# ibas 权限设置说明

## 权限

### 概念

系统中的权限按控制对象分为数据权限和功能权限两大类，按权限级别分为完全、只读和无三级。

具体来说，数据权限为系统用户是否可以对系统中现有数据（BO对象）进行查询和保存操作的控制。拥有完全权限即可以查询到数据，并且可以对查询到的数据进行修改保存；只读权限即可以查询到数据，但是不能修改查询到的数据；无权限即查不到数据也不能对数据进行修改。

功能权限为系统用户是否可以主动打开系统应用的控制。完全权限即可以在系统导航位置找到直接进入系统应用的入口，可以打开对应系统应用的操作界面；只读权限会隐藏系统导航位置的应用入口，但如果其他应用如果调用该应用，仍然可以打开对应系统应用的操作界面；无权限即系统导航位置没有应用入口，也不允许其他应用调用该应用。

### 原理

数据所有者：根据数据DataOwner字段找到对应的系统用户为当前数据的所有者。

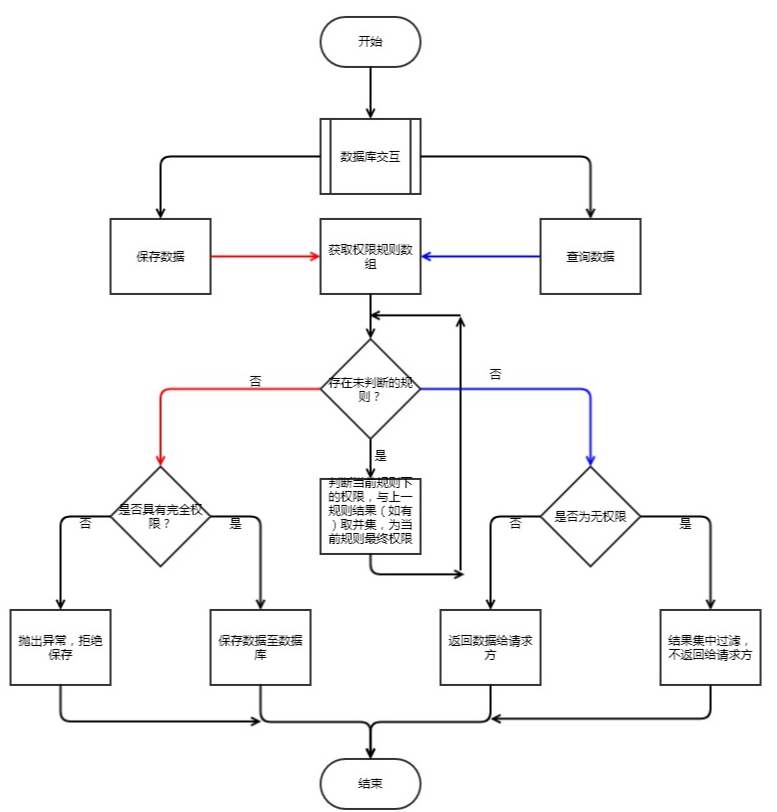
团队成员：根据数据TeamMembers字段找到的所有系统用户为当前数据的团队成员。

系统内置若干规则，管理员针对特定用户和数据类型设置每个规则具有的权限，在数据查询或保存时，依次判断各规则下当前用户的权限。

现有规则如下：

1. 自身权限：当前用户等于数据所有者 适用此规则
2. 岗位权限：根据系统中岗位设置，当前用户等于数据所有者的上级、下级或同级，适用此规则
3. 项目权限：根据数据的所属项目，当前用户为项目的项目经理或项目成员，适用此规则
4. 审批权限：如当前数据存在审批请求，且当前用户为审批请求的某一审批步骤所有者，适用此规则
5. 其他权限：上述规则都不适用的，适用此规则

备注：如数据同时满足上述规则中的多条规则，则取其并集为当前用户对此数据的最终权限。



岗位设置 ([参考地址](https://wenku.baidu.com/view/7331a99358fafab068dc0229.html))

### 职位

即工作（Job）,它是指企业员工所从事工作的类别。

职务由一组主要职责相似的职位（或岗位）所组成，是指承担一系列工作职责的某一任职者所对应的组织位置，它是组织的基本构成单位，它是由实现企业职能的一个个具体活动所构成的相对独立体。比如会计、研发、顾问、质检员等。

### 岗位

即具体位置（Position）,它是指在一个特定的企业组织中、在一个特定的时间内、由一个特定的人所担负的一个或数个任务所组成。

简单地讲，岗位与任职者一一对应。这里强调的是“组织位置”，也就是说，岗位是组织的一个节点，因为组织工作（业务）层次或工作（业务）流程流转的需要而存在，是指企业的某个员工需要完成的一个或一组任务。

### 职位与岗位的关系

岗位与人对应，只能由一个人担任，一个或若干个岗位的共性体现就是职位，即职位可以由一个或多个岗位组成。

### 系统实现

系统设置职位表和岗位表，岗位表按照公司组织架构上下级关系设置，每个岗位需要先选择职位，并指定用户，用户可以同时担任多个岗位。



项目表为主子结构，主表为项目基本信息，包含项目负责人，子表指定项目成员。



权限一般只与职位关联，不与岗位关联，对于个别例外情况，应在用户上设置权限，用户的最终权限为用户的权限加上用户所对应职位的权限。



问题

1. 项目上设权限，不同项目权限不同
2. 各个规则权限之间取并集？

模拟场景:

用户A填报销单，一般情况下上级B可以看到A的所有报销单，故设置用户A的岗位-上级权限为只读（或完全）。

用户A同时属于一个项目P的项目成员，上级B不属于此项目，项目权限设置为非项目成员不能看到此项目的报销单，故设置项目-非项目成员权限为无。

现A填了一张项目P的报销单，若权限取并集，B应该可以看到A的这张单据。

若想逻辑按照项目-非项目成员权限为无执行，让B看不到报销单，权限不能简单取并集。