LLOYD'S

# Delegated Contract Manager (DCM)

## Access Control Briefing Call

## Session 2

LLOYD'S

# Today's agenda

1. Registrant and Admin Domain Request
2. Admin Domain Refresher
3. Access Control Overview
4. Access Control Design Process
5. Access Control Definitions
6. User Group Hierarchies
7. Registration Data Visibility
8. Managing Agent User Group Hierarchy
9. Access Control Design Support
10. Next steps

LLOYD'S

# Admin Domain refresher (from 9th March briefing call)

## What is an Admin Domain?

- Administrative Domains (or 'Admin Domains') enable organisations to group participants and manage their access controls under one umbrella.

## How many Admin Domains does my organisation require?

- Lloyd's recommends that organisations opt for a single Admin Domain where possible as segregated of participants can still be achieved using separate Managerial Groups.
- Some organisations, such as those with more complex legal structures, may require multiple Admin Domains if complete segregation of participants and Devolved Admins is required, with no visibility between participants.

LLOYD'S

# FOR ACTION: Onboarding Registrant Email (to be submitted by 26th March)

Last week (on the 9th March), Change Leads should have received the Registrant and Admin Domain email, which requests them to confirm:

1. **Registrant per legal entity**, to commence the onboarding process.
2. **Admin Domain(s) per organisation**, to commence access control design approach.

If your organisation has not received the Registrant and Admin Domain email, please contact DAChangeSupport@Lloyds.com.

- Lloyd's *recommends* that organisations opt for a single Admin Domain, where possible.
- Organisations with more complex legal structures may require multiple admin domain(s) if complete segregation of entities is required.

**The decision on Admin Domain(s) is the responsibility of your organisation, and the appropriate option will depend on how your organisation wants to manage user access controls across your organisation.**

**If you do not complete this information by the 26th March you risk not being able to onboard your organisation on schedule and in time for go-live.**

LLOYD'S

# Access Control Overview

## How has DCM Access Control been designed to benefit the market?

- Following **strong market feedback,** Lloyd's has built **a flexible solution** that enables organisations to **segment their users' access** and **control user group hierarchies** to suit their needs.
- Due to the flexible functionality, **organisations will need to carefully design their access control approach and manage their end-user permissions to ensure users can only access data which is relevant to their needs and can only perform appropriate actions in the system**.

## Which organisations need to design their Access Control approach?

- Any Broker, Managing Agent, direct-deal Coverholders or Service Company that conducts DA business (and therefore uses the DCM system) will need to design their Access Control approach.

## Who needs to be involved in designing your organisation's Access Control approach?

- We recommend that relevant personnel from within your organisation, such as Compliance Officers, Heads of DA, Legal representatives, Heads of IT and senior DA Managers are involved in designing your Access Control approach.
- Having designed your Access Control approach, the **nominated Devolved Administrators (or 'Devolved Admins') from your organisation will be responsible for administering your access control set-up and allocating end-user permissions**, both for initial onboarding and business as usual.

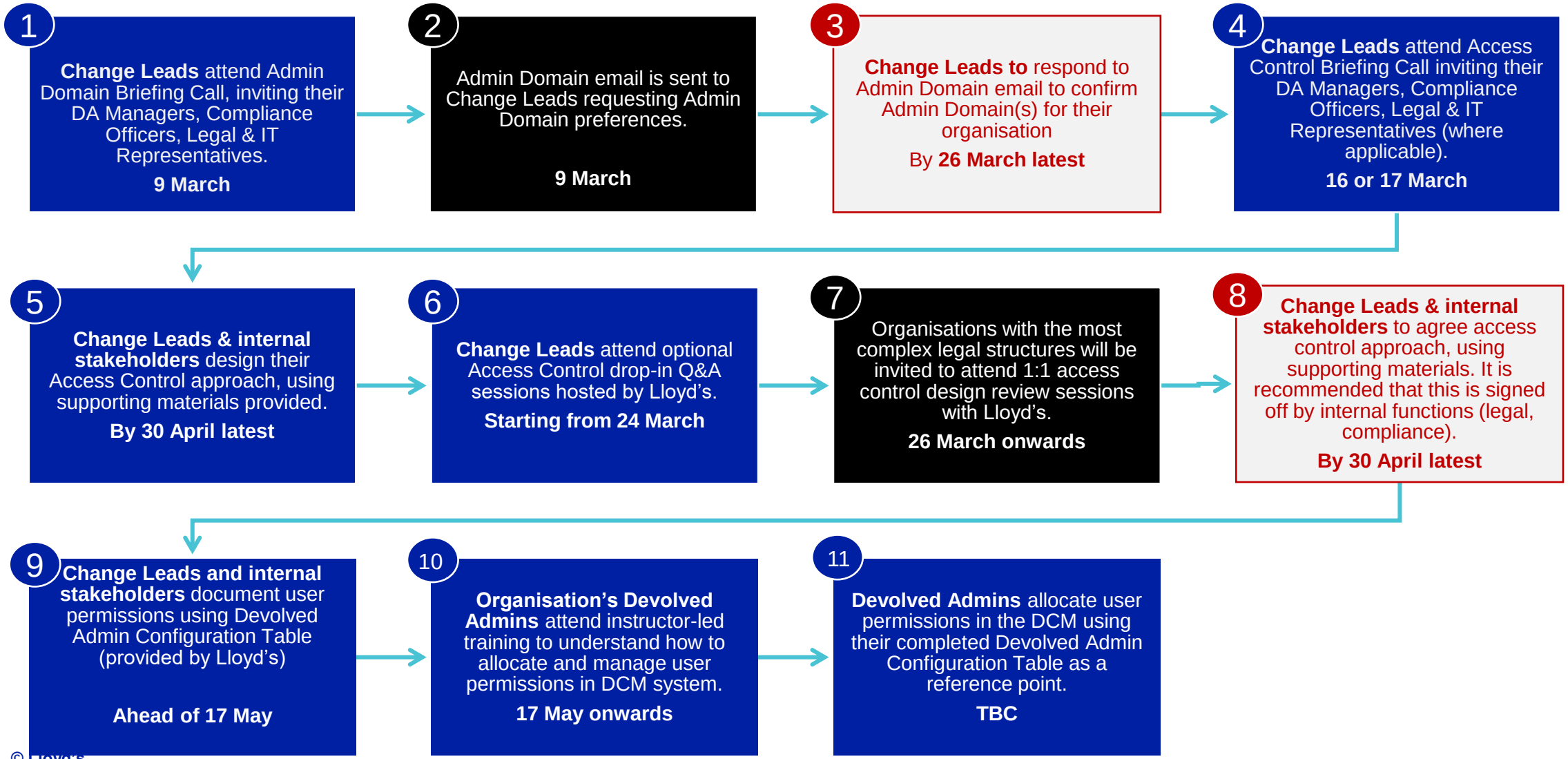
LLOYD'S

# Access Control Design Process

Action from Lloyd's

Action for market organisations

Onboarding Deadline



LLOYD'S

# Access Control definitions

## Access Control

- Access Control refers to the process of managing visibility of registration data (within an organisation and externally) and allocating user permissions to individual users.

## Participants

- The types of participant we refer to in Delegated Contract Manager are Brokers, Managing Agents, deal-direct Coverholders, Service companies and their associated identifiers e.g., CSNs and syndicate numbers.

## User Group Hierarchy

- A User Group hierarchy denotes the relationships between the Domain User Group, Managerial Groups and User Groups. A User Group's position in the hierarchy determines the registration data that its users can access.

## Devolved Admin User Group

- Devolved Admins are nominated individuals within an organisation responsible for setting up and maintaining the user group structure of an Admin Domain determined by their organisation. They are also responsible for adding / removing users within these groups and assigning permissions (e.g., Read only, Read Write and Read Write Submit).
- Devolved Admins will be restricted to one Admin Domain only, in the same way that other users are.

LLOYD'S

# Access Control definitions

## Domain User Group

- Each Admin Domain has one Domain User Group which is set up automatically and cannot be removed.
- This group will be given visibility of all data and tasks within the system that are associated with the participants within the Admin Domain.
- If you do not wish to use this Group, it is not mandatory to add any users.

## Managerial User Group

- Each participant within an Admin Domain will need to be associated with a Managerial Group.
- Managerial Groups can be shared across multiple participants.
- When a task is shared, visibility is granted to the Managerial Groups of all participants on the contract.
- Users in these Groups can choose to grant other User Groups within their hierarchy visibility of this task.

## User Group

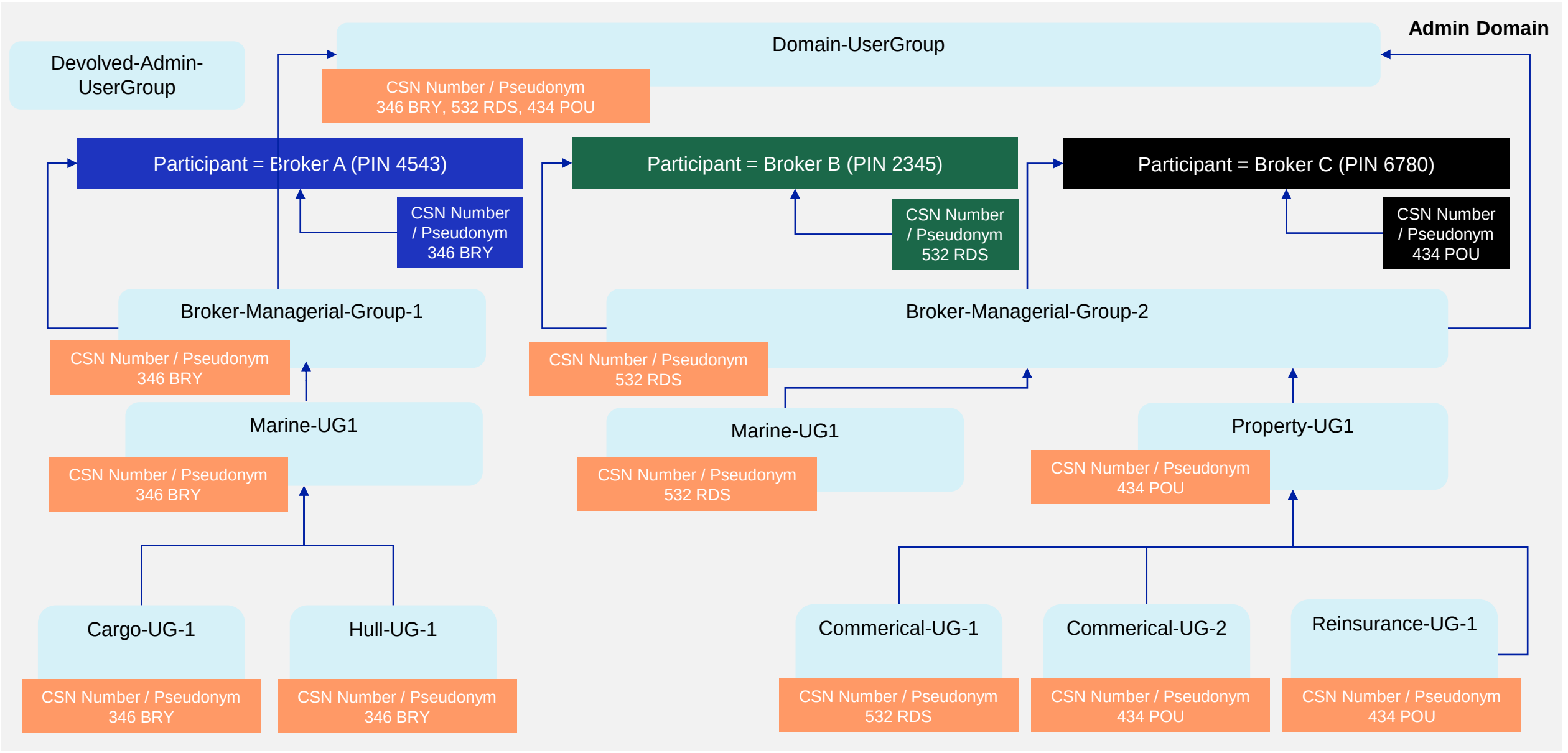
- User Groups are used to segregate access to registrations within your organisation by allowing you to logically group users.
- The system allows you the flexibility to organise your users into simple or complex structures in order to achieve the separation you require.
- The user groups exist in the system as a hierarchy, where a user group's position in the hierarchy dictates their visibility of registration data.

LLOYD'S

# Example - User Group Hierarchy- Broker

*Names are illustrative*

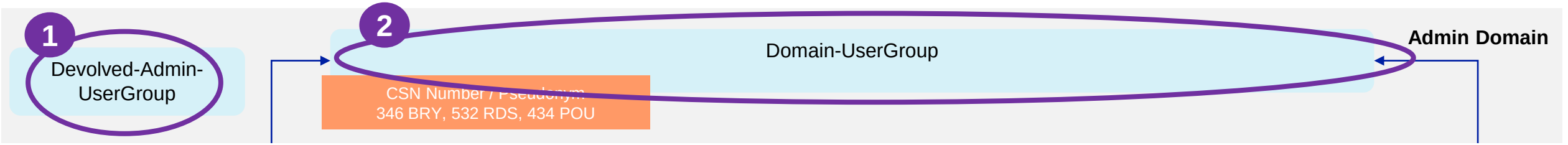
Blue boxes are user groups



# User Group Hierarchy: Domain User Group

*Names are illustrative*

Blue boxes are user groups




## 1. Devolved Admin Group

- Each Devolved Admin User Group must contain at least 2 Devolved Admins per admin domain, who are selected by your organisation.
- Devolved Admins will only be able to perform activities, such as assigning permissions and allocating users to user groups, within their Admin Domain.
- Devolved Admins may be part of other user or managerial groups if required. For example, if the head of DA wants to be the Devolved Admin to control allocating permissions but also wants to be in managerial and user groups to create registrations, then this is possible.

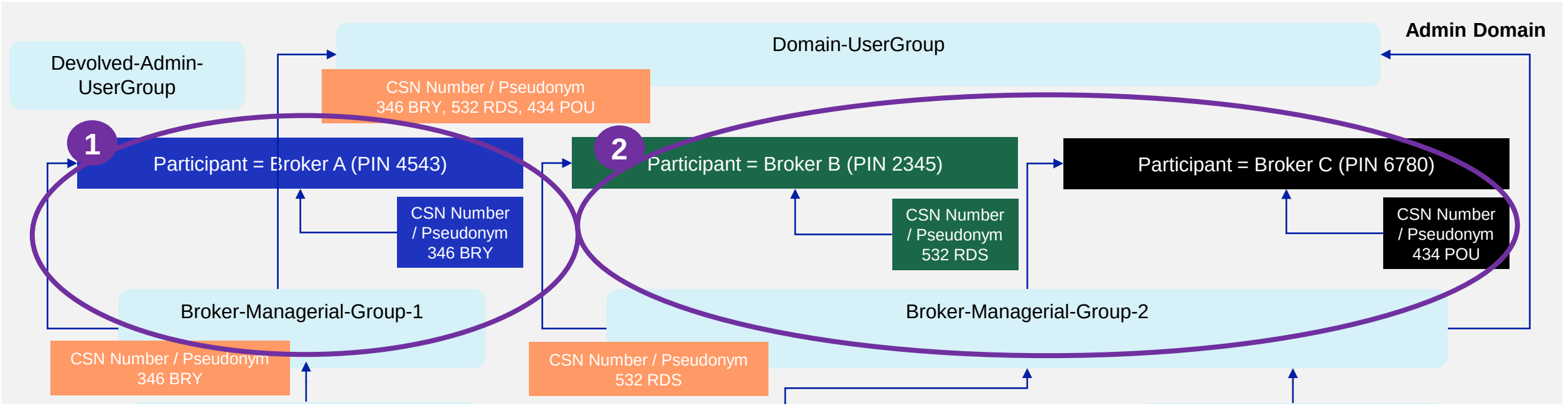
## 2. Domain User Group

- The Domain User Group is automatically created when Lloyd's sets up your Admin Domain. However, it is not mandatory to assign any users to this group and can therefore be left empty if not required.
- Those placed in the Domain User Group will have visibility of registration data associated with any User or Managerial groups within its Admin Domain.
- It is up to you who and if you put any users in the Domain User Group, but examples may include CEOs or Heads of IT; effectively, anyone who may want report on your entire Admin Domain.

# User Group Hierarchy: Managerial Group

*Names are illustrative*

Blue boxes are user groups




## Managerial Group

- Users in Managerial Groups have the ability to assign visibility of registration data to those in user groups indirectly or directly below it in the User Group Hierarchy.
- The Managerial Group is the group that, when a participant is granted visibility of registration data and they are not the contract administrator, is initially granted visibility and is responsible for granting any further visibility within the user group hierarchy.
- If the appropriate segregation is achieved by the creation of managerial groups for users in an organisation, there is no requirement to create further user groups below this in the user group hierarchy.
- Once the appropriate groups have been granted visibility, assigning tasks in the system can be done by the managerial group.

**1.** Participants must be related to one (and only one) Managerial group.

**2.** One Managerial Group can be associated with multiple participants.

LLOYD'S

# User Group Hierarchy: User Group

*Names are illustrative*

Blue boxes are user groups

## User Group

User Groups can be arranged in hierarchical relationships referred to as either **'parent-child' relationships** or '**sibling' relationships**.

### 1. Parent-child relationships

• Parent-child relationships represent a flexible way of providing visibility and oversight of user groups below it in the hierarchy.

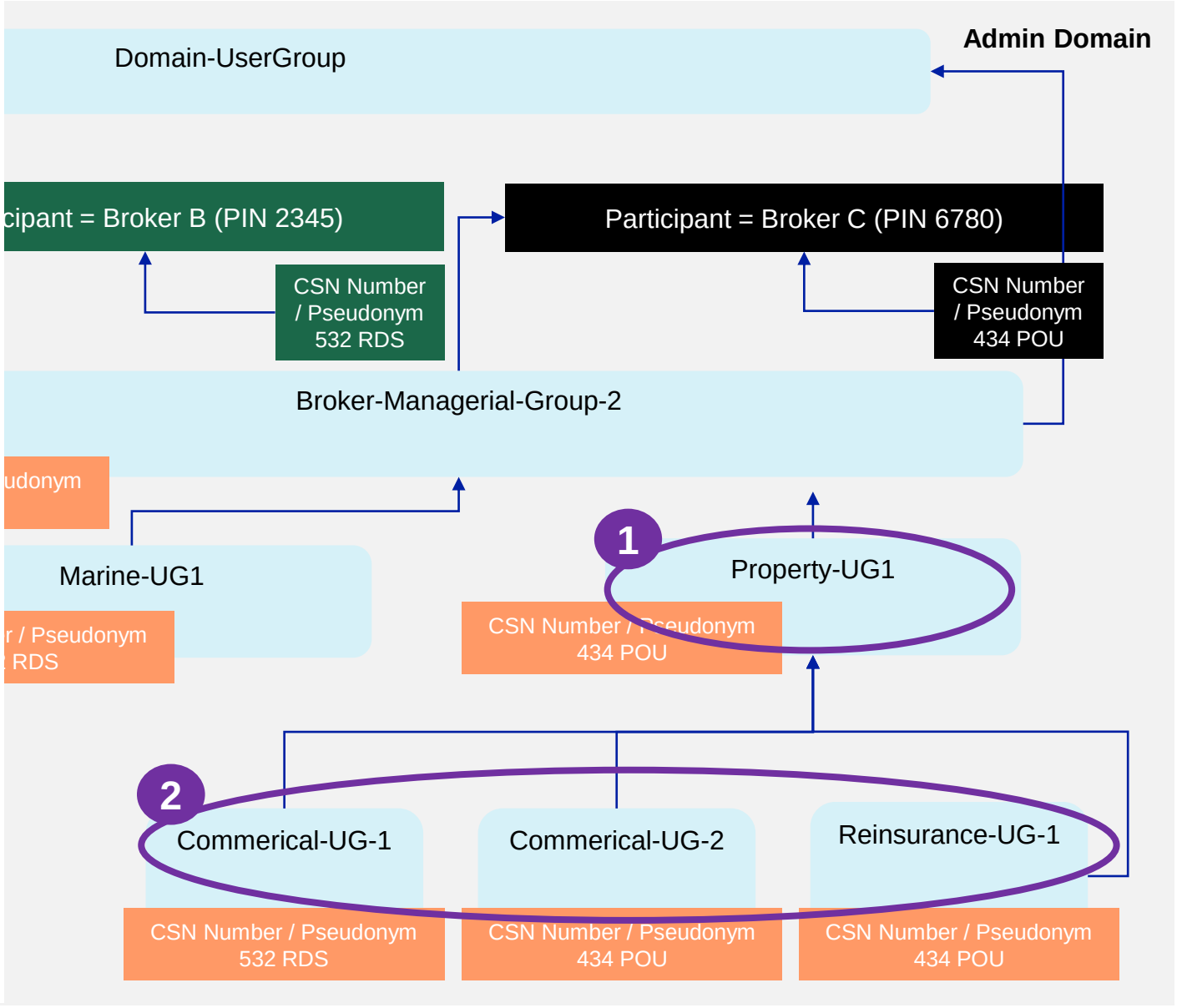
• Property UG1 is an example of a 'parent' user group, whose 'children' are those user groups below it in the User Group hierarchy, namely Commercial UG1, Commercial UG2 and Reinsurance UG1.

• As the parent user group, Property UG1 has visibility of all registration data in its 'children' user groups.

### 2. Sibling relationships

• User Groups can be arranged in 'sibling' relationships, meaning they sit on the same level as other user groups.

• Unlike parent-child relationships, there is no automatic visibility of registration data across sibling user groups.

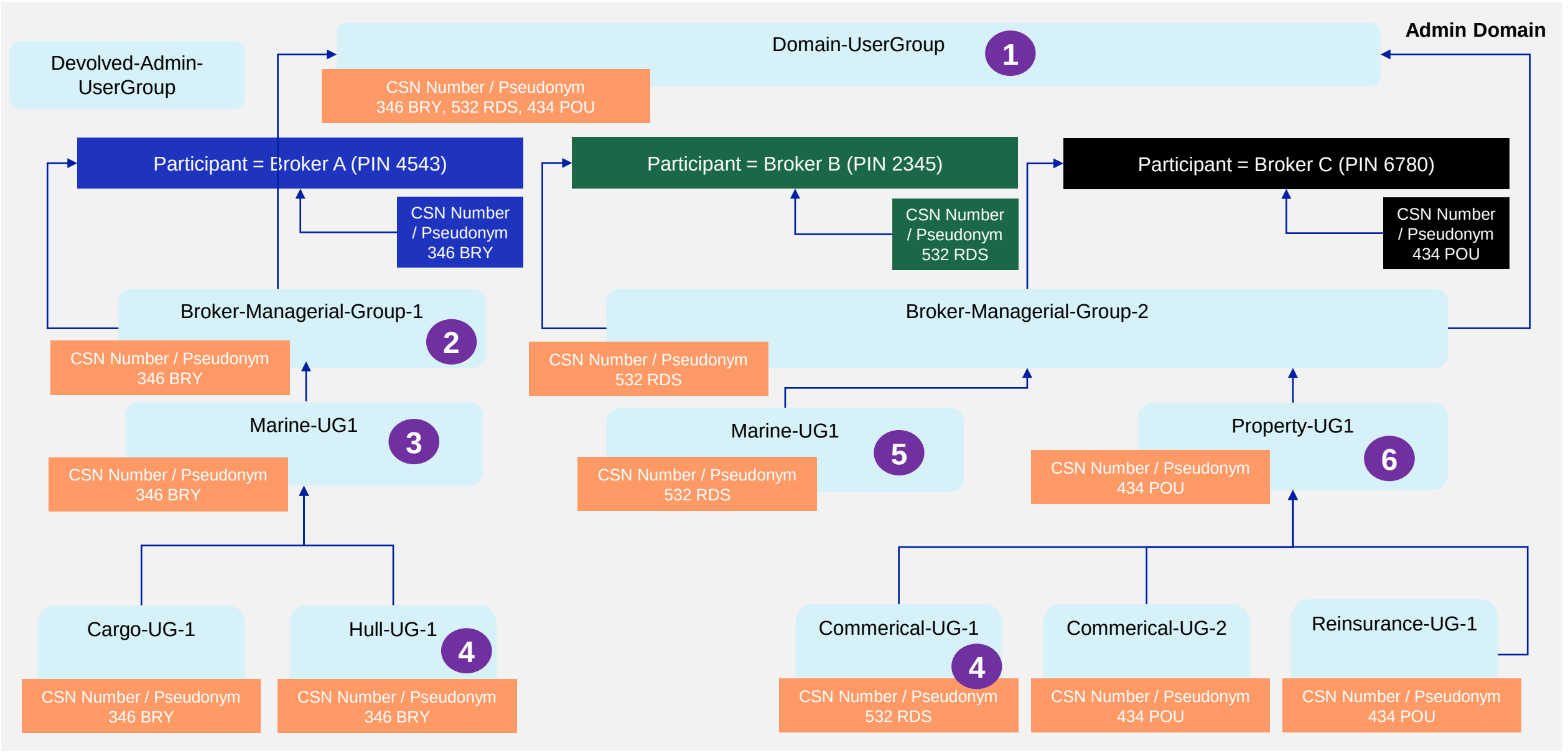


LLOYD'S

# Registration Data Visibility

*Names are illustrative*

Blue boxes are user groups



LLOYD'S

# Notes for slide 13:

### 1. User 1 is part of Domain User Group

- User 1 has oversight and can report on all groups within this Admin Domain.
- User 1 could be anyone who requires this functionality, such as the CEO or Head of IT.

### 2. User 2 is part of Managerial Group 1

- User 2 has visibility of registration data in all User Groups underneath it in the hierarchy (i.e., Marine UG1, Cargo UG1 and Hull UG1).
- User 2 can grant visibility of registration data to the Marine UG1, Hull UG1 and Cargo UG1.

### 3. User 3 is part of a Marine UG1

- User 3 has visibility of all user groups below it in the hierarchy, known as its ‘children’ i.e., cargo UG1 and Hull UG1.
- User 3 cannot grant access as it is only part of a user group (and not a managerial group).

### 4. User 4 is part of Hull UG1 and Commercial UG1

- User 4 has visibility of registration data assigned to its user groups, which are Hull UG1 and Commercial UG1.
- User 4 does not have visibility of registration data in Cargo UG1, Commercial UG2 or Reinsurance UG1, which are its 'sibling' groups (to the side).
- User 4 doe not have visibility of registration data in Marine UG1 or Property UG1 (above them in hierarchy).
- If, like User 4, you have access to multiple user groups, when creating a registration, you will be prompted by the system to choose the CSN to which the contract relates.

LLOYD'S

# Notes for slide 13:

### 5. User 5 is part of Marine UG1

- Marine UG1 (to which User 5 is assigned) and Property UG1 are ‘sibling’ groups, meaning they are unable to view each other’s registration data.
- Similarly, even though Commercial UG1, Commercial UG2 and Reinsurance UG1 are in a lower level in the User Group Hierarchy than Marine UG1, User 5 would be unable to view any registration data relating to these groups as Marine UG1 is not their ‘parent’ group.

### 6. User 6 is part of Property UG1

- User 6 will be able to view registration data relating to Commercial UG1, Commercial UG2 & Reinsurance UG1, as these are its 'children' User Groups.
- Property UG1 has CSN 434, meaning users within this group will be able to create registrations relating to this CSN.
- Please note that CSNs are associated to User Groups by the Devolved Admins; however, you do not have to associate a CSN to a user group. A User Group which does not have an associated CSN will not be able to create registrations, however it can still be granted visibility of them.
- Despite being associated with CSN 434, users in Property UG1 (such as User 6) will also be able to view data relating to Commercial UG1, which has CSN 532. However, it will be NOT be able to perform any actions as their contract administrator does not share the same CSN.
- User 6 will NOT be able to view **all** registration data relating to CSN 532, only that assigned to Commercial UG1 (as it is a ‘child’ user group).

LLOYD'S

# Managing Agent: User Group Hierarchy

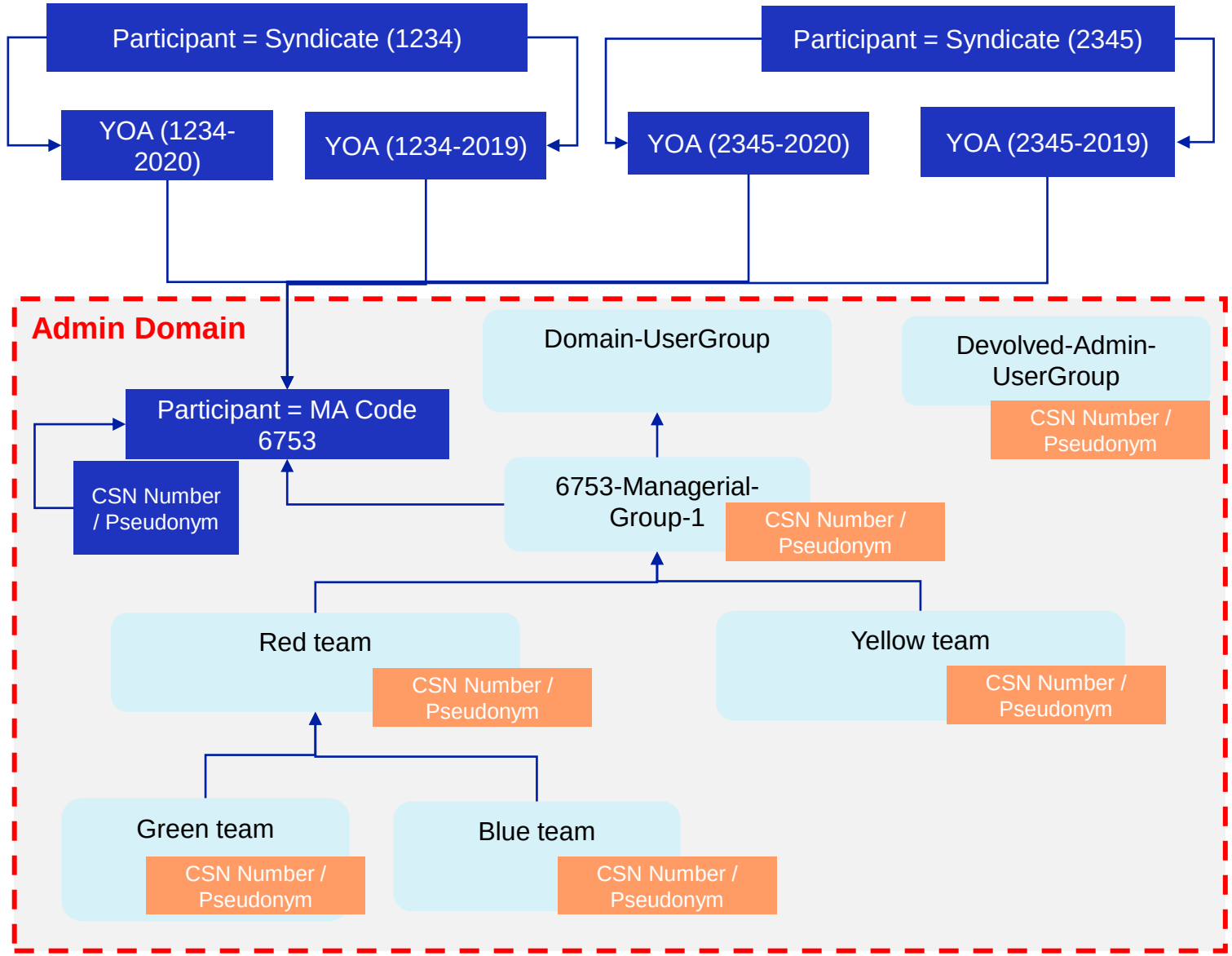
## Scenario 1:

1. Broker creates registration in DCM.
2. Registration is shared with/submitted to Managing Agent.
3. Managing Agent (in Managerial Group) grants visibility to relevant User Group(s) and selects a user to complete (as required).

## Scenario 2:

1. Service company / in-house broker creates registration (user selects which CSN & group this applies to).
2. Managing Agent (in Managerial Group) grants visibility to relevant User Group(s) and selects a user to complete (as required).

***System will have to look for the active MA-YOA relationship***



LLOYD'S

# Notes for slide 16:

The content on slides 10-13 still applies to Managing Agents, however the key difference is that you will only have 1 participant which is attached to its own Managerial Group – this participant is the Managing Agent.

Your syndicate(s) will be automatically associated with the Managing Agent using their Syndicate Year of Account.
These syndicates will need to be arranged in User Groups (below this Managerial Group) in whichever way best suits your needs.

If a syndicate has multiple CSNs, Lloyd's recommends creating a User Group for each CSN to ensure segregation of syndicate registration data (if required).

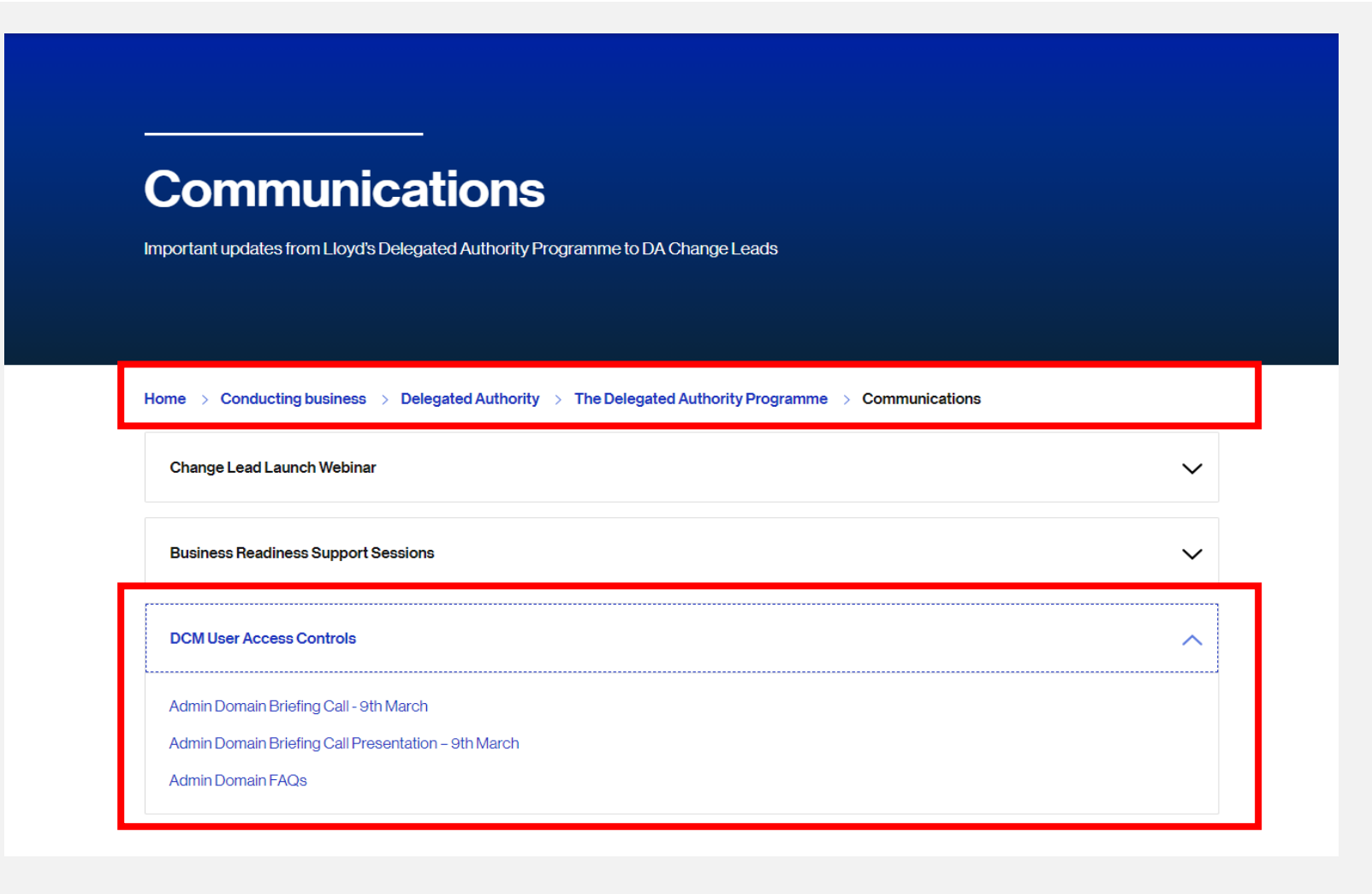
The relationships are at Managing Agent level on Atlas and will not be changing.

LLOYD'S

# Access Control: Supporting materials

| | 1 | 2 | 3 |
|---|---|---|---|
| | Admin Domain and Access Control FAQs | Access Control Design Tool | Devolved Admin Configuration Table |
| Overview | Admin Domain and Access Control FAQs to support understanding and knowledge. | Document to support organisations with designing their user group hierarchies. | Template for organisations to record their users' permissions and user groups. |
| Action for the market | Change Leads and Internal Stakeholders to review FAQs to **inform the design of your organisation's access controls and User Group hierarchies.** | Change Leads and Internal Stakeholders to use tool to **design and document your organisation's User Group hierarchies** | Change Leads and internal stakeholders to **complete the Devolved Admin Configuration Requirements Table prior to their Devolved Admins attend instructor-led training.** |

# Access Control Support Materials on Change Lead site




https://www.lloyds.com/conducting-business/delegated-authorities/the-delegated-authority-programme/communications

LLOYD'S

# Weekly Access Control 'Drop-In' Q&A Sessions – Optional

**Invites to the Q&A have not been issued yet and will be issued on a rolling basis**

| 24th March | 1st April | 14th April | 22nd April | 29th April |
|---|---|---|---|---|
| 10 – 11 am | 10 - 11am | 9:30 – 10:30am | 10 – 11am | 10 -11 am |

These weekly drop-in Q&A sessions are an opportunity for Change Leads, Compliance Officers, IT representatives to attend and ask questions that will support organisations in defining and documenting their access control approach.

LLOYD'S

# Next steps

- If you have not already, **complete** the Registrant and Admin Domain email which was sent out last week (9th March) and emailed to Dachangesupport@Lloyds.com – to be **completed by 26th March.**
- **Use** the supporting materials to start designing and documenting your organization's access control approach – **to be completed 30th April.**
- **Review and share** this presentation with all relevant stakeholders, such as DA Managers, Compliance Officers, IT representatives within your organisation.
- **Look out** for the invites to the weekly 'drop-in' access control sessions and invite relevant internal stakeholders.