27001.CN

IT外包项目信息安全管理实践

Sky Huang

2022.01.29

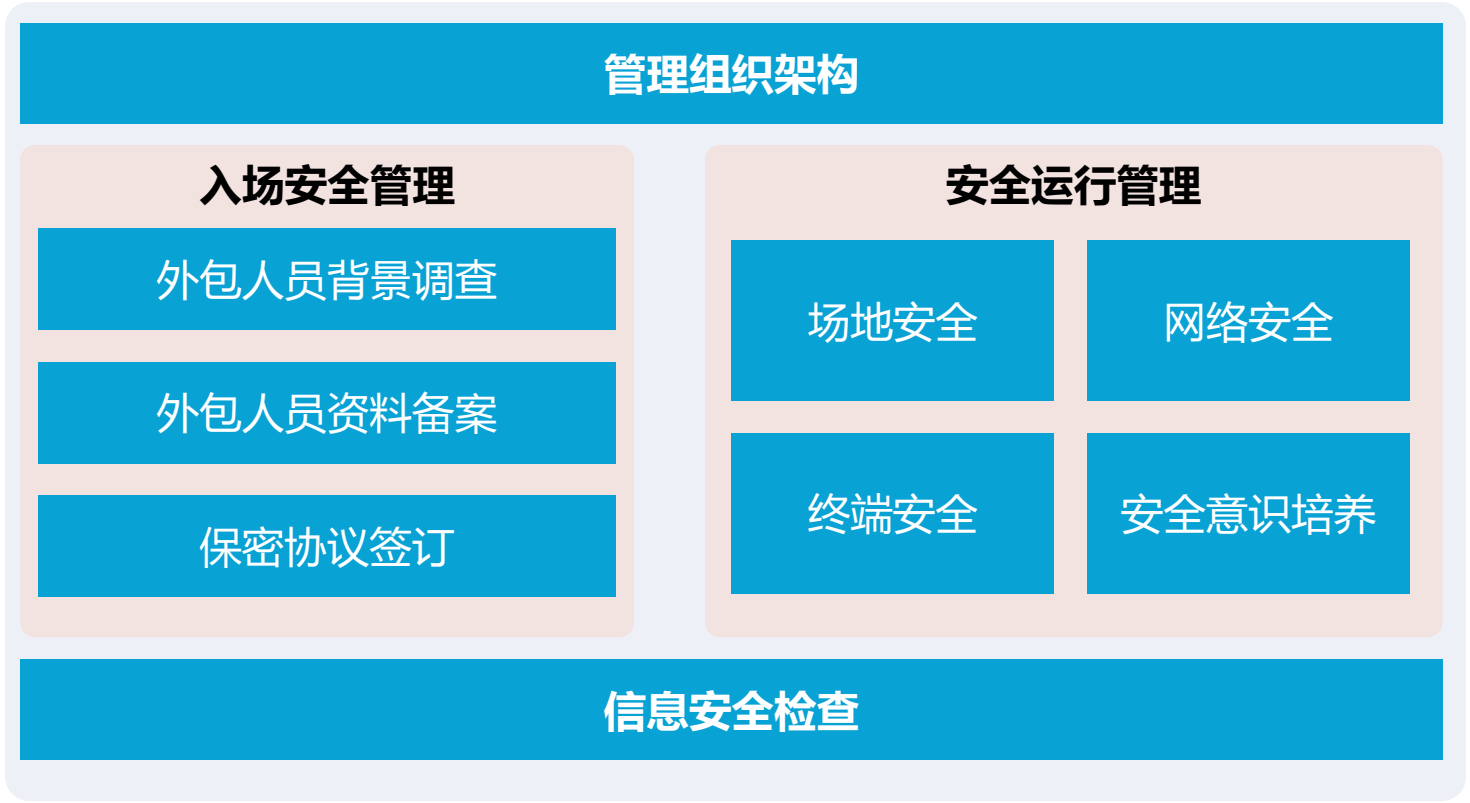
sky.huang@27001.cn

资料参考：《中小银行自主可控外包管理模式》王健/明立松/郝志萍

IT外包项目面临的主要信息安全风险

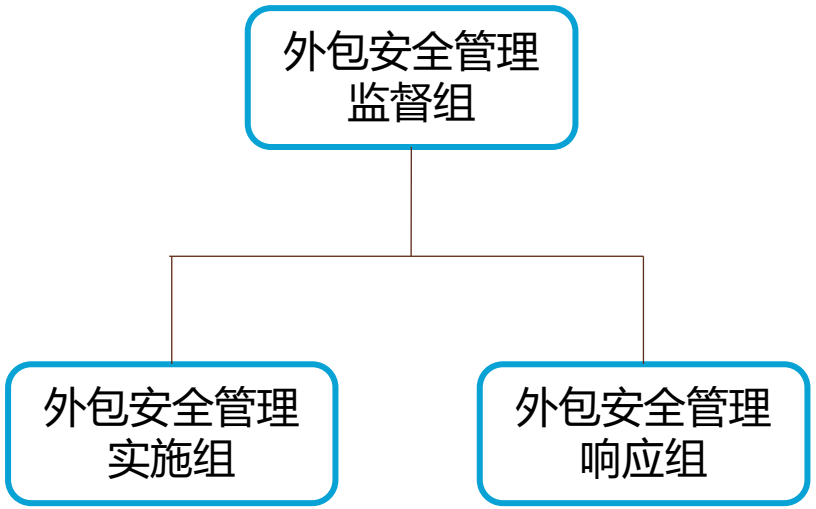
序号	脆弱性	威胁
1	物理访问管理缺失	未授权的物理访问
		私自接入网络设备
		设备丢失或损坏
		机房物理环境被破坏
		敏感数据被盗取
		存有敏感数据的介质未经授权带出
2	网络管理缺失	未授权人员接入办公网络
		外包人员使用通信设备进行非法活动
		数据存储介质遭窃取
		信息交换过程中数据被窃取
3	终端使用管理缺失	外包人员随意使用USB或网络端口
		内部系统遭受恶意代码攻击
		内部系统被病毒感染

IT外包项目信息安全管理框架



管理组织架构

序号	组别	职责
1	外包安全管理监督组	负责制度外包安全管理策略和办法，并督促实施；
		监督外包安全事件应急过程与结果；
		监督提高外包人员安全意识措施执行情况；
		根据风险评估结果和整改建议，改进外包安全防护措施
		协调信息安全组织，以及和其他部门的工作。
2	外包安全管理实施组	负责落实外包安全管理办法；
		负责执行外包安全管理措施（场地安全、网络安全、终端安全）；
		负责执行提高外包人员安全意识的措施；
		配合外包安全检查工作；
		配合外包安全事件应急处理。
3	外包安全管理响应组	负责建立外包安全事件应急与处理机制（管理组织、报告路线、处置方案）；
		负责组织调查并处理外包重大安全事故，提出整改和补救措施，并监督执行；
		及时研究、分析外包安全事件，提出预防措施。



入场安全管理

序号	安全要求	要求落实说明
1	保密协议签订	项目实施前，与外包服务商签订保密协议
2	外包人员背景调查	验证外包人员学历、学位证书、以往工作经历等
3	外包人员资料备案	外包人员的基础信息
		外包人员在项目中充当的角色
		外包人员相关资料复印件
		服务商为外包人员开具的无违法乱纪行为保证书
		外包人员阅历资料
		外包人员以个人名义签署的保密协议

外包服务过程中的安全管理措施

场地安全

- 物理安全管理
- 设备安全管理
- 机房安全管理

网络安全

- 网络隔离措施
- 操作流程监控
- 传输安全管理

终端安全

- 设备端口管理
- 应用安全管理
- 系统安全管理

安全意识培养

安全培训

进场发放安全小册子

开展服务商年度安全培训

宣传海报

张贴安全规范海报

张贴安全警示标签

教育短片

公共电视播放安全短片

组织外包人员共同拍摄

桌面提醒

公共电脑设安全提醒桌面

信息安全检查

1 物理安全检查

2 数据安全检查

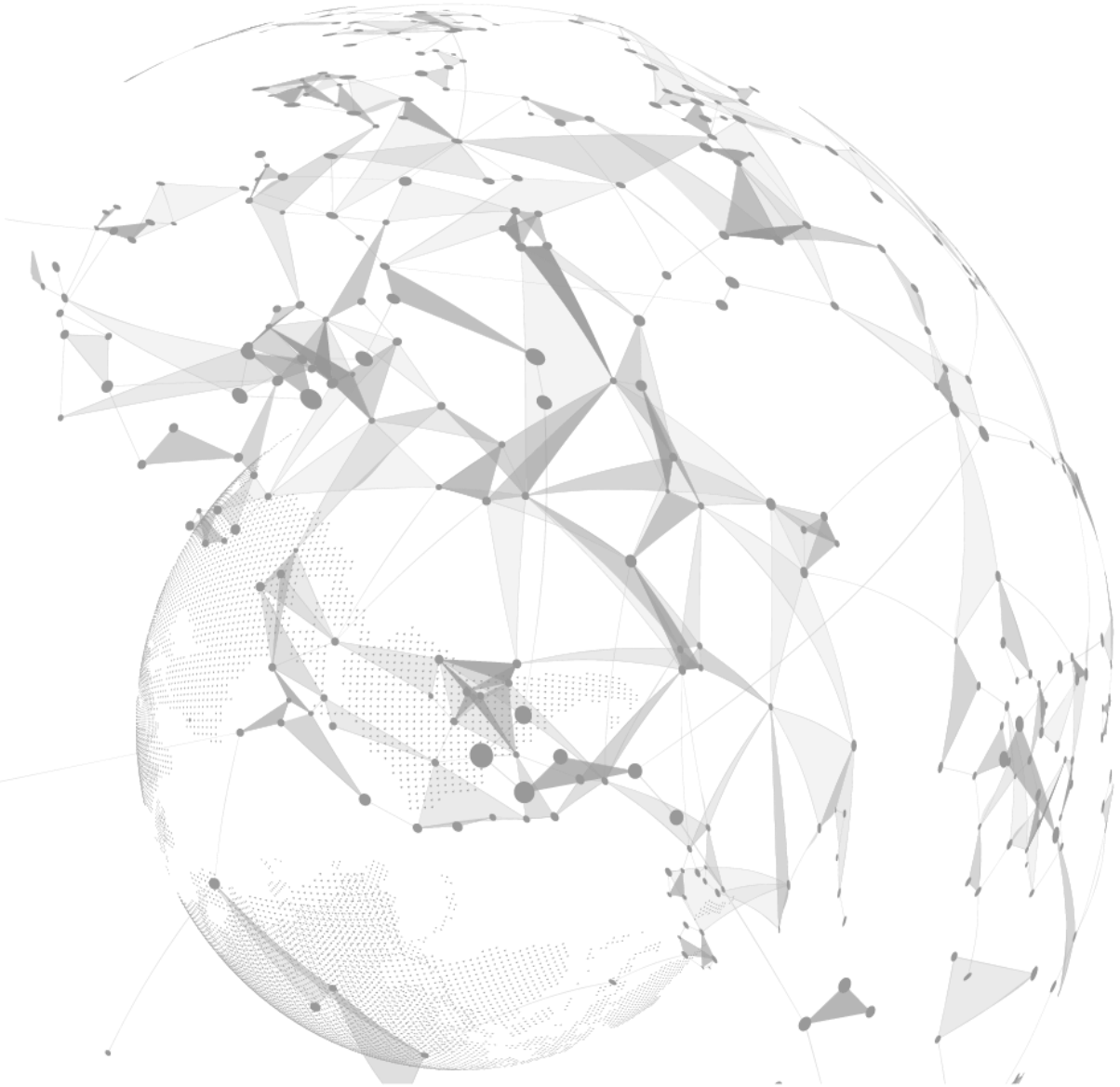
3 逻辑访问控制安全

4 公共媒介安全检查

5 通信及操作安全检查

6 业务连续性

27001.CN



Thanks
And Your Slogan Here

Sky Huang
www.27001.cn