# 公司情况与安全落地

## 安全落地

技术岗里，开发、运维，都没有落地这个说法，唯独安全有落地这个说法。这是因为，开发及运维工作的落地，不需要其他部门配合，自己部门本身具备一切落地的要素。哪怕是体系化的复杂一些的工作，比如重构，也不需要其他部门的配合。

而体系化的企业安全建设里，落地建设就离不开其他部门的配合。单应用安全里的SDL，其落地就折磨了数不清的安全从业者。

## 公司战略

安全工作的落地，跟安全在公司内部的战略位置，是息息相关的。而战略位置，跟公司规模关系不大。大型的集团公司，不一定自建安全团队，可能就外包就够了。没有盈利的小公司，也不一定不会招聘安全人员。

安全的战略位置一般为三种状态，挂件安全、一般安全、核心安全。

挂件安全状态，就是没有多少存在感，没有多少权力的状态，其本身存在的意义，只是为了合规等，公司有这么一个角色就行，水平无所谓，能干活就行。

一般安全状态，就是跟其他部门平齐的状态。这种战略位置比较容易达成，只要出现一次稍大一些的安全事故，影响到业务，公司对安全的重视程度就会拉齐到这种。这种状态下，其他部门会尊重安全的专业意见，安全具备与业务部门PK的资格，在事务重要性的PK上，安全是可能赢的。

核心安全状态，这种就比较难达成。私企就只有像谷歌、微软这种大型、轻资产、科技公司才是这样的。安全负责人是总裁级别，能参与公司层面的决策，公司层面的小会是有位置的。

防杠声明，以上三种状态纯属个人推测，属主观臆断。对于公司来说，只有适合的，而毫无疑问，老板的观点才是最适合公司的观点。安全从业者也不要对号入座。

## 落地措施

根据安全在公司战略位置的不同，其安全组织、团队规模、人员职级、薪资范围、落地程度、落地内容等都会有所不同。

核心安全里，可能会存在安全委员会这种虚拟组织，企业安全是全体部门的分内职责。安全团队规模会很大，可能每个业务，每个分公司都有一定规模的团队。安全在公司具备话语权。安全的人员职级，会普遍较高，网络安全各方面的内容都能够进行落地，会采用自研的方式来对自身企业进行安全防护，甚至有能力将安全能力做成安全产品对外提供。有人员专门从事安全研究工作，引领网络安全攻防的发展。安全负责人会完全脱离一线的工作。对一线工作的指导，也有各方面的负责人处理。

一般安全里，在高优先级的项目中，能调动其他部门资源。安全团队规模，会有一个阈值，感知很明显的清晰的阈值。安全具备协商权，无决策权。网络安全能够落地一些方面，能够有预算去采购一些商业化的产品来进行安全建设。能有专门从事安全运营的岗位，去运营设备与系统，解答其他部门的疑问，处理一些非技术方面的杂事。安全负责人，无法完全脱离一线工作，会涉及到对一线具体工作的指导。

挂件安全里，安全部门完全没法干涉干预其他部门。团队人也比较少，负责人会直接参与直接负责一线工作。安全落地的方面也不会全面，无法全面。落地出来的内容会类似打补丁似的状态，这里一块，那里一块。会采用很多开源的系统工具，可能能够在开源基础上做一些使用优化，规则优化，但无法涉及开源底层。公司完全没有预算去采购商业化的安全产品。也不会有人帮忙推动其他部门落地安全内容，完全靠安全自己去推动。

## 落地推动

不考虑PMO的情况。

安全的落地推动，分两种角色，这两种角色的负责内容不一样，其推动策略方式也会有所不同。

一种是项目负责人角色，就是出项目方案的那个。出方案的时候就应该对方案涉及的其他部门，工作内容，落地顺序，大概时间，互相协作方式等有一个预期，在进行项目沟通方案沟通的时候，就应该将这些信息同步给关联方。这样关联方会对项目整体有个了解，再根据其部门本身的工作事务，在其制作工作计划的时候会更加恰当一些。所以安全项目方案沟通的时间点，也最好选在季度OKR或KPI制定之前。然后项目进行中，需要与关联方有密切的沟通，及时同步所有进度。可能一个项目涉及的部门有好多，是有顺序进行的，及时同步信息也有助于接下来的部门有心里预期。

一种是安全这边的项目执行者的角色，就是实际落地项目方案人。在进行自身的工作落地的时候，应该及时跟两方面同步进度跟困难。一方面是项目负责人，一方面是当前的其他部门的对接人。这样在安全归属范围内的工作完成之后，对接部门因为有预期，他能够安排好人来做接下来的工作。

然后执行角色，还应该继续跟进对接人的落地进度。因为后面工作可能牵涉到其他部门或回到安全自身，安全也需要及时的信息以便调整工作安排。

整体项目应该有时间预期，项目如果能在预期内完成，那么协作部门如何进行时间安排，安全其实没必要干预。

如果是因为对项目复杂度估计不足导致的时间紧，如果能加班解决就加班解决，无法加班解决，那么就要调整方案。同时，也不应该期待对接部门因为安全事务安排加班。

如果是因为安全这边的落地执行者的失误原因，导致无法按预期完成，那么就考虑一下KPI。同时看看能不能安排更多的人力进入，以进行补救。

如果协作部门的对接人的时间安排，归属于协作部门的工作，可能无法在预期内完成。这时候才可能需要引入PMO或高级角色，对事务优先级进行相关判断并做出优先级安排。由安全负责人跟协作部门领导，进行一些沟通，目的在于整体项目的按时完成，看能不能通过一起加班等手段来完成，实在没有办法才考虑再进行一下升级，拉更高的领导来进行决策。

## 心里预期

入职时最好能够了解以上信息，以便能对安全工作有相关的心里预期。

安全的战略位置，牵涉的可能还有年终奖、调薪与晋升、工作顺利程度、技能发展、职业发展等等。

有了匹配的心里预期，才能在公司比较顺畅的进行工作。否则，面对一些协作工作，可能会产生比较大的情绪。

而且技术人员相对业务人员可能更加单纯，不太擅长处理这些，会工作的很不开心。

希望大家都能有清晰的自身定位，清晰各种选择面对的是什么，理智分析利弊，做出适合自己的选择。