安踏信息安全管理体系实践

——数据安全管理

署名：陈东海
职称：安踏集团信息管理中心总监

目 录
content

- 安全需求及解决方案
- 安全管理体系建设历程
- 安全管控蓝图规划
- 成果展示

扫码观看大会视频

一、安全需求及解决方案

小故事，大启发

100万的保险箱

需要3个悍匪

1辆车，才能偷走。

公司损失:100万

客户信息的电脑

只要1个商业间谍

1个U盘，就能偷走。

公司损失：
所有客户！

扫码观看大会视频

内部 与 外部 驱动安踏加大保护核心信息资产

随着安踏市场竞争力的提升，居于国内领先地位的研发产品越来越多，信息资产的价值也越来越大

云平台、电子商务、移动化等信息化技术在提升业务效率的同时，引入了了更多的安全风险

凯觊安踏核心信息资产的不法分子及竞争对手越来越多了

安踏如何应对？

安全建设势在必行

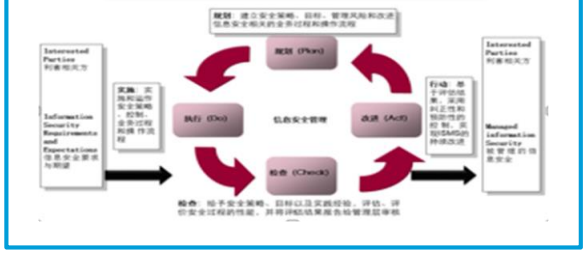
构建信息安全体系，保障业务持续发展

扫码观看大会视频

从组织架构，流程体系和技术平台三个方面建立起安踏的信息安全体系，保护公司的信息资产，避免经济损失。

安全建设

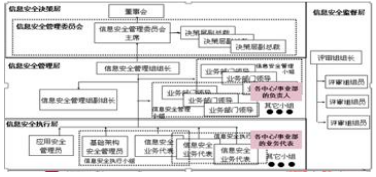
安全管理模型



资产分级

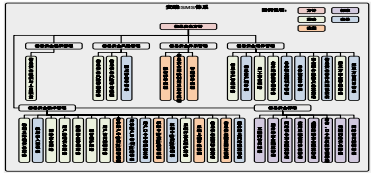
安全运营

组织



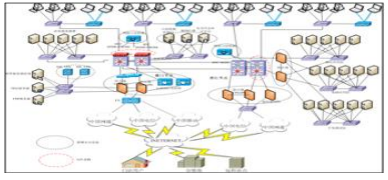
- 设置信息安全组织架构
- 公司任命，自上而下推进

流程



- 识别核心信息资产
- 合理的安全管控流程

技术

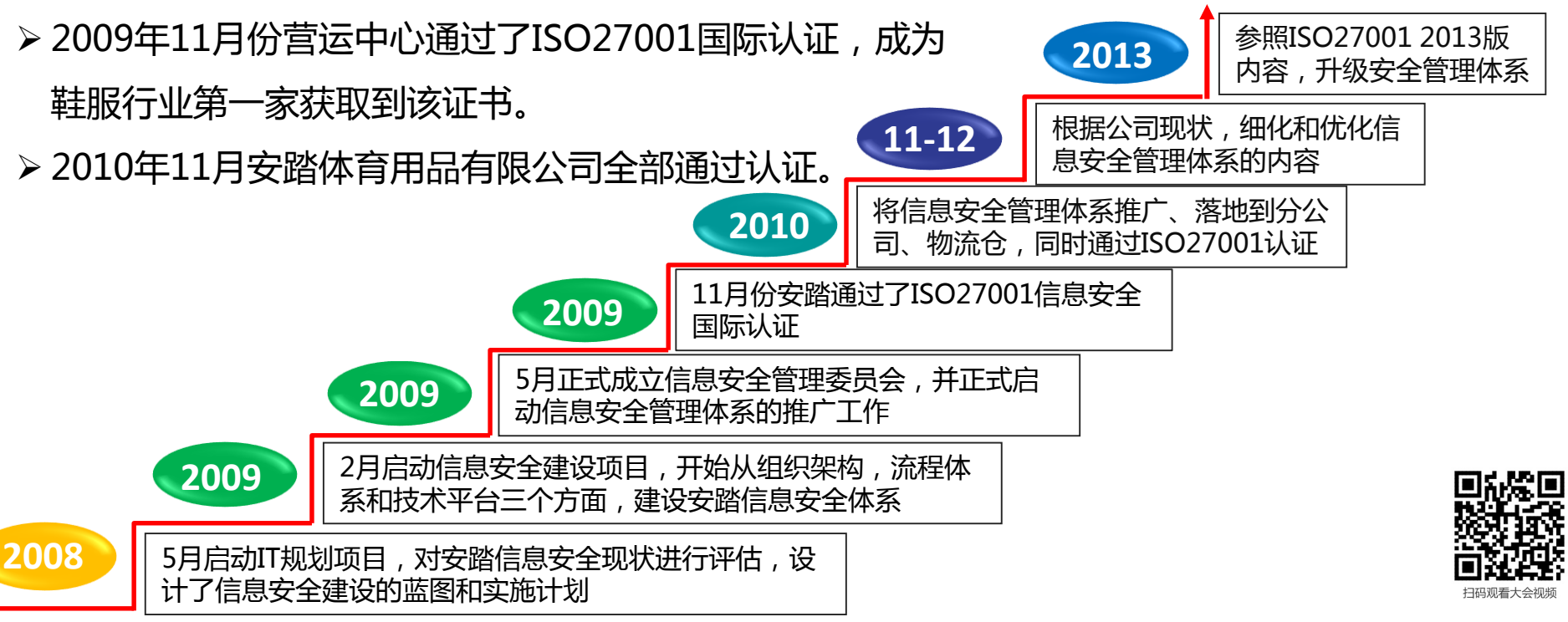


- 信息资产管控技术方案
- 内、外技术防御体系

扫码观看大会视频

二、安全体系建设历程

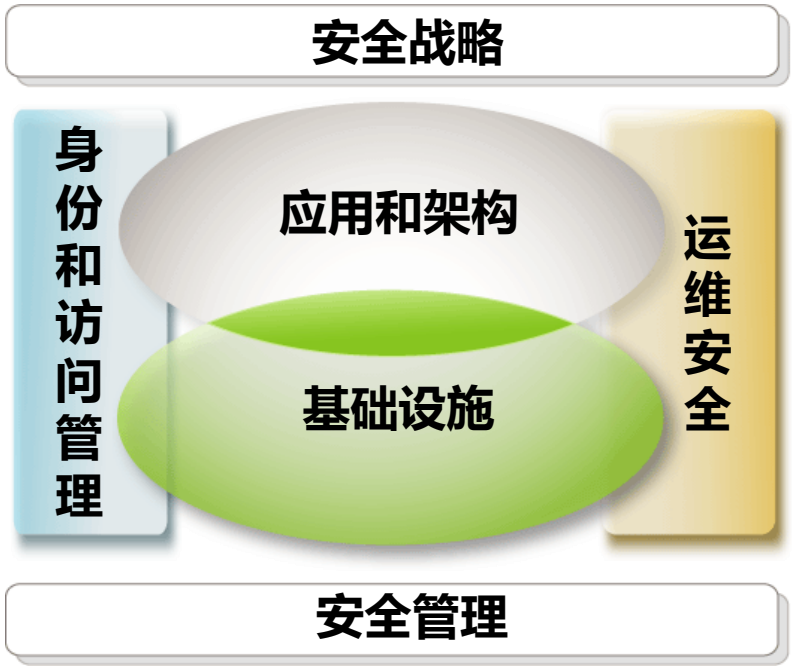
- 安踏08年启动IT蓝图规划，从组织架构、流程体系、技术平台三个方面，逐步建立并完善了公司的信息安全能力；
- 2009年11月份营运中心通过了ISO27001国际认证，成为鞋服行业第一家获取到该证书。
- 2010年11月安踏体育用品有限公司全部通过认证。



扫码观看大会视频

三、安全管控蓝图规划

安全管控的蓝图规划



基于安踏安全规划目标及原则，结合安全能力现状，从安全架构的六个方面详细定义了各领域的功能组件，制定了以下完整的信息安全蓝图框架：

① 安全战略

② 应用及架构安全

③ 基础设施安全

④ 身份与访问管理、

⑤ 运维安全及安全管理

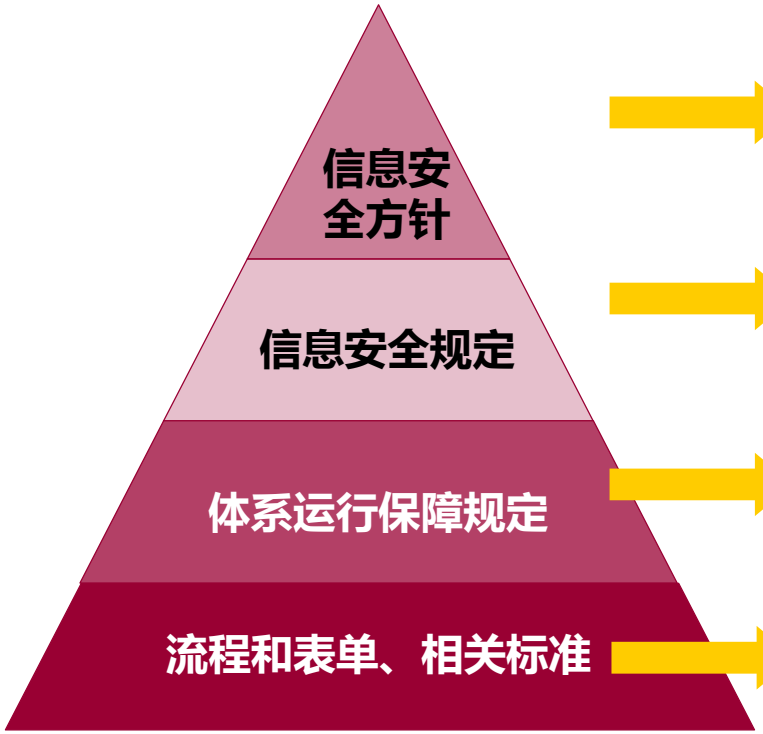
扫码观看大会视频

安全管控的蓝图规划

- 信息安全蓝图框架 - 详细功能组件

四、安全成果展示

健全的安全管理体系



本方针是安全管理体系的总则，其目的是建立战略性的安全指导方针，为公司的信息安全提供管理方向与支持

信息安全规定涉及到个人计算机，风险评估，第三方外包， 网络访问，业务连续性，介质处理，防病毒，信息安全评审，工作环境，安全事件，系统用户管理等领域。

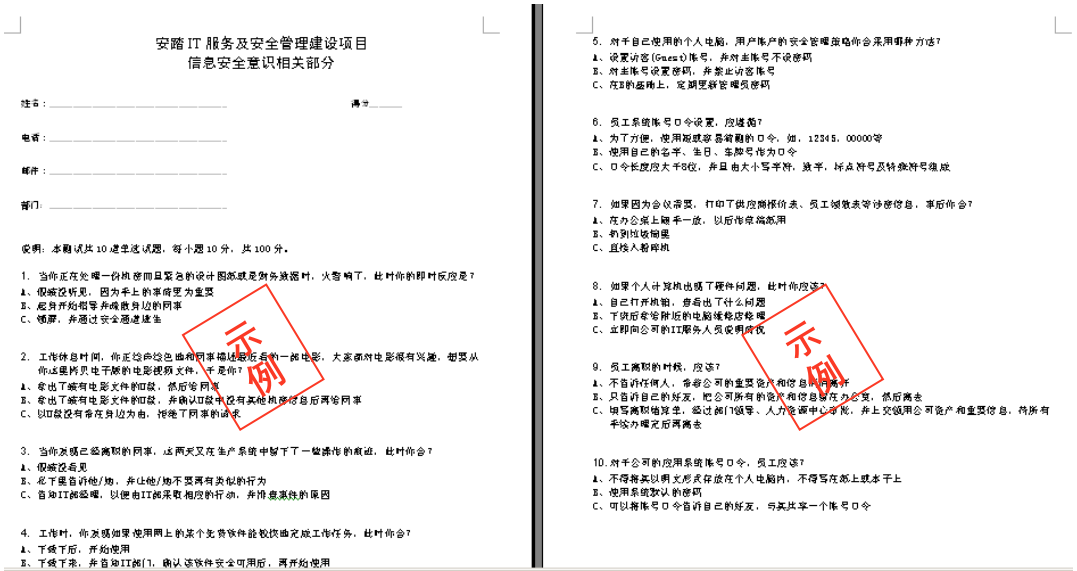
为了保障以上的规定的顺利执行，制定了相应的支持和保障性的规定，例如安全评审

针对具体规定有相应的操作流程和表单，为了实现具体的安全标准，还有相应的标准文档

扫码观看大会视频

人员的安全意识提升

信息安全意识的提高是企业信息安全建设成功的关键。



安踏IT服务及安全管理建设项目
信息安全意识相关部分

注名：_____ 得分_____

电话：_____

邮件：_____

部门：_____

说明：本题试共10道单选试题，每小题10分，共100分。

1. 当你正在处理一份机密而且紧急的设计图纸或是财务报表时，火警响了，此时你的即时反应是？
A、假装没听见，因为手上的事情更为重要
B、起身开始招呼并疏散身边的同事
C、镇静，并通过安全通道逃生

2. 工作休息时间，你正给亲密而相熟同事描述最近看的一部电影，大家都对电影很有兴趣，都要从你这里拷贝电子版的电影视频文件，于是你？
A、拿出下载有电影文件的U盘，然后给同事
B、拿出下载有电影文件的U盘，并确认U盘中没有其他机密信息后再给同事
C、以U盘没有存在身边为由，拒绝了同事的请求

3. 当你发现已经离职的同事，还两天又在生产系统中留下了一些操作的痕迹，此时你会？
A、假装没看见
B、私下提告诉他/她，并让他/她不要再有类似的行为
C、告知IT部经理，以便由IT部采取相应的行动，并消息事件的原因

4. 工作时，你发现如果使用网上的某个免费软件能较快地完成工作任务，此时你会？
A、下载下后，开始使用
B、下载下来，并告知IT部门，确认该软件安全可用后，再开始使用

5. 对于自己使用的个人电脑，用户账户的安全管理策略你会采用哪种方法？
A、设置访客(Guest)账号，并对主账号不设密码
B、对主账号设置密码，并禁止访客账号
C、在B的基础上，定期更新管理员密码

6. 员工系统账号口令设置，应遵循？
A、为了方便，使用短或容易猜测的口令，如，12345，00000等
B、使用自己的名字、生日、车牌号作为口令
C、口令长度应大于8位，并且由大小写字符，数字，标点符号及特殊符号组成

7. 如果因为会议需要，打印了供应商报价表、员工领款表等涉密信息，事后你会？
A、存办公桌上随手一放，以后作草稿纸用
B、扔到垃圾桶里
C、直接入碎纸机

8. 如果个人计算机出现了硬件问题，此时你应该？
A、自己打开机箱，查看出了什么问题
B、下供后拿给附近的电脑维修店修理
C、立即向公司的IT服务人员报修故障

9. 员工离职的时候，应该？
A、不告诉任何人，备份公司的重要资产和信息到离职
B、只告诉自己的好友，把公司所有的资产和信息都存办公室，然后离去
C、填写离职申请单，经过部门领导、人力资源中心审批，并上交领用公司资产和重要信息，待所有手续办理完后再离去

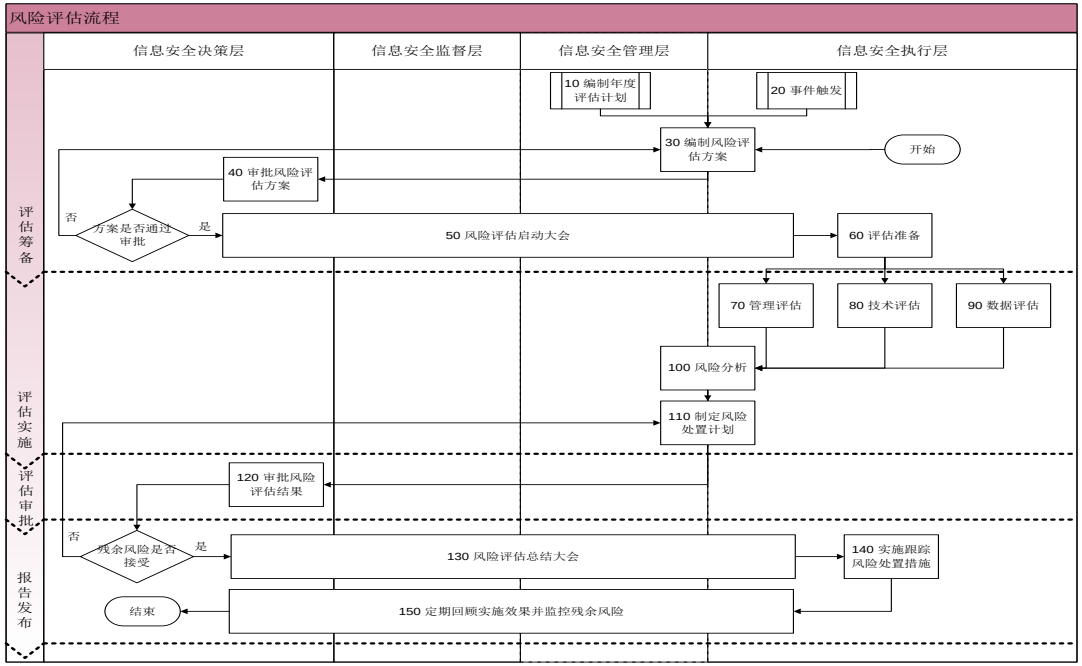
10. 对于公司的应用系统账号口令，员工应该？
A、不得将其以明文形式存放在个人电脑内，不得写在纸上或本子上
B、使用系统默认的密码
C、可以将账号口令告诉自己的好友，与其共享一个账号口令

每年线上信息安全意识培训试题

扫码观看大会视频

建立体系流程 - 风险评估流程

全面了解信息资产面临的风险，并采取恰当措施予以处理，从而降低风险对公司造成的损失。

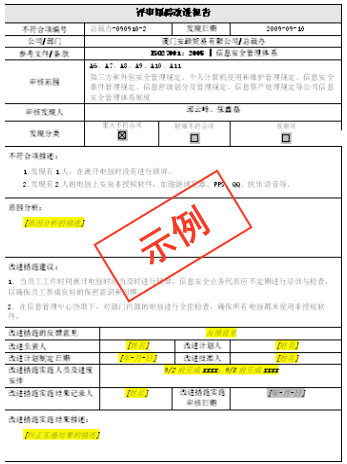


- **评估筹备**：编制年度评估计划、事件触发、编制风险评估方案、审批风险评估方案、风险评估启动大会、评估准备
- **评估实施**：管理评估、技术评估、数据评估、风险分析、制定风险处置计划
- **评估审批**：审批风险评估结果
- **报告发布**：风险评估总结大会、实施跟踪风险处置措施、定期回顾实施效果并监控残余风险

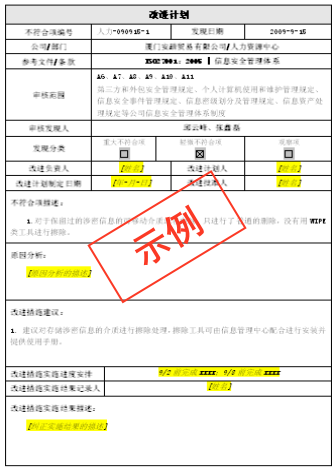
扫码观看大会视频

建立体系流程 - 安全评审流程

建立有效的信息安全评审机制，以公司安全管理体系的规定为准则，开展对信息安全工作的监督与评审，定期对信息安全管理体系健全性和符合性进行评审改进。



评审跟踪改进报告



改进计划

信息安全评审检查表

序号	不符合项编号	不符合项具体情况	改善完成情况
1	器材-090924-1	涉密信息在互联网进行传输时，未进行加密	待观察
2	器材-090924-2	未按信息密级划分的相关规定，对涉密信息实施密级标识、标注等操作；同时对涉密信息的分类和保管措施缺少了解。	待改进
3	器材-090924-3	发现 1 人在离开电脑时未进行锁屏。	待改进

不符合项报告

扫码观看大会视频

建立体系流程 - 业务连续性

建立业务连续性的管理，减小重大故障和灾难对公司关键业务的影响，特规定业务连续性管理的要求，包括风险评估、业务影响分析、制定计划、测试计划、更新计划等内容。

分销系统数据库备份策略清单

服务器	数据库	备份方式	备份时间	相同备份文件保存份数	存储介质	存储位置	过期处理	作业名称
192.168.9.200	AntaDRP	全备	每周一21:00	1	移动硬盘(ANTA01)	U:\DB_BAK\Full_Bak\AntaDRP\AntaDRP_full.bak	覆盖原备份文件	AntaDRP_每周一21点覆盖全备
		差备	每天0:00点起，每隔6小时备份一次	1	移动硬盘(ANTA01)	U:\DB_BAK\Differential_BAK\AntaDRP	自动删除超过1天的备份文件	AntaDRP_每6小时差备
		磁盘柜镜像	每天2:00	1	服务器(192.168.9.201)	M:\	覆盖原磁盘柜	
		日志备份	每天3:00	1	移动硬盘(ANTA01)	U:\DB_BAK\Log_BAK\AntaDRP\AntaDRP.trn	覆盖原备份文件	AntaDRP_每天3点日志备份.Subplan_1
	AntaMTPhoto	全备	在每周 星期二，星期日的 19:00:00 执行。	1	移动硬盘(ANTA01)	U:\DB_BAK\Full_Bak\AntaMTPhoto\AntaMTPhoto_full.bak	覆盖原备份文件	AntaMTPhoto_每周二、日19点覆盖全备
		差备	每天在 0:30:00 和 23:59:59 之间、每 6 小时 执行。	1	移动硬盘(ANTA01)	U:\DB_BAK\Differential_BAK\AntaMTPhoto	自动删除超过2天的备份文件	AntaMTPhoto_每6小时差备
		磁盘柜镜像	每天2:00	1	服务器内置硬盘(192.168.9.201)	M:\	覆盖原备份文件	
	AntaWDPhoto	全备	在每周 星期一，星期日的 19:00:00 执行	1	移动硬盘(ANTA01)	U:\DB_BAK\Full_Bak\AntaWDPhoto\AntaWDPhoto_full.bak	覆盖原备份文件	AntaWDPhoto_每周一、日19点覆盖全备
		差备	每天0:00点起，每隔6小时备份一次	1	移动硬盘(ANTA01)	U:\DB_BAK\Differential_BAK\AntaWDPhoto	自动删除超过2天的备份文件	AntaWDPhoto_每6小时差备
		磁盘柜镜像	每天2:00	1	服务器内置硬盘(192.168.9.201)	M:\	覆盖原磁盘柜	

备份策略清单

业务流程	系统软件故障	系统硬件故障	环境灾害	网络服务中断
基础资料、销售管理、成品采购、仓库管理、渠道管理、商场管理、财务管理、系统管理	4	5	5	5
ITIL流程	4	4	4	4
客户服务	4	5	5	4
费用报销系统业务流程	5	5	5	5
人力资源管理业务	4	4	4	3
OA办公自动化审批流程	4	4	4	4
供应链、生产制造相关流程	5	5	5	3
财务管理相关流程	5	5	5	3
生产材料出入库、计件工人计算工资	4	4	4	3
邮件服务系统	5	5	5	5
VPN	5	5	5	5
AD	5	5	5	5

业务影响分析结果

业务流程	支持的系统	RTO级别（业务最大允许停顿时间）	RPO级别（最大可以忍受的数据丢失时间）
基础资料、销售管理、成品采购、仓库管理、渠道管理、商场管理、财务管理、系统管理	安踏分销系统、安踏儿童分销系统、安踏库存查询系统、安踏订货会系统、安踏POS系统	36小时	6个小时
ITIL流程	IT服务平台	12个小时	24个小时
客户服务	客服系统	12个小时	12个小时
费用报销系统业务流程	EAS费用报销系统	12个小时	24个小时
人力资源管理业务	HR系统	12个小时	24个小时
OA办公自动化审批流程	OA系统	12个小时	24个小时
供应链、生产制造相关流程	用友生产系统	24个小时	24个小时
财务管理相关流程	用友财务系统	24个小时	24个小时
生产材料出入库、计件工人计算工资	ANTA系统	12小时	24个小时
邮件系统	邮件系统	12个小时	24个小时
VPN	VPN	12个小时	不适用
AD	AD	4个小时	24个小时

RTO&RPO

事件主题	环境灾难		
事件描述	由于自然或人为失误造成环境灾难使机房设备完全损毁		
处理人员	协调人	苏兆新	[联系电话]
	首选处理人	陈蕊华	[联系电话]
			[联系电话]
	备份处理人	温世源	[联系电话]
	其他	设备厂家远程支持	[联系电话]
通报人员	信息中心	周达文	[联系电话]
		刘昊	[联系电话]
		陈百岳	[联系电话]
	业务部门	应用系统相应管理员	[联系电话]
		陈新田	[联系电话]
	其他	全员通知	[联系电话]
应急处理步骤	准备阶段	1. 根据资产清单，确认损毁设备清单及配置参数；2. 申请购买设备进行采购流程。3. 通知数据备份管理员准备数据备份恢复及设备硬件完备状态时间点；4. 通知应用系统管理员数据恢复时间点。	
	实施阶段	1. 硬件设备环境重新搭建；2. 备份管理员执行数据恢复；3. 应用系统管理员检查应用系统状态及数据完整性。	
	善后阶段	1. 全员通知应用系统修复，及数据丢失量；2. 填写故障处理报告；3. 统计灾难造成的损失；4. 向领导特别汇报事件过程及故障恢复经过。	
备选方案	准备阶段		
	实施阶段		
	善后阶段		
注意事项	1. 远程容灾对关键系统是必须的。		
参考资料及工具			

应急预案

业务连续性方案演练计划			
演练时间	[年-月-日]	上次演练时间:	[年-月-日]
演练方式	□书面演练 □仿真 □系统恢复演练 □备用系统或场所的恢复测试演练 □第三方提供的设施和服务演练 □全面演练		
演练范围			
演练目的:			
演练内容:			
演练时间进度安排: （可附上甘特图说明）			

演练报告

扫码观看大会视频

建立体系流程 - 权限管理

岗位职责调研

业务部门培训，原始资料的提供和收集，需由业务部门负责人审核确认

系统权限导出

导出并整理现有系统的用户及权限

根据CIA，评估出系统优先顺序

比对差异

核对两者差异，将差异部分整理成表，并与业务部门接口人沟通讨论确认

调整系统权限

根据最终确认结果调整系统权限，并跟进后续问题

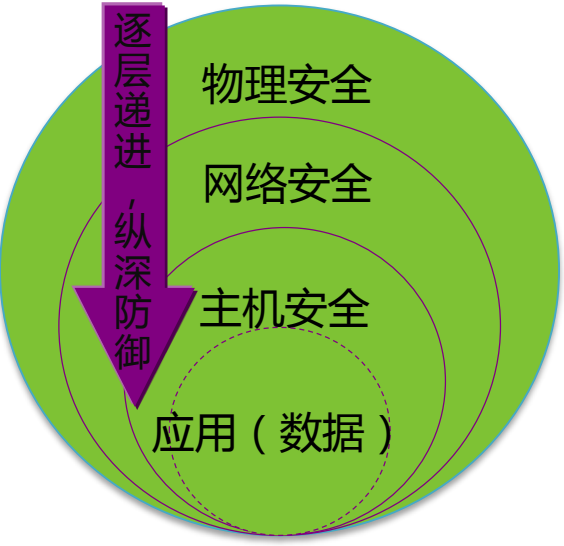
推广及维护

推广至其他业务部门，并保持定期核查权限机制

持续改进

建立体系流程 - 技术平台

信息安全防护我们通过与战略合作伙伴深信服合作，构建于应用系统之下的基础设施层面的安全防护，包括物理安全、网络安全及主机层面的安全防护，例如深信服NGAF实现ACL,IPS,WAF等功能，AC实现上网行为的控制及监督，WOC/SSLVPN实现全国组网等等。



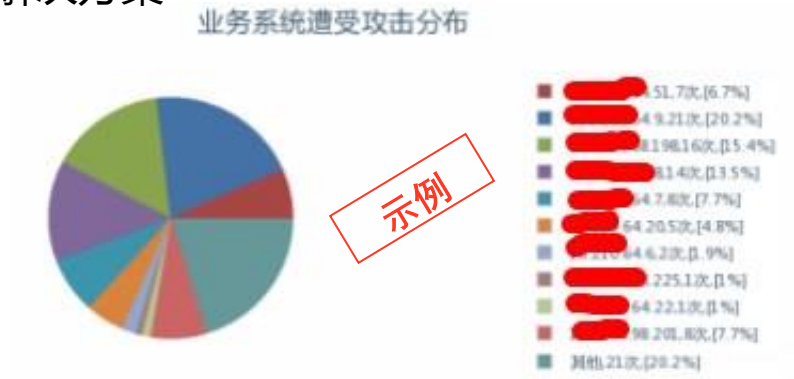
物理安全防护	指信息资产所处的物理环境的安全，物理安全保证计算机、网络设备、UPS等硬件自身的安全性。
网络安全防护	采用边界防护手段，实现网络中的连接设备及安全防护引入的设备、网络基础设施的安全防护。
主机安全防护	在主机层面采用信息保障技术，确保业务数据在服务器与桌面主机时保持可用性、完整性和保密性。
应用安全防护	对于应用系统本身的防护和对于应用间数据接口，远程终端数据访问的安全防护。

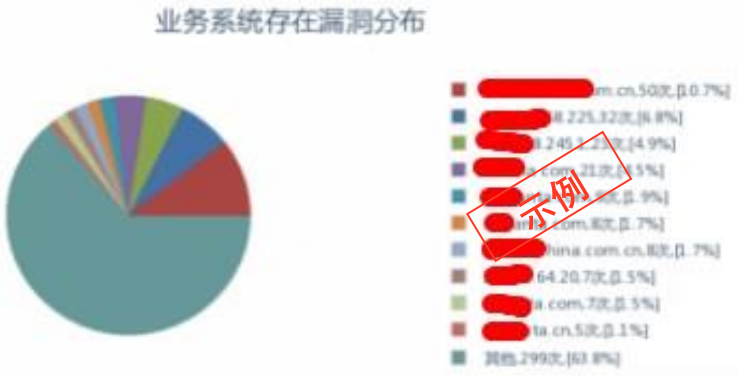
建立体系流程 - 技术平台

1、**可视是安全的基础**，通过深信服NGAF进行**持续监测**，了解整个网络当前的风险状况，以及风险状态走势

2、**快速响应**，**找出风险**状况较严重的业务系统，以及危害较大的攻击和漏洞

3、**简单易用**，可以帮忙用户快速定位，清晰了解攻击来源、危害等信息，提供相对应的解决方案



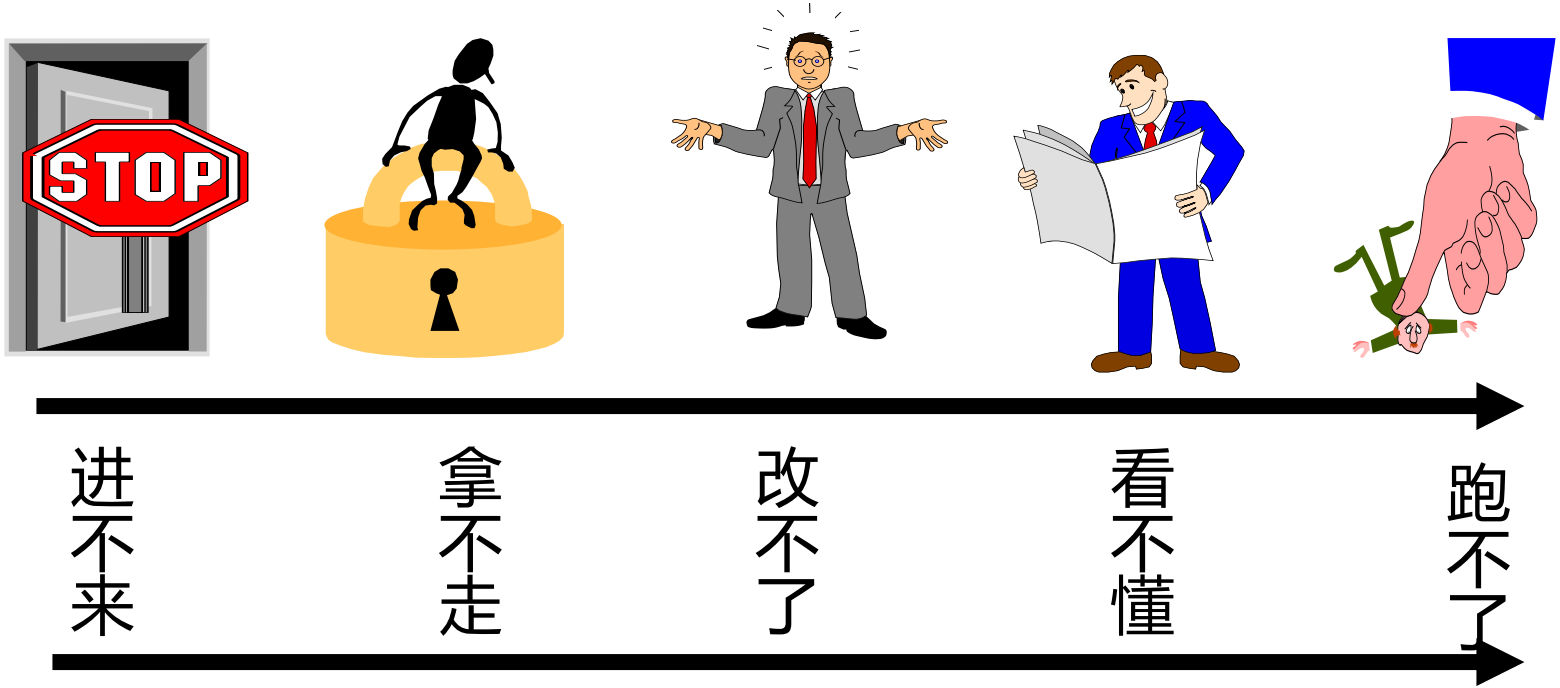


扫码观看大会视频

案例分享

扫码观看大会视频

安全工作的目的



ANTA

云栖社区
yq.aliyun.com

2016 The Computing Conference

THANKS

SANGFOR
深信服科技

2016 杭州·云栖大会
THE COMPUTING CONFERENCE

扫码观看大会视频