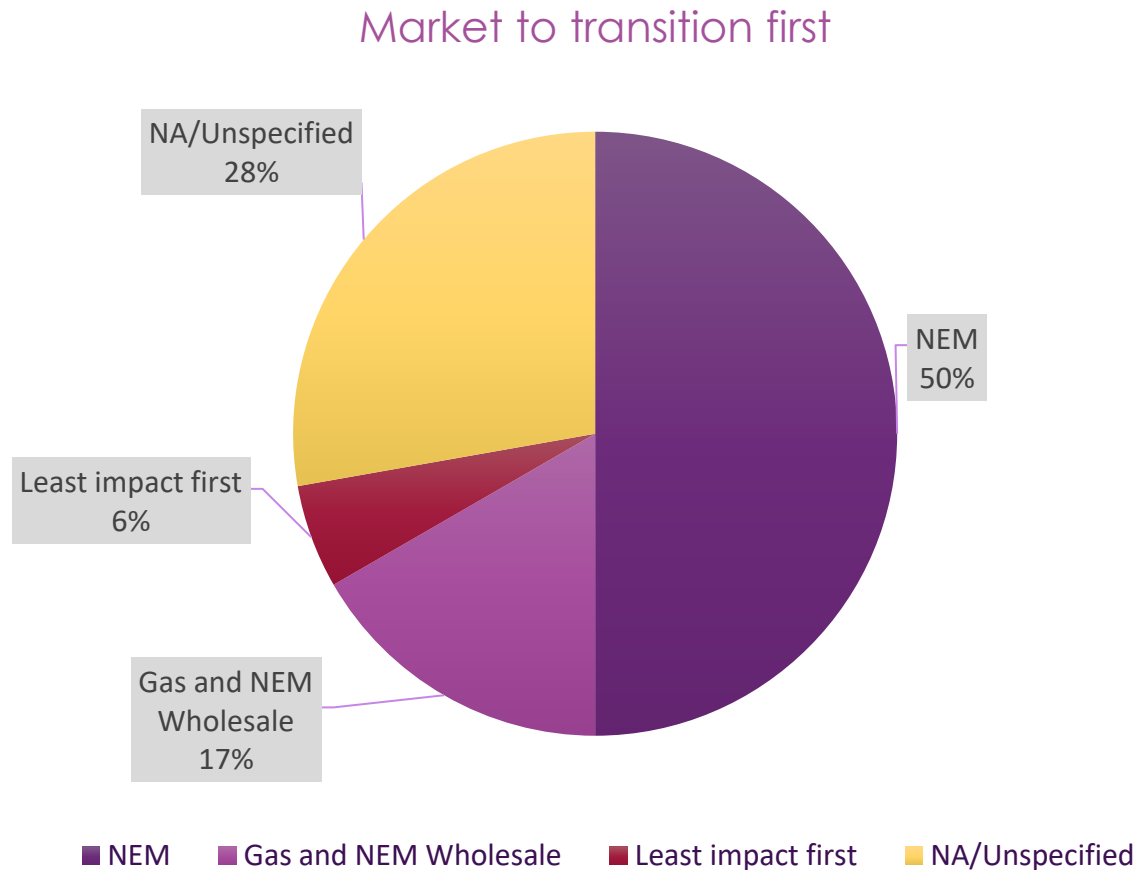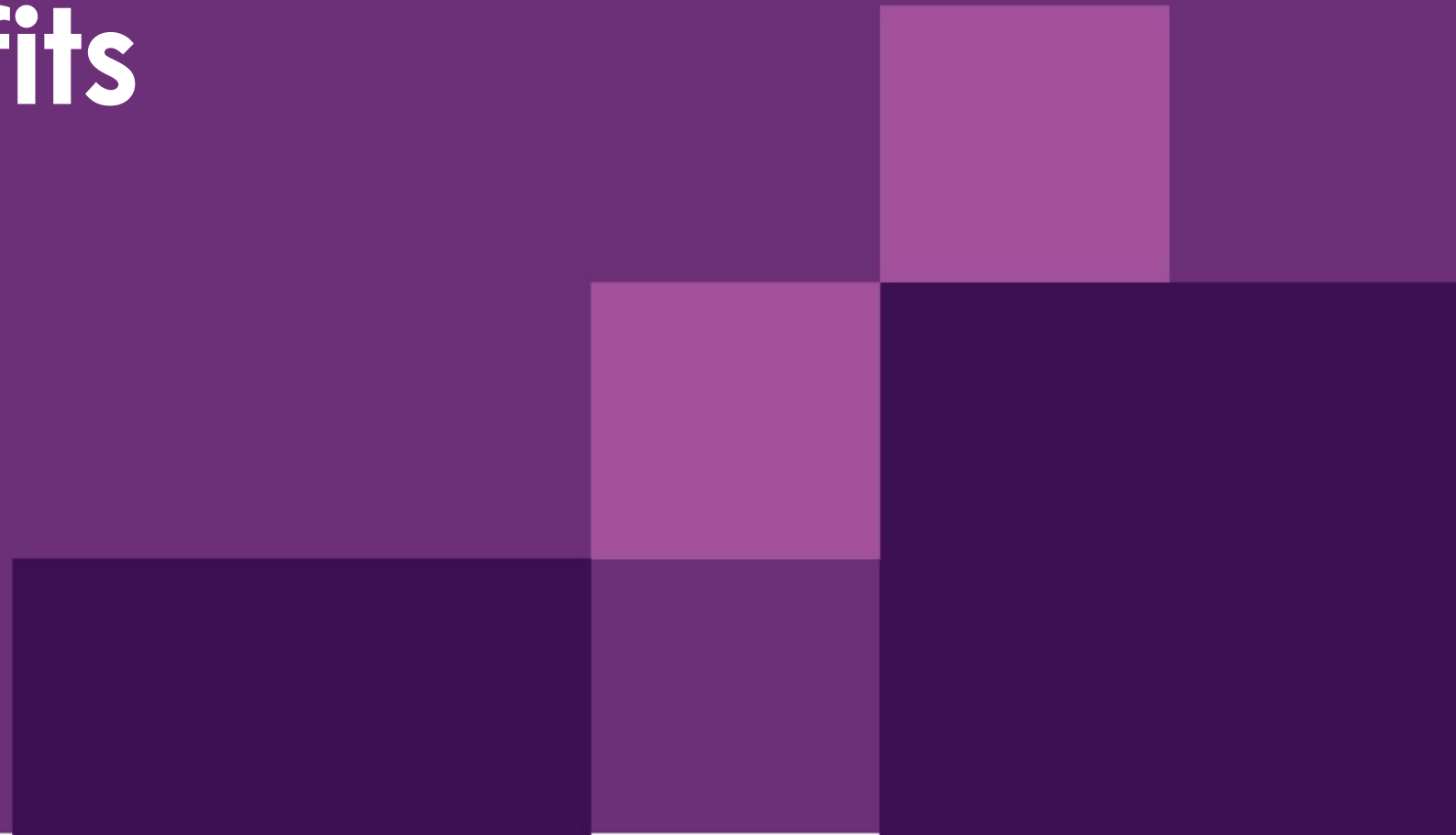
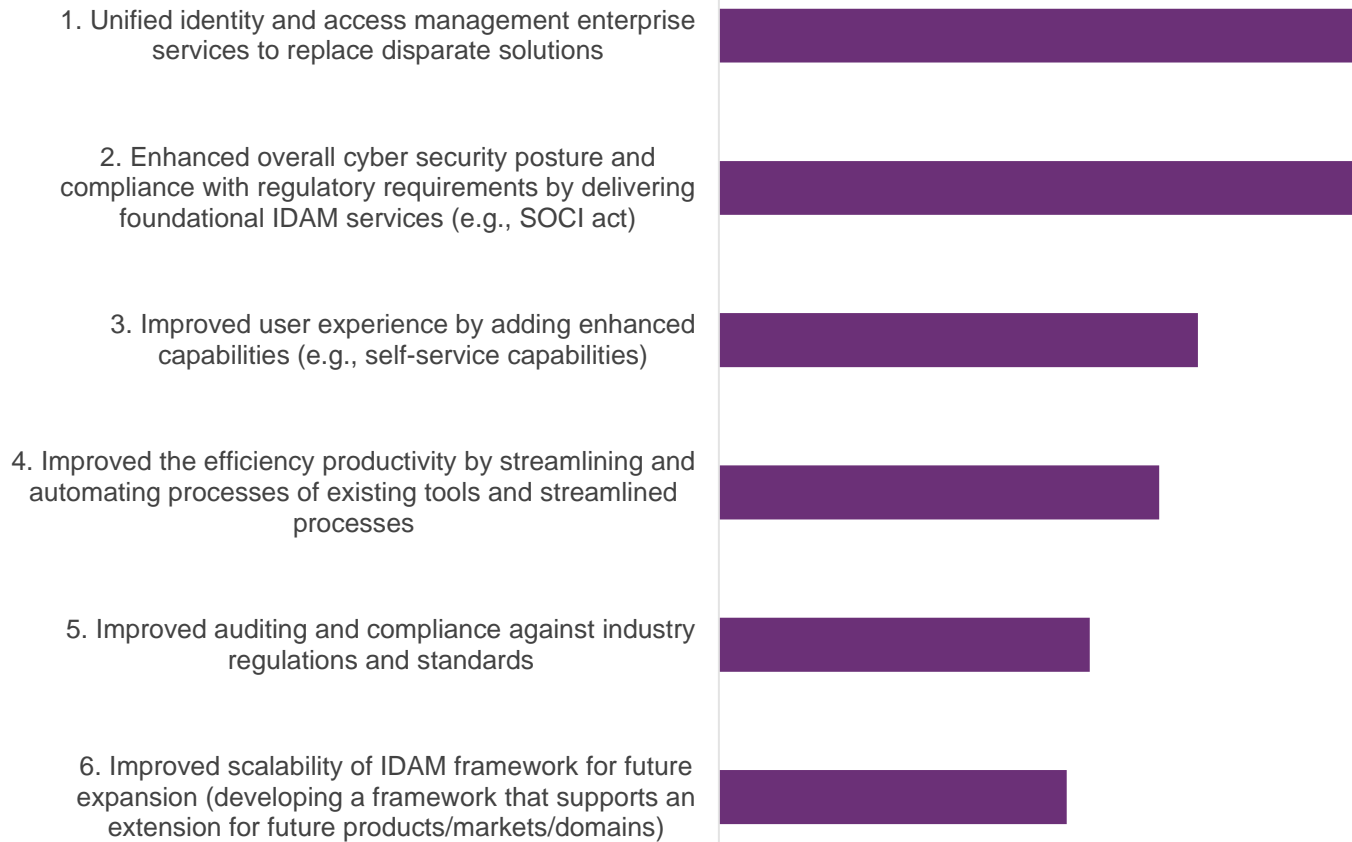Additional observation from the Survey
- The majority of respondents voted transitioning NEM market first, and of those, they preferred NEM Wholesale to be transitioned first.
- Some respondents recommended considering an incremental transition so that the lessons learned in smaller segments can be applied to the remainder.
- Few respondents suggested that MSATS should not be the initial system to be replaced.
- Some respondents voted for the option with the least impact (quick win).

IDAM Benefits

IDAM Benefits

Normalised ranking of the IDAM Benefits based on the survey results

1. Unified identity and access management enterprise services to replace disparate solutions

2. Enhanced overall cyber security posture and compliance with regulatory requirements by delivering foundational IDAM services (e.g., SOCI act)

3. Improved user experience by adding enhanced capabilities (e.g., self-service capabilities)

4. Improved the efficiency productivity by streamlining and automating processes of existing tools and streamlined processes

5. Improved auditing and compliance against industry regulations and standards

6. Improved scalability of IDAM framework for future expansion (developing a framework that supports an extension for future products/markets/domains)

According to the survey results, the respondents considered **unified IDAM services** and improved **cyber security** as the most significant benefits.

Survey results representing the criticality of the IDAM benefits to Participants organisation

Legend: Rank 1, Rank 2, Rank 3, Rank 4, Rank 5, Rank 6
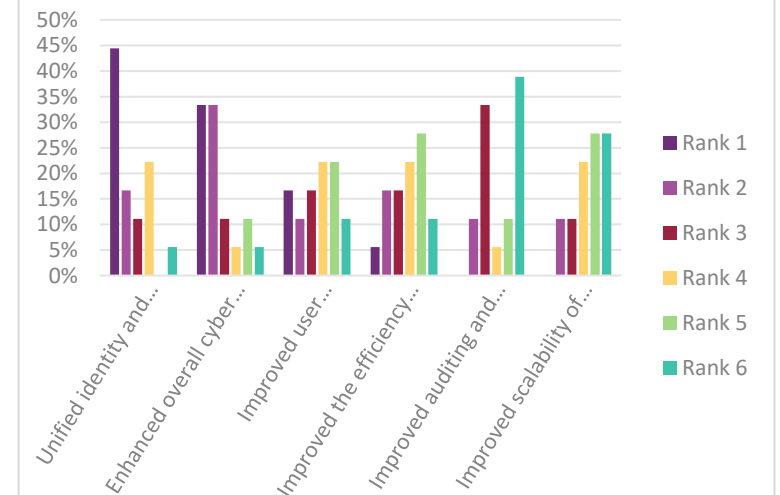
Portal Consolidation Participant Pain points and Priorities

Executive Summary

The aim of portal consolidation is to enable a **unified stakeholder experience** that **hosts web applications**. The portals framework is an enabling platform **that supports energy market participants and other partners** to consume AEMO browser services in a **secure manner**. This initiative focuses on establishing an **internet-facing and mobile portal** for hosting AEMO browser services for use by both registered and non-registered NEM users including personalisation features.

As a result of the Industry Pain Points workshop, the following points were highlighted as the areas of concern by industry participants

User Experience	**Training, Support and Documentation**	**Cost & Complexity**	**Future Needs and Capabilities**
• **Disparate portals:** AEMO's browser services are exposed over a disparate range of portals that require uses to switch between multiple URLs and maintain multiple credentials. • **Cross browser compatibility**: Browser standards should be supported for endpoints and different devices e.g., Chrome, Safari, IE, Edge, mobile devices	• Inadequate resources for **training, support, and documentation** was highlighted. Participants struggle with unclear and scattered documentation, inadequate support from AEMO, and a lack of comprehensive knowledge of the portals.	• Maintenance of the disparate portals appears to be costly (e.g., costs associated with training users and support costs).	• **Personalisation features:** Currently there are inadequate personalisation features available on the portal (e.g., participants cannot create shortcuts to access web applications per their requirements)

Observations from Survey

The survey results highlighted that industry participants support the pain point of disparate portals to be the most pressing concern, followed by incomplete training materials and documentation.

There was feedback received that is **not in-scope** for this portal consolidation initiative specific to browser services, additional fields and functionality. This feedback will be directed to the other initiatives that are making changes in the specific areas:

X Secure connectivity to the portal – Secure URL will not change, login mechanism of secure connectivity will be addressed by IDAM.

X Creating new web-applications is not part of the scope of portal consolidation.

X Having MSATS-like equivalent for Retail Gas / having a single portal for both Elec and Gas – The FRC target state initiative within NEM reform will consider this in-scope.

What is Portal Consolidation?

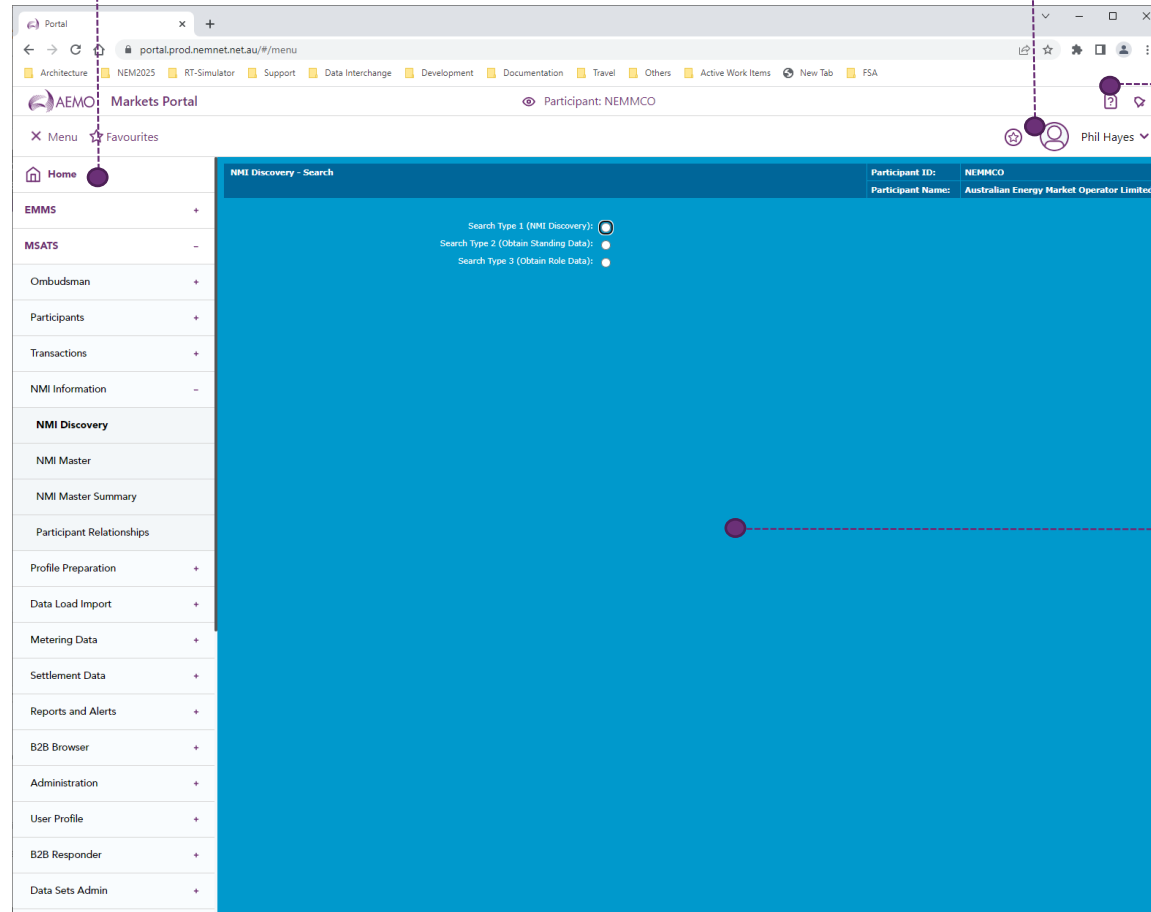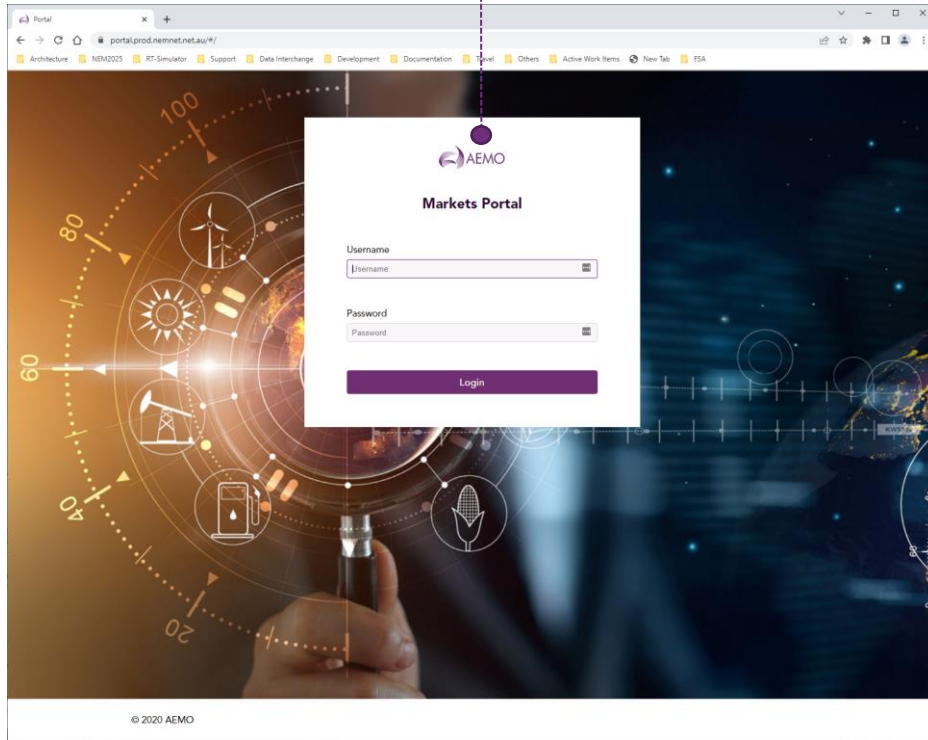Portal URL and
Login page ✓

Portal Menu ✓

Portal Personalisation ✓
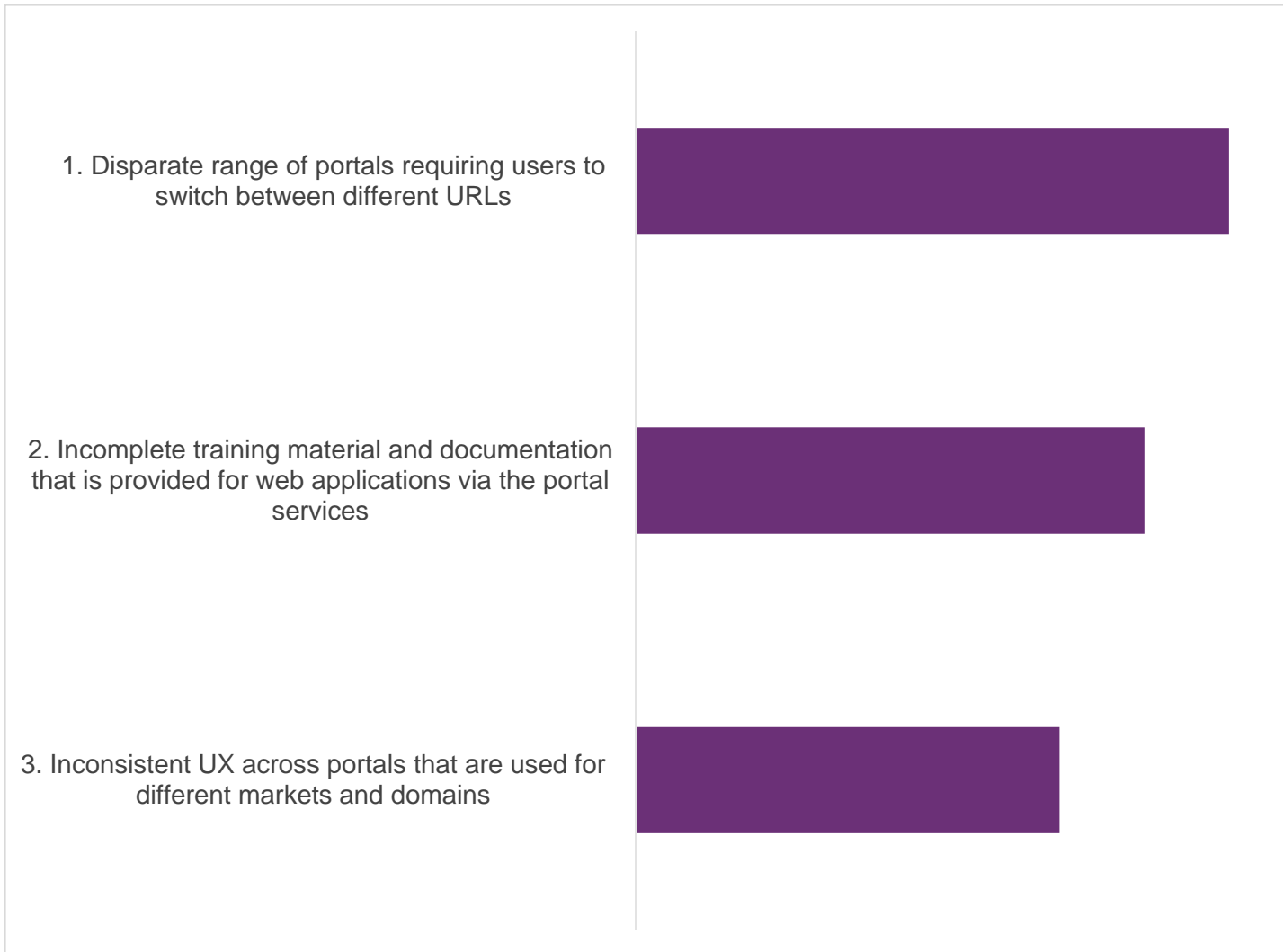
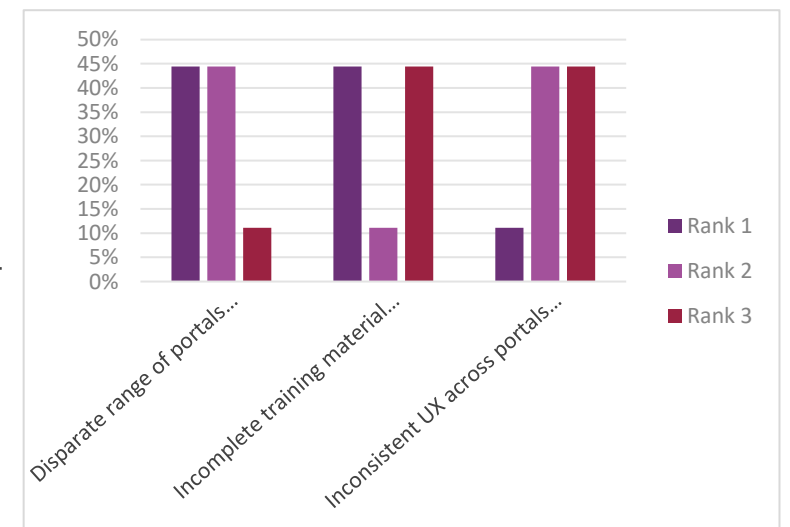Portal Online Help ✓

Web Application ✗

KEY

✓ In scope
✗ Out of Scope

User Experience Pain points Ranking

Normalised Ranking of User Experience Pain points based on the survey response

1. Disparate range of portals requiring users to switch between different URLs

2. Incomplete training material and documentation that is provided for web applications via the portal services

3. Inconsistent UX across portals that are used for different markets and domains
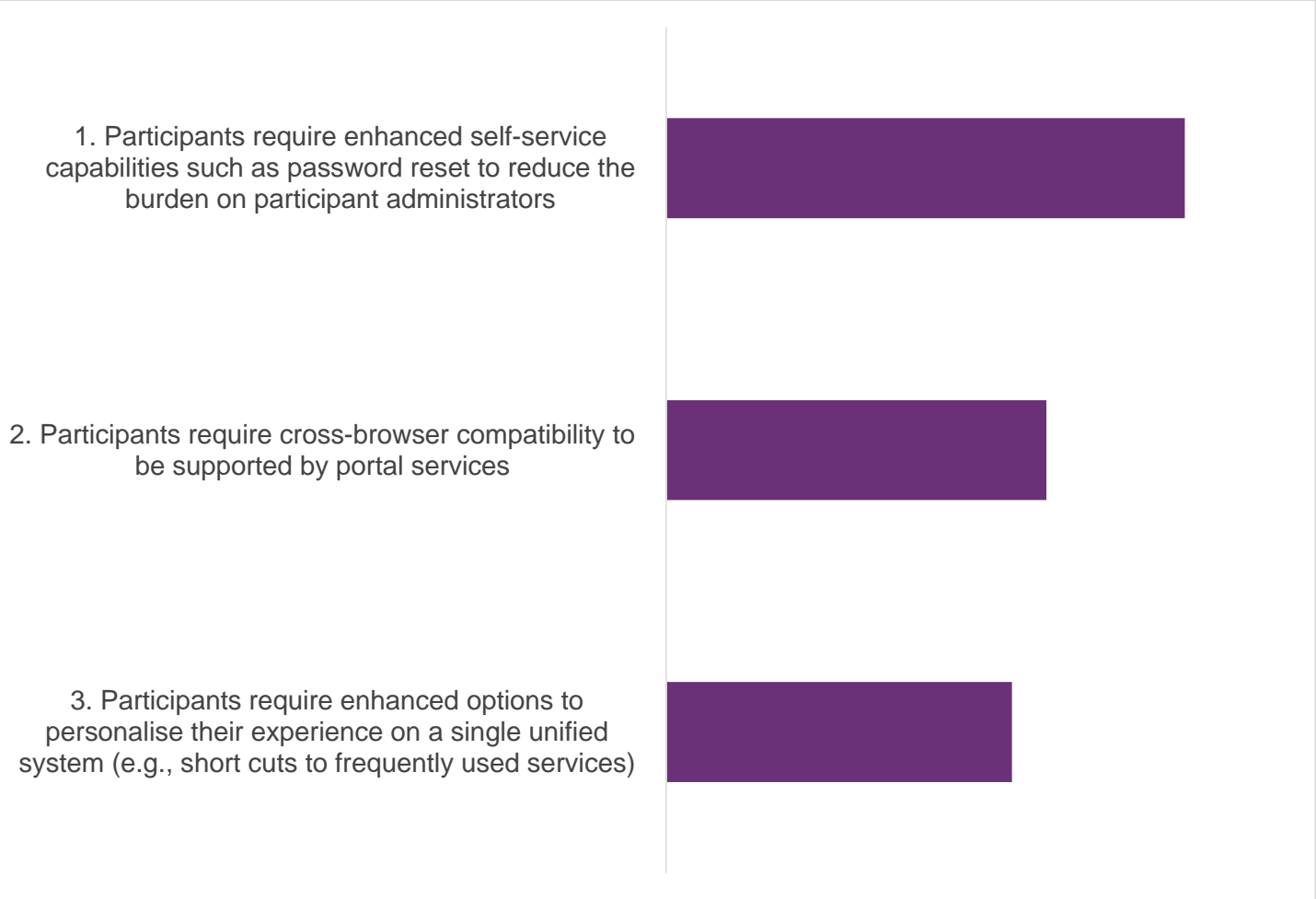
According to the survey results, the respondents considered Disparate range of portals as the most significant pain point

**Survey results representing the ranking of the PC pain points**

Legend:
- Rank 1
- Rank 2
- Rank 3

X-axis categories: Disparate range of portals..., Incomplete training material..., Inconsistent UX across portals...

Y-axis: 0% to 50%

27

Future Needs and Capabilities Ranking

Normalised Ranking of the capabilities required in the target state based on the survey response

1. Participants require enhanced self-service capabilities such as password reset to reduce the burden on participant administrators

2. Participants require cross-browser compatibility to be supported by portal services

3. Participants require enhanced options to personalise their experience on a single unified system (e.g., short cuts to frequently used services)

According to the survey results, the respondents considered enhancing self-service features as the top priority for portal consolidation

Survey results representing the ranking of the PC pain points

Rank 1
Rank 2
Rank 3

28
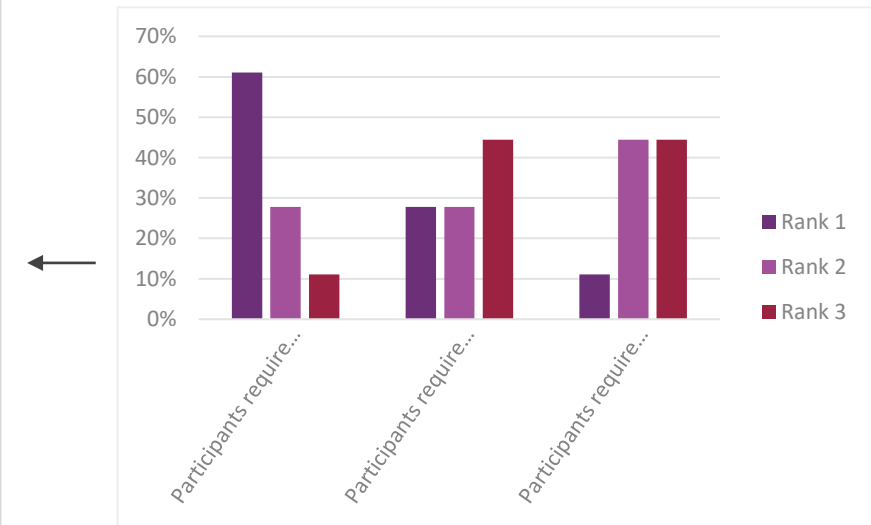
MarketNet Vs Internet

We requested participants to provide any additional feedback on MarketNet Vs Internet. Out of the responses received, the results showed that :

- **Majority respondents supported internet** over MarketNet with the caveat that it is accompanied by a robust security network.
- **Some respondents picked MarketNet** due to security benefits and dedicated tunnels available via MarketNet.

Majority of respondents preferred Internet over MarketNet. Comments included:

I Say: MarketNet is complex to set up and requires substantial IT setup.

I Say: Moving to internet access provides cost reduction and simplification of catering for disaster recovery scenarios

I Say: MarketNet provides a barrier to undertaking business activities efficiently, providing an illusion of security within our systems.

I Say: Preference is API-only internet. MarketNet is an old and costly method that is not adding much value in current world
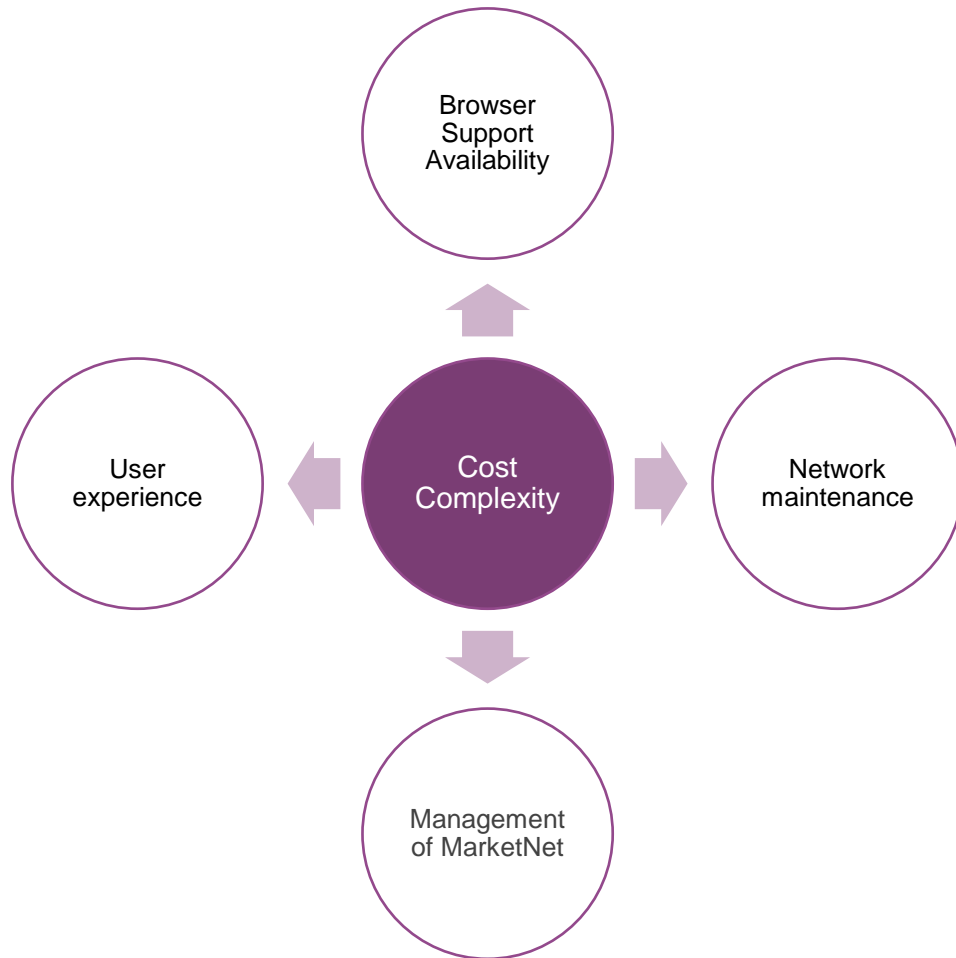
I Say: There are security benefits in requiring all information to be accessed only via secure, dedicated tunnels..

Q. On the assumption that IDAM proceeds and provides more modern and secure identity services, which browser services should be accessible over the internet?

Respondents came back with the following responses

- MSATS
- All services – External Authenticated Portals (accessed by Market Participants and other External Users).
- Services should be identified on cost-effective implementation that does not duplicate access (barring a transitional period).

Cost & Complexity Challenges

```
        ┌─────────────┐
        │   Browser   │
        │   Support   │
        │Availability │
        └─────────────┘
              ↑
┌──────────┐     ┌──────────┐     ┌──────────┐
│   User   │  ←  │   Cost   │  →  │ Network  │
│experience│     │Complexity│     │maintenance│
└──────────┘     └──────────┘     └──────────┘
              ↓
        ┌─────────────┐
        │ Management  │
        │ of MarketNet│
        └─────────────┘
```
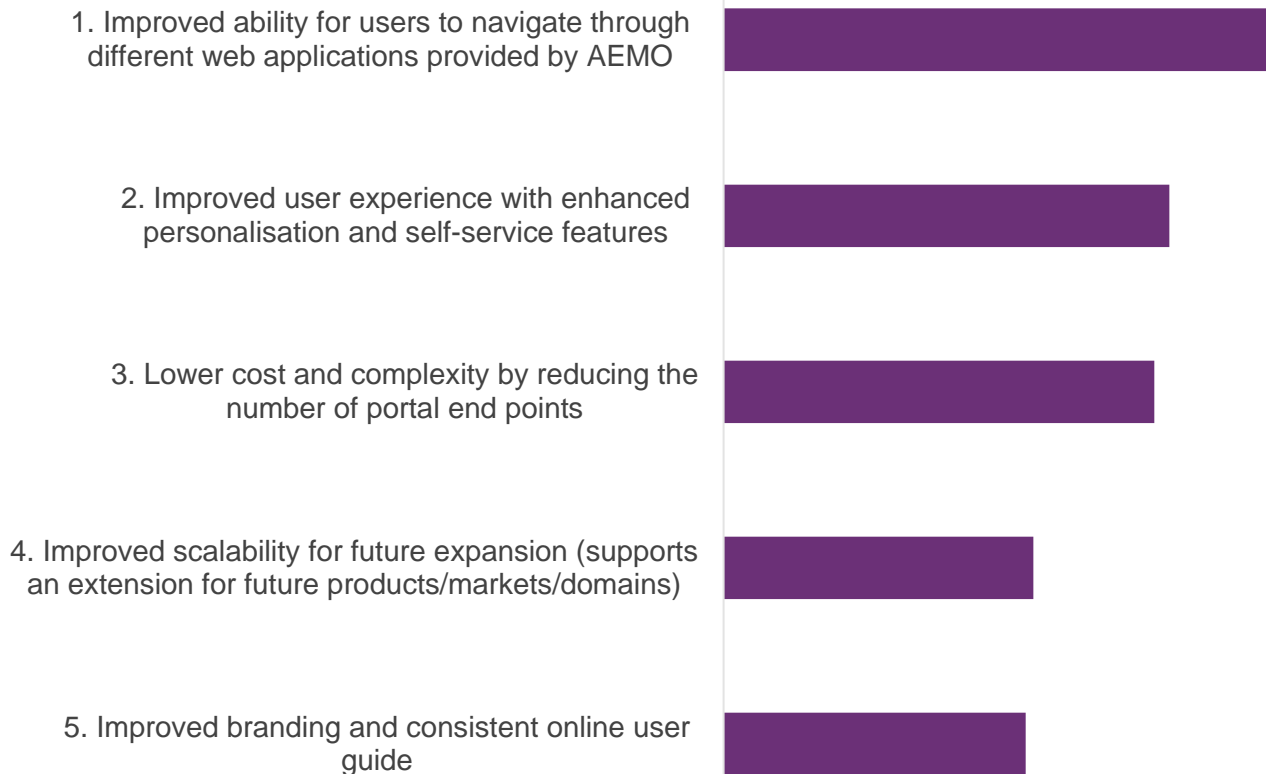
We requested participants to provide feedback on any factors contributing to high costs to their organisation and received comments on the themes of browser support availability, network maintenance, management of MarketNet and User Experience.

We also received feedback on some concepts that are **out of scope** for portal consolidation and will be directed to the broader strategic foundational initiatives:
- Secure integration into AEMO systems to enable real time data access to help streamline functions and lower operating costs.
- Data sharing contributing to cost reduction
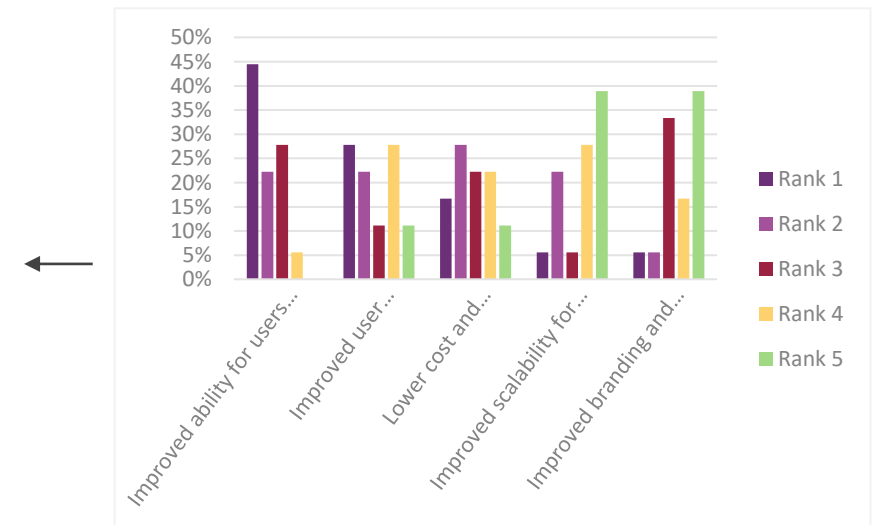- Usage of API's to reduce costs

PC Benefits and Priority

Normalised Ranking of PC benefits and priorities based on the survey response

1. Improved ability for users to navigate through different web applications provided by AEMO

2. Improved user experience with enhanced personalisation and self-service features

3. Lower cost and complexity by reducing the number of portal end points

4. Improved scalability for future expansion (supports an extension for future products/markets/domains)

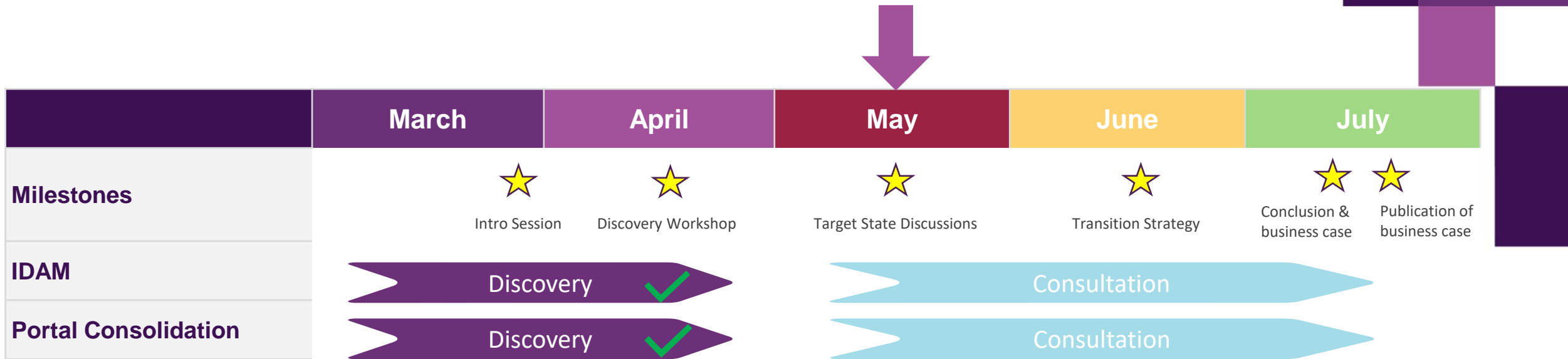5. Improved branding and consistent online user guide

According to the survey results, the respondents considered improving navigation through the web apps provided by AEMO as the most important benefit from portal consolidation for their organisation

Survey results representing the ranking of the PC benefits and Priority

Next steps

	March	April	May	June	July
Milestones	⭐ Intro Session	⭐ Discovery Workshop	⭐ Target State Discussions	⭐ Transition Strategy	⭐ Conclusion & business case ⭐ Publication of business case
IDAM	Discovery ✔		Consultation		
Portal Consolidation	Discovery ✔		Consultation		

- AEMO thanks stakeholders for their invaluable contribution in the Discovery Phase of IDAM and Portal Consolidation.

- The collected data aided in the development of the IDAM and Portals target state solution and support the development of the transition strategy and business case in the next stages of the consultation.

- AEMO welcomes any additional feedback or queries to NEMReform@aemo.com.au.

Legend: ⭐ Milestone

Please reach out

NEMReform@aemo.com.au

AEMO | NEM Reform Program

For more information visit

aemo.com.au