XX 信息安全保障体系规划建议书

2011/06

[文档信息]

文档名称			
文档管理编号			
保密级别	机密	文档版本号	V1.3
制作人	XXX	制作日期	
复审人		复审日期	
扩散范围			
扩散批准人			

[版本变更记录]

时间	版本	说明	修改人

目录

1 引言

为满足保监会、公安部等行业及国家监管层面的要求，同时满足我集团信息系统发展的现实安全需要，与我集团打造富有竞争力的现代化保险行业相匹配，集团必须要建立一个涵盖技术、管理、运维三个层面的全面、扎实、稳定的信息安全体系（如图 1-1 所示）。

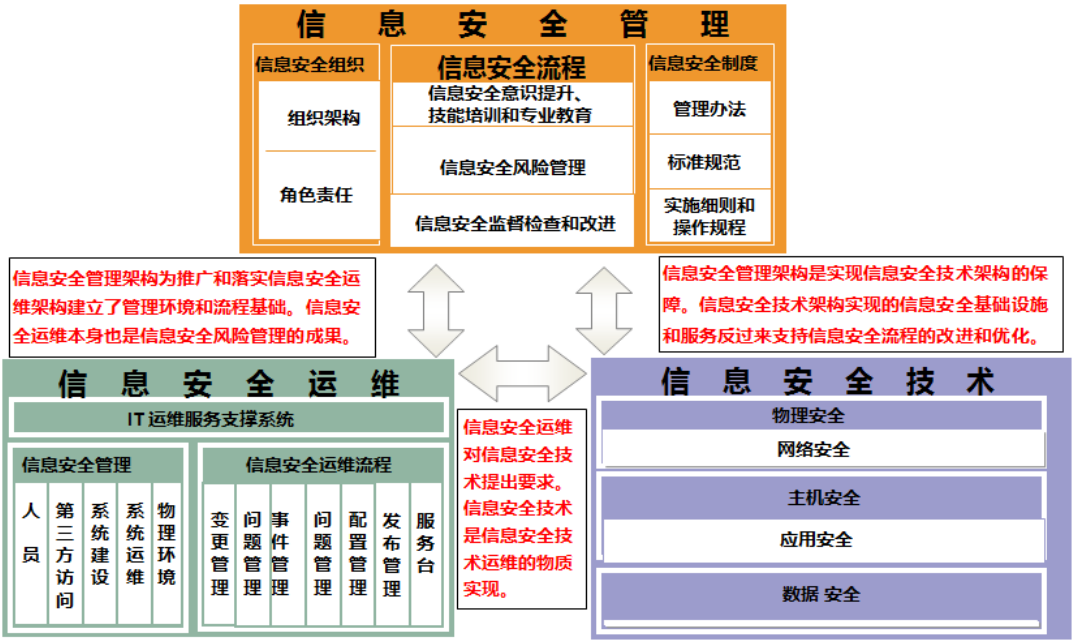


图 1-1

2 XX 信息安全保障体系规划目标

以保障系统和网络资源可用性为中心，切实提高信息安全管理水平，全面提升信息系统的整体安全防护和抗风险能力，为集团信息化发展总体目标的实现奠定坚实的安全保障基础。

具体如下：

- 保证业务系统的连续可用性，防止业务中断，防止数据丢失；
- 实现对应用系统与数据库系统的访问控制和授权管理，防止非法的和非授权的访问，保证信息资源与业务数据的安全；

- 确保业务工作责任与操作行为的不可否认性，防止抵赖，实现操作可审计、事件可追查、行为可监管；
- 保证业务数据和信息在传输、使用与存储过程中的真实性、完整性和保性；
- 保证整个信息系统的实体安全，提高信息系统安全管理水平，提高信息系统安全服务与应急响应能力。
- 保证互联网、电子商务及内网安全，防范来自互联网的恶意攻击，保证生产网、内网信息安全，保证业务持续性。

3 XX 信息安全保障体系规划思路

XX 整体设计思路是“生产第一、安全第一”的指导思想，立体多层次安全防御，与应用整合的安全架构。

- 立足从使用价值角度考虑安全建设，建立符合集团实际的整体安全系统。
- 强化层次、区域划分，分层次、分重点的进行立体防御，对特殊的功能区域单独防护。
- 防御遵循 P2DR 安全模型，制定符合集团实际情况安全策略，并采取访问控制和入侵检测技术等相结合，在实现访问控制基础上，加强安全事件的检测与预警、审计，实时掌握安全威胁，及时分析安全风险，并通过分析结果强化现有的安全配置，保持最佳的安全状态。
- 依据国际、国内及监管部门的法律法规，建设信息安全系统，来满足监管部对信息安全保障体系建设要求。
- 建立健全信息安全监控体系，加强应急演练，提高信息安全的预警、防范和处置能力。
- 建议加强安全意识教育和安全培训，并把此项工作长期开展。

4 XX 信息安全保障体系规划依据

（1） 国际信息安全标准

- ISO 27001 标准
- ISO 20000 标准
- IT 基础架构库（ITIL）

（2） 国内信息安全标准

- 等级保护建设（GB 17859-1999）
- 等级保护技术要求（GB/T 22239-1999）

（3） 监管部门(保监会)

《关于进一步加强保险系统信息安全保障工作的通知》

《中国保险业发展“十一五”规划信息化重点专项规划》

5 XX 信息安全保障体规划内容

5.1 XX 信息安全保障体系规划总述

任何一个体系的实现，均不可能一蹴而就，必须要分阶段、有步骤、循序渐进的实现。集团整体的信息安全体系覆盖面大、涵盖内容多、涉及人员广，必须要根据集团内现实情况、遵照监管安全要求、借鉴行业成功经验，在专业的安全专家的指导下，统筹规划、分步实现。

XX 信息安全保障体系规划按照短期（今年）、中期（明年）、长期（后年）、由易到难、整体上大致分为三个阶段（如图 5-1-1 所示）：

一、 **短期规划——体系框架设计搭建**。即第一阶段：IT 基础设施安全建设阶段

二、 **中期规划——体系框架细化落实**，即第二阶段：IT 基础运行环境安全建设阶段

三、 **长期规划——体系形成持续优化**，即第三阶段：IT 整体运营流程安全建设阶段

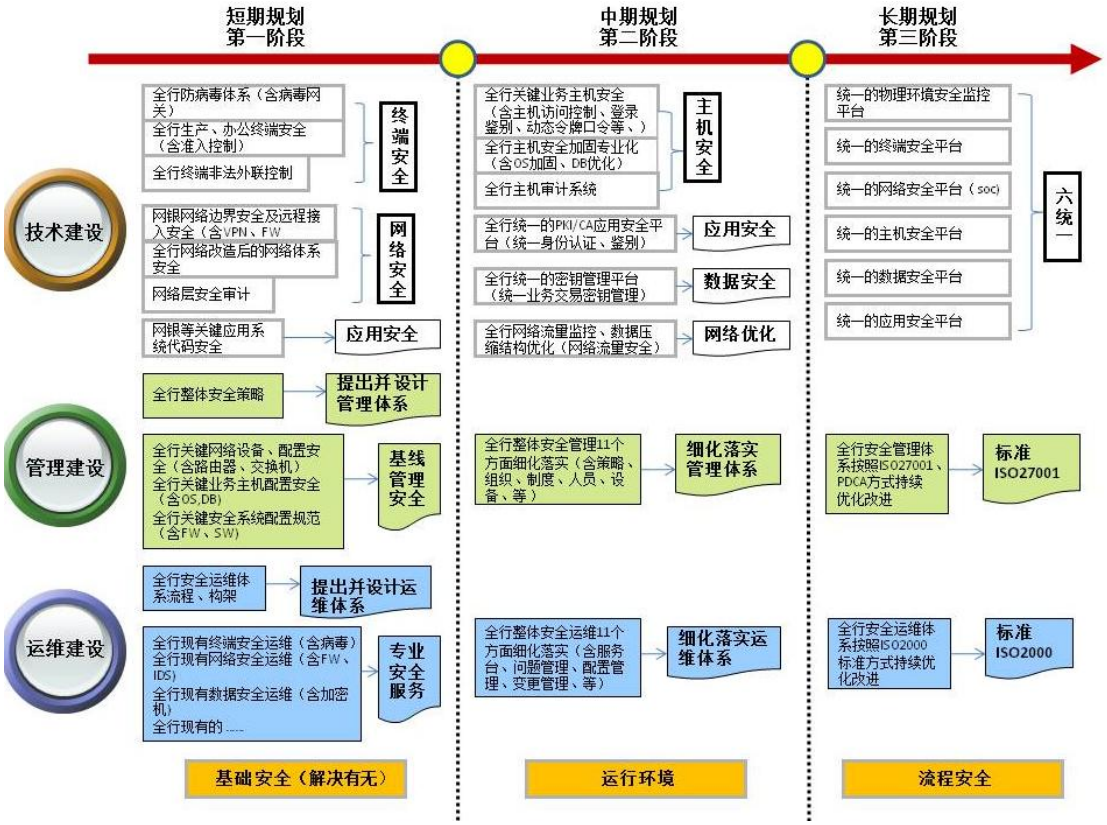


图 5-1-1

5.2 XX 信息安全体系规划细化说明

5.2.1 短期规划——体系框架设计搭建

第一阶段：IT 基础设施安全建设阶段，重点解决 XX 现有的安全系统的缺失项，即，我们自身已发现、已暴露的明显安全问题，解决安全技术或安全措施在集团的有无问题，满足监管要求，提出并搭建集团的安全体系框架。

本阶段安全体系建设的重点应突出在：通过自身已发现、已暴露的明显安全问题，找出集团病毒、终端、网络、运维等 IT 基础设施的安全风险，予以防范控制。具体的安全工程体现在如下方面：

5.2.1.1技术层面

集团第一阶段解决 IT 基础设施安全建设阶段，**重点是加强对网络安全与主机安全的建设，以及物理安全的建设**，具体如下：

1. 网络安全

网络安全规划重点是加强对边界安全项目、安全设备管理系统项目、网络层面的审计系统项目。

一、 边界安全

(一) 安全域划分

依据集团管理模式与现有业务对网络划分安全域，如：核心区域、办公区域、电销区域、广域网区域、外联区域、管理区域、电子商务区域、互联网区域、业务一区、业务二区、业务三区等，以下是对划分的安全区域（如图 5-2-1 所示），通过安全技术结合网络实际情况，依据等级保护技术要求，规划出适合我集团网络安全边界技术体系。

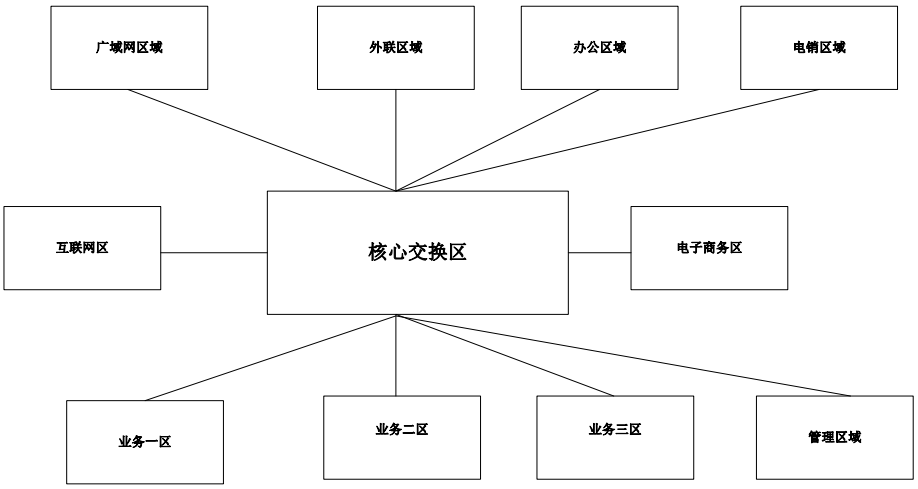


图 5-2-1

（1） 核心区域

核心区域为数据中心各功能区域提供路由、数据交换服务。建议内网与互联网应该物理隔离，如不能物理隔离，可以部署物理隔离网闸系统（或者防火墙系统），推荐部署物理隔离网闸系统来,保障业务网络中信息的安全。

（2) 电子商务区域

电子商务区域主要提供网上保险业务。以下是保障电子商务业务系统安全技术与规划拓扑（如图 5-2-2 所示）

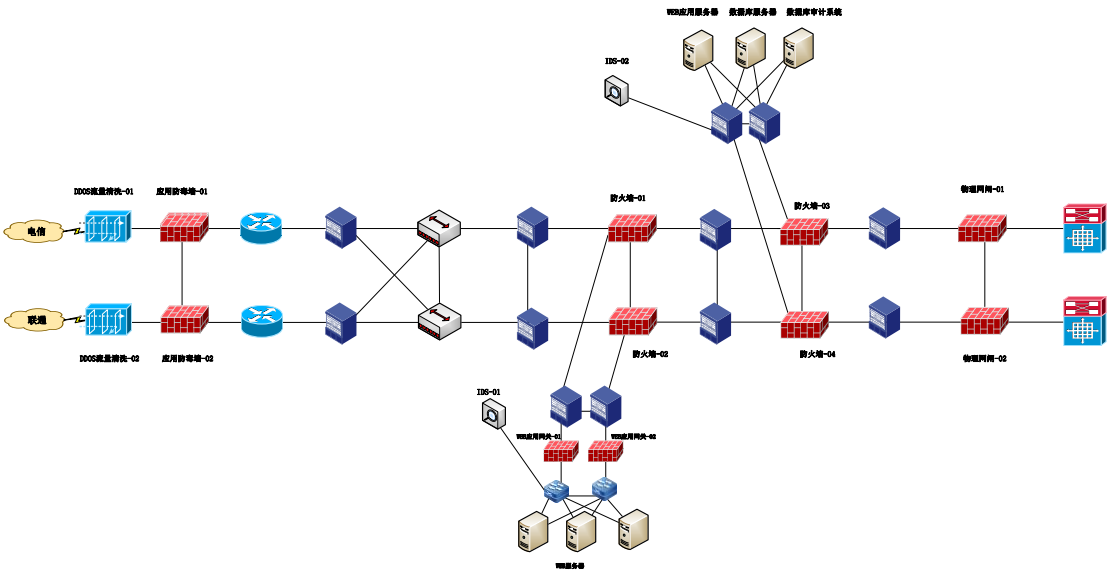


图 5-2-2

- 电子商务区域与 Internet 之间部署抗 DDoS 攻击系统，对来自互联网的 DDoS 攻击流量进行清除，同时保证正常访问流量的通过。
- 电子商务区域与 Internet 之间部署防火墙系统（外层防火墙），将电子商务 WEB 服务器保护在防火墙的一个单独的安全区域中，实现来自外网的访问控制。部署网络 IPS 设备，分别监控电子商务 WEB 服务器和电子商务 DB 服务器数据流量，对网络上传输的数据包进行深层分析，阻断各种恶意流量，提高业务系统的可用性，可有效地发现防火墙无法识别的特殊的应用层攻击行为。
- 电子商务 WEB 区域与后台数据库/应用服务器区域及信息中心网络之间设置防火墙系统（内层防火墙），实现电子商务 WEB 服务区与后台 APP 服务区之间的访问控制，电子商务 DB/APP 服务区与内部生产区域之间的访问控制，采用与外部防火墙异构的防火墙产品，即使攻击者成功获得外墙的控制权，也不能轻易攻入业务网络。

- 电子商务 WEB 区域购置 WEB 应用安全网关，对电子商务 Web 应用系统提供深度防护，实现 Web 系统漏洞扫描功能，检测 Web 应用程序是否存在 SQL 注入、跨站脚本漏洞。事中，对黑客入侵行为、SQL 注入/跨站脚本等各类 Web 应用攻击、DDoS 攻击进行有效检测、阻断及防护。事后，针对当前的安全热点问题，网页篡改及网页挂马，提供诊断功能，降低安全风险，维护网站的公信度。
- 电子商务 APP/DB 区域部署数据库审计系统，记录电子商务应用系统中对于数据库的操作行为，通过协议分析能够查询每个操作的详细报文，对安全事件能够快速精确地定位。
- 在内层防火墙与内网核心交换机之间部署物理网闸系统，实现在同一时间最多只有一个同隔离设备建立非 TCP/IP 协议的数据连接，抵御来自互联网接入区域的病毒及其他攻击等。

（3） 业务区域

业务区域（业务一区、业务二区、业务三区）主要是财险业务系统资源，以及健康险与寿险业务，还有集团业务。以下是规划技术与拓扑（如图 5-2-3 所示）

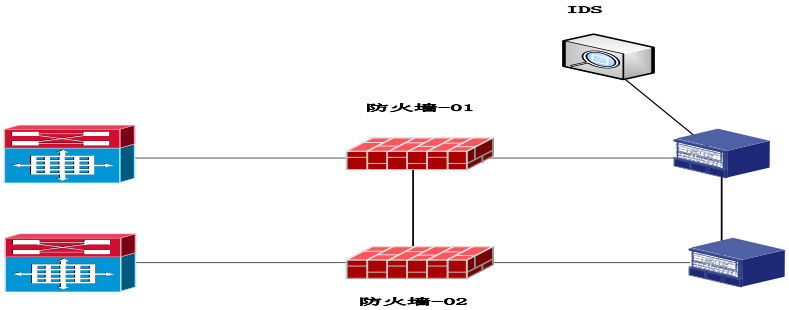


图 5-2-3

在核心区域与业务区域之间部署防火墙系统，实现对进出财险业务、寿险业务、及健康险业务、及集团业务等流量进行控制，实现安全区域安全隔离及阻止非法访问。部署 IDS 系统，实现对进出财险业务、寿险业务、及健康险业务、及集团业务等流量实时检测，监控各种网络行为，对违反安全策略的流量，IDS 系统告警响应（如短信、声音、邮件等），还可以与防火墙等网络设备进行联动，来阻断攻击流量，被入侵攻击后，入侵检测系统可以提供详细的攻击信息，便于取证分析。对于资源共用的区域，可以通过基于 VLAN 的方式来实现共享业务的隔离，并且在各汇集交换机控制 VLAN 三层接口的互通，来控制不需要互相访问的网络资源。

（4） 互联网区域

互联网区域主要是提供集团上互联网， 以下是规划技术与拓扑（如图 5-2-4 所示）

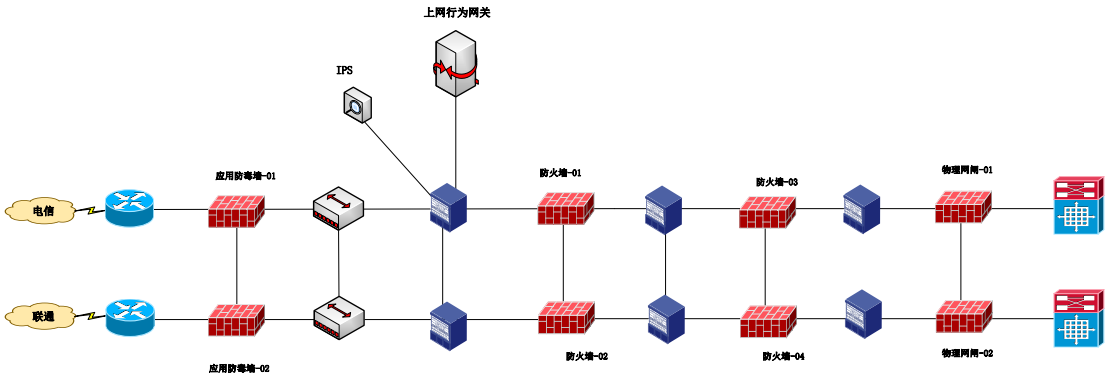


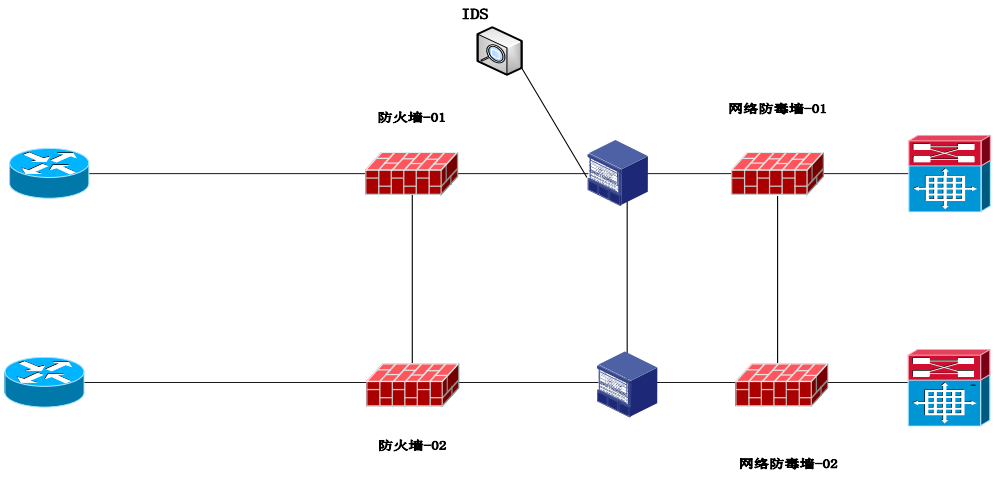
图 5-2-4

- 在互联网接入区域部署异构双层防火墙系统，保障了内网信息安全。

- 部署 IPS 系统，实现对访问互联网专网流量实时检测，监控各种网络行为，对违反安全策略的流量主动阻断。
- 在互联网出口部署应用层防毒墙，实现自动识别恶意站点，在连接层进行实时拦截。对网络流量深度检测，识别病毒、木马、恶意插件、钓鱼程序等各类应用层威胁并实时阻断，同时具备断电直通功能。
- 部署上网行为系统，实现对用户访问的网页进行精确分类，对各种互联网应用协议进行精确识别，为关键业务应用保障足够可用带宽；支持对用户实名制审计， 支持对 POP3、SMTP 协议收发邮件进行完整内容审计等。
- 在内层防火墙与内网核心交换机之间部署物理网闸系统，实现在同一同一时间最多只有一个同隔离设备建立非 TCP/IP 协议的数据连接，抵御来自互联网接入区域的病毒及其他攻击等。

（5） 外联区域

外联区域，通过专线连接合作伙伴，为合作方提供外联服务，如：银行业务等。以下是规划技术与拓扑（如图 5-2-5 所示）

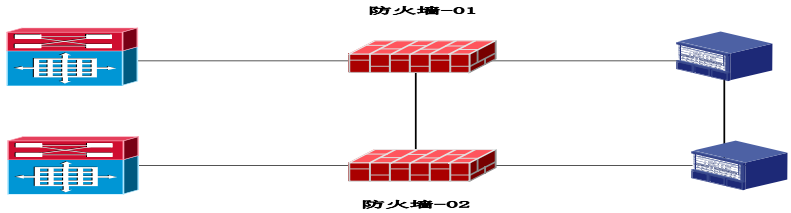


如图 5-2-5

在外联区域部署防火墙系统，对访问集团外联业务进行控制，实现安全区域安全隔离及阻止非法访问，并通过 NAT 屏蔽内网真实地址。集团部署 IDS 系统，实现对进出集团人民银行等流量实时检测，监控各种网络行为，对违反安全策略的流量，IDS 系统告警响应（如短信、声音、邮件等），还可以与防火墙等网络设备进行联动，来阻断攻击流量，被入侵攻击后，入侵检测系统可以提供详细的攻击信息，便于取证分析。部署网络层防毒墙实时拦截恶性病毒向其它区域扩散，要求可用性高，软硬件 bypass，不影响业务正常使用。

（6） 办公区域（电销区域）

办公区域提供集团 OA 系统、邮件系统等各业务系统。以下是规划技术与拓扑(如图 5-2-6 所示)

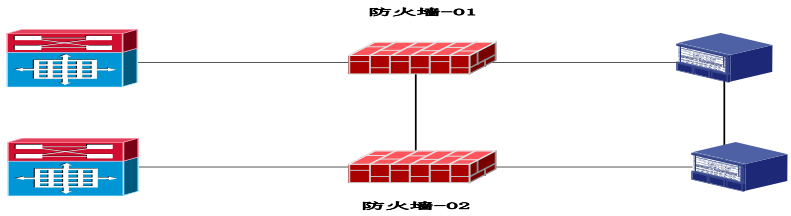


如图5-2-6

建议集团部署防火墙系统，对访问办公区系统（如OA系统、等），流量进行控制，阻止非法访问。

（7） 管理区域

管理区域提供集团网管系统、安管系统、运维系统等各种系统。以下是规划技术与拓扑(如图 5-2-7 所示)



如图 5-2-7

结合集团业务实际情况，集团部署防火墙系统，对访问业务一区系统（网管系统、运维系统等），流量进行控制，阻止非法访问。

二、 安全设备管理系统

依据等级保护技术要求结合集团网络实际情况，部署安全设备管理系统，对集团业务区（含一区、二区、三区）、外联接入区、互联网接入区，所有的安全设备（如防火墙、IDS/IPS、UTM、防病毒网关等），进行集中监控和告警管理。实现对安全设备的安全策略进行集中配置、分发和管理，协助用户实时掌握设备工作状态和安全状况，确保用户网络的安全运行和管理的一致性。对所有监控指标产生的告警进行集中的响应。支持声、光、电等各式告警方式，并能够通过手机短信、电子邮件等发出告警。能够自动或者手工地与客户网络中各种异构的网络设备和安全设备进行策略联动，例如向思科和华为交换机下发端口策略，向防火墙和 IDS 下发安全策，支持整体运行报表报告，为管理员提供决策支持的参考数据。

三、 网络审计系统

依据等级保护技术要求结合集团网络实际情况，集团部署安全审计管理系统，对集团业务区（含一区、二区、三区）、第三方接入区、互联网接入区，所有的安全设备（如防火墙、IDS/IPS、UTM、防病毒网关等）进行集中的安全日志审计，

应实现以下功能：

满足来自各种安全设备等日志收集，并进行存储、监控、分析、报警、响应和报告。可以随时了解整个IT系统的日志吞吐情况，在实时的日志分析中及时发现系统异常和安全事件，通过告警模块如邮件等方式及时通知管理员。在事后分析和报表中提供多种多样的运行分析报告，及时发现安全漏洞和非法访问行为，判断性能瓶颈和预测性能波动，同时为系统今后的战略规划提供依据。有助于完善组织的IT内控与审计体系，从而满足各种合规性要求，并且使组织能够顺利通过IT审计。

四、 AAA系统

依据等级保护技术要求结合集团网络实际情况，集团部署AAA系统，对登录网络设备用户提供统一安全管理。实现了对用户身份认证、授权（授权是用户和设备被给予对受控制的网络资源的访问权限的过程，授权行为发生在认证之后，当一个用户或设备已成功的认证之后，授权可以限制用户或者设备访问什么样的服务或执行什么样的命令）、审计（记账功能可以跟踪网络中发生的事件，提供网络环境的安全性。鉴于认证和授权对用户和设备访问网络资源进行了限制，记账就负责进一步的工作并记录被认证或被授权的行为。另外，记账也可以用来跟踪接入设备状态和TACACS+/Radius通信）。

2. 主机安全

主机安全规划重点是加强对端点准入安全项目、防病毒安全项目。

(一) 端点准入

依据等级保护技术要求结合集团实际情况，通过部署端点安全准入系统，对集团终端进行统一安全管理，并通过设定不同安全策略，来管理不同类别终端系统安

全。实现以下功能：

- **终端接入管理**

移动存储介质注册管理，访问控制，透明加密，移动存储介质认证，终端用户注册管理。

- **终端安全加固和运行监控**

补丁分发管理，病毒库升级管理，操作系统登录安全增强，网络参数监控终端，计算机资源占用监控，计算机帐号监控，与防火墙系统联动及接入控制，流量监控，资源与资产管理安全预警（资源滥用、资产变更、补丁与病毒库升级、非法访问、设备状态异常等）

- **用户行为监控和审计**

进程与服务监控，程序黑白名单管理，软件安装审计，即时通讯监控（QQ、MSN、UC、OIC）邮件监控，网络浏览审计，网络访问控制，屏幕监控

- **内网机密信息保护**

计算机终端外设管理，移动存储介质认证管理，内网用户认证，打印监控，文件操作审计，文件加密，计算机终端非法外联监控，内网接入控，网络共享访问监控。

(二) 防病毒系统

依据等级保护技术要求结合集团实际情况，针对集团不同类别终端系统的病毒防护进行技术规划

- 在内网部署两级管控的防病毒系统，即总控端—防病毒服务器（办公系统和

生产系统分别部署防病毒服务器），统一制订安全策略和下发特征码；集中监控防病毒运行情况，包括如防病毒客户端部署数量、客户端特征码更新情况、前十位病毒、前十大感染病毒客户端等；当新病毒爆发还没有获得最新病毒码时，根据病毒行为从总控端统一下发安全策略阻止病毒继续更大范围扩散；

- 部署邮件防病毒网关，实现对来自互联网的邮件病毒和垃圾邮件的检测和过滤；邮件防病毒网关能够自动识别恶意邮件发件源，并实时阻断；
- 在互联网出口部署应用层防毒墙，防毒墙通过对云端数据库进行查询自动识别恶意站点，在连接层进行实时拦截。对网络流量深度检测，识别病毒、木马、恶意插件、钓鱼程序等各类应用层威胁并实时阻断，同时具备断电直通功能；
- 在电子商务互联网出口，部署应用层防毒墙防范来自互联网的恶意代码威胁植入到电子商务服务器；
- 在网络汇聚点如第三方接入区等区域，部署网络层防毒墙实时拦截恶性病毒向其它区域扩散，要求可用性高，软硬件bypass，不影响业务正常使用；

3. 物理安全

依据等级保护技术要求结合集团机房环境情况，集团部署机房监控管理系统，对集团机房设备与环境统一监控，应实现以下功能：

- 可以对机房市电供电情况进行监控，对市电电压波动范围实时监测；
- 可以监测机房环境的温度、火警、浸水漏水等参数，并产生报警信息；
- 可以对机房内带干接点输出的UPS、精密空调监控报警；
- 可以设备电话号码接警，带有系统管理密码，提高安全性；
- 可以选择设置手机号码实现短信告警接警，远程掌控机房环境；
- 带有报警联动输出口，可供其他设备采集结合扩展实用；
- 可以通过短信远程查询各个监测参数，即便放假、出差也不会错失情报；

5.2.1.2管理层面

第二阶段管理体系规划主要项目:全行整体安全体系策略项目，提出并设计集团管理安全体系框架项目。

(一) 信息安全策略

信息安全策略是为信息安全提供管理指导和支持的一系列策略文件，通过该文档中所描述的条目进行信息安全建设过程的审核与评估，来得到信息安全建设与信息安全目标的符合度。制定适合组织安全策略，通过工程项目实施来对策略落地。集团信息安全策略框架规划如下:

- 对现有信息资产进行评估

对集团的信息安全资产进行充分的评估，可以发现集团信息系统风险点，通过制定相应的安全策略来控制风险。集团应该制定含技术、管理、运维这三个维度的安全策略，只有完善这三个方面的策略，才能制定适合集团需求的安全策略。

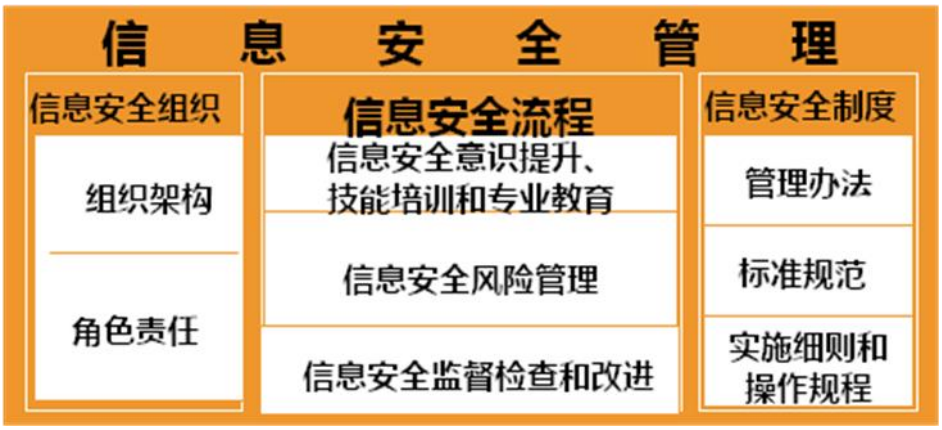
- 制定安全策略框架

依据等级保护技术要求、ISO27001 标准，结合实际情况组织的信息安全策略框架如下：

主策略是信息安全总体目标，子策略是依据等级保护技术要求与 ISO27001 制定。

(二) 信息安全管理体系

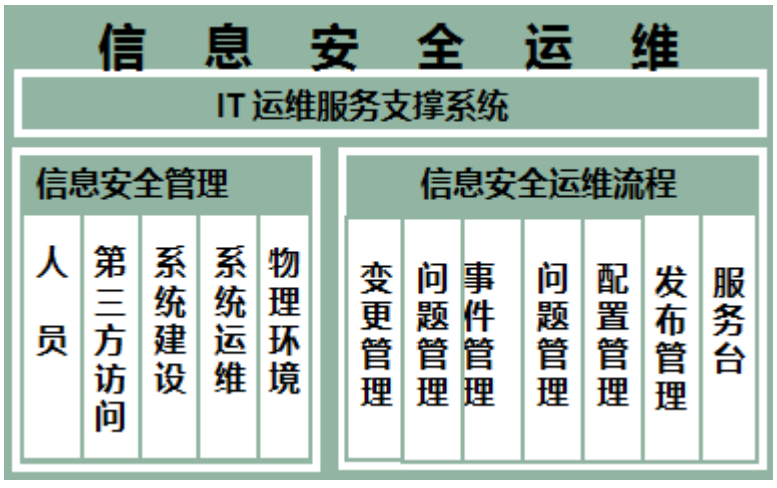
信息安全管理体系框架设计是依据 ISO27001 与等级保护技术要求，并结合实际情况，设计框架如图



5.2.1.3运维层面

集团整体安全运维体系项目，提出并设计集团运维安全体系框架。集团现有终端安全运维项目（含：防病毒），集团现有网络安全运维项目（含：防火墙、入侵检测等安全设备）、集团现有数据、主机、应用等安全运维项目（含：加密机等），采用专业化的安全运维服务，解决集团基础设施安全运维问题。

信息安全管理体系框架设计是依据 ISO2000 与 ITIL 要求，并结合实际情况，设计框架如图



5.2.2 中期规划——体系框架细化落实

第二阶段：IT 基础运行环境安全建设阶段，在补充、解决了集团安全技术或安全措施的明显不足和缺失项后，重点进行数据、应用等较高和较难层面的安全

体系建设，将网络优化、安全管理、安全运维进行细化、充实、落地，解决集团 IT 运行环境安全问题，对集团的整体安全体系框架进行细化完善。

具体的安全工程体现在如下方面：

5.2.2.1技术层面

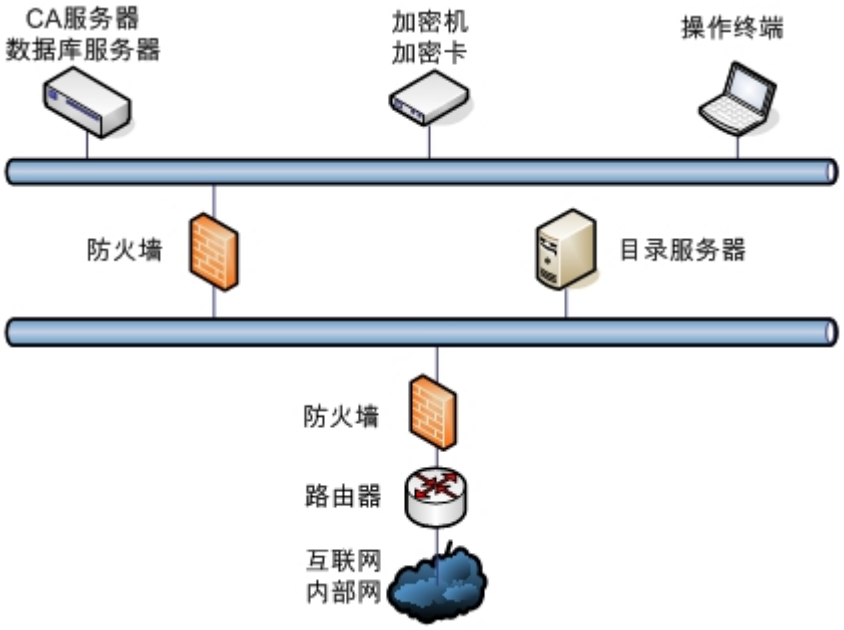
集团第二阶段解决 IT 基础运行环境安全建设阶段，**重点是加强对应用安全与数据安全的建设，**如下：

- **应用安全**

应用安全规划重点是集团 PKI 信任体系项目与应用系统资源监控平台项目。

（一） PKI 体系建设

依据等级保护技术要求结合集团实际情况， 建议集团建立 PKI 体系，并将其嵌入集团重要应用之中，以下是具体规划内容与拓扑(如图 5-2-11 所示)



- 在内网建设 CA 服务器。密钥生成和管理由证书服务器密码机负责。CA 服务器负责证书的申请、签发、作废和管理。
- 采用一主两从 LDAP，内网部署一主一从，外网部署一从。内网的主 LDAP 数据自动推送到内网从 LDAP，手工导入到外网从 LDAP。CA 服务器的证书和 CRL 列表定期发布到内网主 LDAP。
- 操作终端提供证书申请的管理和日常操作。

- 在内网部署电子签名中间件，进行双向的签名和验签。管理终端完成证书的申请和发放工作；采用数据库，用于证书服务器生成证书和 CRL 的存储。
- 为应用服务器颁发服务器证书，为个人用户颁发个人证书。登录时，实现双向验证，确保应用服务器身份和个人身份的真实性；
- 手持 USB KEY，带有密码芯片算法的 KEY，存储量大于等于 32K，用于私钥存储。

  实现功能如下：

  通过强身份认证手段的采用，确保用户身份的真实性。通过电子签名，确保数据的不可否认性、不可抵赖性和事后可追溯性。所投资的安全设备，可以为其它业务系统提供安全服务。

（二） 应用监控管理系统

依据等级保护技术要求结合集团实际情况，建议集团部署应用监控管理系统，对集团重要应用系统进行统一监控。实现:应用监控管理系统通过 Web 浏览器对各种操作系统和应用程序进行监控，监控对象包括应用服务器、Web 服务器、数据库管理系统、操作系统、网络服务等；当被监控的应用出现故障或超过监测的阈值时，应用监控管理系统会产生相应的告警，并提供故障原因的分析，帮助管理员快速进行问题定位。

应用监控管理系统可以通过电子邮件、短信等方式通知用户，也可执行外部命令对故障进行修复；通过集成的报表功能，还能方便地进行趋势分析并把握系统的能力限度。

- **数据安全**

数据安全规划重点是密钥管理平台项目与数据防泄漏系统项目

（一） 密钥管理平台

依据等级保护技术要求，结合集团实际情况，集团部署一套密钥管理平台，对集团密钥进行管理。实现了以下功能：

- 密钥对的生成，支持预生成和实时生成；
- 密钥对加密存储；

- 密钥对备份和恢复；
- 密钥对归档；
- 密钥对下载服务；
- 密钥对撤消服务；
- 密钥对恢复服务。

（二）数据防泄漏系统

依据等级保护技术要求结合集团实际情况，建议集团部署数据泄漏保护系统对重要核心业务数据进行保护，实现以下功能：

- **用户管理:**采用多角色的访问控制技术对用户进行管理，角色之间互相监督、协调合作,提供灵活安全认证机制和统一授权管理方案,从根源上保证数据安全
- **外设管理:**全程管控移动存储设备使用生命周期，加密存储信息，有效的防范数据泄露，灵活支持内网专用和内外网通用两种策略模式，外设权限细粒度划分，确保外出数据不泄密。全面管理计算机连接移动设备的端口，保护企业免遭数据丢失风险
- **策略管理:**统一管理安全策略，具备智能学习功能，支持策略模板定制和全局策略控制方式。设置离线策略，随时掌控离线终端安全；配置白名单策略，实现自动解密，提高工作效率
- **日志审计:**记录全面的、可追溯的日志。日志内容存放安全且查询方便，充分考虑到海量日志记录时服务器自身安全，支持分类检索、排序、多格式数据输出
- **备份还原:**提供数据库和文件自动备份功能，以及数据库迁移的功能，备份的文件按照不同版本备份，最大限度保障文件的完整性，使服务器能够随时恢复至先前状态

- **主机安全**

主机安全规划重点是集团关键业务主机安全项目（含：主机访问控制、登录鉴别、动态令牌等），全行关键集团系统安全加固项目（含：操作系统加固、数据库优化），集团关键主机安全审计项目

（一） 主机身份认证系统

依据等级保护技术要求结合集团实际情况，集团对登录重要PC服务器、小型机、重要PC终端的用户，部署动态口令系统（也可以部署PKI体系，实现对主机身份系统认证）.。

- 防止账号和密码泄露时可能造成的各种损失，提高用户账号的安全性。
- 方便密码管理，通过动态口令令牌产生口令，避免密码遗忘或记错。
- 使用方便，无需安装任何软件，也无需连接计算机。

（二） 主机安全审计系统

依据等级保护技术要求结合集团实际情况，集团部署主机审计系统，收集各种重要主机系统日志，并能实现原始记录的智能存储；在安全信息的处理方面，通过安全信息的统一化、聚合及时地产生告警和安全事件；在安全信息可视化方面，提供了基于Web的监控门户以及预定的上百种报表，为客户集中管理、集中监控、有效审计等服务。

（三） 主机系统安全加固

主机加固方法

进行操作系统安全加固的方法有多种，通常包括选用安全的专用的操作系统、采用垫片技术等，但是这些技术手段往往要中断业务的运行，并且是否会对业务系统产生不可预知的影响，所以目前并不推荐这两种方法。

目前主流的系统加固还是通过以下一些手段来实现：

- 强制访问控制功能；
- 实现内核级的文件访问控制

允许用户制订文件/目录访问规则，任何用户（包括系统管理员）对敏感文件或目录进行创建、删除、修改、读取等操作时，将根据规则进行过滤（允许或拒绝）；

- 注册表的访问控制

允许用户制订"只读"注册表项列表，任何用户（包括系统管理员）对“只读”注册表项进行写操作将无条件拒绝；

- 进程访问控制

允许用户制订受保护的进程列表，任何用户（包括系统管理员）无权停止受保护进程；

- 服务访问控制

通过及时发现新增服务，并立即强行终止和删除新增服务，达到对服务进行访问控制的目的；

- 文件的完整性检测

由用户指定需要建立校验信息的关键性只读目录及数据文件名称，检测程序自动记录目录中所有文件的基本属性及内容校验和。通过定期进行校验和的有效性检测，可以达到验证重要文件或目录完整性的目的；

- 服务的完整性检测

检测程序自动记录目录中所有服务的基本属性及内容校验和。通过定期进行校验和的有效性检测，可以达到验证服务完整性的目的；

- WEB请求监测过滤

监测所有用户提交的GET、POST请求，监测服务器的返回信息，防止非法的请求和返回非法的信息；

- 系统自身的保护功能
- 保护系统自身进程不被异常终止、伪造、信息注入。

配置安全增强与加固

充分利用操作系统自带的安全机制是增强系统安全性的重要而可行的措施，尤其是对于一些需要重点防护的重要服务器。安全配置要点包括：

- 根据需要对操作系统进行必要的内核配置裁减；
- 服务配置；
- 用户帐户/口令安全配置；
- 审计策略；
- 注册表配置；
- 文件系统权限；
- WEB服务器的脚本配置；
- 系统补丁。

数据完整性

除了对系统配置进行加固以外，如何保证相关数据的完整性，防止人为的或无意的更改导致系统不可用也是我们要考虑的一个问题。主要包括：

- 如何保证系统日志的完整性，防止破坏者进行日志的删除和更改；

- 如何保证业务系统应用文件的完整性，防止被非法篡改；
- 如何保证系统配置文件的完整性，包括策略配置文件以及一些基础的服务配置文件；
- 如何实现在数据完整性被破坏后，能够及时地发现并进行恢复。

依赖系统平台安全性

数据库系统都运行在特定的平台之上，我们可以参照操作系统安全解决数据库运行平台安全。并且数据库系统也有补丁，我们可以跟踪不同的数据库厂商提供的资料，及时地对数据库进行不定更新。

数据库系统配置优化

无论是从数据库本身配置，还是从代码角度来考虑，优化总是可以提高数据库系统的性能。所以我们可以进行各项参数的优化，保证数据库系统具备高可用性。另外需要重点关注的是代码安全，这也是当今业界流行的话题。和数据库进行连接的程序代码是否安全至关重要，甚至攻击者会从代码中轻易的发现数据库的具体结构和连接信息，从而获取管理权限。

数据完整性

数据库系统的安全需求，首先应满足完整性要求，数据库的完整性包括：

- 物理上的数据库完整性

预防数据库数据物理方面的问题，如掉电以及当被灾难破坏后能重构数据库；

- 逻辑上的数据库完整性

保持数据的结构，比如：一个字段的值的修改不至于影响其他字段。

为维护数据库的完整性，一方面，必须有访问控制机制，确保只有授权用户才能进行数据查询、更新或删除； 另一方面，还必须根据应用系统的不同特点，周期性地对数据库文件做备份，数据库管理系统必须维护对事务的记录，必须有一套恢复机制，以便在系统出错后能及时恢复、重建数据库，最低限度减少损失。门户网站的各种数据库系统建设都必须满足完整性的要求，必须具备访问控制、备份恢复机制。

用户认证

数据库管理系统要求进行严格用户认证，确保每个用户身份被正确地识别，既便于审计追踪也为了限制对特定的数据进行访问。

在门户网站中，数据库系统设计一定要按照不同角色严格设置用户权限，防止安全问题的发生。

访问控制

允许用户只访问被批准的数据，以及限制不同的用户有不同的访问模式，如读或写。

数据库通常根据用户访问特权在逻辑上将数据分离。如一般用户访问一般数据、计财部门可以得到收入进度数据以及人事部门可以得到工资数据等。

数据库管理指定应该允许谁访问哪些数据，这些数据可以是字段或记录，或者甚至是元素级的。数据库管理系统必须实施这一访问策略，授权访问或者禁止访问所指定的数据，而且存取方式多种多样。数据库管理系统能批准一个用户或者程序有权读、改变、删除或附加一个值，增加或删除整个字段或记录，或者重新组织整个的数据库。

- **网络安全**

  集团网络流量监控、数据压缩、结构优化项目（网络流量安全），对集团网络安全体系进行优化、提升。

（一）网络流量优化系统

依据等级保护技术要求结合集团实际情况，集团部署网络流量优化系统，对**互联网**或者**广域网**流量进行监控、分析、及优化。实现以下功能：

- 增强了带宽使用与网络流量的可视化程度
- 保障了关键业务应用的高效、有序运行
- 提高了带宽使用效率，降低了 IT 投资成本
- 降低了网络运维管理成本，减少了日常网络使用投诉
- 提高了员工工作效率、保障关键人员使用，降低了人力成本
- 完善的流量报表为分析、优化、备查提供了强有力的依据
- 提高了网络运行的可靠性、可控性、安全性及可预见性

5.2.2.2管理层面

集团整体安全管理 11 个方面的细化、落实（含：策略、组织、制度、人员、设备等），细化、落实集团安全管理体系。

集团第二阶段主要项目是信息安全策略咨询项目与信息安全管理体系咨询项目。

（一） 信息安全策略

第一阶段规划信息安全策略框架，依据 ISO27001 与等级保护，细化安全策略框架，对框架内容进行细化，如：

- **技术策略**

避免将重要网段部署在网络边界处，且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

- **管理策略**

信息系统部每年均需编制一份生产性信息系统清单，详细列出现存所有生产性硬件、软件和通信连接设备。

- **运维策略**

管理层必须制定并定期更新和检验业务恢复计划，对发生业务中断事件时如何启用备用设施、使员工继续正常操作作出规定。

（二） 管理体系

第一阶段规划是管理体系框架，第二阶段依据 ISO27001 与等级保护，细化管理体系框架，主要从下面几个方面进行规划。

- **组织安全**

一是要建立企业信息安全管理组织体系，要配备总部和直属企业两级信息安全领导小组、信息安全管理部门、信息安全员，将企业信息安全的责任层层分解，责任到人，落到实处。

二是要按照内控要求，配备信息技术、信息安全岗位人员，要把决策与执行分开、执行与监管分开，相互约束，相互促进，防止关键岗位人员监守自盗。

三是要加强信息安全教育和信息安全、保密知识普及，让广大干部职工了解什么需要保密、失密的后果以及应该如何保密。

四是要加强信息安全管理人员和技术人员专业知识、专业技能培训，比他们掌握常用信息安全技术，学会定密、监控、防范、处置查证。

- **管理制度**

集团需要制定信息安全管理规章制度，如保密制度、机房管理办法、网络运行管理办法、各应用系统运行管理办法、设备维护工作行为规范、值班制度、网站内容更新管理办法、应急预案等要健全岗位责任制，明确机房管理员、网络管理员、系统管理员、数据库管理员、服务台工作人员、现场服务人员等岗位职责，落实到人，奖惩结合要结合信息技术服务管。

5.2.2.3运维层面

集团整体安全运维需要从 11 个方面的细化、落实（含：服务台建设、配置管理、变更管理、问题管理等），细化、落实集团安全运维体系。

建立信息安全运维流程,依据 ISO20000 或者 ITIL，建立监控、事件管理、问题管理、变更管理、配置管理、信息发布、等流程，使安全工作规范化要有计划地组织好信息安全评估和应急演练。

5.2.3 长期规划——体系形成持续优化

第三阶段：IT 整体运营流程安全建设阶段，在集团的整体安全体系框架细化完善的基础上，重点解决流程安全问题，通过技术体系的“六统一”，管理和运维体系的“两个标准化”建设，全面实现集团的整体信息安全体系，并能够持续改进、优化。具体的安全工程体现在 SOC 项目建设与信息安全服务项目。

5.2.3.1技术体系“六统一”

统一的物理环境安全监控平台、统一的终端安全平台、统一的网络安全平台（SOC）、统一的主机安全平台、统一的数据安全平台、统一的应用安全平台，符合、满足保监会、公安部的安全监管要求，实现涵盖物理、终端、网络、主机、数据、应用六大层面安全体系。

第三阶段建设重点是 SOC 平台建设，最终形成六统一系统模式，以下是规划

内容：

对于集团网络来说，应该本着重点防护，分步实施的策略来进行信息安全建设。建议在第二阶段依据 ISO2000 与 ITIL 制定适合集团运维流程，当这套运维流程成功实施，运行并积累一定经验后，可以通过部署 SOC 平台来实现自动化运维流程管理。

所部署的 SOC 平台应该具备以下一些功能：

◆ 管理对象

被监控管理的目标包括：网络系统、服务器主机、数据库、安全产品、业务应用。按照不同的关键业务点来划分进行资产管理。

◆ 运维管理

网络安全的最重要目标就是保障系统的安全、可靠的运行，也就是保障业务的连续运行，这也是我们所熟知的安全三性中的可用性。对系统进行基于业务的监控管理，包括：资产管理、流程管理、知识管理等。

◆ 网络管理

网络系统作为业务应用的载体，对其的监控管理也非常重要，我们采用网管技术对网络系统进行监控管理。内容包括：拓扑展示、设备发现、管理工具

◆ 安全管理

网络安全运行管理中心的核心内容，从安全策略管理、事件管理、脆弱性管理、风险管理、配置管理等方面，实现安全管理。

◆ 输出

通过报表、报警、工单的方式，得出相应的输出。包括：视图、资产报表、风险报告、安全状态、趋势分析、脆弱性报告、知识库、专家建议等。

信息安全保障体系建设是一项长期的工作，不可能一毗而就，也不可能一步到位，必须与时俱进，持续完善。通过信息安全风险评估方法，发现信息安全风险，对技术体系优化及改进。建议采用专业的安全服务来实现信息安全体系优化与改进。

5.2.3.2管理体系“ISO27001 信息安全风险管理国际标准”

按照 ISO27001 标准，采用 PDCA 的方式方法、持续优化改进集团整体信息安全管理体系，建议采用专业的安全服务来实现信息安全体系优化与改进。

5.2.3.3运维体系“ISO20000 运维国际标准”

按照并采用 ISO20000 运维国际标准，持续优化改进集团整体信息安全运维体系，建议采用专业的安全服务来实现信息安全体系优化与改进。

6 建立专业的安全服务建议

在前面的第一阶段运维体系规划中我们已经提出，应该“借助专业的第三方安全服务，专业的安全服务是建立一个能够持续运行，动态更新的网络安全体系的技术保障。和关键环节。

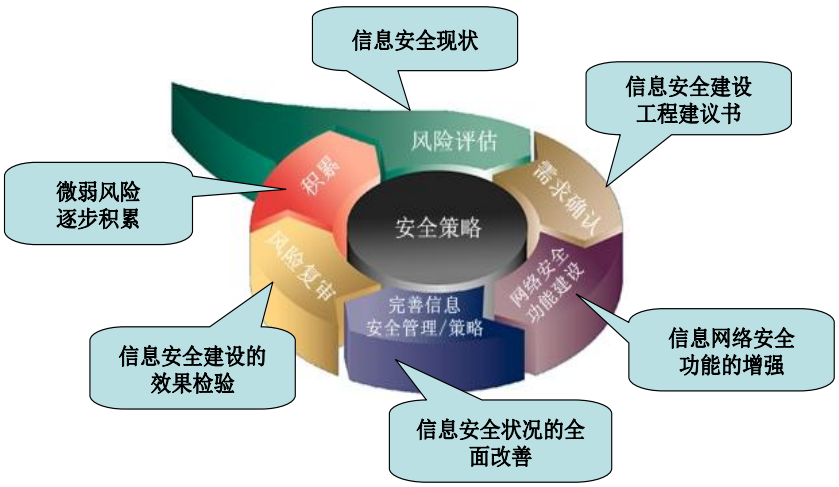


图 5.5 动态信息安全体系建设过程

动态信息安全体系建设是一个周期性的循环过程，每个建设周期都是以安全策略为核心，以风险评估为开端，通过需求确认、网络安全功能建设、完善信息安全管理/策略、风险复审、风险积累的过程，建立信息安全体系。

对于现阶段的集团信息安全系统来说，我们建议通过以下方面来实现动态的信息安全体系建设过程。

6.1 服务内容

6.1.1 安全更新服务

服务项	服务编号	服务任务	服务目标
防病毒系统更新	AV-UPD	更新防病毒服务器病毒库，并进行服务状态检查。	保证 XX 防病毒服务器具备最新的病毒特征库，并能够正常提供服务。
WSUS 补丁管理系统更新	PAT-UPD	更新补丁服务器安全补丁，并进行服务状态检查。	保证 XX 补丁管理服务器具备最新的补丁更新程序，并能够正常提供服务。
IDS 更新	IDS-UPD	更新 IDS 系统事件特征库，并进行服务状态检查。	保证 XXIDS 系统具备最新的事件特征库，并能够正常提供服务。
安全网关更新	GW-UPD	更新安全网关相关特征库（病毒定义库、攻击特征库、垃圾邮件特征库等），并进行服务状态检查。	保证 XX 安全网关具备最新的特征库，并能够正常提供服务。

6.1.2 安全检查服务

服务项	服务编号	服务任务	服务目标
上线安全检查	APP-CHK	检查业务系统上线之前安全配置情况，并实施安全加固。	保证总行业务系统符合安全配置要求。

系统脆弱性检查	SV-CHK	检查运行中的业务系统、网络支系统的包括 OS、数据库和应用服务等的各组件安全状态，并实施安全加固。	保证总行业务系统、网络系统具备最佳的安全配置。
符合性检查	CMP-CHK	检查服务器、网络和安全系统配置是否符合技术规范要求，并提供改进方案。	保证总行和支行的服务器、网络和安全系统配置符合总行和相关主管机构要求。
常规巡检	GEN-CHK	检查网络和安全设备、网络基础服务系统的运行状况。	保证总行和支行的网络相关系统、基础服务等运行正常。

6.1.3 安全分析服务

服务项	服务编号	服务任务	服务目标
计算机安全事件分析	HST-ALS	分析计算机病毒状况、补丁状况及其他安全事件，并提供改进建议。	及时掌握计算机安全事件发生状况，提供持续性预防与改进。
网络安全事件分析	NET-ALS	分析网络异常事件，并提供改进建议。	及时掌握网络安全事件发生状况，提供持续性预防与改进。
安全预警	GEN-ALS	分析业内最新的计算机病毒、操作系统补丁、网络设备更新程序、应用服务更新程序等安全事件，针对性地提供预防和	及时掌握行业内安全事件状况，提供持续性预防与改进。

		改进建议。	

6.1.4 安全支持服务

服务项	服务编号	服务任务	服务目标
计算机安全事件技术支持	CLE-SEV	对终端计算机由于病毒、补丁、程序异常等引起的事件提供支持。	及时有效处理终端计算机安全事件。
网络安全系统技术支持	SYS-SEV	对防火墙、VPN 和 IDS 等安全系统提供支持。	及时有效处理 XX 技术支持请求，提高安全技术水平。
运维管理支持	OPT-SEV	对关键区域安全系统提供管理和维护支持。	及时有效处理变更事件。
系统测试	PDT-SEV	对安全技术、安全产品和安全解决方案进行测试。	选择符合要求的安全技术、安全产品和安全解决方案。
应急响应	EMR-SEV	对紧急事件提供应急响应服务。	及时有效处理重大安全事件。

6.1.5 安全咨询服务

服务项	服务编号	服务任务	服务目标
编写安全策略	POLICY-ASS	编写信息安全策略。	完善信息安全策略。
编写安全技术规范	SPEC-ASS	编写相关安全技术规范。	完善安全技术规范。
编写安全配置标	CONFIG-ASS	编写安全配置标准。	完善安全配置标准。

准			
培训	TRAINING-ASS	提供技术和管理培训。	提高安全管理水平。

6.2 服务范围

6.2.1 安全更新服务

服务项	服务编号	服务频率	服务范围
防病毒系统更新		每日	XX 防病毒服务器
WSUS 补丁管理系统更新		半月	XX 补丁管理服务器
IDS 系统更新		每周	XXIDS
安全网关更新		每日	XX 互联网安全网关

6.2.2 安全检查服务

服务项	服务编号	服务频率	服务范围
上线安全检查		需要	总行新上线业务系统
系统脆弱性检查		季度	总行核心机房业务系统、网络和安全系统
符合性检查		每支行一年一次 /总行每季度	XX
常规巡检		每支行一年一次 /总行每月	XX

6.2.3 安全分析服务

服务项	服务编号	服务频率	服务范围
计算机安全事件分析		半月	XX
网络安全事件分析		每月	XX
安全预警		需要	XX

6.2.4 安全支持服务

服务项	服务编号	服务频率	服务范围
计算机安全事件技术支持		日常	XX
安全系统技术支持		日常	XX
运维管理支持		日常	XX 授权系统
系统测试		需要	总行
应急响应		需要	XX

6.2.5 安全咨询服务

服务项	服务编号	服务频率	服务范围
编写安全策略		需要	总行

编写技术规范		需要	XX
编写配置标准		需要	XX
培训		需要	XX

6.3 服务报告(文档)

6.3.1 安全更新服务

服务项	报告(文档)编号	报告(文档)名称	报告(文档)周期
mcafee 防病毒系统更新	服务编号+文档名称+时间（下同）	日常更新报告	每周
		更新异常报告	需要
		系统变更报告	需要
WSUS 补丁管理系统更新		日常更新报告	每月
		更新异常报告	需要
		系统变更报告	需要
IDS 更新		日常更新报告	每周
		更新异常报告	需要
		系统变更报告	需要
安全网关更新		日常更新报告	每周
		更新异常报告	需要
		系统变更报告	需要

6.3.2 安全检查服务

服务项	报告(文档)编号	报告(文档)名称	报告(文档)周期
上线安全检查	服务编号+文档名称+时间（下同）	系统安全分析	需要
		系统安全检查报告	需要
		系统加固建议书	需要
		系统加固报告	需要
系统脆弱性检查		检查计划	每季度
		安全检查报告	每季度
		系统加固建议书	每季度
		系统加固报告	每季度
符合性检查		符合性检查计划	需要
		符合性检查报告	需要
		改进建议书	需要
常规巡检		常规巡检计划	需要
		安全巡检报告	需要

6.3.3 安全分析服务

服务项	报告(文档)编号	报告(文档)名称	报告(文档)周期
计算机安全事件分析	服务编号+文档名称+时间（下同）	病毒事件分析	每半月
		补丁管理事件分析	每月
网络安全事件分		网络安全事件分析	每月

析		预防与改进建议	每月
安全预警		安全预警？	每季度
		预防与改进建议	每季度

6.3.4 安全支持服务

服务项	报告(文档)编号	报告(文档)名称	报告(文档)周期
计算机安全事件技术支持	服务编号+文档名称+时间（下同）	事件处理纪录	每周
		问题分析	需要
		事件支持总结	每半月
		预防与改进建议	需要
安全系统技术支持		事件处理纪录	每半月
		问题分析	需要
		事件支持总结	每月
运维管理		变更记录	需要
		实施方案	需要
		配置文档	需要
测试服务		测试方案	需要
		测试计划	需要
		测试报告	需要
应急响应		应急响应报告	需要
		预防与改进建议	需要

6.3.5 安全咨询服务

服务项	报告(文档)编号	报告(文档)名称	报告(文档)周期
编写安全策略		信息安全策略	需要
编写安全技术规范		安全技术规范	需要
编写安全配置标准		安全配置标准	需要
培训		培训讲义	需要
		培训考核报告	需要

6.4 安全咨询与应急响应

6.4.1 安全咨询

（一） 现状调查和风险评估

现状调查和风险评估是建立 XX 信息安全保障体系的基础和关键，在整个集团信息安全建设项目过程中，现状调查和风险评估的工作量占了很大比例，现状调查和风险评估的深度直接影响信息安全体系能否与集团实际情况相一致且具有可操作性。

现状调查和风险评估的主要目标包括对 XX 信息系统进行全面的现状调查、建立保护对象框架和根据保护对象框架进行风险评估。

■ 全面的现状调查

全面现状调查是本项目十分关键的步骤，现状调查的广度和深度将对保护对象框架的建立和风险评估带来非常十分重要的作用。在全面现状调查中 XX 信息系统的场所、环境、网络、网络设备、主机、操作系统、数据库、中间件、应用软件、业务流程、管理制度和组织机构将得到全面的调研。

■ 风险评估

风险评估的目的是了解 XX 信息系统的安全现状，以便在安全体系的实施过程进行需求分析和解决方案设计。风险评估过程包括对 XX 信息系统的资产安全价值、弱点严重性、威胁可能性和现有安全措施等进行估值，并通过这些因素计算风险值。

风险评估的具体目标包括：

准确地获得 XX 信息系统安全现状；

获得 XX 信息系统风险现状，为安全对策框架设计提供依据。

（二） 安全策略制定及方案设计

为迎接 XX 信息业务的飞速发展而带来信息安全方面的挑战，规范 XX 信息系统的安全维护管理，促进安全维护和管理工作体系化、规范化，提高信息和网络服务质量，提高网络维护队伍的整体安全素质和水平，需要制定安全方针和系列安全制度和规范。安全方针的目标是为信息安全管理提供清晰的策略方向，阐明信息安全建设和管理的重要原则，阐明信息安全的所需支持和承诺。

安全策略是指导 XX 信息系统维护管理工作的基本依据，安全管理和维护管理人员必须认真执行本规程，并根据工作实际情况，制定并遵守相应的安全标准、流程和安全制度实施细则，做好安全维护管理工作。

安全策略的适用范围是 XX 信息系统拥有的、控制和管理的所有信息系统、数据和网络环境，适用于属于 XX 信息系统范围内的所有部门。对人员的适用范围包括所有与 XX 信息系统的各方面相关联的人员，它适用于全部应用 XX 信息的员工，全部 XX 范围内容的维护人员，集成商，软件开发商，产品提供商，顾问，临时工，商务伙伴和使用农行信息系统的其他第三方。

安全策略体系建立的价值在于：

◆ 推进信息安全管理体系的建立

- 安全策略和制度体系的建设
- 安全组织体系的建设
- 安全运作体系的建设

◆ 规范信息安全规划、采购、建设、维护和管理工作，推进信息安全

的规范化和制度化建设

6.4.2 安全应急响应方案

（一） 安全事件响应的概念和基本流程

应急响应也叫紧急响应，是安全事件发生后迅速采取的措施和行动，它是安全事件响应的一种快速实现方式 。应急响应是解决网络系统安全问题的有效安全服务手段之一。其目的就是最快速度恢复系统的保密性、完整性和可用性，阻止和减小安全事件带来的影响。

识别出现安全事件的场景包括：

- 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；
- 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；
- 拒绝服务，正常用户不能正常访问服务器提供的相关服务；
- 系统性能严重下降，有不明的进程运行并占用大量的 CPU 处理时间；
- 在系统日志中发现非法登录者；
- 发现系统感染计算机病毒；
- 发现有人在不断强行尝试登录系统；
- 系统中出现不明的新用户账号；
- 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；
- 文件的访问权限被修改；
- 因安全漏洞导致的系统问题；
- 其它的入侵行为。

集团根据自己信息系统实际情况，需要制订应急响应演练计划，明确应急响应组织、响应人员、人员职责、响应方式、工作内容，定期对相关人员进行应急响应培训，定期组织应急响应演练。

各部门领导及管理员应当对紧急响应流程的演习和执行情况进行有效的监督和管理。

（二） 建立应急响应组织

应急响应组织是为了有效处理安全事件，协调各相关部门和人员而成立的机构。

应急响应组织的组织结构如下图所示：

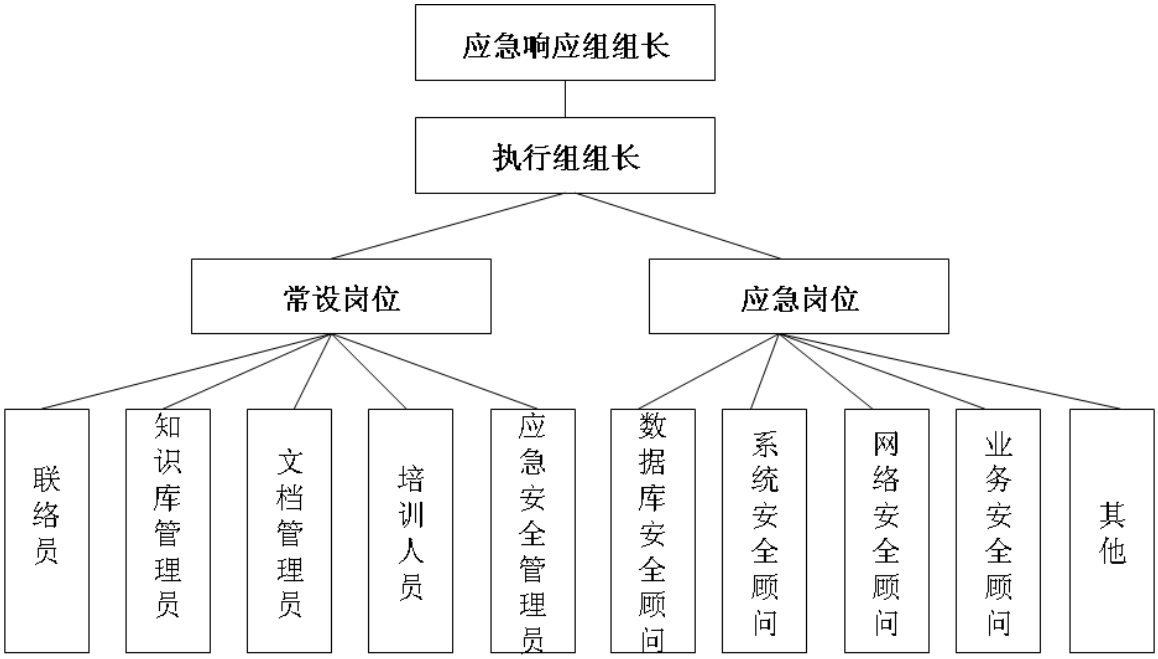


图 5.6 应急响应组织结构

应急响应组织主要由应急响应组组长、执行组组长、常设应急响应岗位和应急岗位等组成。

- 应急响应组组长：可由山西网通的高管层担任。
- 执行组长：可由主管安全的部门负责人来担任。
- 应急岗位（即安全顾问）：发生紧急事件，需要临时抽调的安全专家，精通业务流程并熟知系统及网络结构的资深安全专家担任，也可以是外聘的专业安全服务公司。
- 常设岗位（安全管理员/文档管理员/联络员）：由专门的应急响应技术人员担任，负责发现、预警、记录、报告、响应安全事件。

职责划分

- 应急响应组组长

接受执行组长的报告，作决策

工作分配，协调整个事件的处理过程

◆ 执行组长

接收报告，判断是安全问题抑或安全事件

选择人员建立紧急事件响应小组

制定应急响应计划

应急响应验收、监督

◆ 常设岗位

系统、网络、数据、业务方面的安全专家在应急响应过程中，作为应急响应小组成员，实施应急响应计划。

◆ 安全管理员

接收报告、采取初步行动，根据得到的报告判断是一个安全问题还是一个安全事件，评估事件紧急程度，确定响应策略，并将它提交高层；

参与决策过程，根据自己对 IT 应用要求的保护程度评估选择措施；

报告安全问题和安全事件；

按照应急响应策略实施应急措施。

◆ 文档管理人员

收集汇总应急响应相关报告、文档

应急响应事件知识库维护

◆ 知识库管理员

负责维护应急响应体系知识库

◆ 联络员