**Practice this only in Service-Now Demo instance**

**Roles and ACL**

**Pre Requisite**

1. Create a new group “ITIL Grp1”.Add 3 users to this group.Give ITIL role to this group.
2. Create a new group “ITIL Grp2”.Add 3 users to this group.Give ITIL role to this group.
3. Create a new group “End User Grp” with no roles. Add 3 users to this Group.
4. Open the incident form. Create a ACL rules

**Assignment**

**Record Level**

All the fields should be editable for “ITIL Grp1” when incident is ACTIVE.

(Hint :- read ,write ACL)

**Field level**

* “Work notes” field should be editable only to “ITIL Grp1”
* Additional comments should be editable to both “ITIL Grp1” and “End User Grp”.
* “Assigned to” field should be editable only to members of the “Assignment group”.

Hint :- write ACL)

* Create an ACL to allow visibility of “**State”** field only to “ITIL Grp1”.

(Hint :- Read ACL) .

PS :- Verify by impersonating ITIL Grp2 members that state field in not visible to

Members of this group when incident is active.

**List View Level**

* Create a ACL on the incident table such that Configuration Item, Assignment group and Assigned to fields should not be editable to any role from list view(list layout).Only admins should be able to edit these fields from list view.

(Hint :- List\_edit ACL)