重点

EMPHASIS

网络安全

“3保1评”

CONTENTS

01 PART ONE

什么是“3保1评”

什么是“3保1评”

网络安全领域

3保1评

分保

涉密信息系统分级保护

指涉密信息系统的建设使用单位根据分级保护管理办法和有关标准，对涉密信息系统分等级实施保护

等保

网络安全等级保护

指国家通过制定统一的安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护

关保

关键信息基础设施保护

针对面向公众提供网络信息服务或支撑能源、通信、金融、交通、公共事业等重要行业运行的信息系统、工业控制系统等关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护

密评

商用密码应用安全评估

是指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。

02 PART TWO

相关的法律法规依据

相关的法律法规依据

分保

涉密信息系统分级保护

《关于加强信息安全保障工作中保密管理的若干意见》（中保委发[2004]7号）
《涉及国家秘密的信息系统分级保护管理办法》（国保发[2005]16号）

《国家保密法》（2010年）
第二十三条 存储、处理国家秘密的计算机信息系统(以下简称涉密信息系统)按照涉密程度实行分级保护。

《网络安全等级保护条例（征求意见稿）》
第四章 涉密网络的安全保护
第三十五条【分级保护】涉密网络按照存储、处理、传输国家秘密的最高密级分为绝密级、机密级和秘密级。

相关的法律法规依据

等保 网络安全等级保护

《中华人民共和国计算机信息系统安全保护条例》（国务院147号令，1994年）
《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）
《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
《信息安全等级保护管理办法》（公通字[2007]43号）
《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）
《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》(发改高技[2008]2071号)

《网络安全法》2016年

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改

等级保护2.0元年

2019年 5月13日正式发布等级保护2.0版本《信息安全技术网络安全等级保护基本要求》

相关的法律法规依据

关保 关键信息基础设施保护

中华人民共和国网络安全法

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

中华人民共和国密码法

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

关键信息基础设施安全保护条例(征求意见稿)

第六条 关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。

相关的法律法规依据

密评

商用密码应用安全评估

《中华人民共和国密码法》

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

第三十七条 关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

《国家政务信息化项目建设管理办法》

第二十八条第三款

对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。

03 PART THREE

分保工作简介

分保工作简介

涉密信息系统

是指由计算机及其相关和配套设备、设施构成的，按照一定的应用目标和规则存储、处理、传输国家秘密信息的系统或者网络。

涉密系统分级保护是指

涉密信息系统的建设和使用单位根据分级保护管理办法和有关标准，对涉密信息系统分等级实施保护，各级保密工作部门根据涉密信息系统的的保护等级实施监督管理，确保系统和信息安全。

保护对象

所有涉及国家秘密的信息系统，重点是党政机关、军队和军工单位。

分保 **涉密信息系统分级保护**

分保工作简介

系统定级：根据其涉密信息系统处理信息的最高密级，可以划分为秘密级、机密级和机密级（增强）、绝密级三个等级。

	物理安全	运行安全	信息安全保密
秘密级	强	强	强
机密级	更强	更强	更强
机密增强级	在机密级的基础上，增加要求		
绝密级	最强	最强	最强

分保工作简介

01

系统定级

明确系统所处理信息的最高密级，确定系统保护等级。

02

方案设计

进行风险评估，设计方案，并通过专家论证，负责系统审批的保密工作部门应参加论证。

03

工程实施

组建工程监理机构，细化管理制度，监督工程实施，或选择具有涉密资质的工程监理单位进行监理。

04

系统测评

系统工程实施完毕后，建设使用位向国家保密局涉密信息系统保密测评中心及分中心申请完成系统测评。

05

系统审批

涉密信息系统在投入运行后前，经保密工作部门审批。

06

日常管理

日常管理包括基本管理要求，人员管理、物理环境与设施管理、信息保密管理等。

07

测评与检查

涉密信息系统投入运行后还应定期进行安全保密测评和检查。

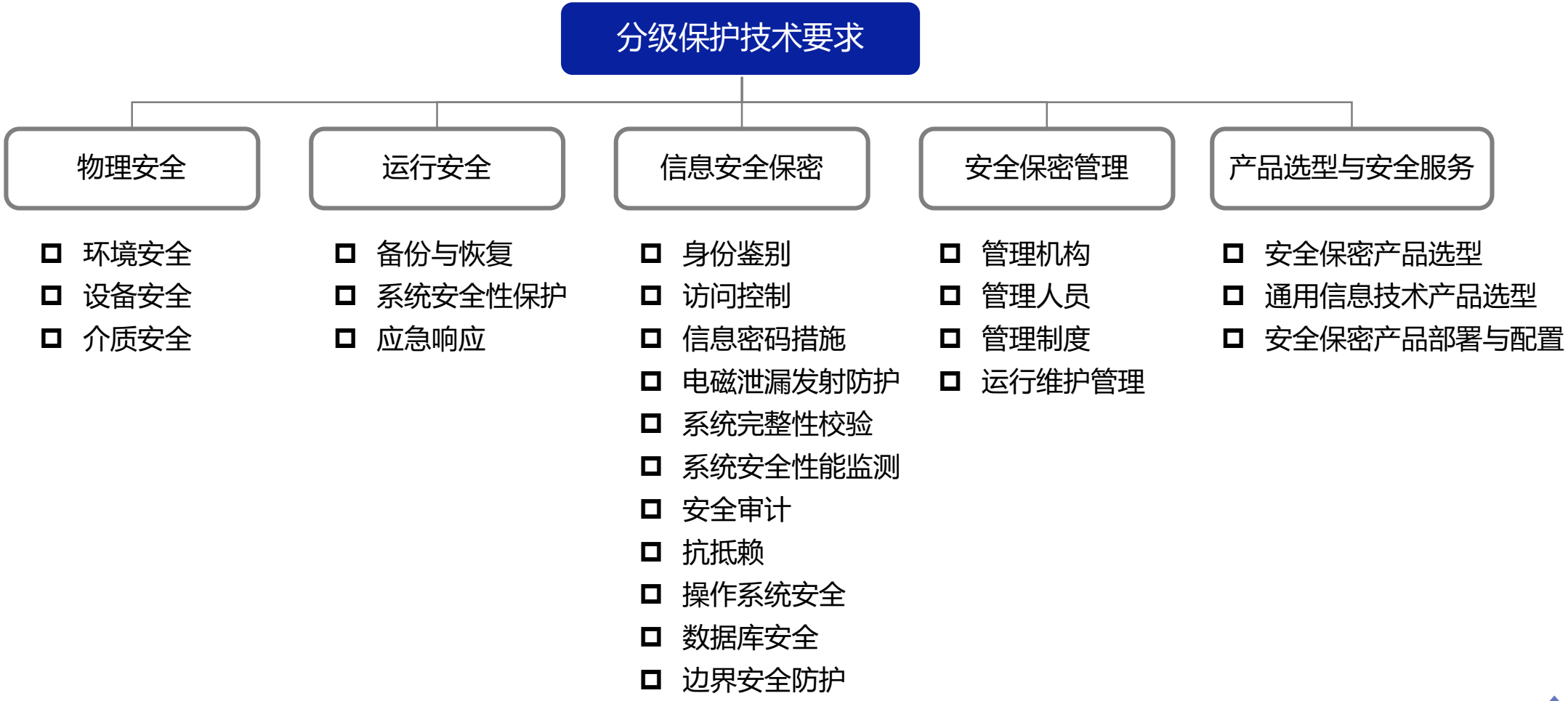
08

系统废止

废止涉密信息系统应向保密工作部门备案，并按照保密规定妥善处理涉及国家密信息的设备、产品和资料。

分保工作流程

分保工作简介



分保工作简介

- 新建涉密网络都须经过测评（国家保密局设立或者授权的保密测评机构）、审批（地市以上保密局）才能正式投入运行
- 涉密网络投入运行后，应接受保密局组织的安全保密风险评估，秘密级、机密级每两年至少一次，绝密级每年至少一次
- 涉密网络中使用的信息设备，应当从国家有关主管部门发布的涉密专用信息设备名录中选择
- 未纳入名录的，应选择政府采购目录中的产品，确实需要选用进口产品的，应当进行安全保密检测，安全保密产品应通过国家保密科技测评中心检测
- 计算机病毒防护产品应选用取得计算机信息系统安全专用产品销售许可证的可靠产品
- 密码产品应当选用国家密码管理局批准的产品

04 PART FOUR

等保工作简介

等保工作简介

等保 网络安全等级保护

01

指国家通过制定统一的安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护

02

信息安全等级保护

指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和储存、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

03

保护对象

运营商和服务提供商:电信、广电行业的公用通信网、广播电视传输网等基础信息网络，经营性公众互联网信息服务单位、互联网接入服务单位、数据中心等单位的重要信息系统。

重要行业:铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源、能源、交通、文化、教育、统计、工商行政管理、邮政等行业、部门的生产、调度、管理、办公等重要信息系统。

重要机关:市（地）级以上党政机关的重要网站和办公信息系统。

等保工作简介

01.

第一级
自主保护级

信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

02.

第二级
指导保护级

信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

03.

第三级
监督保护级

信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

04.

第四级
强制保护级

信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

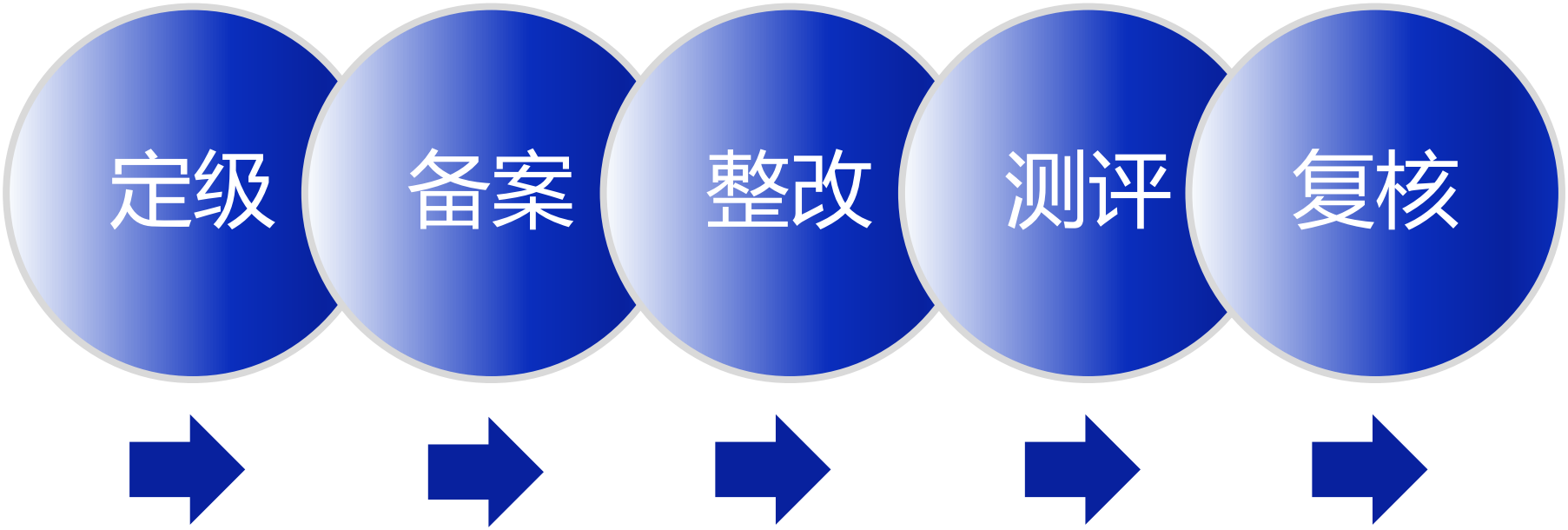
05.

第五级
专控保护级

信息系统受到破坏后，会对国家安全造成特别严重损害。

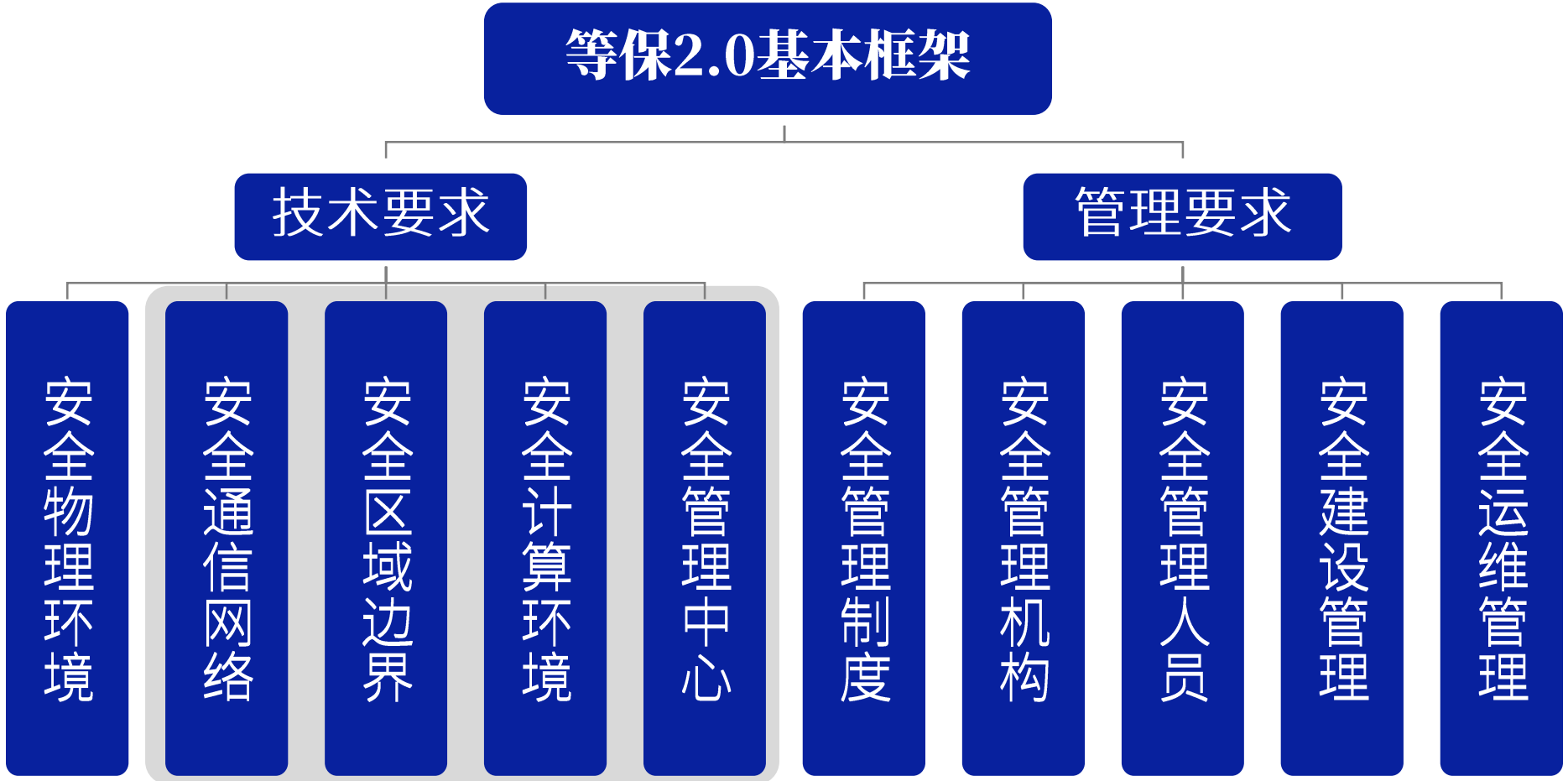
等保系统定级

等保工作简介



等保工作流程

等保工作简介



等保2.0充分体现了“一个中心三重防御“的思想，一个中心指“安全管理中心”，三重防御指“安全计算环境、安全区域边界、安全网络通信”，同时等保2.0强化可信计算安全技术要求的使用

等保工作简介

安全管理中心

- 大数据安全
- IT运维管理
- 堡垒机
- 漏洞扫描
- 网站监测预警
- 等保安全一体机
- 等保建设咨询服务

建设要点

- 对安全进行统一管理与把控
- 集中分析与审计
- 定期识别漏洞与隐患

安全通信网络

- 下一代防火墙
- VPN
- 路由器
- 交换机

建设要点

- 构建安全的网络通信架构
- 保障信息传输安全

安全区域边界

- 下一代防火墙
- 入侵检测/防御
- 上网行为管理
- 安全沙箱
- 动态防御系统
- 身份认证管理
- 流量安全分析
- WEB应用防护
- 准入控制系统

建设要点

- 强化安全边界防护及入侵防护
- 优化访问控制策略

安全计算环境

- 入侵检测/防御
- 数据库审计
- 动态防御系统
- 网页防篡改
- 漏洞风险评估
- 数据备份
- 终端安全

建设要点

- 强调系统及应用安全
- 加强身份鉴别机制与入侵防范

等保2.0技术保护方案规划

等保工作简介

序号	等保所需产品	等保二级	等保三级
1	防火墙	必备	必备
2	入侵防御	必备	必备
3	日志审计	必备	必备
4	漏洞扫描	必备	必备
5	上网行为管理	必备	必备
6	WFA应用防火墙	可选	必备
7	堡垒机	可选	必备
8	数据库审计	可选	可选
9	网站防篡改	可选	必备
10	运维管理系统	可选	可选
11	网络版杀毒软件	必备	必备
12	未知威胁防御	可选	可选

序号	等保所需产品	等保二级	等保三级
13	安全流量分析	可选	可选
14	等保一体机	可选	可选
15	垃圾邮件网关	可选	必备
16	沙箱系统	可选	可选
17	态势感知	可选	可选
18	终端准入系统	可选	必备
19	VPN网关	可选	可选
20	虚拟化安全系统	可选	必备
21	网闸	可选	可选
22	动态防御系统	可选	可选
23	网站监测预警系统	可选	可选
24	备份与恢复系统	可选	必备

等保2.0网络安全设备配置建议

等保工作简介

安全管理制度

- 制定安全策略
- 建立安全管理制度
- 专人负责制定和发布管理
- 定期评审和修订管理制度

安全管理机构

- 设立相应领导、管理、审计、运维机构和岗位
- 配备系统管理、审计管理和安全管理员
- 明确授权和审批事项和制度
- 加强内部和外部安全专家沟通协作
- 定期审核和检查安全策略和安全管理制度

安全管理人员

- 考核录用人员专业技能，签署保密协议。
- 离岗人员及时回收权限、证照等
- 加强安全意识和安全技能教育培训
- 定期进行安全技术考核

安全建设管理

- 等保定级和备案
- 安全方案设计
- 安全产品采购和使用
- 自主和外包软件开发管理
- 安全保护工程实施管理
- 安全防护测试验收
- 系统验收交付
- 定期等保测评
- 监督、评审和审核安全服务提供商

安全运维管理

- 运行环境管理
- 被保护资产管理
- 信息存储介质管理
- 设备维护管理
- 漏洞和风险管理
- 网络和系统安全管理
- 恶意代码防范管理
- 系统、变更配置和密码管理
- 备份与恢复管理
- 安全事件和应急预案管理
- 外包运维管理

等保2.0安全管理规划

05 PART FIVE

关保工作简介

关保工作简介

关保

关键信息基础设施保护

针对面向公众提供网络信息服务或支撑能源、通信、金融、交通、公共事业等重要行业运行的信息系统、工业控制系统等关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护

关键信息基础设施

是指面向公众提供的网络信息服务或支撑能源、交通、水利、金融、公共服务、电子政务公用事业等重要行业和领域以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。

保护对象

电信、广播电视、能源、金融、交通运输、水利、应急管理、卫生健康、社会保障、国防科技等行业和领域中一旦遭到破坏或者丧失功能，会严重危害国家安全、经济安全、社会稳定、公众健康和安全的业务。

公众服务：如党政机关网站、企事业单位网站、新闻网站等;
民生服务：包括金融、电子政务、公共服务等;
基础生产：能源、水利、交通、数据中心、电视广播等。

关保工作简介

关键信息基础设施安全防护能力

依据**5个能力域**完成程度的高低进行分级评估，包括**3个能力等级**，从能力等级1到能力等级3，逐级增高，能力等级之间为递进关系，高一级的能力要求包括所有低等级能力要求。

关键信息基础设施安全防护所需具备的能力

包括识别认定、安全防护、检测评估、监测预警、事件处置5个方面的关键能力，每个安全能力包含若干能力指标，每个能力指标包含若干评价内容。

关键信息基础设施安全防护能力等级	等级特征
能力等级1	能识别相关风险，防护措施成体系，能够开展检测评估活动，具备监测预警能力；能够按规定接受和报送相关信息；在突发事件发生后能应对并按计划恢复。
能力等级2	能清晰识别相关风险，防护措施有效，能够检测评估出主要安全风险，主动监测预警和态势感知，事件响应较为及时，业务能够及时恢复。
能力等级3	识别认定完整清晰，防护措施体系化、自动化高，能够及时检测评估出主要安全风险，使用自动化工具进行监测预警和态势感知，信息共享和协同程度高，事件响应及时有效，业务可近实时恢复。

关保工作简介

关键信息基础设施安全防护能力评价内容

- 能力域级别评价
- 等级保护测评
- 密码测评

01

关键信息基础设施安全防护能力评价前

关键信息基础设施应首先通过相应等级的等级保护测评和相关密码测评。

02

关键信息基础设施安全防护能力评价时

组织应按照评价内容和评价操作方法开展评价工作，给出对每项评价指标的判定结果和所处级别，得出每个能力域级别，综合5个能力域级别以及等级保护测评结果得出关键信息基础设施安全防护能力级别

03

关键信息基础设施安全防护能力评价完成

对应能力等级1的关键信息基础设施等级保护测评结果应至少为中；对应能力等级2的关键信息基础设施等级保护测评结果应至少为良；对应能力等级3的关键信息基础设施等级保护测评结果应为优。

关保工作简介

“关保”流程主要包括

- 识别认定、安全防护、检测评估、监测预警、事件处置五个环节。

“关保”的“安全防护”环节要求

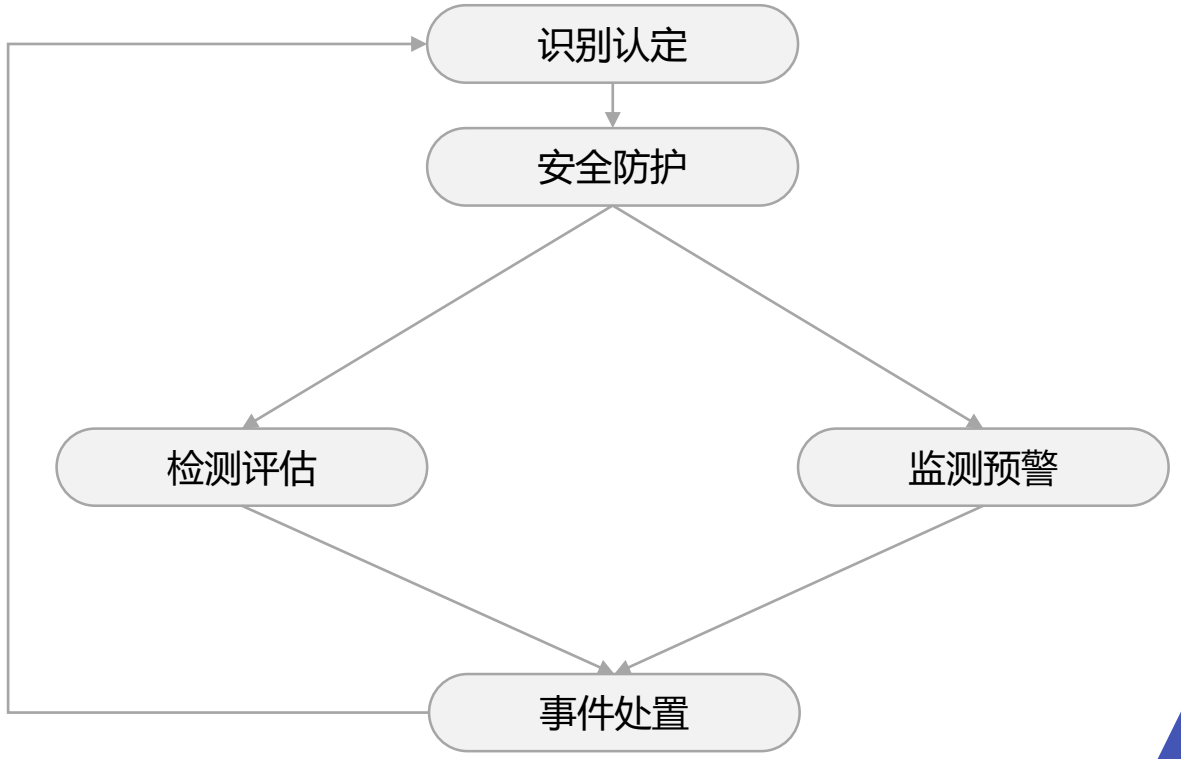
- 关键信息基础设施的运营者开展等保定级备案、安全建设、整改、测评及自查工作

“关保”基于等保的基础

- 加强关键信息基础设施关键业务的安全保护，

“关保”的实施流程

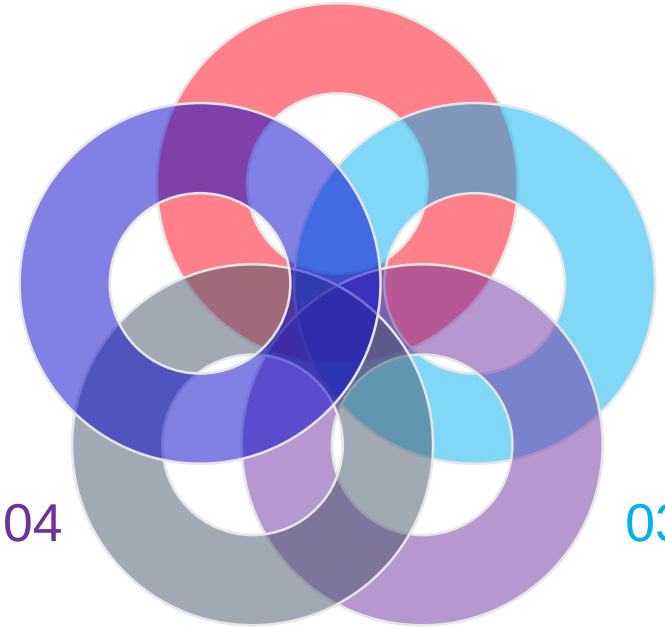
- 包含“等保”的同时增加更多动态风控的内容，比“等保”更加严格且全面。



关保工作简介

01 识别认定

•运营者配合安全保护工作部门，开展关键信息基础设施识别和认定活动，围绕关键信息基础设施承载的关键业务，开展风险识别。本环节是开展安全防护、检测评估、监测预警、应急处置等环节工作的基础。



02 安全防护

•运营者根据已识别的安全风险，在规划、人员、数据、供应链等方面制定和实施适当的安全防护措施，确保关键信息基础设施的运行安全。本环节在认定关键信息基础设施及识别其安全风险的基础上制定安全防护措施。

03 检测评估

•为检验安全防护措施的有效性，发现网络安全风险隐患，运营者制定相应的检测评估制度，确定检测评估的流程及内容等要素，并分析潜在安全风险可能引起的安全事件。

04 监测预警

•为检验安全防护措施的有效性，运营者制定并实施网络安全监测预警和信息通报制度，针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出安全警示。

05 应急处置

•根据检测评估、监测预警环节发现的问题，运营者制定并实施适当的应对措施，并恢复由于网络安全事件而受损的功能或服务，动态识别关键信息基础设施的安全风险。

06 PART SIX

密评工作简介

密评工作简介

密评

商用密码应用安全评估

是指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。

商用密码

- 是指对不涉及国家秘密内容的信息进行加密保护或安全认证所使用的密码技术和密码产品。商用密码技术是商用密码的核心，是信息化时代社会团体、组织、企事业单位和个人用于保护自身权益的重要工具。国家将商用密码技术列入国家秘密，任何单位和个人都有责任和义务保护商用密码技术的秘密。

商用密码安全性评估

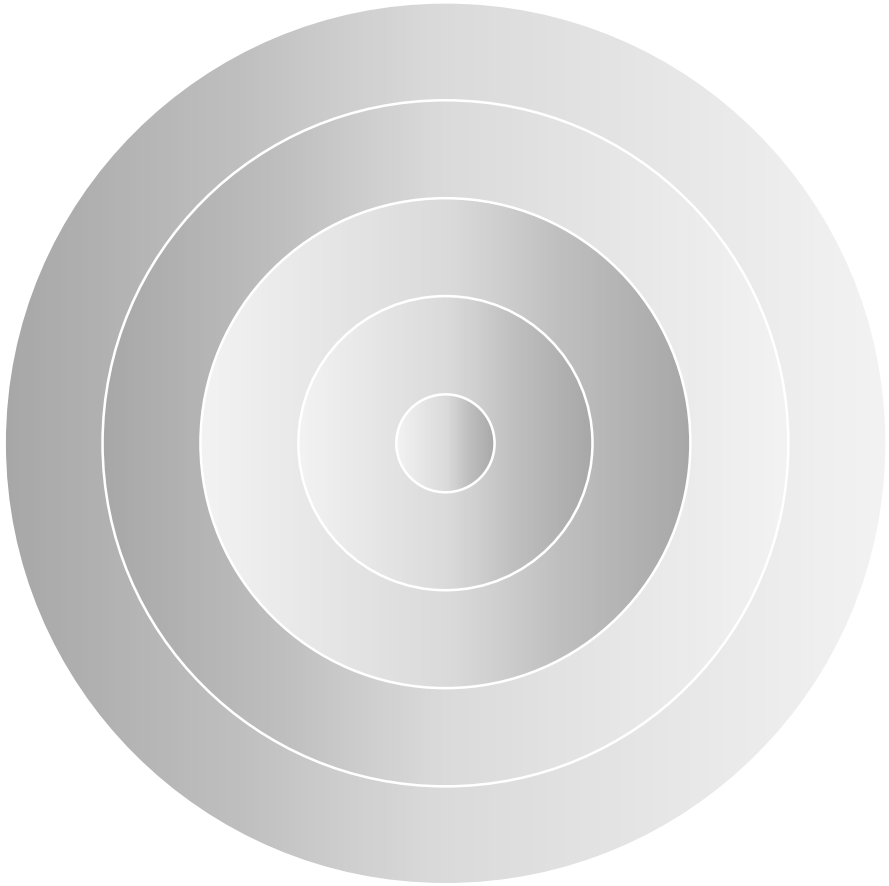
- 商用密码应用安全性评估（简称“密评”），是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

密评的意义

- 为了解决商用密码应用中存在的突出问题，为网络和信息系统的安全提供科学评价方法规范商用密码的使用和管理。改变商用密码应用不广泛、不规范、不安全的现状，确保商用密码在网络和信息系统中有效使用，切实构建起坚实可靠的网络安全密码屏障。开展密评，是国家网络安全和密码相关法律法规提出的明确要求，是法定责任和义务。

保护要求：信息系统中的身份鉴别、数据加密、数据签名等密码技术功能由密码算法、密码技术、密码产品、密码服务等提供。从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全的各个层面提供全面整体的密码应用安全技术支撑，从而保障信息系统的用户身份真实性、重要数据的机密性和完整性、操作行为的不可否认性。

密评工作简介



01

基础信息网络：

•电信网、广播电视网、互联网。

02

重要信息系统：

•能源、教育、公安、测绘地理信息、社保、交通、卫生计生、金融等涉及国计民生和基础信息资源的重要信息系统。

03

重要工业控制系统：

•核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要工业控制系统。

04

面向社会服务的政务信息系统：

•党政机关和使用财政性资金的事业单位和团体组织使用的面向社会服务的信息系统。

需要做密评的系统和单位

密评工作简介

第一级

是信息系统密码应用安全要求等级的最低等级，信息系统管理者可按照业务实际情况自主应用密码技术应对可能的安全威胁。

第二级

是在第一级的等级要求上，要求信息系统具备身份鉴别、数据安全保护的非体系化密码保障能力，可应对当前部分安全威胁；

第三级

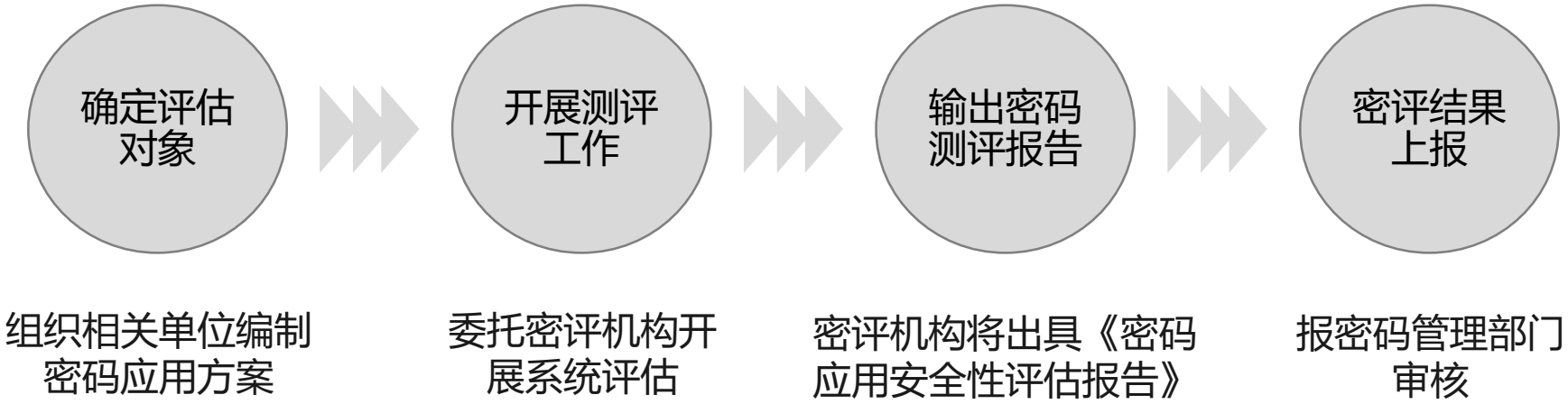
是在第二级的等级要求上，要求更强的身份鉴别、数据安全、访问控制等方面密码应用技术能力与管理能力，要求信息系统建设有规范、可靠、完整的密码保障体系，是体系化密码应用引导性要求；

第四级

是在第三级的等级要求上，要求更强的身份鉴别、数据安全、访问控制等方面密码应用技术能力与管理能力，信息系统建设有规范、可靠、完整、主动防御的密码保障体系，是体系化密码应用的强制要求；

密码评估等级划分

密评工作简介


确定评估对象
开展测评工作
输出密码测评报告
密评结果上报
组织相关单位编制密码应用方案
委托密评机构开展系统评估
密评机构将出具《密码应用安全性评估报告》
报密码管理部门审核

07 PART SEVEN

3保1评联系与区别

3保1评联系与区别

涉密信息系统分级保护是国家信息安全等级保护的重要组成部分，是等级保护在涉密领域的具体体现

等级保护是关键信息基础设施保护的基础，关键信息基础设施是等级保护的重点防护对象。

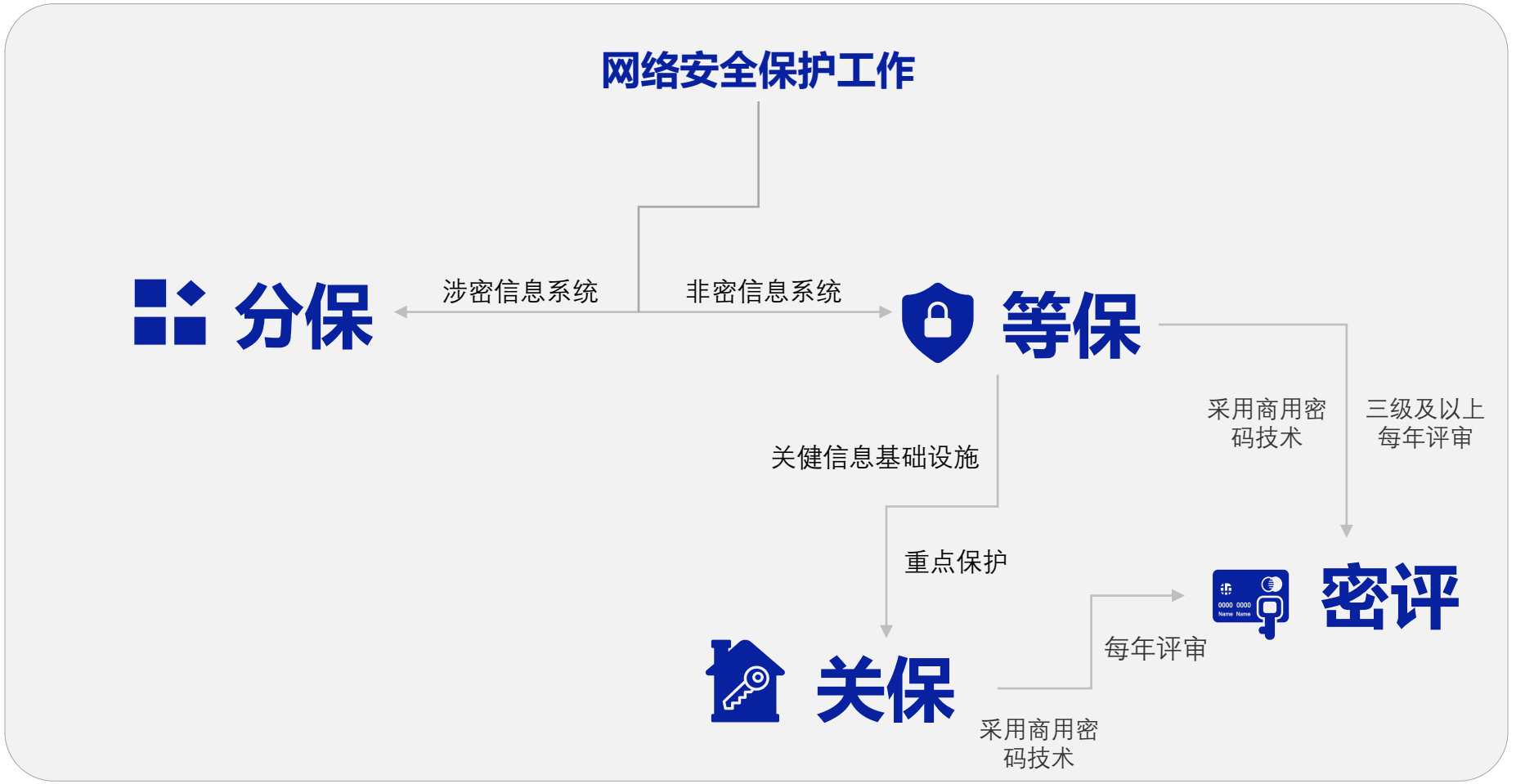
关键信息基础设施必须落实网络安全等级保护制度，开展定级备案、等级测评、安全建设整改、安全检查等强制性及规定性工作；

商用密码应用安全是保障网络和信息系统安全的一项防护措施，也是保障关键基础设施安全的重要手段，关键基础设施必须按照密评相关标准、规定，开展密评工作；

等级保护是支撑国家网络安全的基本制度，开展关键信息基础设施保护和商用密码应用安全评估的基础，若无法将等级保护制度落实到位，则很难实现关键信息基础设施保护到位，商用密码应用安全评估工作也无法顺利进行。

等级保护制度、关键信息基础设施保护、商用密码应用安全评估都是网络安全运营者应履行的责任和义务，并非哪一个重要，哪一个不重要，只是安全防护力度、角度存在一定差异。

3保1评联系与区别


网络安全保护工作
分保
涉密信息系统
非密信息系统
等保
采用商用密码技术
三级及以上每年评审
关健信息基础设施
重点保护
密评
每年评审
关保
采用商用密码技术

3保1评联系与区别

类别	分保	等保	关保	密评
保护要求	《涉及国家秘密的信息系统分级保护技术要求》	《网络安全等级保护基本要求》	《关健信息基础设施网络安全保护基本要求》	《信息系统密码应用基本要求》
职能部门	国家相关保密部门	公安网监部门	公安网监部门	密码管理局
评估标准	《涉及国家秘密的计算机信息系统分级保护测评指南》	《信息安全技术网络安全等级保护测评过程指南》	《信息安全技术关键信息基础设施安全检查评估指南》	《商用密码应用安全性评估测评过程指南》
保护对象	所有涉及国家秘密的信息系统，重点是党政机关、军队和军工单位	重点保护的对象是非涉密的涉及国计民生的重要信息系统和通信基础信息系统；如政府、教育、卫生等重要网站及各种信息系统	关键信息基础设施：如电信、广播电视、能源、金融、交通运输、水利、应急管理、卫生健康、社会保障、国防科技等行业。	关键信息基础设施、网络安全保护第三级以上的系统、国家政务信息系统。

3保1评联系与区别

类别	分保	等保	关保	密评
系统分级	秘密级、机密级和机密级（增强）、绝密级	第一级（自主保护级）第二级（指导保护级 ）第三级（监督保护级）第四级（强制保护级）第五级（专控保护级 ）	参照等保，重点保护	一至四级逐级增强保护能力
工作流程	系统定级、方案设计、工程实施、系统测评、系统审批、日常管理、测评与检查和系统废止	定级、备案、整改、测评、复核	识别认定、安全防护、检测评估、监测预警、事件处置	确定评估对象、开展测评工作、输出密码测评报告、密评结果上报
测评内容	物理隔离 安全保密产品选择 安全域边界防护 密级标识	安全物理环境 安全通信网络 安全区域边界 安全计算环境 安全管理中心 安全管理制度 安全管理机构 安全管理人员 安全建设管理 安全运维管理	合规检查 安全技术检测 分析评估	总体要求 密码功能要求 密码技术应用要求 密钥管理 安全管理

REPORT IS COMPLETED
THANK YOU

没有网络安全

就没有国家安全