LLOYD'S

DCOM Access Control

Admin Domain

Briefing Call - Session 1

LLOYD'S

Today's agenda

1 | Registrant and Admin Domain email

2 | User Access Control Introduction

3 | User Access Control Process

4 | User Access Control Definitions

5 | Admin Domain Overview

6 | Single Admin Domain

7 | Multiple Admin Domains

8 | Registrant and Admin Domain email

9 | Next steps

FOR ACTION: Onboarding Admin Domain & Registrant and Email (to be submitted by 26th March)

After this briefing call (9th March) Change Leads will be sent the Registrant and Admin Domain email, which will request 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.

It is vital that Change Leads engage the Head of Delegated Authorities within their organisation, and work with them to validate which Admin Domains should be setup with internal compliance and legal counterparts, before confirming this to Lloyd's by 26 March.

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 access control across different legal entities.

User Access Control: Introduction

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

- During the requirements gathering process for Delegated Contract Manager, Lloyd's received strong feedback on the need to build a flexible solution that enabled organisations to segment their users' access and control user group hierarchies to suit their needs. **Lloyd's has incorporated this feedback and delivered this functionality as part of the first release of Delegated Contract Manager.**
- 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, Coverholder 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.

Access Control Process For Organisations

- **Steps 1 & 2** Today's session (9th March) is focused on Admin Domains
- **Steps 3 & 4** We will host a second briefing call on 16th & 17th March to provide more detail on designing your broader access control approach

1 Determine Admin Domain(s) for organisation	2 Lloyd's configures Admin Domains in the system	3 2nd Access Control briefing call	3 Design Access Control Approach
Change Leads, DA Manager, Compliance Officers legal and IT representatives	Lloyd's	Change Leads, DA Manager, Compliance Officers legal and IT representatives	Change Leads, DA Manager, Compliance Officers legal and IT representatives
Determine the Admin Domain(s) for your organisation and confirm this through the Registrant and Admin Domain email **(email issued 9 March).**	Once organisations have confirmed their Admin Domain(s) via the Registrant and Admin Domain email, Lloyd's will configure these in the system to enable onboarding on schedule.	Attend 2nd briefing call on user access controls and hierarchies to start designing your organisation's access control approach	It is the responsibility of Change Leads work with their compliance and legal teams and Heads of DA to design their organisation's access control approach ahead of Devolved Admins attending training.
Complete by **26th March**	Starts 27th March	16th & 17th March	By 30th April

User Access Controls: Definitions

Access Control

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

Participants

- The types of participant we refer to in Delegated Contract Manager are anyone who can participate on a contract i.e. brokers, Managing Agent, 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 contract registration data that they can access.

Admin Domain(s): Overview

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

Admin Domain(s) **allows:**

- Complete segregation (other than Devolved Admins) of registration data between different entities. This means that users in one admin domain will be unable to view any registration data relating to entities within a different admin domain.
- User Group hierarchies can be used within an Admin Domain to allow segregation within an organisation.
- Participants (Brokers, Managing Agents, Coverholders) and users can only belong to one Admin Domain at a time.
- Organisations with multiple legal entities in a **single Admin Domain** share administrative resources by having the same Devolved Admins manage end users.
- Devolved Admins within an Admin Domain can grant rights to user groups (i.e.. access to specific CSNs) and permissions to the users (i.e. read only, read-write, read, write and submit) to provide specific visibility of registration data.
- Users within a single Admin Domain can be part of multiple Managerial and User groups at the same time. There is no limit to how many users can be in a single group or how many groups a single user may be part of.

Admin Domain(s) **restricts:**

- The visibility of confidential registration data by users within other Admin Domains.
- Participants' and users' ability to be in more than one Admin Domain.
- Devolved Admins from managing access of users from other Admin Domains.

Single Admin Domain

Single Admin Domains

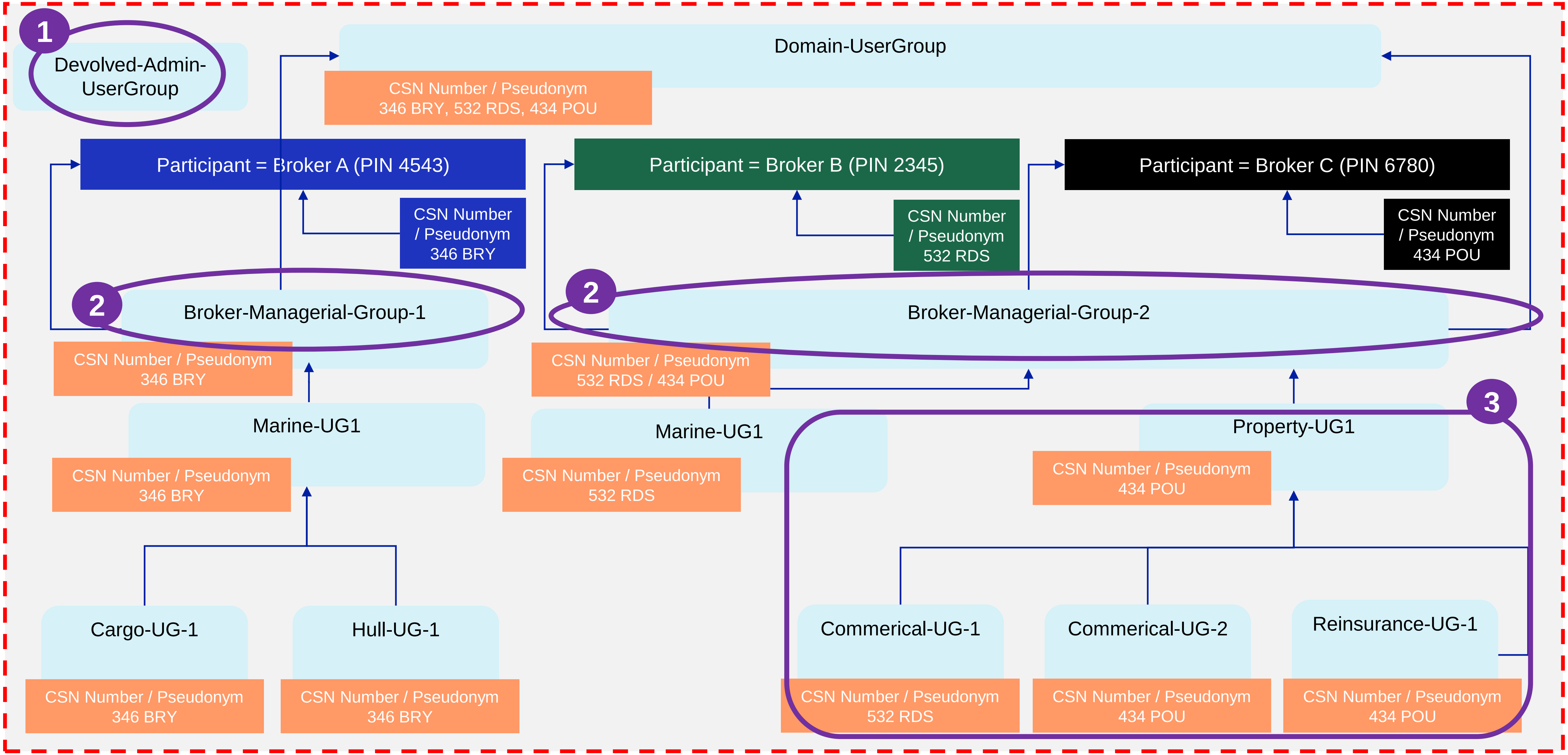
- **It is recommended that organisations with a single participant only set up one admin domain**, as any required segregation of registration data can be incorporated into the design of your organisation's user group hierarchy.
- Users and Devolved Administrators can only be part of one admin domain at a time. This means that they can only manage users, allocate permissions or access registration data within that admin domain.
- Setting up your structure within your admin domain(s) gives you control over your users' visibility of registration data in the system, depending on what user groups you assign them to and/or which managerial groups they belong to. This will enable you to meet the security requirements of your company.
- If you are a single-participant organisation and you believe you require multiple Admin Domains, please contact DAChangeSupport@Lloyds.com.

LLOYD'S

Example - User Group Hierarchy- Broker

Names are illustrative

Blue boxes are user groups



Notes to previous slide

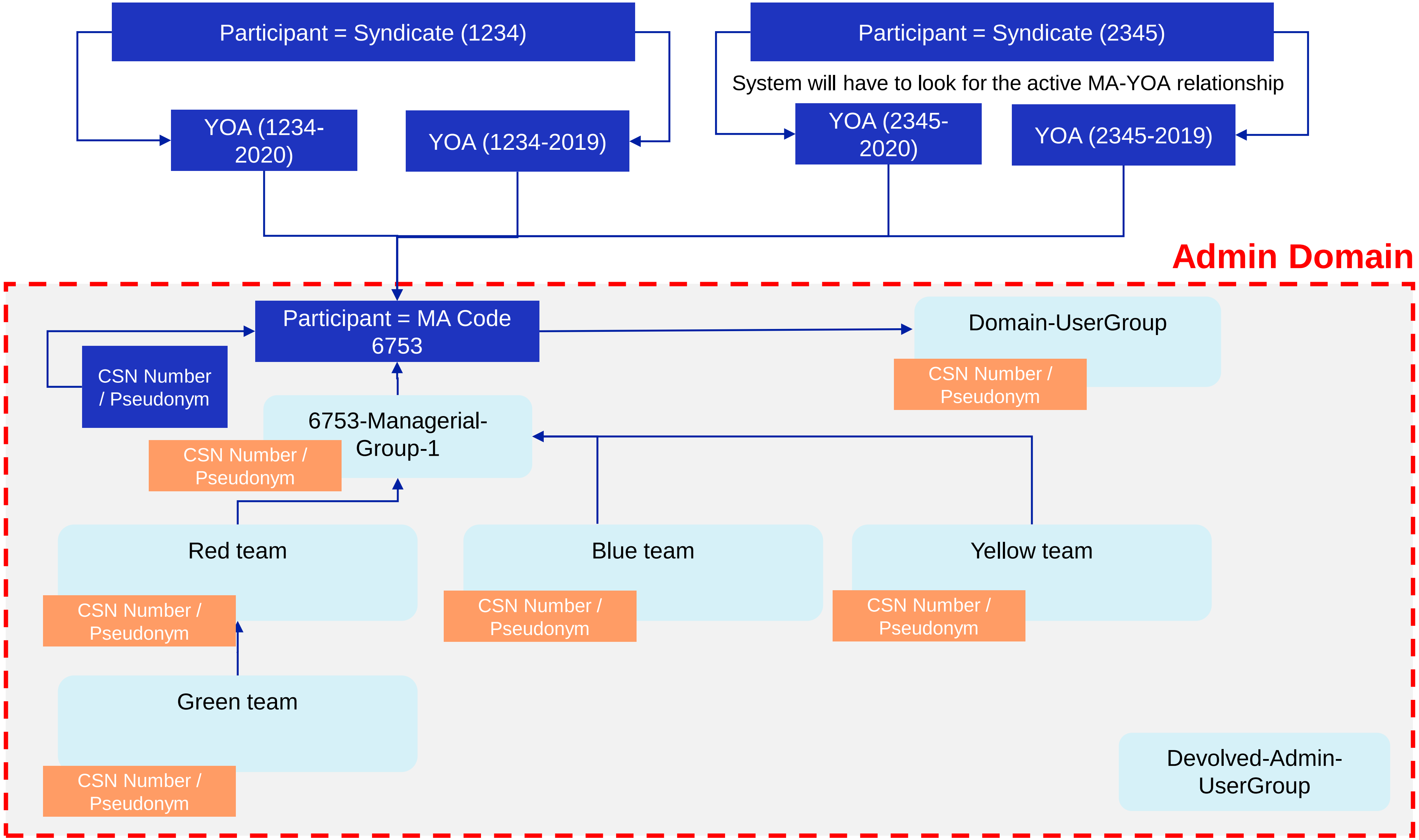
- This is an example broker User Group Hierarchy with 3 broker participants; A (Blue), B (Green) & C (Black).
- **Point 1:** A single Devolved Admin group sets-up the user group hierarchy for the Admin Domain, assigns users to the appropriate groups and allocates permissions e.g. read only, read write, read write submit etc. In this example, the Participants in this organisation are Broker A, Broker B & Broker C, identified by different CSNs/broker numbers & Pseudonyms
- **Point 2:** The use of managerial groups can achieve segregation of one or multiple participants in the admin domain. Here, Broker A has its own Managerial Group and therefore users in this group will NOT be able to view any registration data of participants Broker B and Broker C. However, Brokers B & C are in a shared managerial group so users in these groups WILL have visibility of both participants' registration data (however will NOT be able to view any registration data relating to Broker A). However, if there are some users you wanted in broker group 1 and broker 2, then this is possible Note that each Participant can be associated to only ONE managerial group, however one managerial group can serve multiple Participants.
- **Point 3:** Individual 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 structures that reflect how your teams operate day to day. The user groups exist in the system as a hierarchy and each user group is associated (directly or indirectly) with ONE managerial group through the use of an identifier e.g. CSN/Pseudonym, which rolls up to the Participant(s). User groups above others in the hierarchy will have visibility of the work done by users in the lower user groups. This enables oversight where required. So, in this example, Commercial User group 1 will NOT be able to view any registration data in its 'sibling' user groups; Commercial UG2 & Reinsurance UG1; and vice versa. However, Property UG1, will have visibility of all 3 User groups as they are its 'children' user groups, meaning they are directly below it in the User Group hierarchy.

Please note that individual users in any of the user groups on screen can be assigned permission to Read only, Read Write or Read Write & Submit registration data.

LLOYD'S

Example User Group Hierarchy - Managing Agent

Blue boxes are user groups



Participant = Syndicate (1234)

Participant = Syndicate (2345)

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

YOA (1234-2020)

YOA (1234-2019)

YOA (2345-2020)

YOA (2345-2019)

Admin Domain

Participant = MA Code 6753

CSN Number / Pseudonym

Domain-UserGroup

CSN Number / Pseudonym

6753-Managerial-Group-1

CSN Number / Pseudonym

Red team

CSN Number / Pseudonym

Blue team

CSN Number / Pseudonym

Yellow team

CSN Number / Pseudonym

Green team

CSN Number / Pseudonym

Devolved-Admin-UserGroup

Multiple Admin Domain(s)

Why would an organisation need multiple Admin Domains?

When would multiple Admin Domains be necessary?

- Some organisations, such as those with more complex legal structures, may require multiple Admin Domains if complete segregation of **entities and Devolved Admins** is required, with no visibility of registration data between entities.

How does this work?

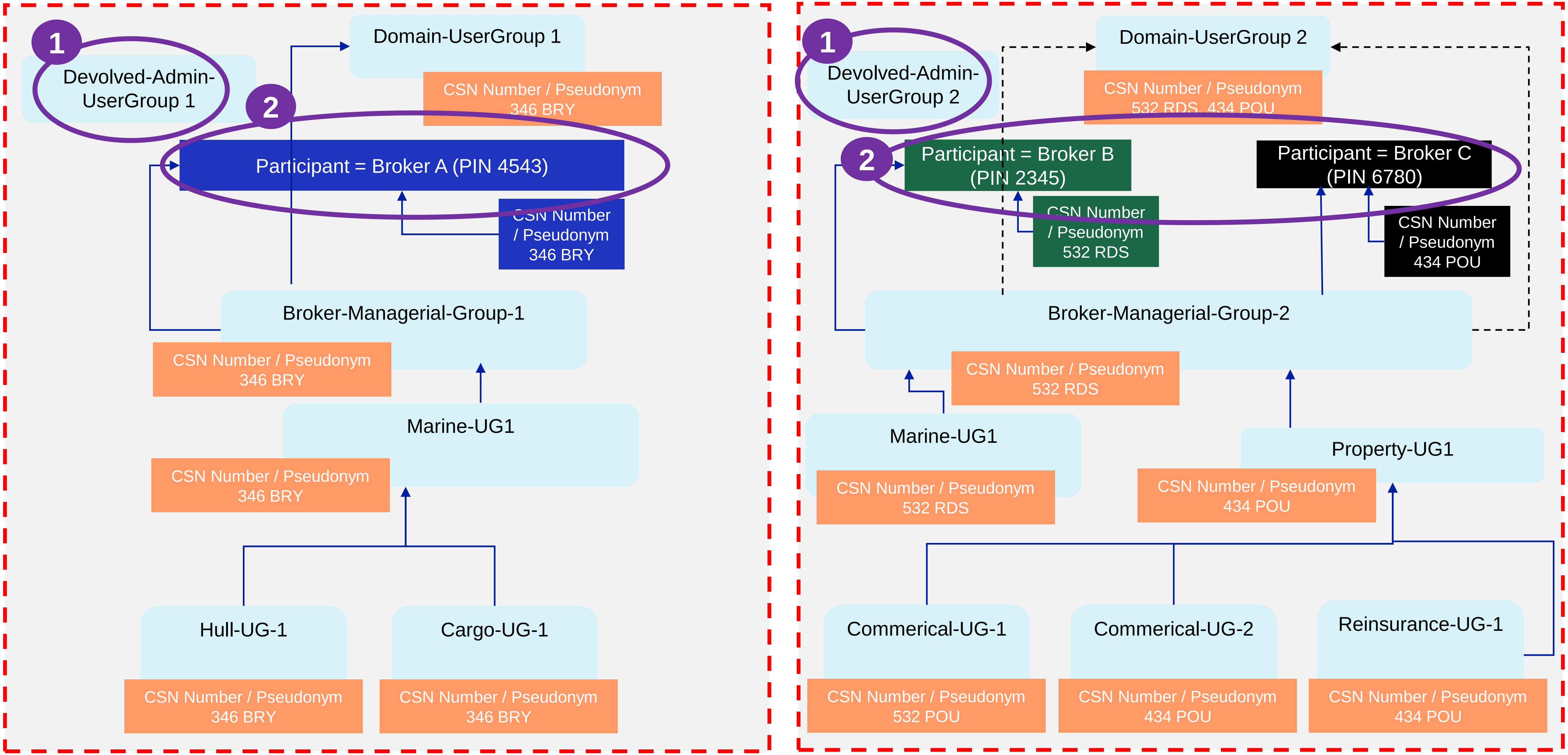
- Each entity which requires complete segregation from other entities will require its own Admin Domain, which will contain its unique User Group hierarchy and Devolved Admin user group.

- Please note that a separate Devolved Admin User Group (containing 2 or more Devolved Admins) will need to be set up for each Admin Domain to manage end users. All users can not be in more than one Admin Domain at any one time.

LLOYD'S

Example - Multiple Admin Domain User Group Hierarchies (Broker)

Blue boxes are user groups



Admin Domain 1

1 Devolved-Admin-UserGroup 1

Domain-UserGroup 1
CSN Number / Pseudonym 346 BRY

2 Participant = Broker A (PIN 4543)
CSN Number / Pseudonym 346 BRY

Broker-Managerial-Group-1
CSN Number / Pseudonym 346 BRY

Marine-UG1
CSN Number / Pseudonym 346 BRY

Hull-UG-1
CSN Number / Pseudonym 346 BRY

Cargo-UG-1
CSN Number / Pseudonym 346 BRY

Admin Domain 2

1 Devolved-Admin-UserGroup 2

Domain-UserGroup 2
CSN Number / Pseudonym 532 RDS, 434 POU

2 Participant = Broker B (PIN 2345)
CSN Number / Pseudonym 532 RDS

Participant = Broker C (PIN 6780)
CSN Number / Pseudonym 434 POU

Broker-Managerial-Group-2
CSN Number / Pseudonym 532 RDS

Marine-UG1
CSN Number / Pseudonym 532 RDS

Property-UG1
CSN Number / Pseudonym 434 POU

Commerical-UG-1
CSN Number / Pseudonym 532 POU

Commerical-UG-2
CSN Number / Pseudonym 434 POU

Reinsurance-UG-1
CSN Number / Pseudonym 434 POU

Notes to previous slide

The previous slide illustrates the use of multiple Admin Domains. In this example, Broker A (PIN 4543) requires complete segregation, so a separate Admin Domain 1 (with Devolved Admin user group) has been set up to accommodate this. It is important to highlight that any users in Admin Domain 1 are unable to also be in Admin Domain 2 (and vice versa). As an organisation, you will need to carefully consider whether this segregation of users is absolutely necessary because this would cause big overheads.

Points 1: Separate Devolved Admin User Groups will need to be set up for each Admin Domain. This means that the Devolved Admins in Admin Domain 1 will be unable to manage or assign permissions to users in Admin Domain 2.

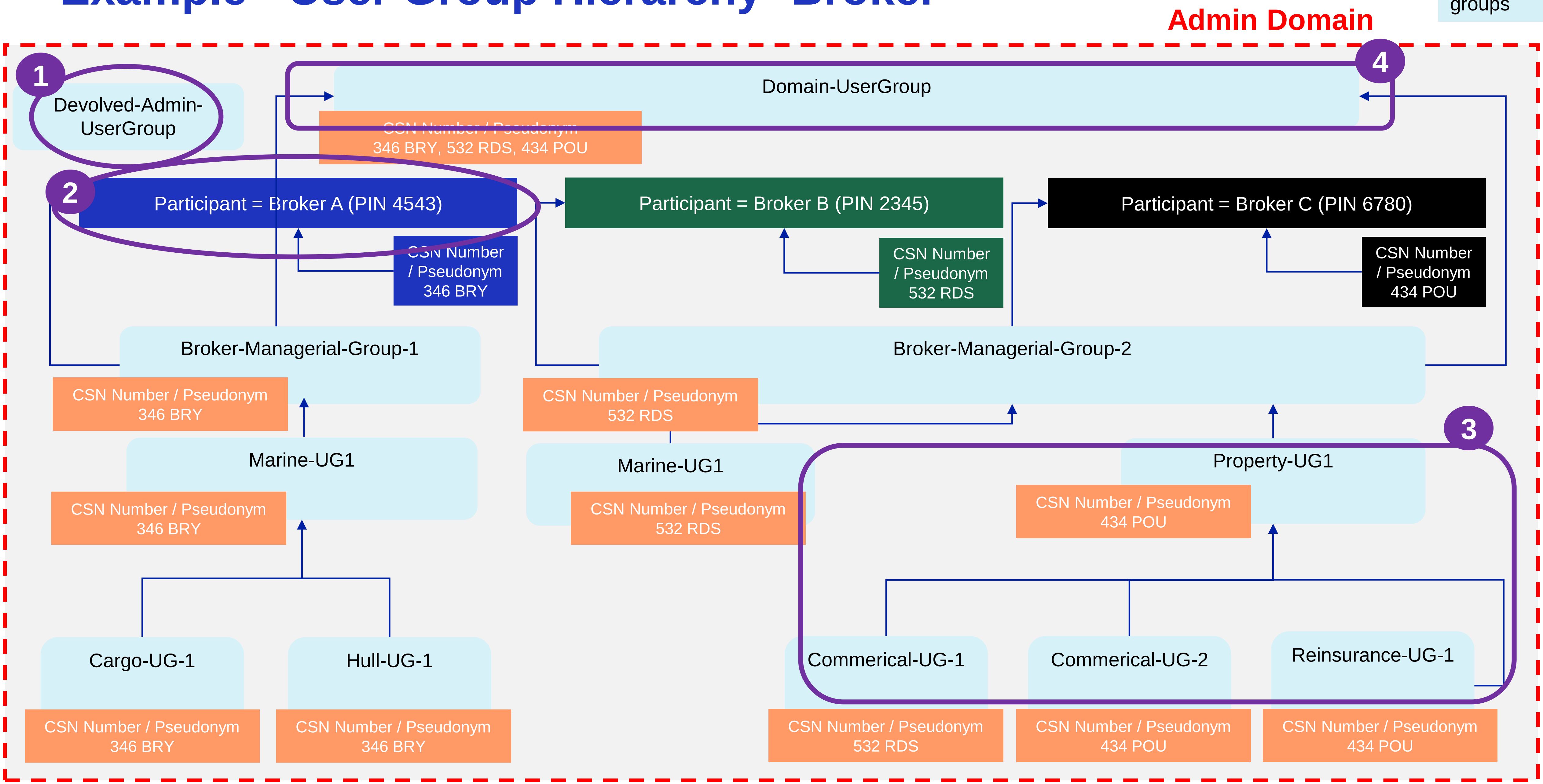
Point 2: This diagram has been created by splitting out the Broker 1 diagram shown earlier (flick to next slide to remind them). As you can see, Broker A has been given its own Admin Domain to ensure complete segregation of registration data **and** Devolved Admins. Organisations will need to assess whether it is completely necessary for your organisation to have multiple admin domains, as similar segregation can still be achieved using a single Admin Domain.

LLOYD'S

Example - User Group Hierarchy- Broker

Names are illustrative

Blue boxes are user groups



Admin Domain
1
Devolved-Admin-UserGroup
4
Domain-UserGroup
CSN Number / Pseudonym
346 BRY, 532 RDS, 434 POU
2
Participant = Broker A (PIN 4543)
CSN Number / Pseudonym 346 BRY
Participant = Broker B (PIN 2345)
CSN Number / Pseudonym 532 RDS
Participant = Broker C (PIN 6780)
CSN Number / Pseudonym 434 POU
Broker-Managerial-Group-1
CSN Number / Pseudonym 346 BRY
Broker-Managerial-Group-2
CSN Number / Pseudonym 532 RDS
Marine-UG1
CSN Number / Pseudonym 346 BRY
Marine-UG1
CSN Number / Pseudonym 532 RDS
3
Property-UG1
CSN Number / Pseudonym 434 POU
Cargo-UG-1
CSN Number / Pseudonym 346 BRY
Hull-UG-1
CSN Number / Pseudonym 346 BRY
Commerical-UG-1
CSN Number / Pseudonym 532 RDS
Commerical-UG-2
CSN Number / Pseudonym 434 POU
Reinsurance-UG-1
CSN Number / Pseudonym 434 POU

Notes to previous slide

In this slide, we can see the exact same user groups as in the previous slide, however they have again been merged into the same Admin Domain but segregation still remains.

- **Point 1:** Only one Devolved Admin User Group is required to manage all users in the Admin Domain. This means that all participants (and the overall organisation) can share administrative resources.

- **Point 2**: **Complete segregation of a participant can still be achieved** through the use of separate Managerial Groups. Broker A has been assigned its own Managerial Group to ensure that Brokers B & C can not view any registration data relating to Broker A.

- **Point 3:** And as we saw earlier, this segregation/control of access to registration data can also be achieved lower down the hierarchy. E.g., Commercial UG1 will be unable to view any registration data in its 'sibling' user groups; Commercial UG2 & Reinsurance UG1; and vice versa. Property UG1, however, will have visibility of all 3 User groups as they are its 'children' user groups, meaning they are directly below it in the User Group hierarchy.

- **Point 4** - If you want to report at domain user group level (e.g. a COO) then in this example they can report across all the user groups as they are part of the same admin domain, whereas in the previous example you would not have been able to report across user groups in multiple admin domains. Please note, adding users to the domain user group is not mandatory. Domain user groups are created by default when Lloyd's set up the admin domain and can be used as required.

FOR ACTION: Onboarding Admin Domain & Registrant and Email (to be submitted by 26th March)

After this briefing call (9th March) Change Leads will be sent the Registrant and Admin Domain email, which will request 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.

- Lloyd's *recommends* that organisations opt for a single Admin Domain, where possible, as segregation 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 entities **and Devolved Admins** is required, with no visibility of registration data between entities.

It is vital that Change Leads engage the Head of Delegated Authorities within their organisation, and work with them to validate which Admin Domains should be setup with internal compliance and legal counterparts, before confirming this to Lloyd's by 26 March.

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 access control across different legal entities.

LLOYD'S

Next steps

- **Review and share** this presentation and the Admin Domain FAQs with your organization's Head of DA, Compliance Officers, Legal and IT representatives. Materials available in the business readiness section of the change lead site.
- **Complete** the Registrant and Admin Domain email which will be sent out today (9th March) – to be completed by 26th March.
- **Attend** the next Access Control Briefing Call on 16th/17th March.
- **Review** the access control and onboarding process and timelines in the appendix.
- **Look out** for invitation to optional weekly access control drop-in sessions (see appendix for dates).
- **Forward** the invite for the next Briefing Call to any relevant internal stakeholders, DA Managers, Compliance Officers, DA Managers, Legal and IT representatives within your organisations.

Appendix

User Group 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 Managerial 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 registration data within your organisation by allowing you to logically group users.
- The system allows you the flexibility to organise your users into structures that reflect how your teams operate day to day.
- It is possible to have multiple user groups at the same level within the hierarchy, and each of these in turn can accommodate a set of lower level ‘child’ user groups. A user can be part of many user groups, at multiple levels in the hierarchy.

Multi-participant organisations with a single Admin Domain

Multi-participant organisations may only require one Admin Domain for the following reasons:

1. Admin domains allow organisations with multiple entities to share administrative resources by having the same Devolved Admins manage their end users.

2. You could have segregation within one Admin Domain by having multiple Managerial Groups for the different participants.

3. If a user is within a User Group that does not have an associated CSN, they will not be able create a registration.

4. It is possible to have multiple ‘sibling’ user groups underneath a managerial group, or layers of ‘parent / child’ groups beneath a managerial group. The total number of layers the system allows is 5, excluding the Domain user group.

5. Each participant and each user can only be part of a single admin domain at a time.

6. Each market participant can only have one managerial group, but one managerial group can be shared across multiple market participants in one admin domain.

7. Users may be given different role types (Read only, Read Write, Read Write Submit) even if within a Domain User Group or Managerial Group. This means that they can still access records for that group, but can only perform the actions that their permissions allow.

8. You have different participant types (Coverholder, Service Company, Broker, MA, Syndicates) within one Admin Domain.

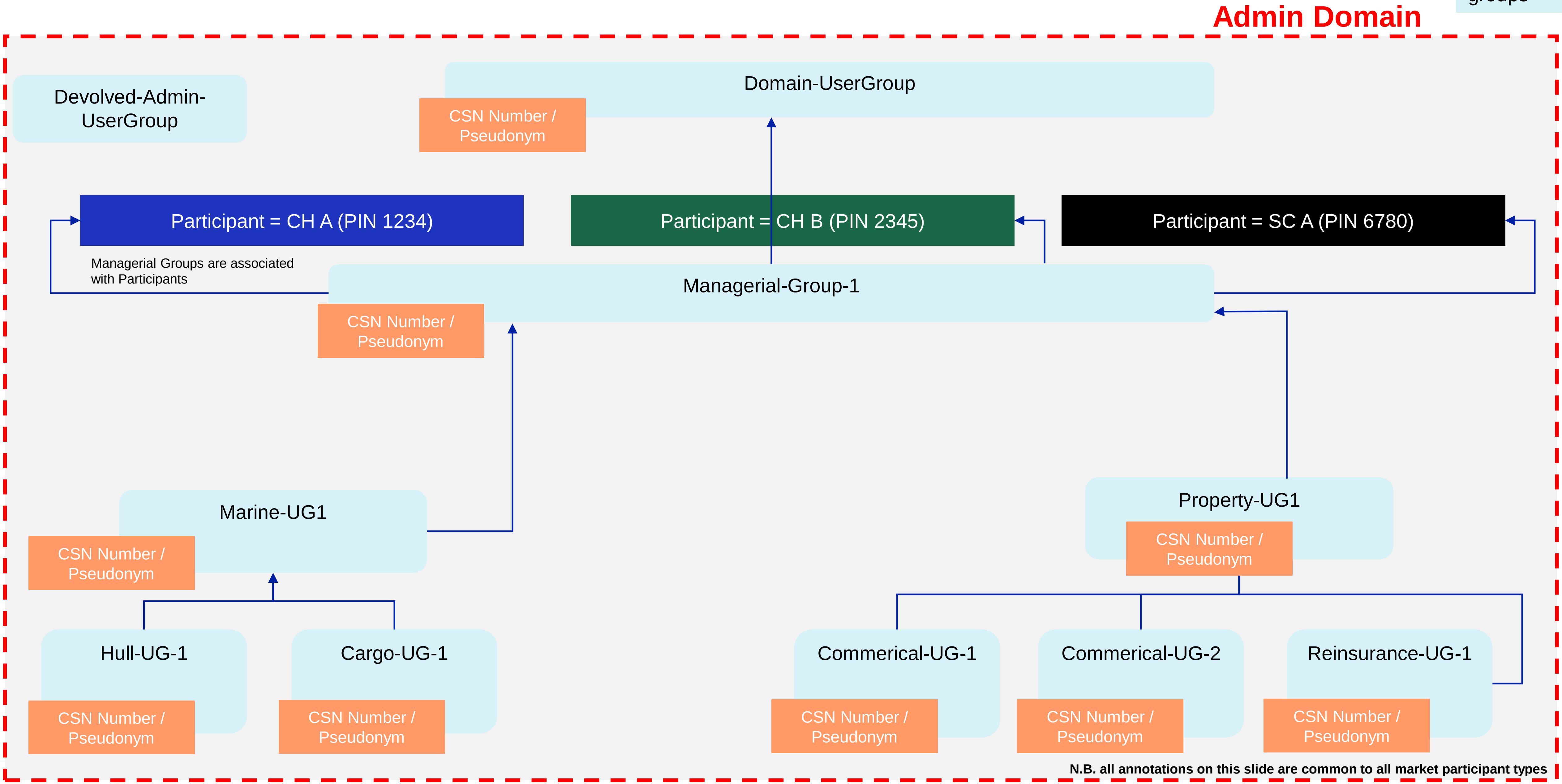
9. Coverholders and Service Companies typically will not have CSNs attributed to them. However, if they do have CSNs they are still able to create registrations.

10. Users will only be able to access records for the user groups to which they belong.

LLOYD'S

Example - User Group Hierarchy (Coverholder/Service Company)

Blue boxes are user groups



Managerial Groups are associated with Participants

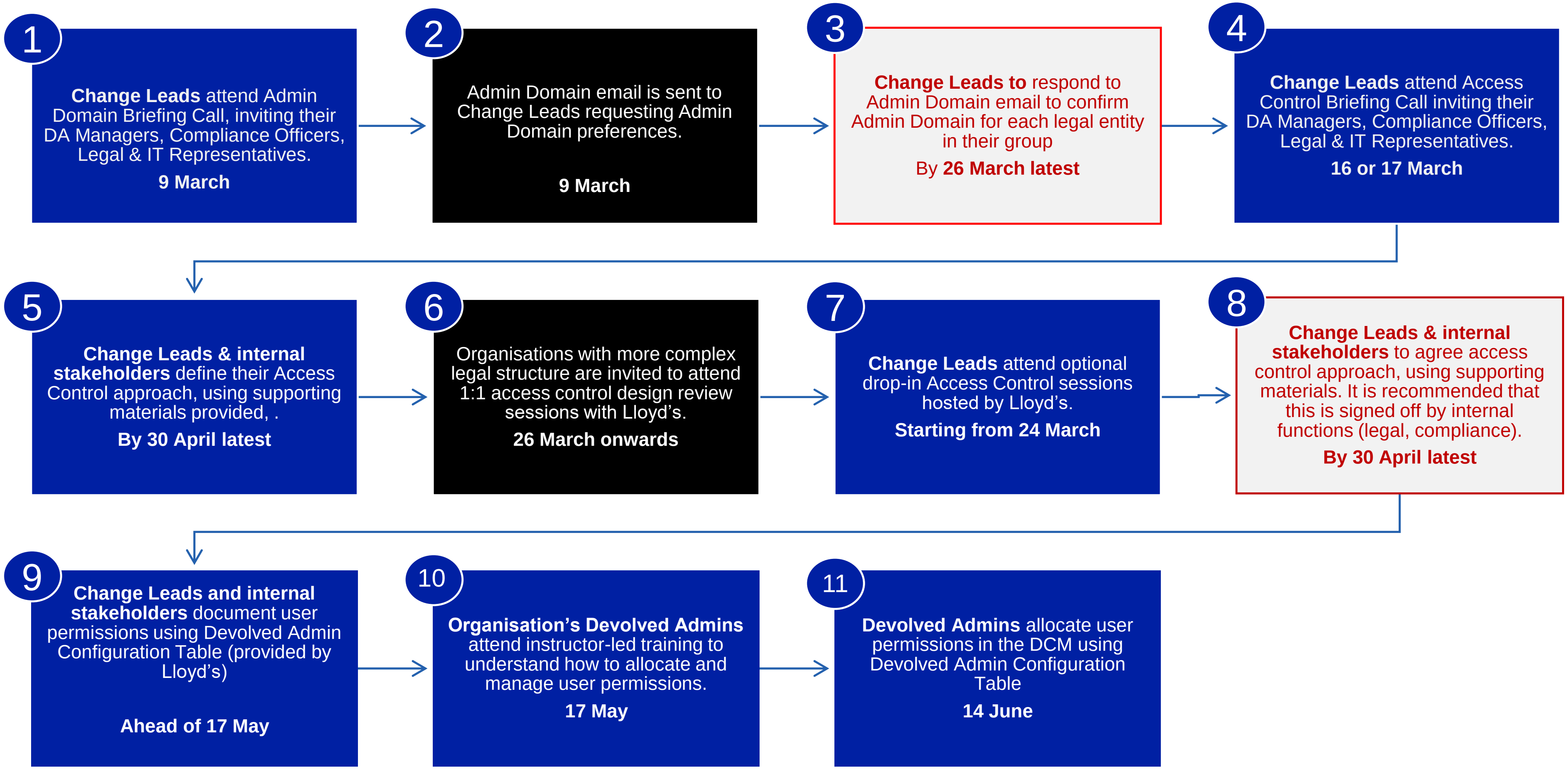
N.B. all annotations on this slide are common to all market participant types

⬛ Action from Lloyd's

🟦 Action for market organisations

🟥 Onboarding Deadline

Access Control Design Process



1 **Change Leads** attend Admin Domain Briefing Call, inviting their DA Managers, Compliance Officers, Legal & IT Representatives.

9 March

2 Admin Domain email is sent to Change Leads requesting Admin Domain preferences.

9 March

3 **Change Leads to** respond to Admin Domain email to confirm Admin Domain for each legal entity in their group

By **26 March latest**

4 **Change Leads** attend Access Control Briefing Call inviting their DA Managers, Compliance Officers, Legal & IT Representatives.

16 or 17 March

5 **Change Leads & internal stakeholders** define their Access Control approach, using supporting materials provided, .

By 30 April latest

6 Organisations with more complex legal structure are invited to attend 1:1 access control design review sessions with Lloyd's.

26 March onwards

7 **Change Leads** attend optional drop-in Access Control sessions hosted by Lloyd's.

Starting from 24 March

8 **Change Leads & internal stakeholders** to agree access control approach, using supporting materials. It is recommended that this is signed off by internal functions (legal, compliance).

By 30 April latest

9 **Change Leads and internal stakeholders** document user permissions using Devolved Admin Configuration Table (provided by Lloyd's)

Ahead of 17 May

10 **Organisation's Devolved Admins** attend instructor-led training to understand how to allocate and manage user permissions.

17 May

11 **Devolved Admins** allocate user permissions in the DCM using Devolved Admin Configuration Table

14 June

Weekly Access Control ‘Drop-In’ Q&A Sessions – Optional

Invites to drop-in Q&A to be issued following the briefing call on 9th March

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

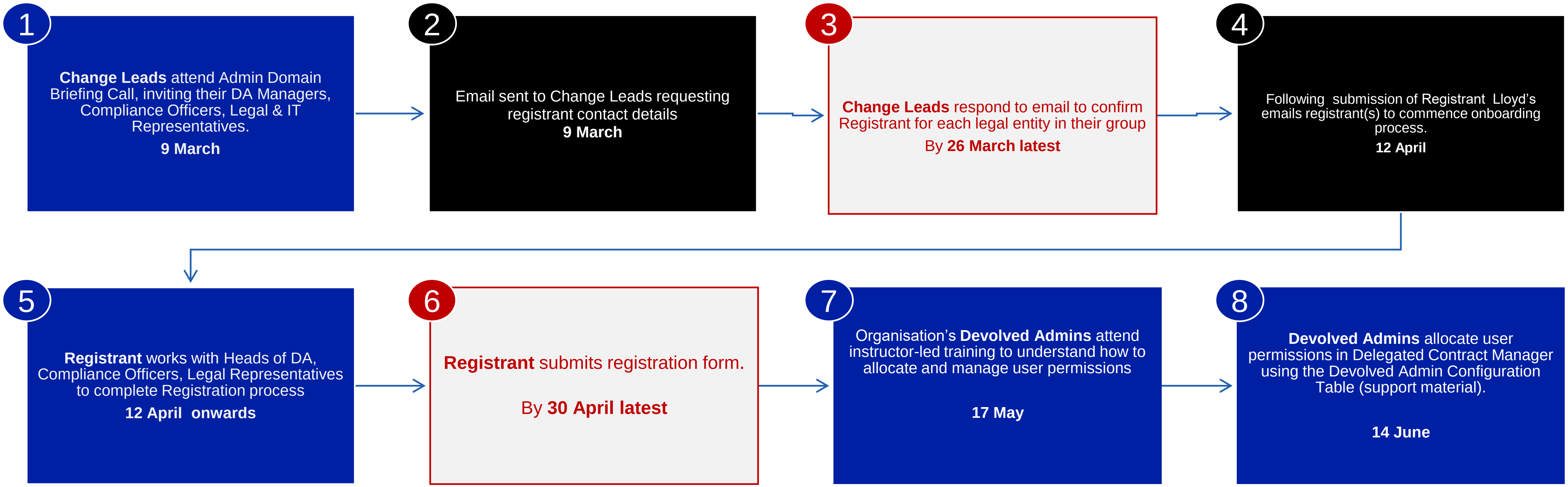
These weekly drop-in Q&A sessions are an opportunity of Change Leads, Compliance Officers, Legal and IT representatives to attend and ask questions that will support the organisations in defining their access control approach.

Onboarding Process

⬛ Action from Lloyd's

🟦 Action for market organisations

🟥 Onboarding Deadline



1 **Change Leads** attend Admin Domain Briefing Call, inviting their DA Managers, Compliance Officers, Legal & IT Representatives.
9 March

2 Email sent to Change Leads requesting registrant contact details
9 March

3 **Change Leads** respond to email to confirm Registrant for each legal entity in their group
By **26 March latest**

4 Following submission of Registrant Lloyd's emails registrant(s) to commence onboarding process.
12 April

5 **Registrant** works with Heads of DA, Compliance Officers, Legal Representatives to complete Registration process
12 April onwards

6 **Registrant** submits registration form.
By **30 April latest**

7 Organisation's **Devolved Admins** attend instructor-led training to understand how to allocate and manage user permissions
17 May

8 **Devolved Admins** allocate user permissions in Delegated Contract Manager using the Devolved Admin Configuration Table (support material).
14 June

Onboarding Process for multi-entity versus single entity

DCM Onboarding Process

	Multi-entity organisation	Single-entity organisation
Organisation	*The parent company of a group of legal entities.*	*An organisation made up of only one legal entity, assuming one admin domain.* If you wish to set up multiple admin domains as a single entity, please contact DAchangesupport@lloyds.com
Admin Domain(s)	• One Admin Domain covering all legal entities • OR multiple Admin Domains if complete segregation (including Devolved Admins) of one or more entities is required.	• In most cases, only one Admin Domain is required for a single-entity organisation. However,
Nominated Registrant	• Each legal entity within the Admin Domain(s) will require its own nominated registrant.	• The single entity will require its own nominated registrant.
Legal Signatory	• Sign the DCM Market User Agreement (MUA) for each legal entity.	• Sign the DCM Market User Agreement (MUA) for the single entity.
Authorised Contact	• Responsible for the creation, approval and management of your organisation's Devolved Administrator(s) per Admin Domain(s).	• Responsible for the approval and management of your organisation's Devolved Administrators.
Devolved Admins	• Each Admin Domain in the organisation will require their own Devolved Admins to allocate user permissions.	• Single Admin Domain has the same Devolved Admins allocating user permissions.

Admin Domain Support Materials

Admin Domain FAQs

To support organization's in determining their Admin Domain, we have provide a list of Admin Domain FAQs in the Communication section of the Change Lead site.

These FAQs will be updated iteratively to include questions asked by the market.

More supporting materials will be provided at the next Access Control Briefing Call on the 16 and 17 March.