



企业数据防泄密实践分享

程龙

大咖安盟会务长
海能达信息安全部负责人



网络安全创新大会
Cyber Security Innovation Summit

目 录

CONTENTS



01 安盟与公司介绍



02 面临的问题与挑战



03 管理措施实践



04 技术措施实践



深圳20多家上市公司IT负责人，2019年8月8日联合成立深圳IT大联盟（简称：安盟），接收IT甲方主管级或技术专家级及以上行业大咖，截至当前安盟平台发展迅猛，成员所属公司达220家起、CIO&CTO&CSO达260人、安盟总成员规模达500人起





图 6：公司研发投入一直保持总收入 11% 以上



资料来源：Wind，中信建投证券研究发展部

图 7：公司 2012-2019 年前三季度营收与归母净利润及增速



资料来源：Wind，中信建投证券研究发展部

提供全系列、多标准的领先专网通信产品

- 数字对讲机与集群系统
- LTE宽带集群系统与智能对讲机
- 执法记录仪
- 指挥调度
- 专网物联网与应急通信
- 集成通信及改装车解决方案
- 卫星通信
- Sinclair天线
- 智能配件



目 录

CONTENTS



01 安盟与公司介绍



02 面临的问题与挑战



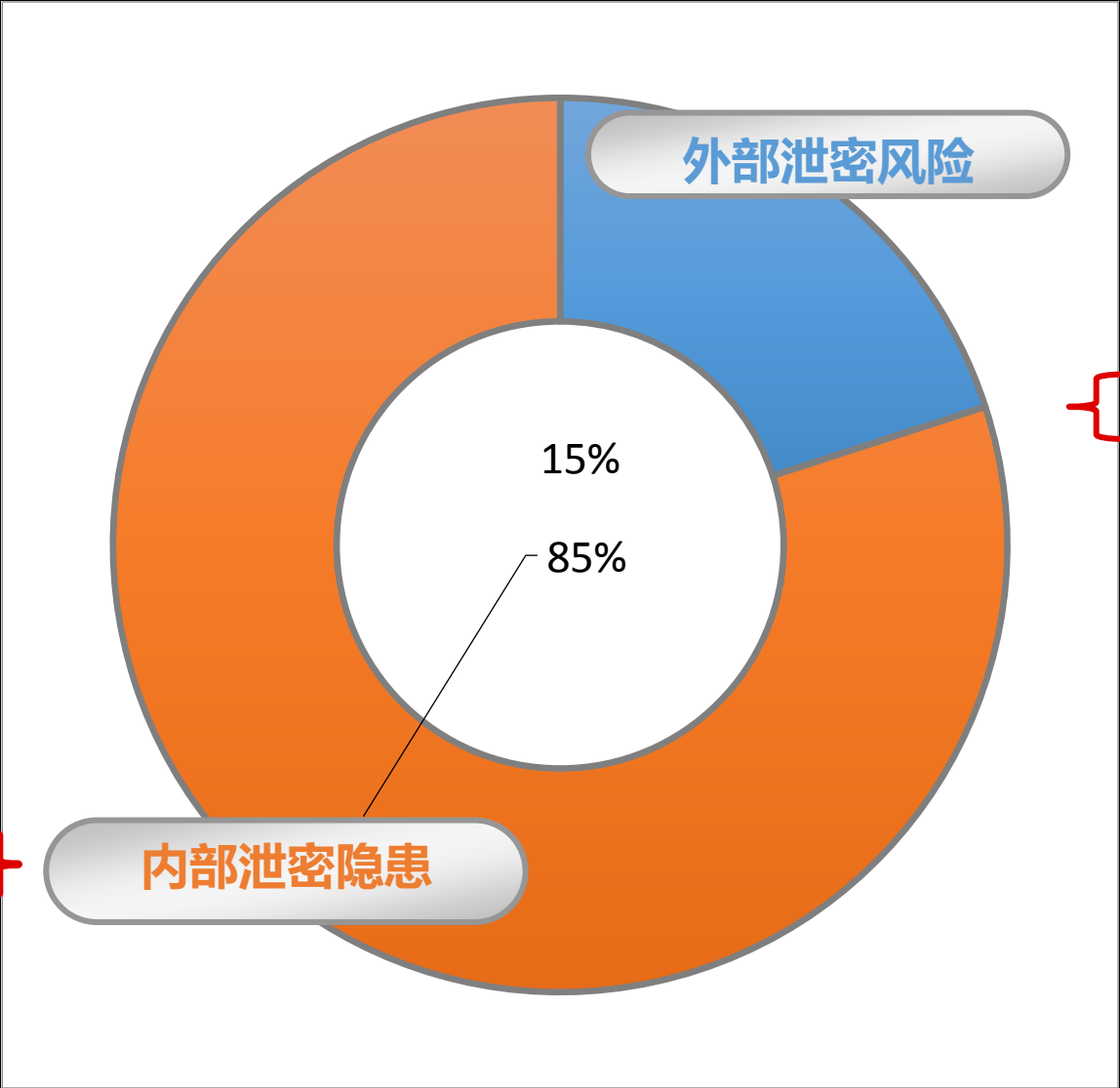
03 管理措施实践



04 技术措施实践



- 有意主动泄密
- 无意被动泄密
- 商业间谍窃密
- 保管不当泄密
- 意识淡薄泄密



- 黑客网络攻击
- 病毒木马入侵
- 设备报废丢失
- 商业诈骗窃取
- 业务协同共享

数据安全风险，“内忧”已远远高于“外患”





面临的挑战（一）：如何实现精准有效防护



网络安全创新大会
Cyber Security Innovation Summit



结构化数据
(数据库数据)



半结构化数据
(邮件、即时通讯中数据)



非结构化数据
(终端零散数据，如文档、图片、音频、视频等)

当前面临的困境：

我们有哪些数据资产？

如何进行数据资产跟踪？

如何对数据资产价值评估？



面临的挑战（二）：如何实现安全与效率最大化



网络安全创新大会
Cyber Security Innovation Summit





面临的挑战（三）：如何实现数据的安全访问控制



网络安全创新大会
Cyber Security Innovation Summit



在职人员



离职人员



合作伙伴/上下游供应商

目 录

CONTENTS



01 安盟与公司介绍



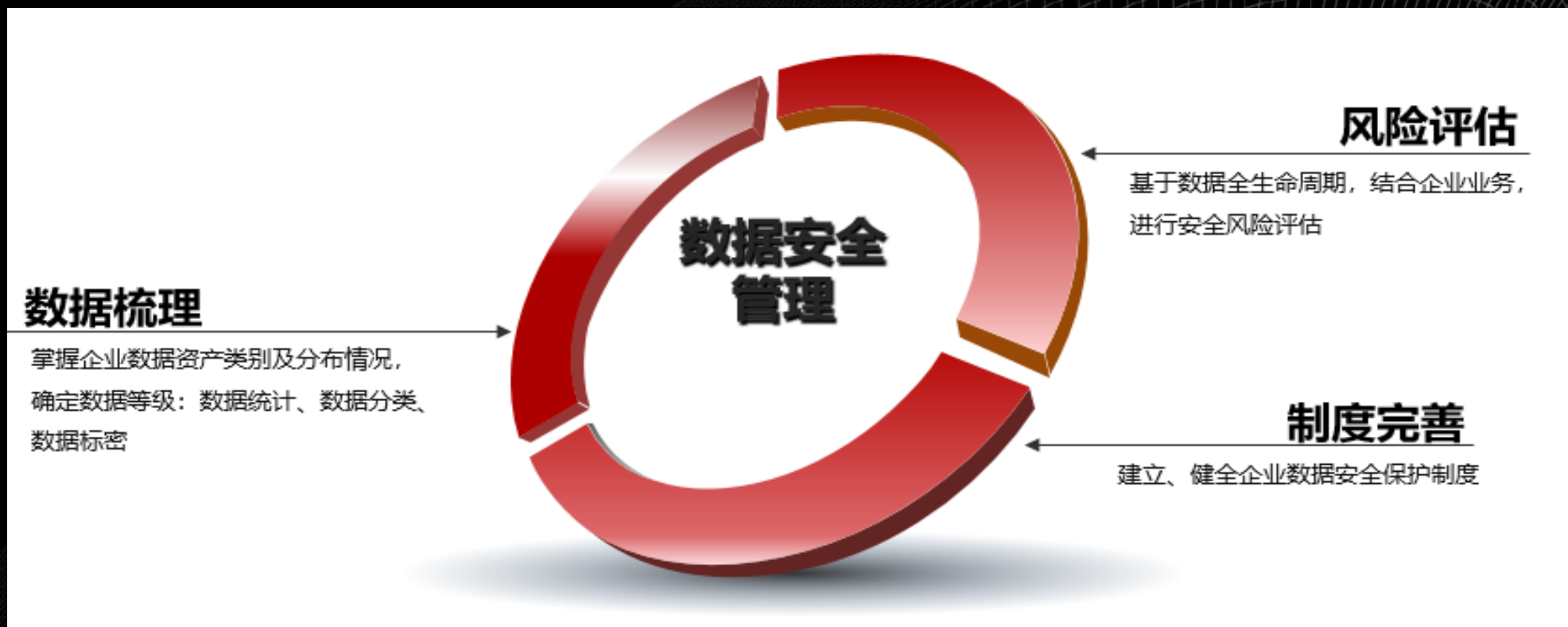
02 面临的问题与挑战



03 管理措施实践



04 技术措施实践





信息分级定义

信息分为企密AAA、企密AA、企密A、公开信息。

- **企密AAA**: 公司最核心、最机密信息, 泄露会给公司核心利益造成毁灭性损害;
- **企密AA**: 公司敏感、核心的信息, 泄露会给公司利益造成损害;
- **企密A**: 泄露可能会给公司造成一定影响的信息;
- **公开信息**: 对外发布的信息, 泄露不会对公司造成影响。

信息定级参考维度

信息分级由各一级部门根据分级定义自行定级, 由一级部门长审核, 主管副总核准。定级可参考以下任一维度。参照:<<信息分级管理基本要求及指南MIT-XX-XXX>>

- 对公司经营战略影响程度;
- 对公司核心竞争力影响程度;
- 对社会公众舆论的影响程度;
- 对公司正常生产运营影响程度;
- 其他方面考量。

信息分级管控策略

信息由各一级部门按照梳理后与信息安全共同商讨的管控措施进行管理, 企密AAA、企密AA由信息安全监察。



企密信息
清册



企密信息
流转流程
梳理及管
控措施



企密信息
管理手册

关键
信息
清册

- 1、各部门风控窗口罗列本部门业务/职责。确定每项业务/职责会产生哪些信息。
- 2、根据定义及判定维度对所有信息进行定级。
- 3、一级部门长及信息安全审核，主管副总核准。

流
转
流
程
梳
理
及
管
控
措
施

- 1、信息安全找各项绝密、机密信息业务担当及接触人员进行流转流程梳理及从产生、存储、流转、销毁全生命周期流程梳理及每个节点的风险评估。
- 2、根据评估的信息安全风险制定相应的管控措施。
- 3、业务担当与信息安全部对每项管控措施达成一致，一级部门长审核，主管副总核准。

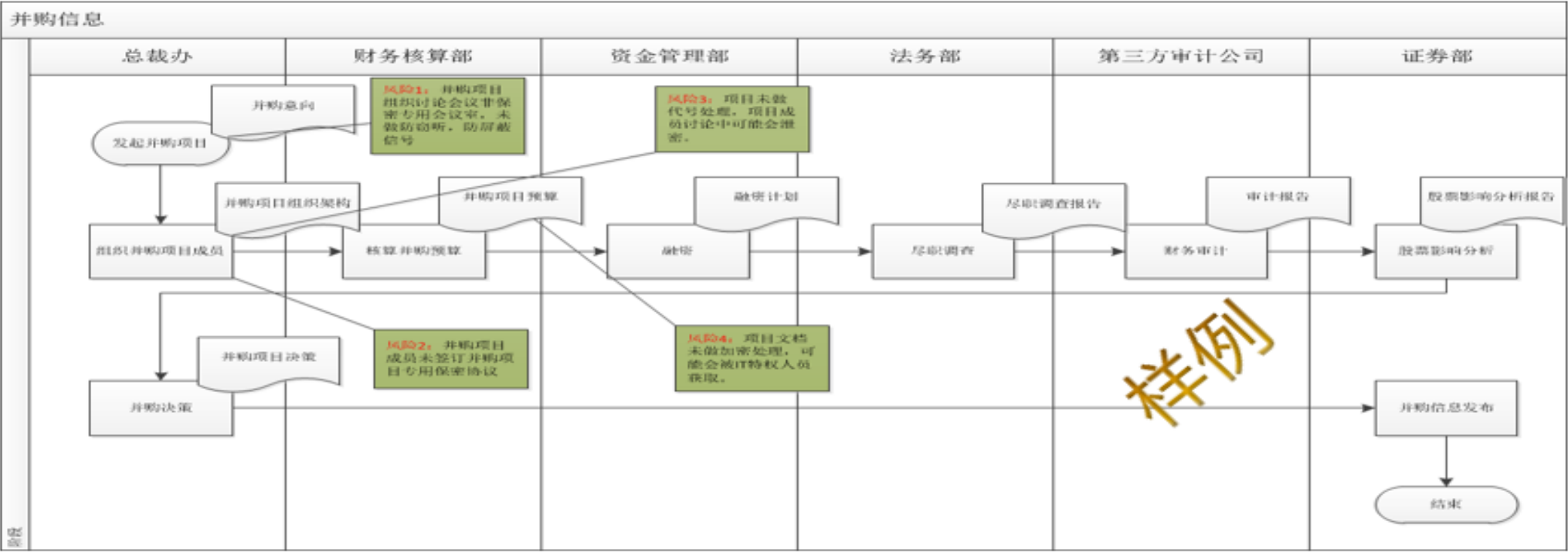


最终成果

关键信息清册

关键信息清册-财务部（样例）										
序号	体系	一级部门	信息	存放形式	机密等级	机密性时效	机密性描述	信息来源	业务担当	备注
1	平台支撑体系	财务部	财务报表	电子档	企密AAA	财务报告公布前为企密AAA，公布后为企密A。	反映公司各方面财务、资金及经营状况，未公布前泄露可能会影响公司股价，公司融资、经营、并购等计划。	产生	张三	
2				纸档	企密AAA			产生	李四	
3				系统数据	企密AAA			产生	王五	

关键信息风险评估底稿



关键信息资产管理手册

序号	体系	一级部门	信息	机密等级	机密时效	存放形式	存放载体	接触人员及权限	流向单位	流向人员及权限	相关业务描述	管控措施	备注
1	平台支撑体系	财务部	财务报表	企密AAA	财务报告公布前为绝密, 公布后为内部	系统数据	ERP系统	总裁/CF0: 完全控制 赵一: 完全控制 钱二: 查看 张三: 修改、导出	/	/	/	1、严格管控系统权限, 所有权限申请、变更、删除均有审批记录。 2、数据导出需要通过审批。	不流向其他单位
2						电子档	电脑	总裁/CF0: 完全控制 李四(合并报表负责人): 完全控制 报表制作人: 修改	/	/	/	1、未公布前合并报表须加密存放。 2、财务报表制作人及CF0终端电脑须做如BIOS加密取消域管理员后台登录权限、取消默认共享目录等设置3、电子档财务报表禁止发给非业务接触人员须CF0或总裁审批。	
3						纸档	保险箱	总裁/CF0: 完全控制 刘七: 完全控制 胡八: 查阅 杨九: 查阅	/	/	/	1、公布前非授权人员借阅需要CF0审批后才能借阅。 2、借阅只能在现场查看, 不能携带出管理员办公室	

目 录

CONTENTS



01 安盟与公司介绍



02 面临的问题与挑战



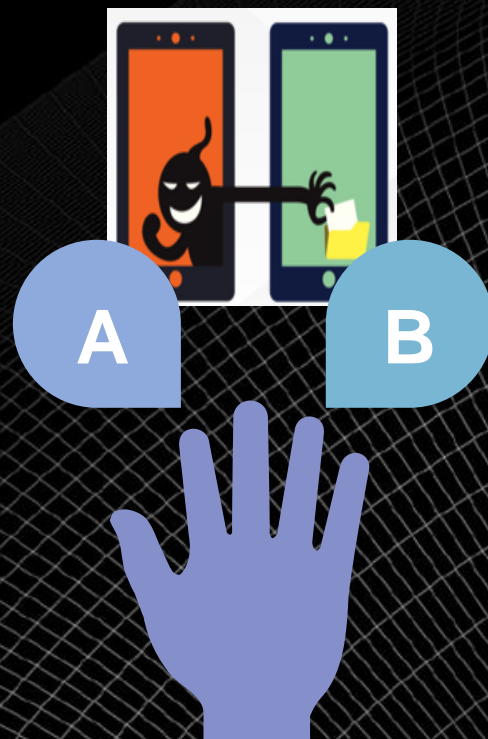
03 管理措施实践



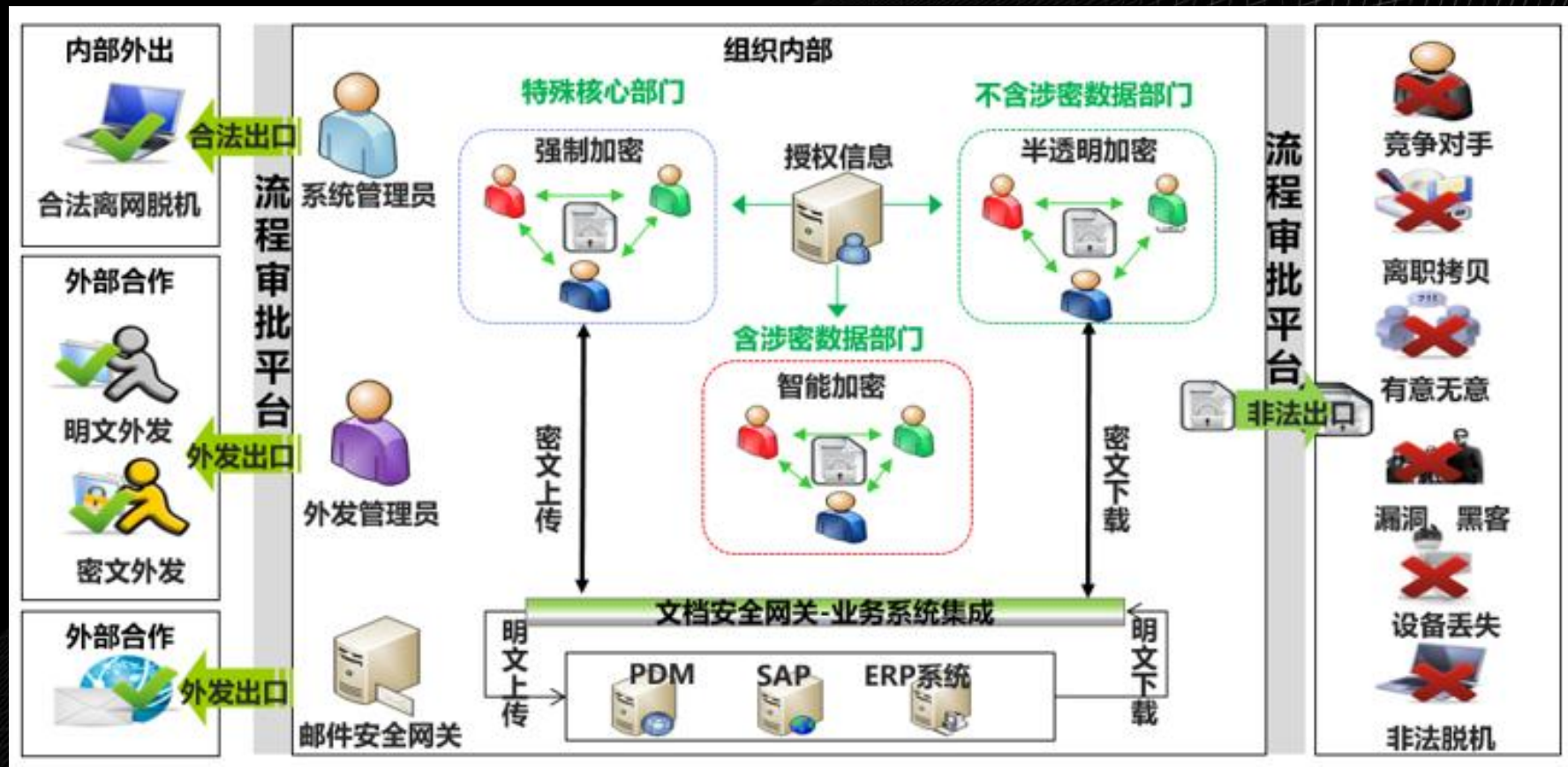
04 技术措施实践



- 对内防内鬼：离职窃取、商业间谍
- 对外防黑客：漏洞利用



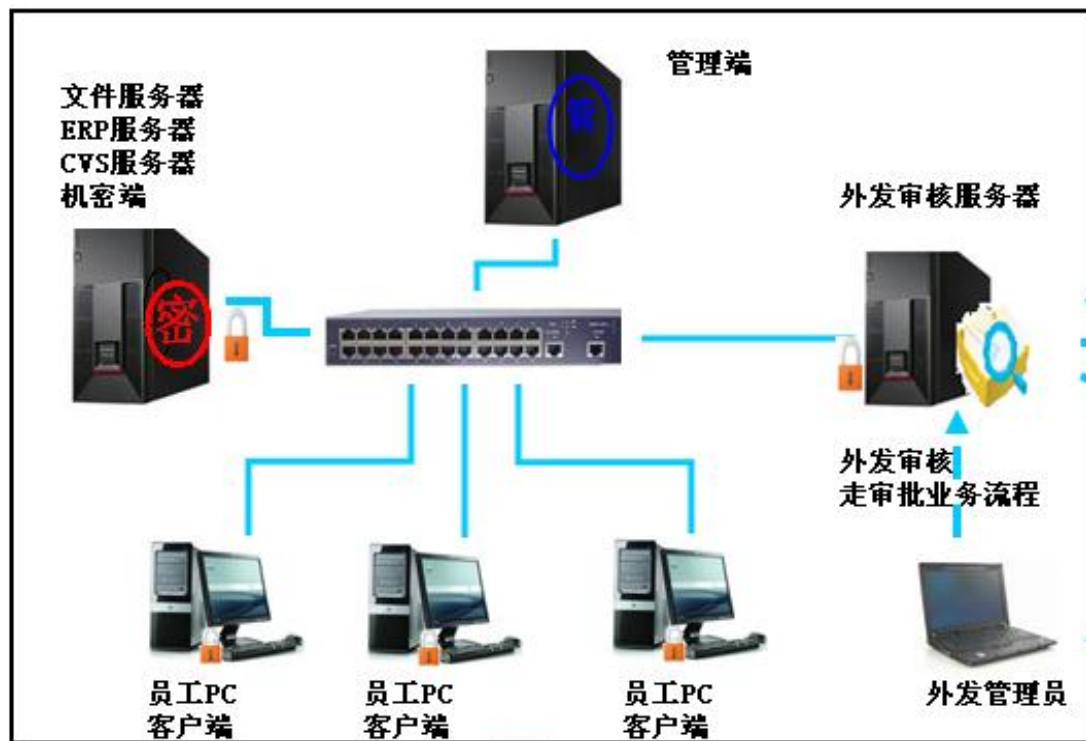
- 打不开：加密
- 看不了：权限
- 拿不走：审批
- 可溯源：水印



非代码、非图纸类安全，加密文档显示水印



代码、图纸类安全
不影响正常使用，支持所有文件格式，只进不出，要出必须走审批（绝密级二级审批，其他一级审批）



机密文件防泄密





外调控制与审计

控制外设准入，过滤传出的数据文件，并对通过的数据进行服务器记录溯源



网络下载



各种
常见串口/U口/网口
烧录工具



- 设备准入
- 烧录传输的数据过滤
- 数据审计





> _ 姓名：程龙

公司：海能达通信股份有限公司

联系方式：13798532806（微信同号）

