

权限模块：不是难，是你们没有认真分析，思考；包括几个关键点，大家思考下？

**权限管理**是一个几乎所有后台系统的都会涉及的一个重要组成部分，主要目的是对整个后台管理系统进行权限的控制，而针对的对象是员工，避免因权限控制缺失或操作不当引发的风险问题，如操作错误，数据泄露等问题。其实权限管理的设计并不难，就目前来说最广泛的是一个账号对应多个角色，每个角色对应相应的权限集（RBAC模型）这种模型基本可以应对所有的问题，且通过角色可以实现灵活且多样的的权限操作需求，我们梳理一下上面主要提到的几个名词：账号、角色、权限。

**账号的定义：**每个员工想要进入系统肯定都会有一个账号，而这个账号就是一把钥匙。我们通过控制账号所具备的权限，进而控制这个员工的授权范围。因此需要告诫员工，账号密码不能轻易提供他人，不然遇到的问题由自己承担。

**角色的定义：**角色管理是确定角色具备哪些权限的一个过程，他是一个集合的概念，是众多最小权限颗粒的组成。我们通过把权限给这个角色，再把角色给账号，从而实现账号的权限，因此它承担了一个桥梁的作用。引入角色这个概念，可以帮助我们灵活的扩展，使一个账号可以具备多种角色。

角色的命名最好按照职位而定，例如市场部普通员工，市场部主管等。因为职位在任何企业都是存在的，且是有限的，并且容易理解，市场部文员那就是市场部文员角色，方便我们配置权限时的判断，避免配置错误。

**权限定义：**权限可以分为三种：页面权限，操作权限，数据权限。

页面权限控制你可以看到哪个页面，看不到哪个页面，很多系统都只做到了控制页面这一层级，它实现起来比较简单，一些系统会这样设计，但是比较古板，控制的权限不精细，难以在页面上对权限进行更下一层级的划分。

操作权限则控制你可以在页面上操作哪些按钮。（延伸：当我们进入一个页面，我们的目的无非是在这个页面上进行增删改查，那在页面上对

应的操作可能是：查询，删除，编辑，新增四个按钮）可能你在某个页面上，只能查询数据，而不能修改数据。

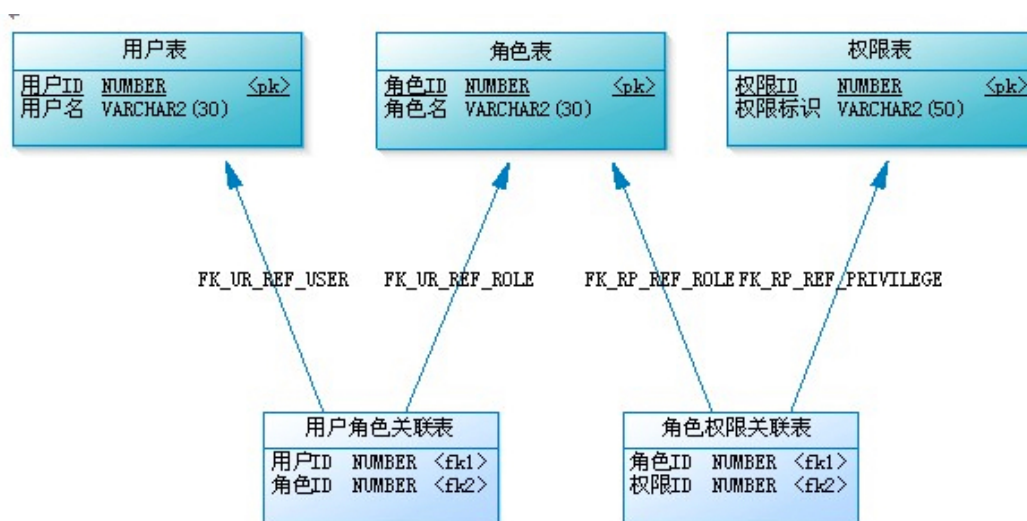
数据权限则是控制你可以看到哪些数据，比如市场A部的人只能看到或者修改A部创建的数据，他看不到或者不能修改B部的数据（延伸：数据的控制我们一般通过部门去实现，每条记录都有一个创建人，而每一个创建人都属于某个部门，因此部门分的越细，数据的控制层级也就越精细，这里是否有其他好的方式除了部门这个维度还有其他什么方式可以控制数据权限，大家可以提出来探讨一下）。

哪个页面要放置哪些权限，完全根据业务需要配置，你只需要把控制权限的地方列出来交给开发就好。

权限列表即树状图谱，权限可对整个页面及页面内的数据、按钮等做限制；

用户角色，包含系统管理员、部门管理员、普通用户；

用户权限，可根据部门划分，可根据用户特殊需求进行赋权；



（图：RBAC权限模型）

1. 树状权限分级结构图：技术人员将开发好的页面或功能配置到权限体系，以树状图进行展示即可；
2. 角色及权限配置：选择系统，查看不同系统的权限角色；角色可以权限管理员添加，不同级别管理员可以设置不同权限的角色，不同级别管理员可以查

看不同级别角色列表；权限系统可适用于单个系统和多系统的权限配置；在角色列表中可以对角色进行修改、删除、查看&添加人员；

- a. 新建角色：包括系统管理员、部门管理员、普通用户，在各个角色中进行权限列表的授权，授权后分配到该角色的用户拥有该角色的所有权限；角色只能有权限管理员进行添加；
- b. 修改角色权限：可对角色类型、角色名称、角色权限进行重新调整；
- c. 删除角色权限：需要提示该角色还有人员，是否强制删除，删除后该人将不再拥有该权限。如果角色不想用或者取消了，你可以将角色设置为无效状态，账户获取角色时会首先判断角色是否有效；
- d. 查看角色权限：点击进入查看页面；
- e. 查看权限人员：

- i. 可查看拥有该权限的人员列，里面可以查询到或者添加到所有的人，管理员可对列表人员进行删除操作，（为什么说添加，因为很多大公司有很多的管理系统，而每一个管理系统只有一部分人用，所以不会把所有人在账户列表显示出来，故用到了添加）；这里需要注意的是账号的禁用，用于防止员工离职后的问题。可以跟人事系统打通，人事那边设置某员工离职后，所有系统账号自动设为禁用。可在该页面进行人员添加，从便捷性上可以提供一个功能批量给某角色添加账户，在新员工入职时特别是同一岗位的，设置的权限时效率会大大提升；

### 3. 个人权限查看：

- a. 查看页面：员工基本信息说明，及拥有的树状权限图谱（不同系统，树状分级展示）；

### 4. 单个权限配置：

- a. 配置页面：选择系统及对应的权限（可多选），输入员工信息，点击确认即可赋权；

### 5. 单个权限申请：权限申请-审批-赋权

申请页面：1、功能页面直接进行申请进入申请页面-填写申请原因-提交-等待管理员审批；2、进入权限申请页面-筛选对应权限-填写申请原因-提交-等待管理员审批；

审批页面：只有管理员才可审批，点击进入待审批列表-填写审批原因-审

批；

权限的分配要合理，很多公司分配给部门权限的时候很随意，部门要什么权限就给什么权限，其实这是有隐患的，我们更多需要更深入的考虑部门能有什么权限，而不是要什么权限，而这一块往往被忽略。

归根到底我想强调一件事情，权限的管理，如何从公司制度上重视，即如何规范权限的分配，即那个部门哪个员工要哪个权限都需要进行审批或邮件知会后才能帮其配置，还有哪些数据要设置权限，哪些操作要设置权限，这些权限管理过程才是权限系统的核心，恰恰这些核心的东西在系统上是体现不出来的。前期的不经意就会在后期会变成麻烦，不仅影响业务效率，更会导致风险危机。

权限管理最终是为了风控，如果权限的风控意识没做好，权限系统做的再好也是枉然。