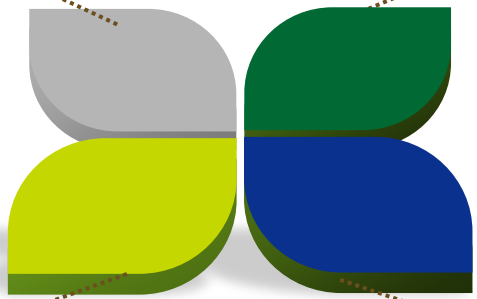
1.2 综合管理模型



信息安全管理

- 信息安全组织
- 信息安全流程
- 信息安全方针
- 信息安全制度
- 合规需求管理

信息安全控制

- 等级定义
- 运作控制
- 技术控制
- 服务控制
- 流程控制
- 资产管理
- 业务连续性管理

信息安全技术

- 物理安全
- 通信安全
- 操作安全
- 数据安全
- 访问控制
- 人员安全
- 备份容灾
- 云安全
- 应用安全

信息安全服务

- 风险评估服务
- 威胁评估服务
- 安全情报
- 安全态势
- 威胁分析、溯源分析
- 等级保护测评
- 安全信息管理
- 安全事件管理
- 身份与访问管理服务
- 基础设施安全管理
- 应用安全服务
- 数据安全服务
- 安全行为捕捉、安全行为分析
- 数据安全行为分析
- 应用风险图谱
- 数据风险图谱
- 行为风险图谱

1.9 安全能力评估（设备）

总结：

1、在基础网络、边界安全等方面比较全面 基本满足业务需求

2、在应用安全、应用数据安全、应用行为方面差距很大

3、在安全运营、安全管理类综合系统，数据挖掘、数据展现方面，基于单个系统实现，未能实现集中管理、集中分析、集中展现、集中审查，安全治理能力方面较差

4、人员结构不合理，在人员能力、组织结构方面需要加强

5、工业网、工业控制网在安全管控、安全隔离方面相对较差

安全治理	安全运营、安全管理				
	安全运维平台（SOC）	风险管理平台（RSM）	安全态势感知平台（外部） 日志分析平台（SIEM）	行为分析平台（IT） （威胁情报、行为分析）	合规审计平台（ADT）
安全技术+安全设备	基础支撑层	基础网络层	边界接入层	系统应用层	生产数据层
	基础环境保障与控制	网络核心安全保障	边界安全保障与控制	应用系统安全与优化	数据安全保障
	•密钥服务管理（数字证书） •时钟服务管理 •强身份认证(IDM/IAM) •设备运维管理（ITSM） •设备运维审计（堡垒机） •合规管理 •高等级数据中心 •专业认证人士 •任职资格 •专职运维人员（基础设施） •企业专网（VPN WAN） •安全区域(生产网络隔离)	•网络监控可视化（NOC） •网络行为分析 •入侵检测（IDS/IPS） •网络访问分区（交换机） •访问控制（交换机、防火墙） •无线网络管理(无线ac) •DNS运维管理 •AD域运维管理 •IP资产管理 •移动设备安全管理 •无线接入分区控制 •IT资产管理	•接入策略定制（防火墙） •入侵攻击防护（IPS） •病毒实时过滤（防毒墙） •带宽保障控制（Mpls VPN） •远程安全接入（SSL Vpn） •网络应用加速（CDN） •上网行为管理（AC） •链路出口管理 •终端接入控制（联软） •终端桌面安全（360天擎） •移动办公接入（无线、802.1X） •移动接入安全（移动设备安全网关） •重要系统隔离保护	•应用安全代理（安全网关） •数据库安全审计 •WEB应用防护（WAF） •邮件服务安全 •系统漏洞评估（漏洞扫描） •主机安全加固 •应用安全管理 •文档加密（亿赛通） •应用之间隔离保护 •数据隔离保护（单数据库） •安全基线管理 •应用基线管理 •数据基线管理 •数据脱敏、加密技术 •数据安全威胁分析	•内容数据监控 •应用变更管理 •涉密数据管理 •配置变更管理 •数据防泄漏 •数据层传输加密（如HTTPS） •统一身份认证(IAM/IDM) •邮件归档管理（邮件归档系统） •邮件内容过滤保护 •用户行为分析 •风险识别、风险分析 •安全舆情分析 •安全动态感知（内网、外网） •合规认证（等保） •合规认证（ISO27001） •数据合规管理（个人信息、隐私保护、重要数据保护、CII保护）
	有，基础阶段	未深入、未涉及			

1.10 安全能力评估（技术能力）

总结：

1、在通信安全、操作安全、访问控制方面具备一定的管理和控制能力，基本满足运维需求

2、物理安全、应用安全、数据安全、网络接入、业务连续性方面覆盖面、能力方面还需提升和改进

3、需提升访问控制能力的精细能力，细化访问控制的颗粒度，提升应用、数据的控制能力和保护能力

物理安全（01）	通信安全（02）	操作安全（03）	应用安全+数据安全（04）	访问控制（05）	人员安全（06）	备份容灾（07）
设备防盗	路由策略	规范、制度	加密	网络分区	身份认证	应用备份
设备防毁	端口策略	安全SOP规范	数字证书	应用访问控制（安全网关）	门禁	数据备份
环境安全	传输加密	行为审计	身份认证	安全代理	权限控制	应用容灾
防电磁泄漏	通信认证	操作回溯	网络隔离	准入控制	行为审计	数据容灾
防线路监听	数字签名	日志管理	代码审计	上网行为管理	越界管理	集群
电源保护	入侵检测	补丁管理	行为分析	防火墙	红区管理	
越界管理	防火墙	密码策略	防篡改	服务控制		
红区管理	流量控制	防病毒	防泄漏	控制策略		
	WIFI 、热点管理	鉴权	敏感字过滤	红区设计		
		终端安全操作	漏洞扫描			
		监督审计	涉密数据保护			
			核心信息保护			

已具备能力　仅覆盖部分业务　有能力执行不好

1.16 安全差距评估 整体评价

整体评估：

1、 在管理制度、网络安全、应用安全、数据安全、终端安全方面已建立相关制度，部署了一些技术手段

2、在行为留痕、事后追溯方面已有一定的能力和经验

3、在权限控制、访问控制等方面存在细节方面的不足

4、事前防御、事中控制方面存在不足

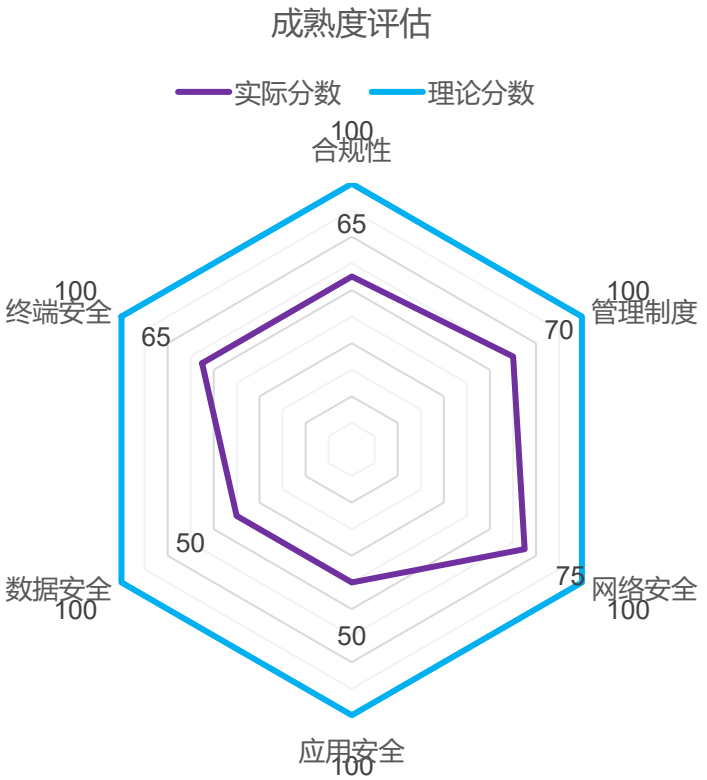
5、在集中管理、集中监控、集中控制、统一管理方面存在不足

6、网络分区保护、数据治理、数据安全治理方面存在不足

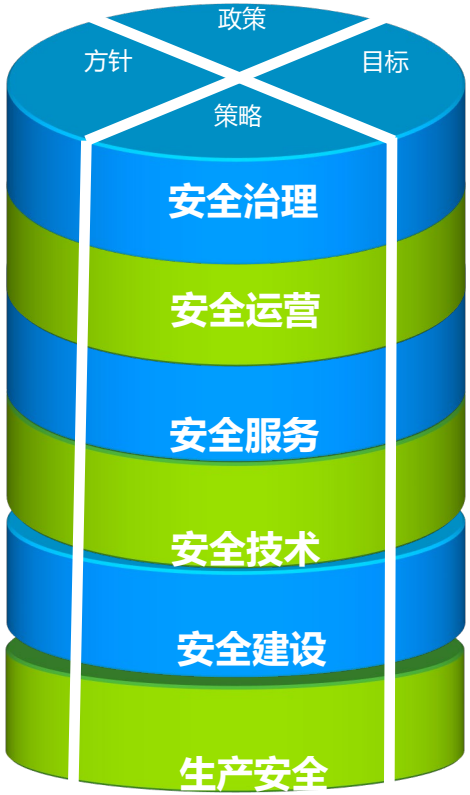
7、对标ISO 27001相关要求，我司在信息安全方面，基本达到60-70分水准，基本满足业务需求

8、合规方面，开展了ISO27001和等级保护的初步工作，需在网络安全法的引导下，提升分享安全合规能力，如个人信息保护、APP合规评估、重要数据保护、跨境保护等方面

9、境外合规方面尚未开展工作， 如GDPR，LGDP等



2.4 信息安全业务全貌-车企典型信息安全体系框架



信息安全体系

安全目标 | 安全策略 | 安全方针 | 安全政策

安全组织 | 安全管理制度 | 安全运营制度 | 合规管理 | 安全审计

生产安全

- 场地安全
- 车间安全
- 人员安全
- 工控网络安全
- 工控系统安全
- 在线监测
- 异常监测
- 数据分析
- 运行控制
- 供应链安全
- 财务安全

安全建设

- 安全框架
- 安全模型
- 安全标准
- 技术控制
- 服务控制
- 风险管理
- 风险控制
- 财务控制
- 应急预案
- 任职资格
- 安全绩效
- 移动安全
- 应用安全
- 数据安全
- 研发安全
- 资产安全
- 终端安全
- 物联网安全
- 车联网安全
- 大数据安全
- 云安全
- 网络安全
- 物理安全
- 其它

安全技术

- 移动安全网关
- 移动终端管理(MDM)
- APP安全管理
- 应用访问控制(堡垒机)
- 应用保护(WAF)
- 脆弱性扫描
- 冗余、灾备
- 加密
- 备份
- 网络隔离
- 防病毒
- 边界安全防御
- 全网监控(NOC)
- IT服务管理(ITSM)
- 资产管理工具
- 抗DDOS
- 统一身份认证
- 终端准入认证
- 数据防泄漏
- 边界保护
- 网络接入认证
- 硬件安全
- 协议安全
- 总线安全
- 多租户隔离
- 虚拟平台安全
- 数据隔离
- 资源管理
- 访问控制
- 服务控制
- 网络分层分级
- 上网行为管理
- 流量控制
- 环境监控
- 企业私网(VPN)
- 消防演练
- 邮件安全网关 防垃圾邮件网关
- SIEM
- SOC
- 行为分析
- 安全情报
- 安全基线
- 数据检测、数据校验
- CDN/SDN
- 无线网络管理

安全服务

- 体系规划
- 体系建设
- 制度建设
- 流程建设
- 项目管理
- 脆弱性扫描
- 安全加固
- 安全培训
- 安全情报
- 服务设计
- 服务交付

安全运营

- 安全管理计划
- 风险评估
- 威胁评估
- 安全事件管理
- 安全监控
- 应急响应
- 网络分析审计
- 应用分析审计
- 数据分析审计
- 安全态势
- 安全演练
- 安全考核
- 安全行为分析

安全治理

- 安全需求管理
- 安全能力管理
- 合规认证
- 合格证管理
- 等级保护
- 分级保护
- 最佳实践
- 跨境安全
- 个人信息保护
- 隐私保护
- 网络安全法
- GDPR

此框架为BMW Global 所用框架

2.5 信息安全规划-

针对业务和信息安全、信息保　密需求，建议从9个方面规划、建设信息安全体系

1）信息安全策略

2）信息安全标准、认证

3）信息安全组织

4）安全建设和运营

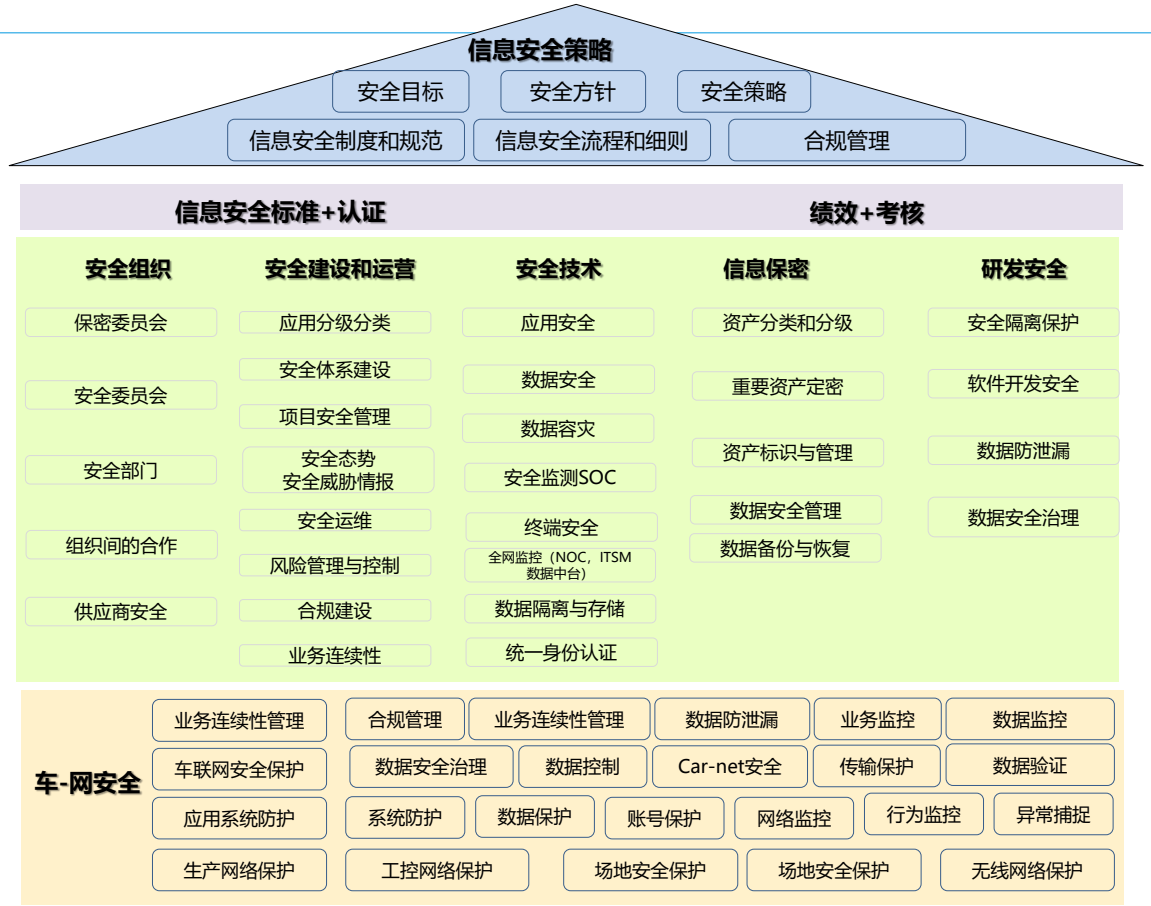
5）安全技术

6）信息保密

7）研发安全

8）信息安全绩效、考核

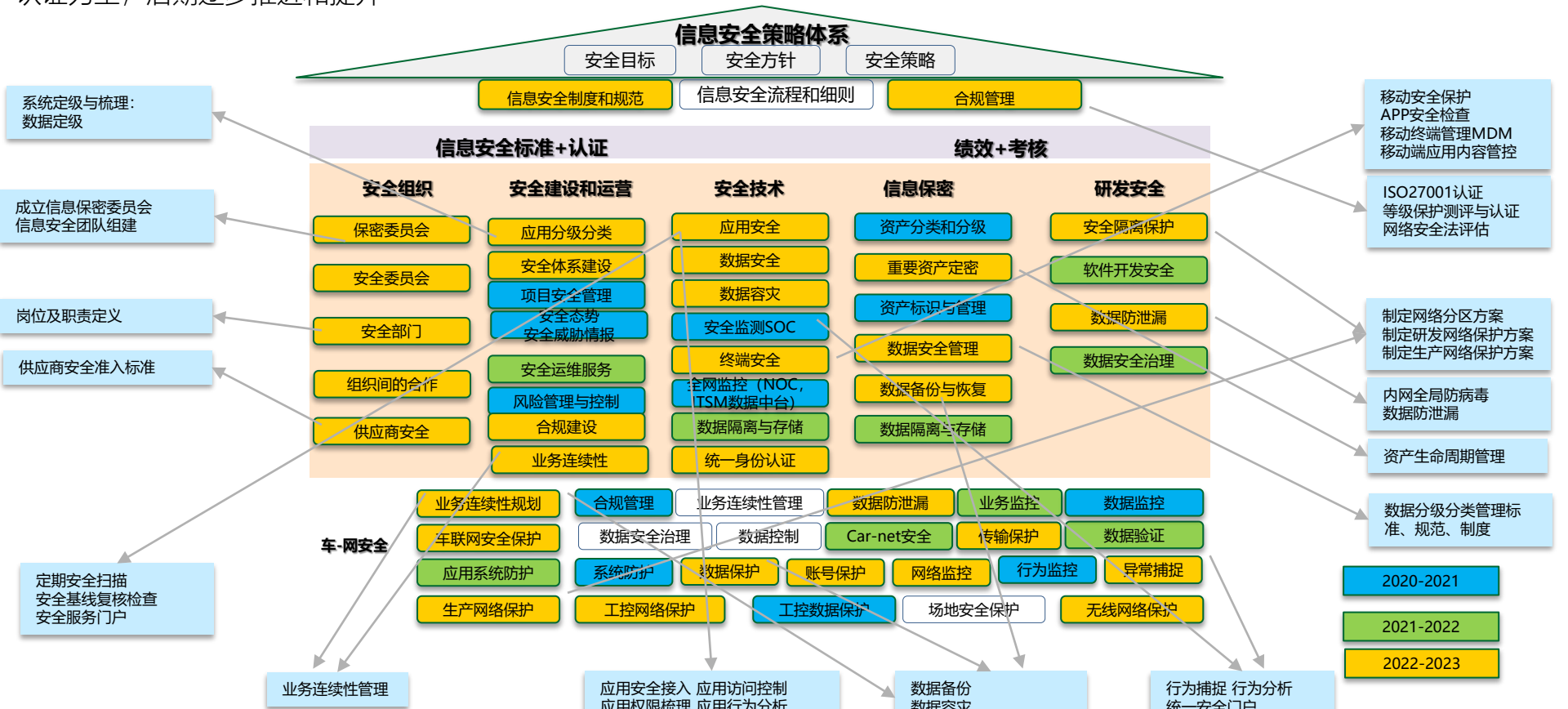
9）车-网安全



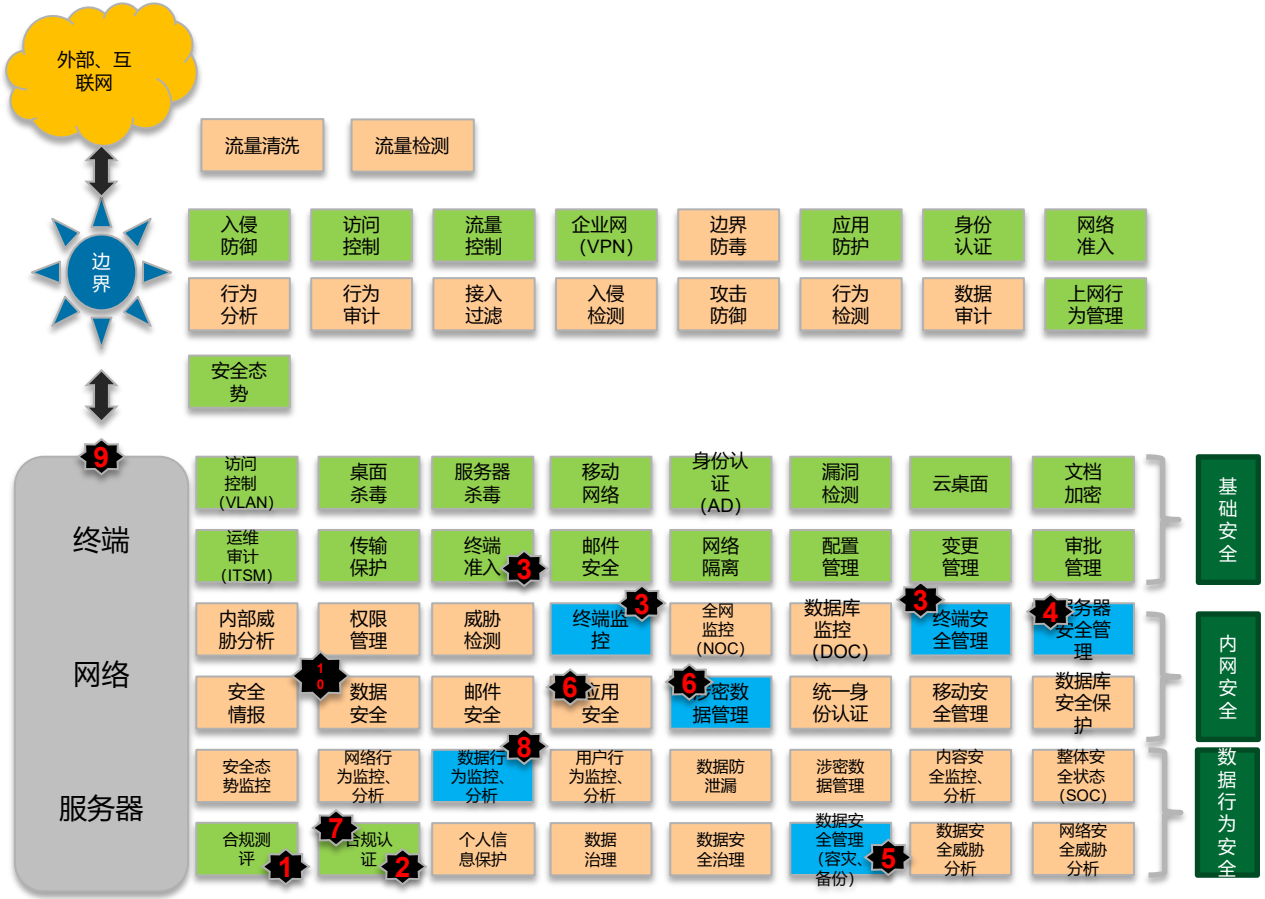
2.7 信息安全规划-技术体系

2.9 信息安全规划-2020~2023重点工作

2020-2022年，围绕公司信息安全目标，在核心数据保护、内网安全保护方面开展工作，前期以能力建设、基础防护、企业合规认证为主，后期逐步推进和提升



2.11 信息安全规划-项目对应关系



序号	项目名称	工作目标
1	APP安全合规评估项目	
2	车辆监控平台合规评估项目	
3	终端管理系统	
4	安全基线管理系统	
5	研发数据灾备二期项目	
6	大研发网络隔离保护项目	
7	官网等级保护合规项目	
8	2020车联网安全态势项目	
9	2020安全服务项目	
10	NAS杀毒项目	

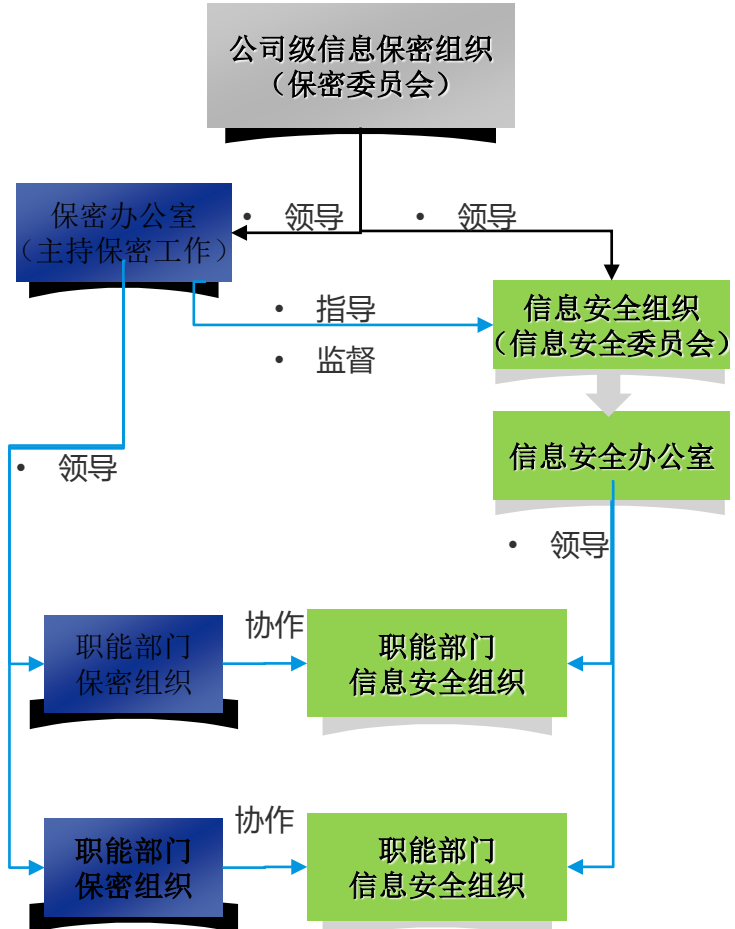
2.12 信息安全规划-2020-2023岗位规划

1— 安全规划	2— 安全服务岗	3— 安全运维岗	4— 安全实施岗
体系+规划	重点项目+服务管理 二线技术支持	一般项目+运维管理 一线技术支持	设备运维、服务支持 一线技术支持
合规	BCM	实施规范	防火墙
风控	认证	接入规范	入侵检测
行业标准	审计方案	安全运维	VPN接入
安全体系	培训	安全服务	DNS
安全制度	服务支持	安全规范	边界隔离
业务安全	合规审计	项目管理	带宽管理
安全技术体系	服务保障	运维规范	渗透测试
安全基线	资质	业务连续性实施	安全扫描 安全评估
安全管理流程	运维保障	监控保障	监控保障
整体安全架构	安全审计		
安全服务体系	交付管理		
数据安全规划	分析报告		
	服务报告		

2.12 信息安全规划-2020-2023岗位规划

岗位领域	岗位名称	建议职级（最小）	数量	任职资格	年限要求	优先级	备注
安全运营岗	安全运营管理	L5	2	CISSP-CAP	>10年	1	
安全服务岗	安全规划主管	L4	1+1	CISSP-ISSAP	5-10年	1	
	安全服务管理主管	L4	1	ITIL+ISSMP	5-8年	2	与运维交付主管互备
	安全运维交付主管	L4	1+1	SSCP或ISSEP	5-8年	3	与运维管理主管互备
	安全审计工程师	L2	1+1	CISA/CISP	3-5年	2	
安全运维岗	安全规范工程师	L3	1+1	CISSP或ISSEP	2-5年	1	
	安全运维工程师	L2	2+2	CCNA+ISSEP	2-5年	1	
安全操作岗	安全工程师（监控、操作、保障）	L2	1+3	CCNA	2-5年	1	短期内可以合一
	合计		15-20				

信息安全业务规划-信息安全组织



信息保密委员会-----信息保密最高决策机构

- ◆ 负责审核公司信息保密目标与方针
- ◆ 总体信息保密规划与重点管控方案

保密办公室—日常管理办公室

- ✓ 日常检查机构，信息保密管理工作
- ✓ 负责信息保密规划和管控方案、制度的制定与落实。
- ✓ 上报检查结果和整改措施

信息安全委员会---- 企业信息安全决策机构

- ◆ 建设信息安全技术体系、建设信息安全管理体系
- ◆ 负责审核公司信息安全方案
- ◆ 配合信息保密要求，建设相关的信息安全能力，全提升信息安全保护能力、提供取证和追溯能力

信息安全办公室—日常管理办公室

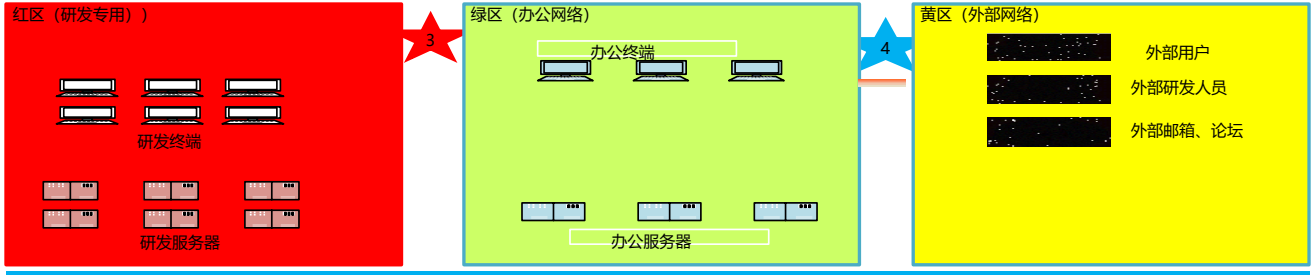
- ✓ 日常检查机构，信息安全管理工作
- ✓ 负责信息安全规划和管控方案、制度的制定与落实
- ✓ 跟进信息安全能力建设过程，上报检查结果和整改措施
- ✓ 主导信息安全事件响应机制，对过程和结果负责

各级业务和管理单位-----信息安全办成员

- ◘ 一把手负责制
- ◘ 负责需求提出
- ◘ 参与方案制定
- ◘ 负责对应业务职能信息安全管理（采购、生产、销售、服务、管理等）
- ◘ 提供资源或支持，确保管理和技术措施落实

数据保护框架—安全分区规划（整体架构）

区域	范围	安全等级	管控方式	安全重点
蓝区	和生产、测试或者工控系统有关的网络和物理区域。生产制造有关的、核心竞争力的信息系统和制造区域	最高	原则上不对外 网络完全隔离 强管控 或强授权访问控制（可信 受控）	保护生产环境
红区	与设计、研发相关的专用区域。主要用于研究人员在进行设计、研发、技术支持等活动所涉及的区域	极高	采用强管控 独立的物理办公区域、专用的门禁、监控、网络设备、安全策略 与互联网强隔离，原则上不允许有数据交互，有特别需求的通过专用的红区互联网DMZ区进行，并需取得一定级别人员审批后方可访问	数据防泄漏 研发信息泄密
绿区（办公区）	非研发设计类的其他的办公、安管、运维系统所在区域，包括 考勤系统、财务系统、在线打印系统、会议室预订系统、文档加密系统、食堂、门卫等	平衡	与互联网可以有数据交互，但是必须经过严格的访问控制策略如准入控制、身份识别、需求审批等 通过交互区实现与红区进行数据交互	内网病毒 内网数据窃取 内网泄密 内网攻击
黄区(互联网区)	用于与互联网或者非本单位网络的基础设施系统。例如：出口防火墙、负载均衡、IPS、上网行为管理、出口路由器交换机等网络及安全设备的区域	中-高	与互联网可以有数据交互，但是必须经过严格的访问控制策略如准入控制、身份识别、需求审批等	外网入侵 外网渗透 外部病毒 邮件泄密 外发泄密



蓝区（工控、生产、车间、试制试验、测试、关键研发）

安全控制点：

1、研发机构单独办公区域或专用网络，该区域或网络重点保护、研发数据根据数据分级分类定义实施脱敏、加密等手段

2、部署数据保护手段（DLP），将机密数据限定受控环境内

3、交互区：

文件和数据经审核后才能被传递到办公网络，在此交互区部署

网络访问控制、外发控制、数据隔离、防泄漏保护、行为审计、流量审计

4、研发审批：

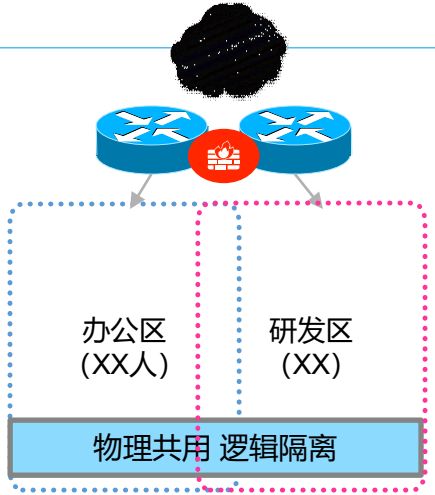
所有研发系统访问都必须被审批，且被监督

所有网络行为、外发行为被审计、被监督

6、绿区出口：

部署准入控制、身份识别、需求审批、上网行为管理、入侵检测、防病毒、入侵防御等手段

数据保护框架—网络分区规划（详细级架构）



- 风险：
- 1.核心交换为单一通道，办公区和研发区只是逻辑隔离，数据泄露风险大，对底层攻击行为防御力度不足
- 2、路由策略全在核心交换上，所有数据都通过核心交换，一旦失效则全网瘫痪
- 3、研发区如果存在病毒、泄密、外发信息行为，需要从大量网络数据、网络行为里捕捉少量数据，难度较大
- 4、研发区域如果存在重大问题，如病毒、泄密、外发信息，需要阻截、捕捉时，可能需要调整核心交换的策略，影响面太大
- 5、由于研发人员与普通办公人员混坐，混用网络，无法有效捕捉、定位、确认违规人员或设备

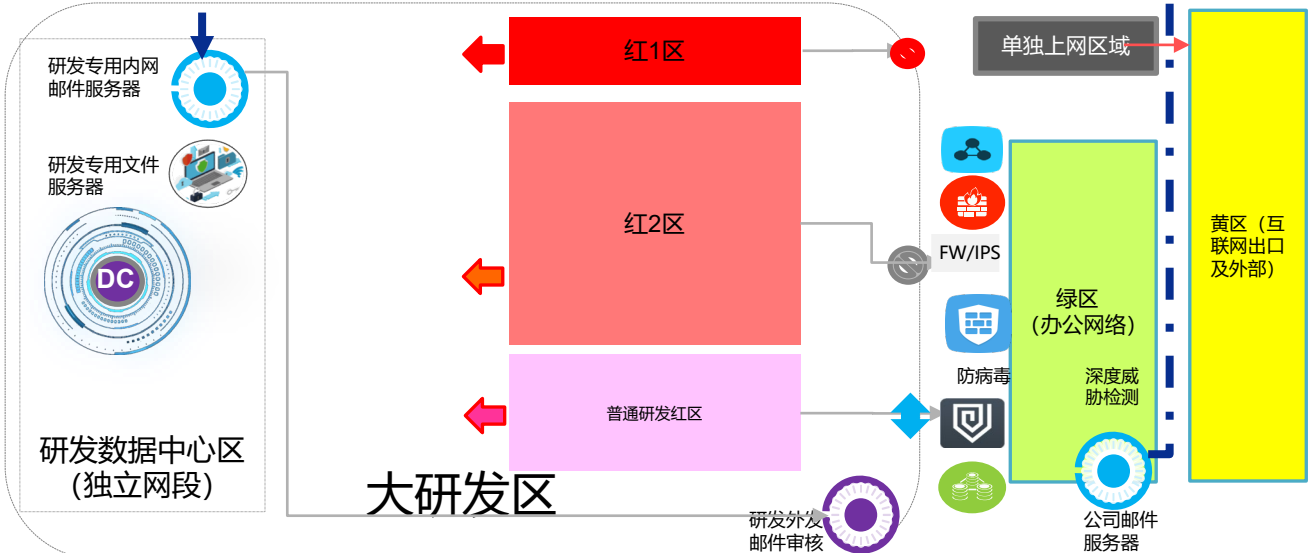
- 前提： 物理上分为4个区域（黄区、红区、绿区、蓝区）
- 其中办公区（绿区）内部拆分出管理区、访客区、会议区

改进：

- 重点保护、保证、研发区域、生产网络、管理区的可靠性和安全性
- 按业务分工 精确拆分、控制不同的网络域（网络分区），匹配、适用不同的安全要求、安全策略、管控方式
- 隔离、控制不同区域之间的数据、流量、行为，更精准定位事件、信息发起点、及时捕捉、控制异常信息来源
- 对业务和流量进行分流、引流控制，避免全网瘫痪风险
- 整体网络架构具备横向扩展能力，根据业务发展状况灵活调整

数据保护框架—研发安全分区规划-根据涉密级别)

区域	范围	安全等级	管控方式	安全重点
红1区	一级、特殊级涉密研发人员 占比<10%	最高	独立的物理办公区域、专用的门禁、监控、网络设备、安全策略；原则上不对外 网络完全隔离；专用打印机、碎纸机、文件服务器 强管控或强授权访问控制（可信 受控）	保护核心涉密信息 保障零泄漏
红2区	二级、三级涉密人员 占比50-60%	极高	采用强管控 与互联网强隔离，原则上不允许有数据交互，有特别需求的通过专用的红区互联网DMZ区进行，并需取得一定级别人员审批后方可访问	数据防泄漏 研发信息泄密
普通研发红区	非涉密研发人员 占比30-40%	平衡	与互联网可以有数据交互，但是必须经过的访问控制策略 如准入控制、身份识别、需求审批等 通过交互区实现与红区进行数据交互	内网病毒 内网数据窃取 内网泄密 内网攻击



0. 红2区和普通研发红区，与现有管控方式保持不变，后期再优化

1.大研发区**内部设置邮件服务器**，内部发送邮件，通过研发专用邮件服务器内部中转（纯内部域名和IP，不对外，如rdmail.bjev）

2、外部人员发送邮件给研发人员，从公司邮件服务器上设置对应的策略，自动转发

3.大研发区**内部设置文件服务器，**研发人员可通过内部文件服务器上传、下载文件，设置不同的权限和访问控制---------可能需要单独采购具备独立、完整控制权的文档管理系统

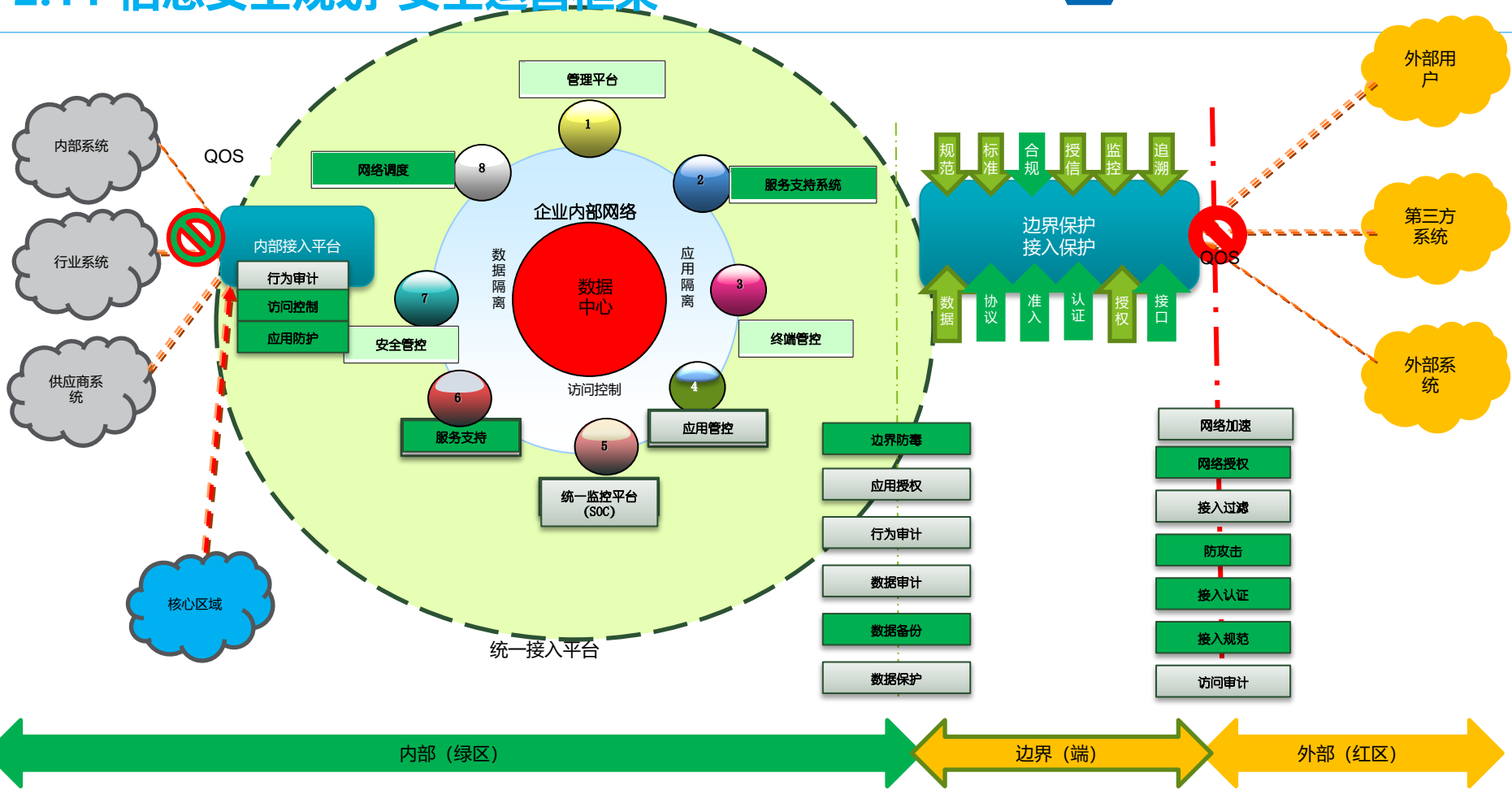
4、 为红1区人员（一级、特殊级涉密人员、部分二级涉密人员）设置**单独的上网区域**，不可连接研发网络，查询的资料可发至外部邮箱，自动中转至研发邮箱

5、研发人员需要向外部发送邮件（尤其带附件的），统一外发至指定邮箱（如outside@rdmail.bjev，由研发内部各部门安全人员审核后，统一外发）

6、一级、特级涉密人员外发信息，需得到保密委员会的审批和审核，再由指定人员单独外发，记录外发日志和内容

7、大研发区网络独立于办公网络，两网络边界设置防毒墙、防火墙、堡垒机、流量控制等防御系统和检测系统，必要时部署行为分析、流量分析、威胁分析等工具

2.11 信息安全规划-安全运营框架



数据保护框架—分层防御

基于网络架构的安全防御规划-分层设计、分层防御、分区保护

1、全局上提供防御服务、监测服务、审计服务、安全技术服务、安全支持服务
2、针对各种请求、数据流（用户端、办公网），在入口提供防御服务，主要包括防攻击、应用保护、数据加密等
3、在数据中心、IT业务系统与入口之间，实施防御服务，主要包括流量清洗、防内外攻击等
4、在办公网络与数据中心、IT系统之间，实施防御服务，主要以防窃听、防篡改、防病毒、数据加密等服务