办公安全对象是办公，应该围绕着办公工作流展开。跟围绕着公司员工。以及办公系统。以及办公区域内的网络主机等。

办公安全的建设理念有零信任。

基础系统通常有 OA，邮箱等办公系统，人人都用的。

各部门也有自己的办公系统，如财务系统，运维系统，开发测试的jira，gitde等系统。

在信息化/it化建设中，在IT的边界，会存在线上行为及线下行为的过渡过程。

在过渡过程中出现办公安全问题。

工作流应是制度制定方面的工作多一些。主要解决先干什么后做什么。

再就是发现不合适的线上线下过渡行为。

安全意识培训，解决办公安全问题。

保密，内鬼，内审内控，解决办公安全。

资产的安全管理，应当放到办公安全这里。

权限管理，IAM

上网行为审计

网络环境安全：纯净的网络环境，没有恶意用户接入，能发现恶意流量，阻止恶意流量。

办公系统安全：系统只有员工能使用，IAM，认证。系统安全配置。系统放在内网，服务用内网IP启动

权限安全：管理混乱忘记删除，IAM统一认证，软件硬件认证统一认证。专用设备。

办公终端安全：EDR，防病毒，零信任终端软件，DLP等

终端软件管理：

<https://www.ibm.com/cn-zh/topics/uem>

jump server + 服务器密钥

服务器安全组规则设置只能jumpserver登录

审计安全组规则，

审计所有ECS是否使用了规定的安全组

通用场景，应设置钉钉审批流。

非特殊场景，邮件审批就可以了。