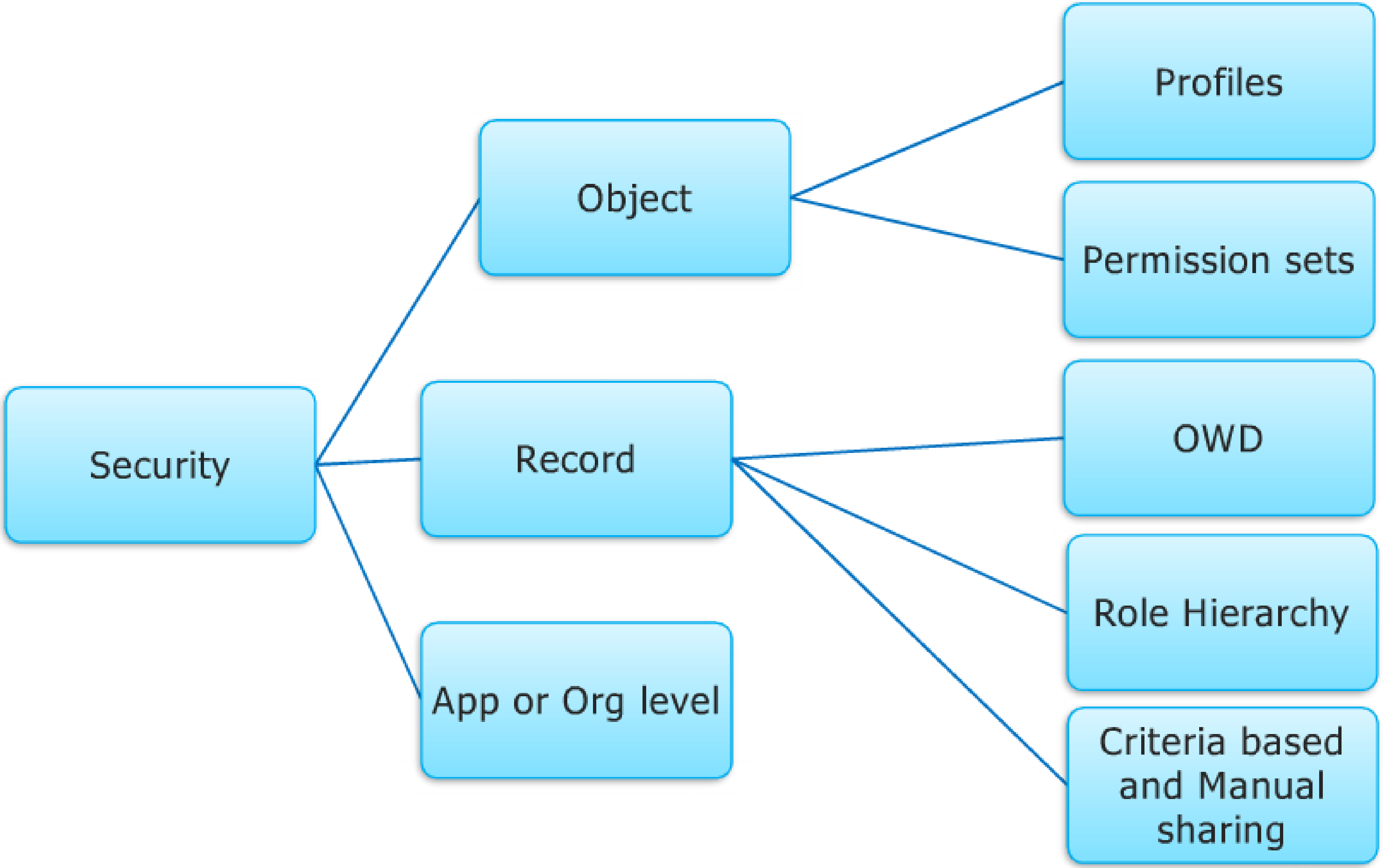
SFDC security model – Part 2

- Object level (Covered in previous slide)
- Record Level
- Field level security

Security Model Mind Map



Security

Object

Record

App or Org level

Profiles

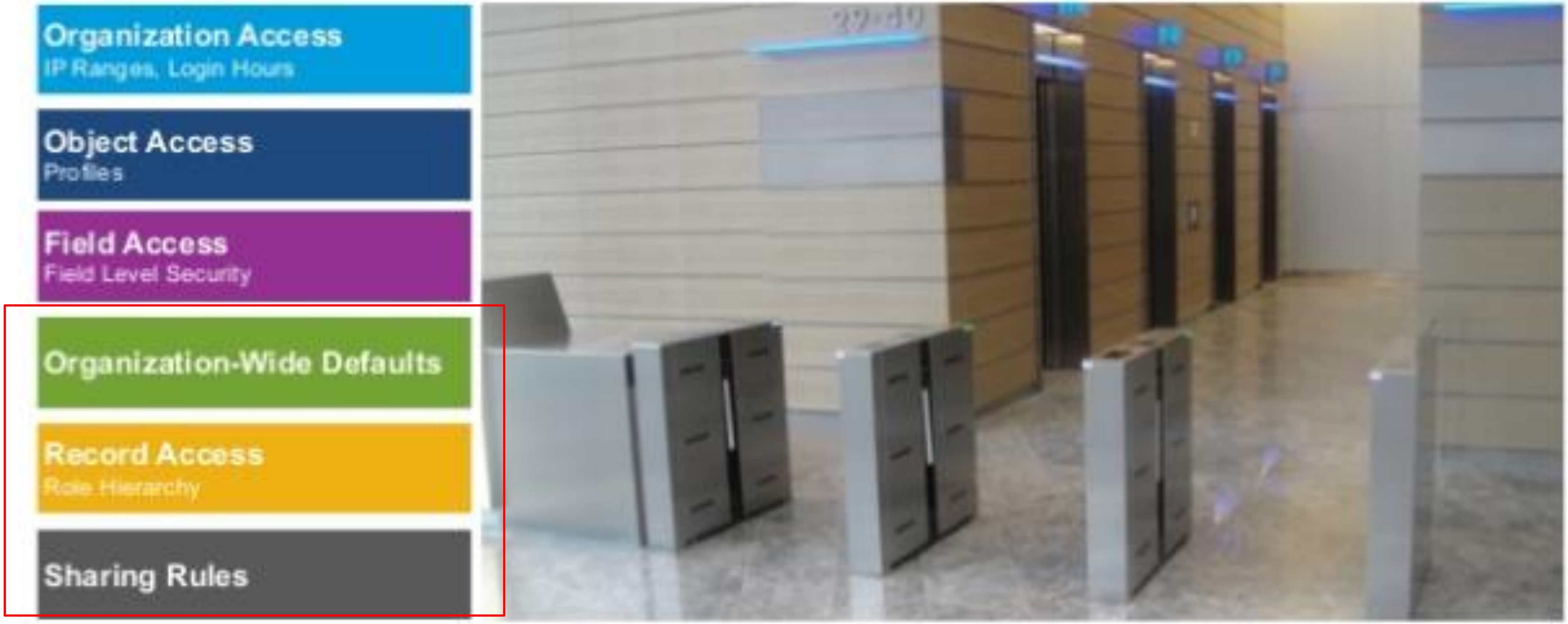
Permission sets

OWD

Role Hierarchy

Criteria based and Manual sharing

Security Settings in Salesforce



Organization Access
IP Ranges, Login Hours

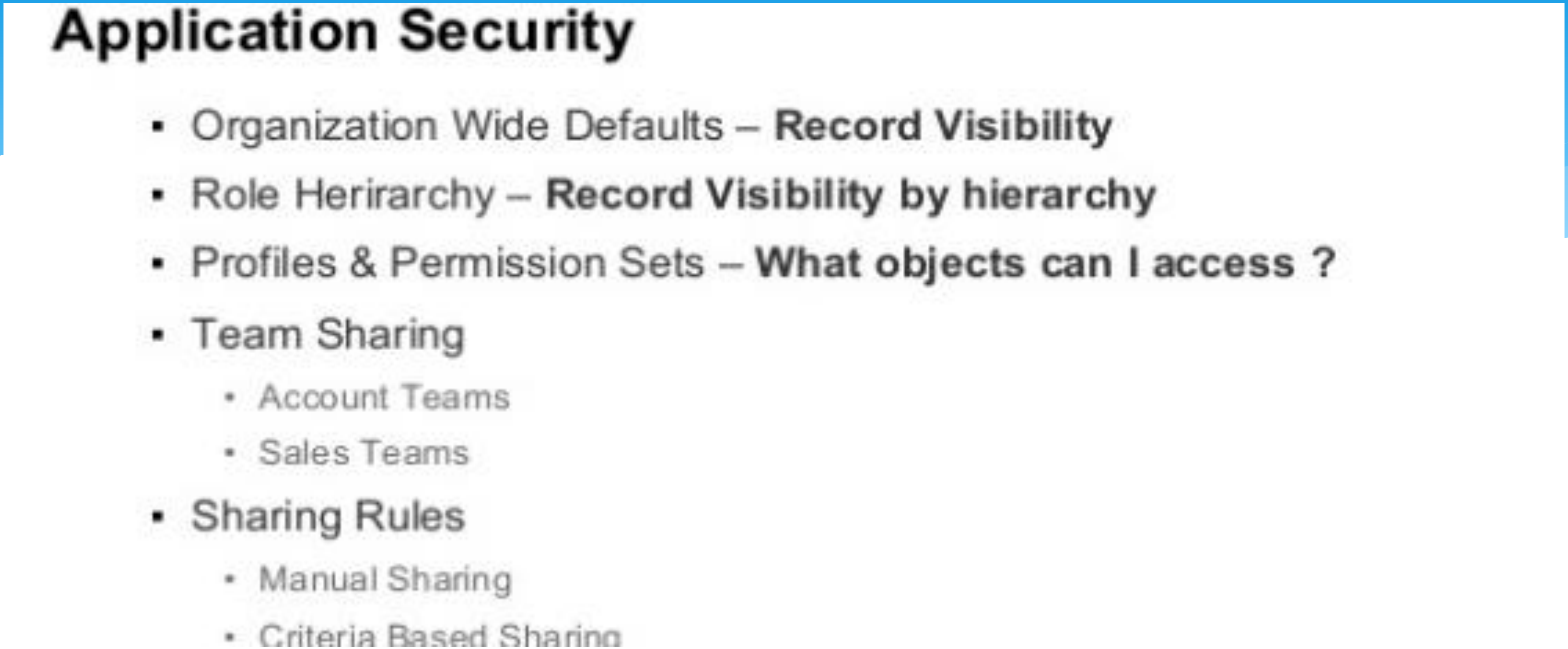
Object Access
Profiles

Field Access
Field Level Security

Organization-Wide Defaults

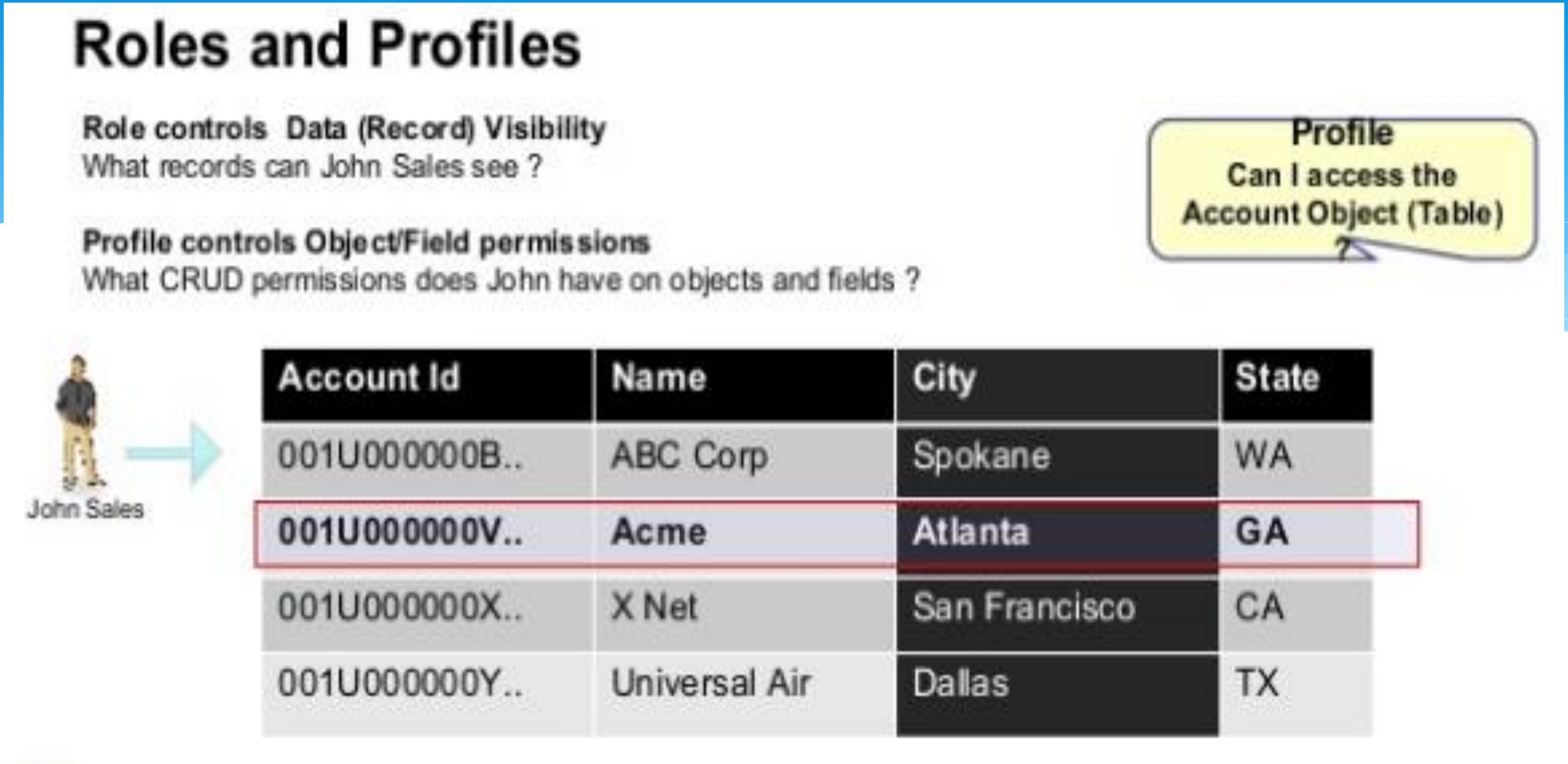
Record Access
Role Hierarchy

Sharing Rules



Application Security

- Organization Wide Defaults – **Record Visibility**
- Role Herirarchy – **Record Visibility by hierarchy**
- Profiles & Permission Sets – **What objects can I access ?**
- Team Sharing
  - Account Teams
  - Sales Teams
- Sharing Rules
  - Manual Sharing
  - Criteria Based Sharing



Roles and Profiles

Role controls Data (Record) Visibility
What records can John Sales see ?

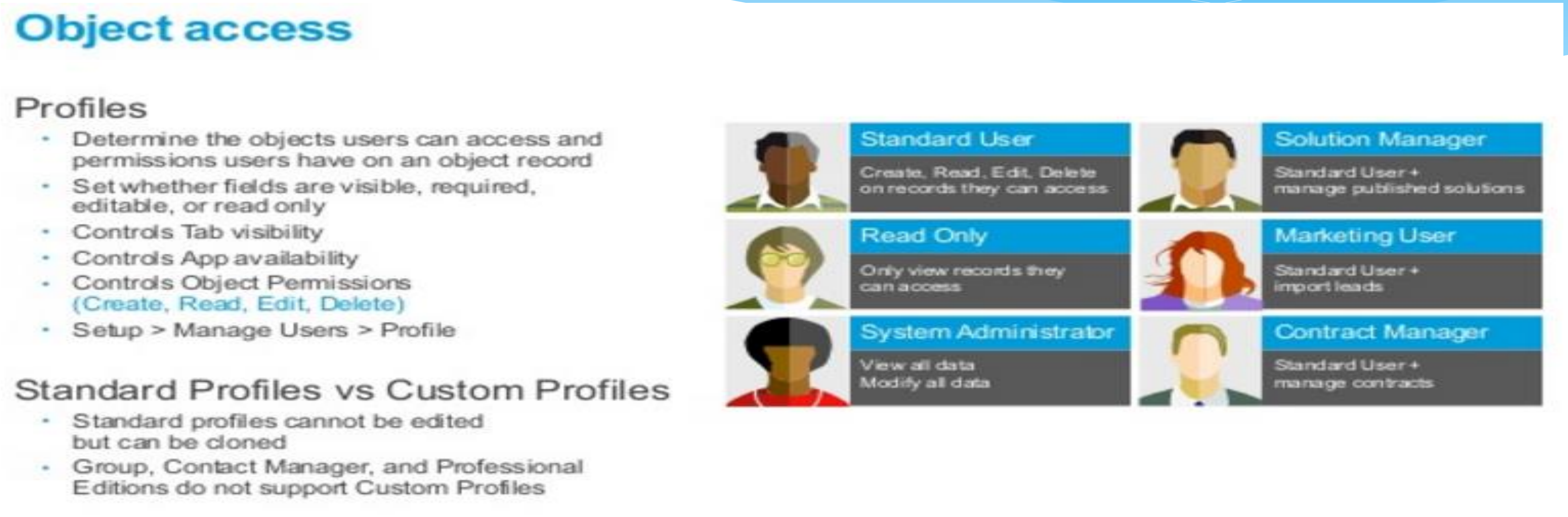
Profile controls Object/Field permissions
What CRUD permissions does John have on objects and fields ?

Profile
Can I access the Account Object (Table)
?

John Sales

Account Id	Name	City	State
001U000000B..	ABC Corp	Spokane	WA
001U000000V..	**Acme**	**Atlanta**	**GA**
001U000000X..	X Net	San Francisco	CA
001U000000Y..	Universal Air	Dallas	TX

Object Level security



Object access

Profiles

- Determine the objects users can access and permissions users have on an object record
- Set whether fields are visible, required, editable, or read only
- Controls Tab visibility
- Controls App availability
- Controls Object Permissions (Create, Read, Edit, Delete)
- Setup > Manage Users > Profile

Standard Profiles vs Custom Profiles

- Standard profiles cannot be edited but can be cloned
- Group, Contact Manager, and Professional Editions do not support Custom Profiles

Standard User
Create, Read, Edit, Delete on records they can access

Solution Manager
Standard User + manage published solutions

Read Only
Only view records they can access

Marketing User
Standard User + import leads

System Administrator
View all data
Modify all data

Contract Manager
Standard User + manage contracts

Field Access

Page Layouts

- Set whether fields are visible, required, editable, or read only

Field-Level Security

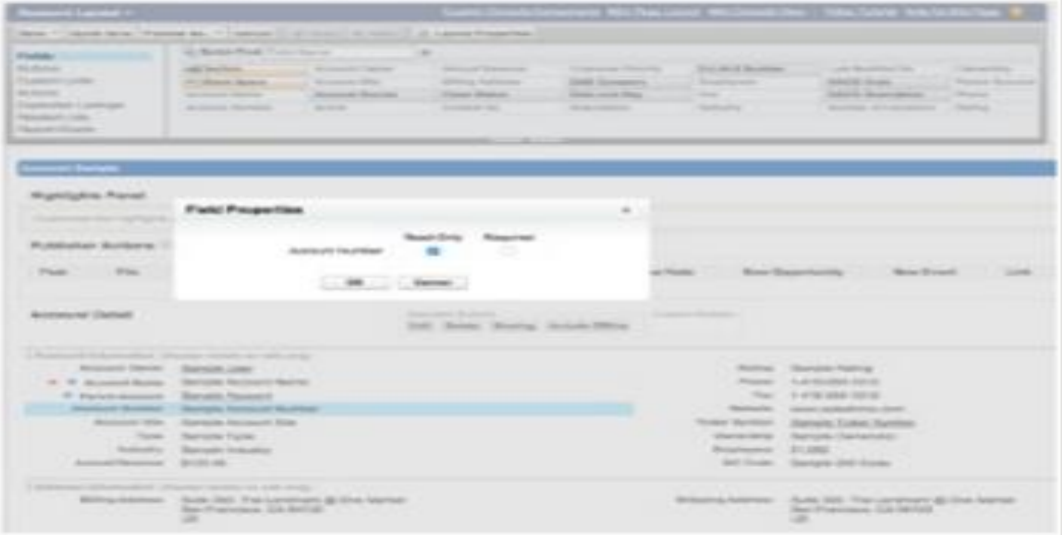
- Further restrict users' access to fields by setting whether those fields are visible, editable, or read only

Permissions

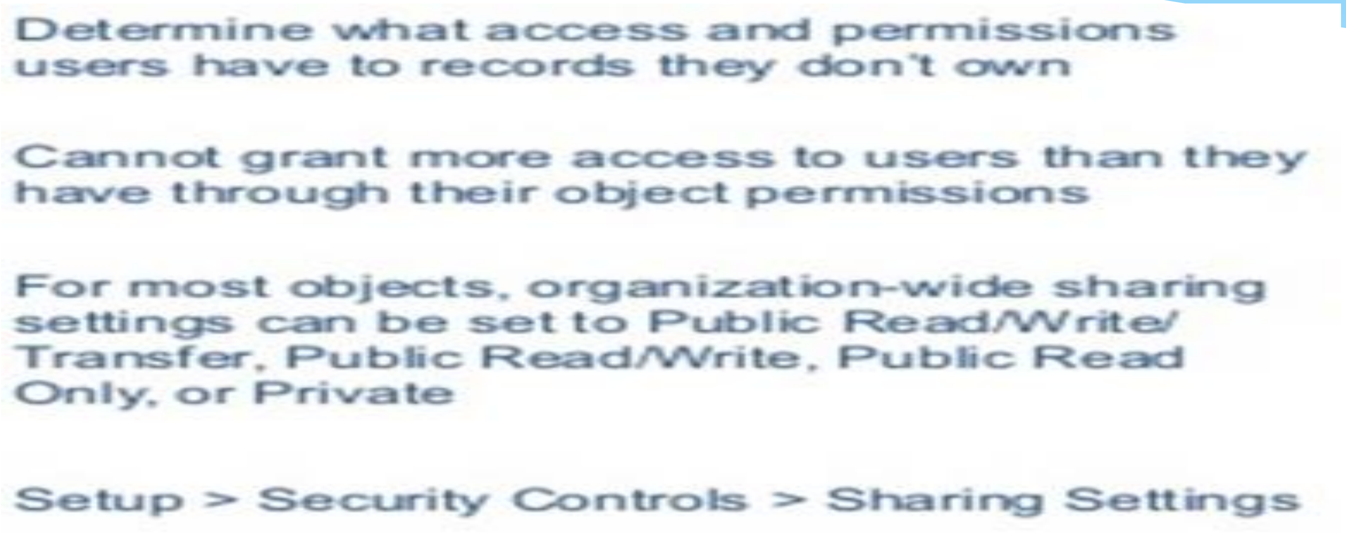
- Some user permissions override both page layouts and field-level security settings. (For example, users with the "Edit Read Only Fields" permission can always edit read-only fields regardless of any other settings)

Universally required fields

- A custom field can be made universally required, which overrides any less-restrictive settings on page layouts or field-level security



Org Wide Defaults



Determine what access and permissions users have to records they don't own

Cannot grant more access to users than they have through their object permissions

For most objects, organization-wide sharing settings can be set to Public Read/Write/ Transfer, Public Read/Write, Public Read Only, or Private

Setup > Security Controls > Sharing Settings

Organisation wide defaults

→OWD decides the basic record level security for users who have access to the object

→OWD decides the access a user has on records the users do not own

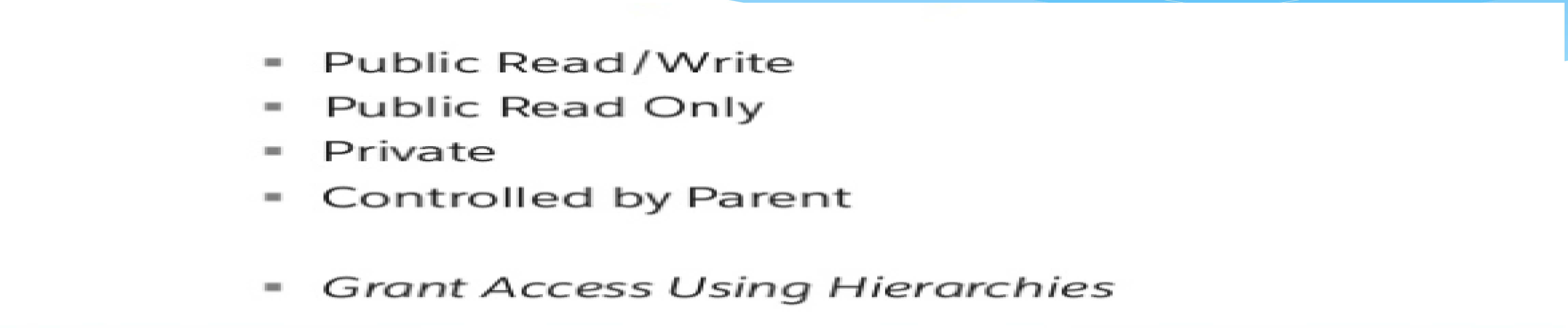
→By default owner of a record will have the access based on the Object level security and other users will have access based on OWD

→Few objects like Lead and Case have Public Read/Write/Transfer

→"Grant Access using Hierarchies" allows the record to be shared with the record owners manager based on Role Hierarchy for all custom objects only. Not available for Standard Objects

→For Objects in a master detail relationship, detail object inherit security of master object. This is not the case in case of lookup

OWD setting for objects



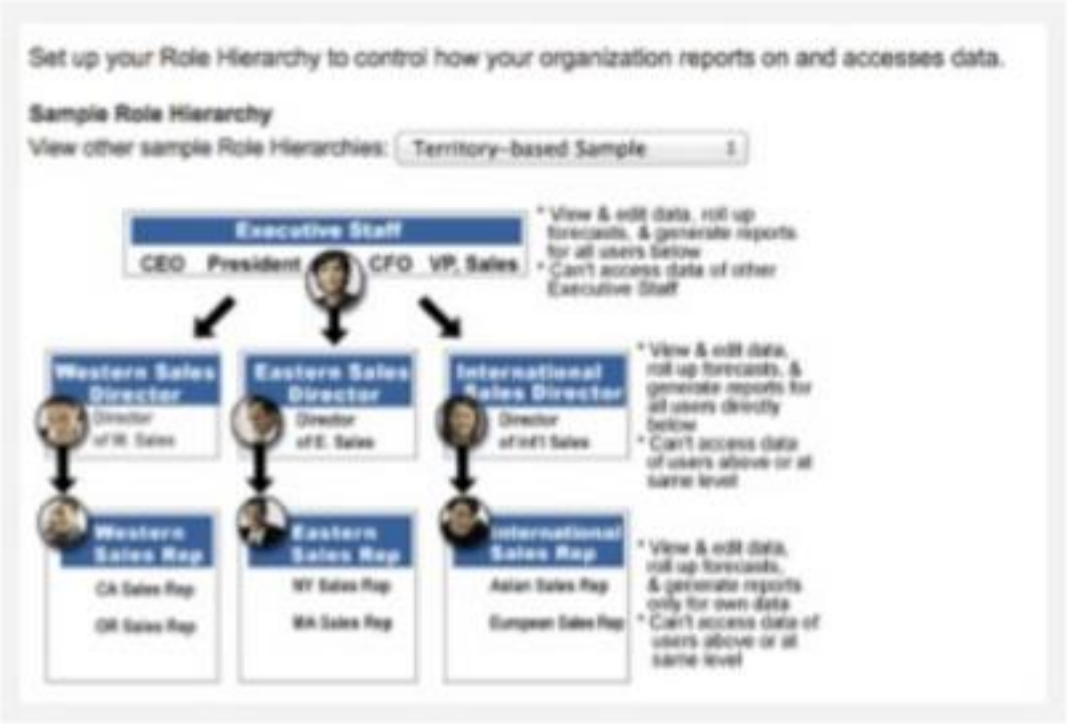
- Public Read/Write
- Public Read Only
- Private
- Controlled by Parent

- *Grant Access Using Hierarchies*

Roles

Role Hierarchy

- Extends access to records when sharing settings are set to anything more restrictive than Public Read/Write
- Cannot restrict record access to less than what is granted through the org-wide defaults
- It is not necessary to create individual roles for each title at your company, rather you want to define a hierarchy of roles to control access of information entered by users in lower level roles
- Setup > Manage Users > Roles



Set up your Role Hierarchy to control how your organization reports on and accesses data.

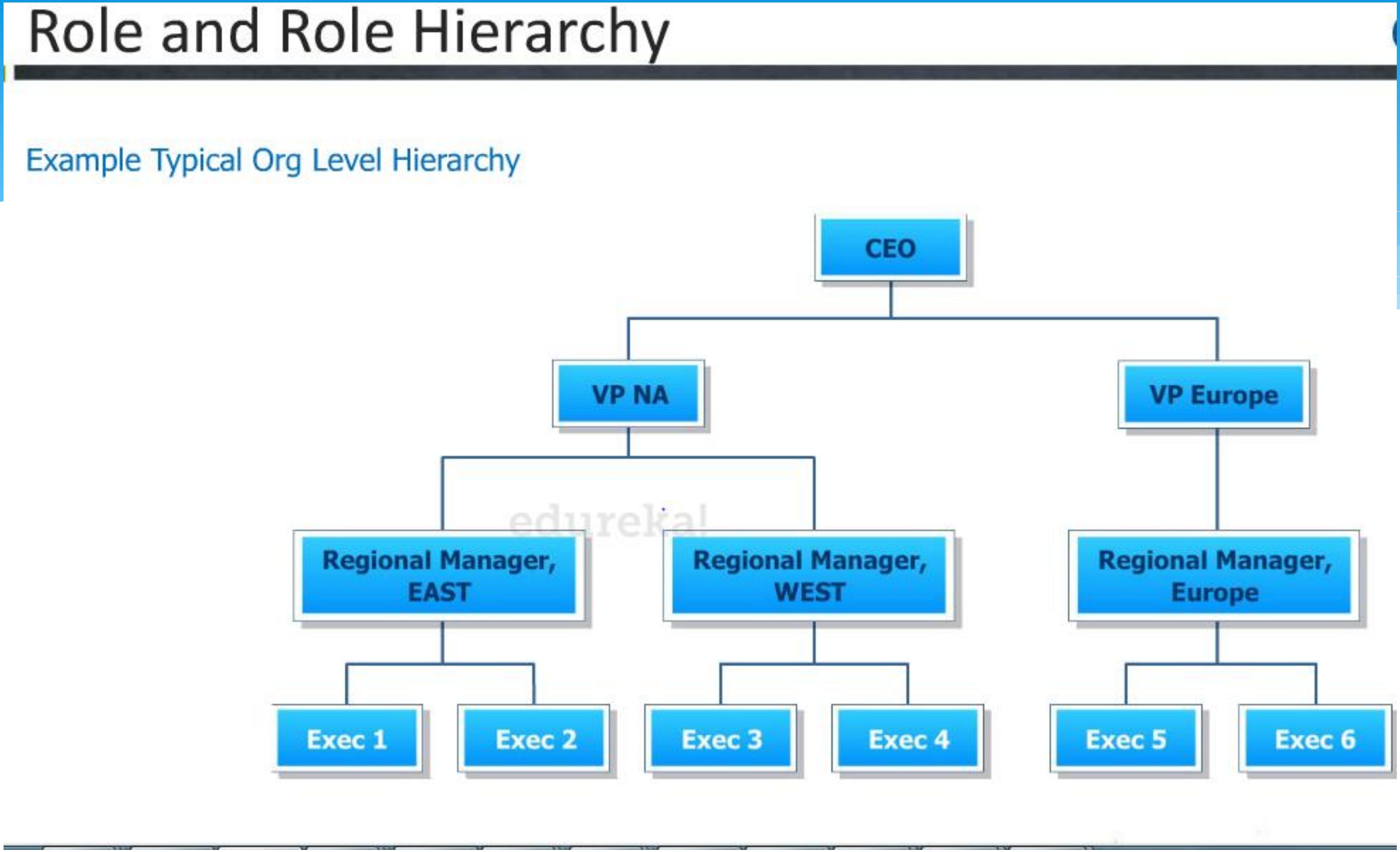
Sample Role Hierarchy

View other sample Role Hierarchies: Territory–based Sample

- View & edit data, roll up forecasts, & generate reports for all users below
- Can't access data of other Executive Staff

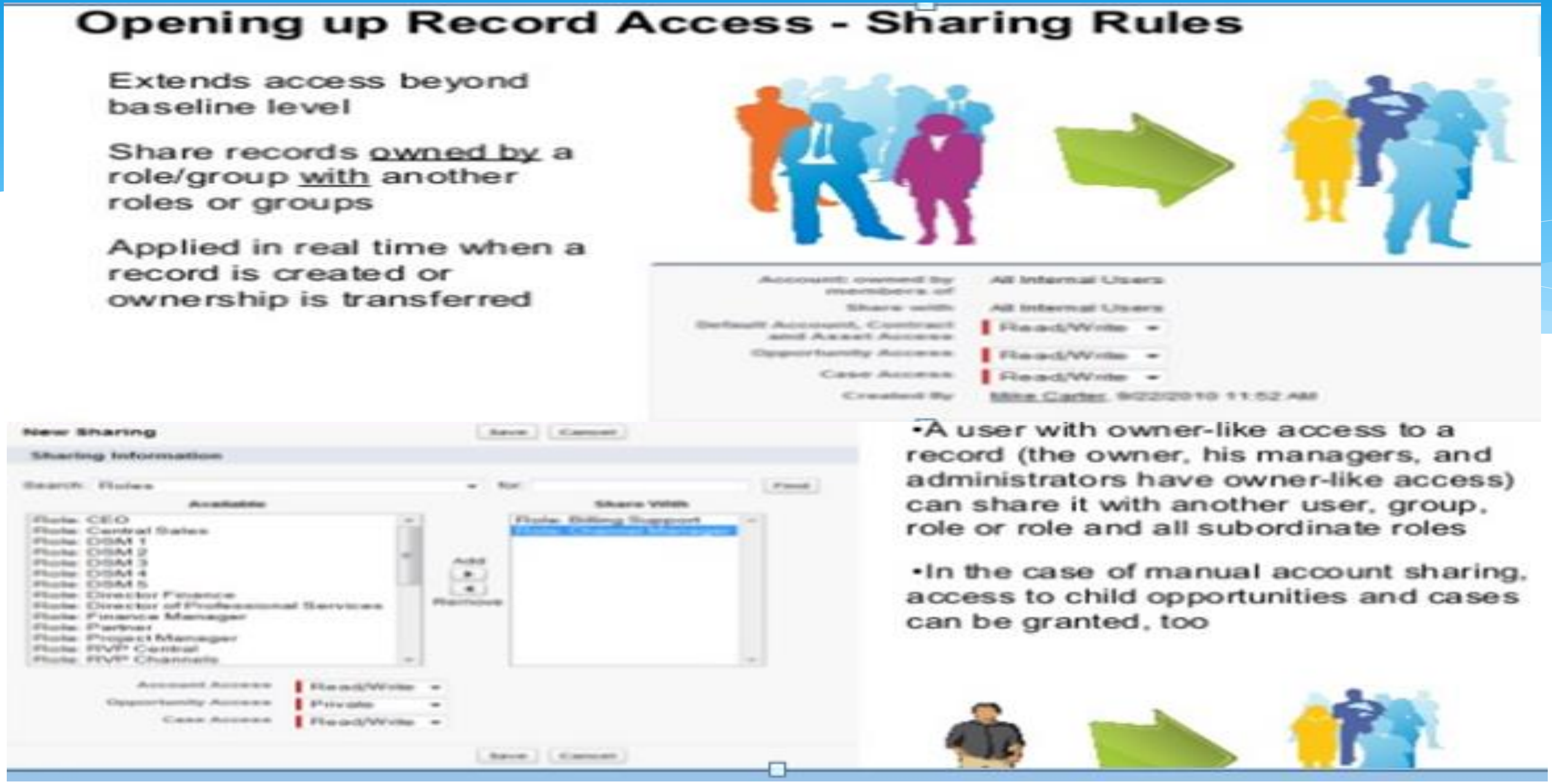
- View & edit data, roll up forecasts, & generate reports for all users directly below
- Can't access data of users above or at same level

- View & edit data, roll up forecasts, & generate reports only for own data
- Can't access data of users above or at same level



Role and Role Hierarchy

Example Typical Org Level Hierarchy



Opening up Record Access - Sharing Rules

Extends access beyond baseline level

Share records owned by a role/group with another roles or groups

Applied in real time when a record is created or ownership is transferred

Account owned by members of: All Internal Users

Share with: All Internal Users

Default Account, Contract and Asset Access: Read/Write

Opportunity Access: Read/Write

Case Access: Read/Write

Created By: Mike Carter, 9/22/2010 11:52 AM

New Sharing

Sharing Information

Search: Roles for:

Available:
Role: CEO
Role: Central Sales
Role: DSM 1
Role: DSM 2
Role: DSM 3
Role: DSM 4
Role: DSM 5
Role: Director Finance
Role: Director of Professional Services
Role: Finance Manager
Role: Partner
Role: Project Manager
Role: RVP Central
Role: RVP Channels

Share With:
Role: Billing Support
Role: Channel Manager

Account Access: Read/Write

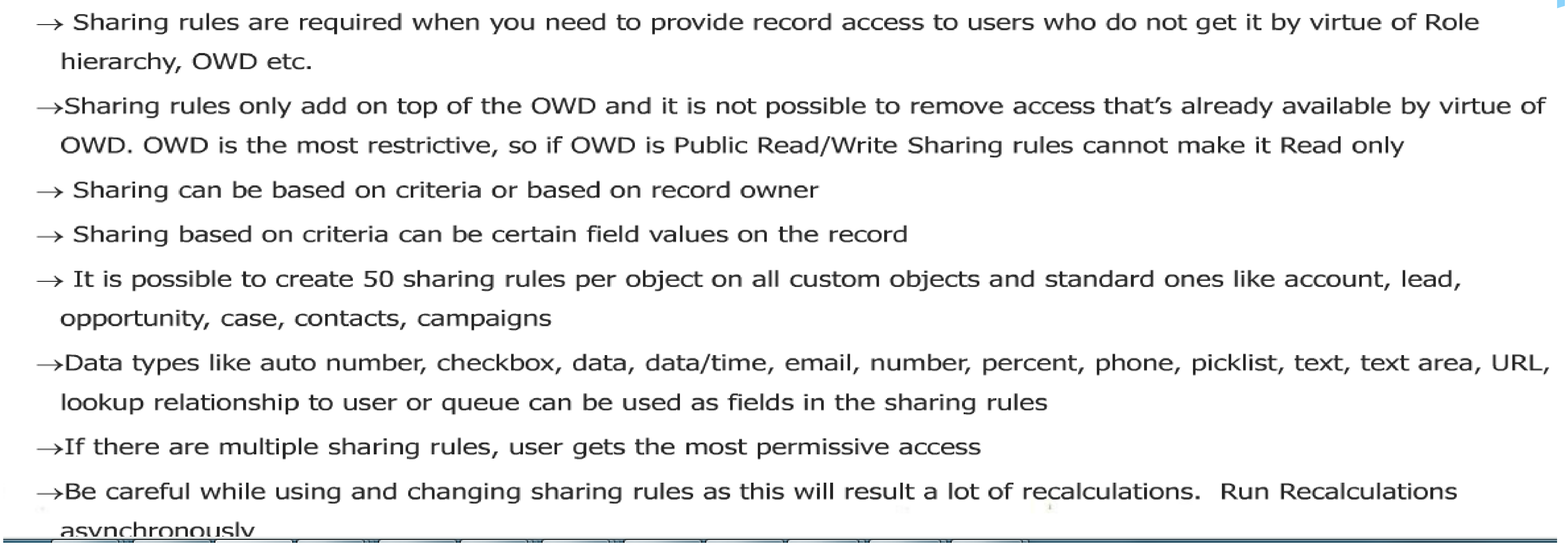
Opportunity Access: Private

Case Access: Read/Write

- A user with owner-like access to a record (the owner, his managers, and administrators have owner-like access) can share it with another user, group, role or role and all subordinate roles

- In the case of manual account sharing, access to child opportunities and cases can be granted, too

Criteria based sharing rules



→ Sharing rules are required when you need to provide record access to users who do not get it by virtue of Role hierarchy, OWD etc.

→Sharing rules only add on top of the OWD and it is not possible to remove access that's already available by virtue of OWD. OWD is the most restrictive, so if OWD is Public Read/Write Sharing rules cannot make it Read only

→ Sharing can be based on criteria or based on record owner

→ Sharing based on criteria can be certain field values on the record

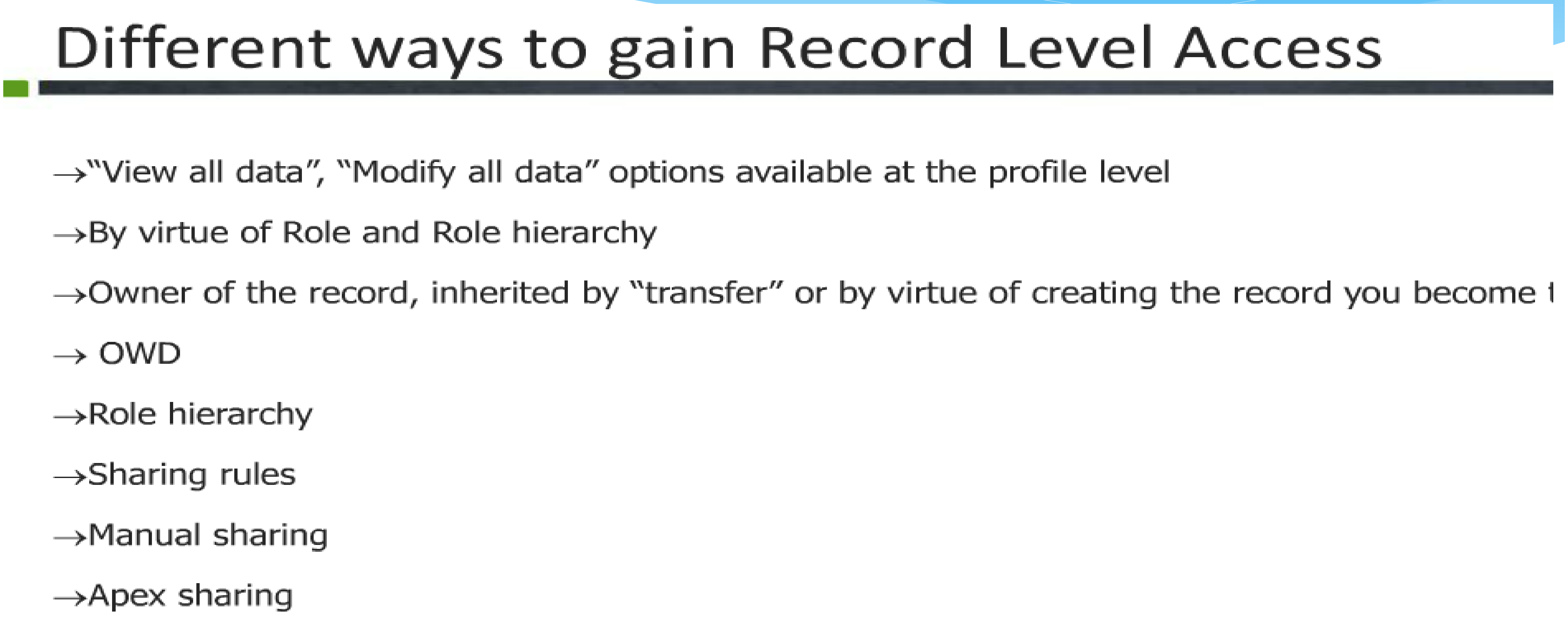
→ It is possible to create 50 sharing rules per object on all custom objects and standard ones like account, lead, opportunity, case, contacts, campaigns

→Data types like auto number, checkbox, data, data/time, email, number, percent, phone, picklist, text, text area, URL, lookup relationship to user or queue can be used as fields in the sharing rules

→If there are multiple sharing rules, user gets the most permissive access

→Be careful while using and changing sharing rules as this will result a lot of recalculations. Run Recalculations asynchronously

Who Owns a Record (Basic record Access Access)



Different ways to gain Record Level Access

→“View all data”, “Modify all data” options available at the profile level

→By virtue of Role and Role hierarchy

→Owner of the record, inherited by “transfer” or by virtue of creating the record you become

→ OWD

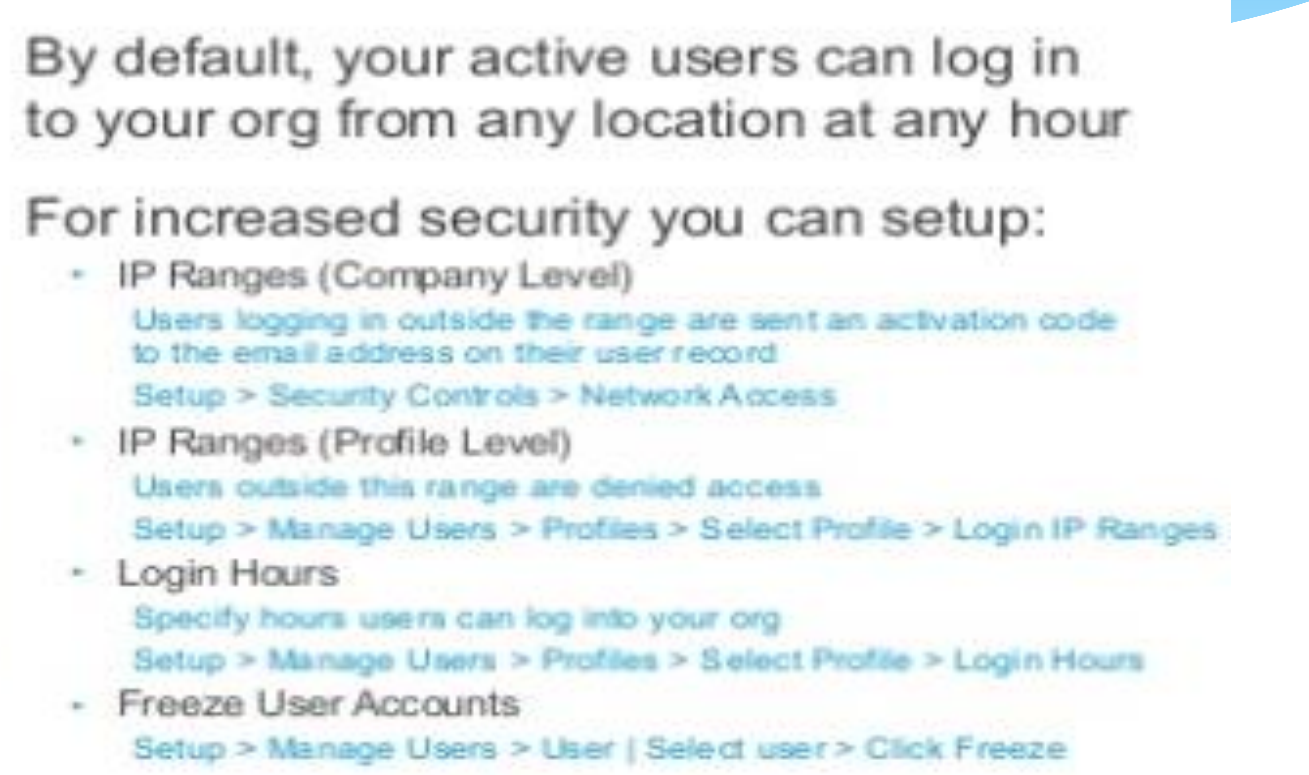
→Role hierarchy

→Sharing rules

→Manual sharing

→Apex sharing

Org Access



By default, your active users can log in to your org from any location at any hour

For increased security you can setup:

- IP Ranges (Company Level)

  Users logging in outside the range are sent an activation code to the email address on their user record

  Setup > Security Controls > Network Access
- IP Ranges (Profile Level)

  Users outside this range are denied access

  Setup > Manage Users > Profiles > Select Profile > Login IP Ranges
- Login Hours

  Specify hours users can log into your org

  Setup > Manage Users > Profiles > Select Profile > Login Hours
- Freeze User Accounts

  Setup > Manage Users > User | Select user > Click Freeze

→In case of student app, we can look at defining OWD requirements for all objects. Main object is Student Master and others will inherit requirements

→As far Student master is concerned students have read access to object and their own record. We can do with OWD as PRIVATE

→Access to other users can be opened up using other features like criteria based sharing, Role and Role Hierarchy

OBJECT	PRINCIPAL	PROFESSOR	STUDENT	SYSADMIN	OWD	LEGEND
STUDENT MASTER	CRUD	CRU	R	CRUD,VA,MA	PRIVATE	CRUD-CREATE, READ, UPDATE, DELETE
STUDENT GRADES	CRUD	CRU	R	CRUD,VA,MA	PRIVATE	VA-VIEW ALL
STUDENT REQUESTS	CRUD	CRU	CRU	CRUD,VA,MA	PRIVATE	MA - MODIFY ALL