关基智能化安全运营服务体系

启明星辰

2021年10月13日

壹

PART ONE

关基的概念及政策标准

贰

PART TWO

关基工作流程

叁

PART THREE

关基智能化安全运营服务体系

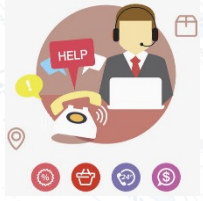
壹

关基的概念及政策标准

什么是关键信息基础设施？

关键信息基础设施定义大致可概括为：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、国防科技工业、重要行业和领域，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、公共利益的网络设施、信息系统。


公共通信



信息服务


能源


交通

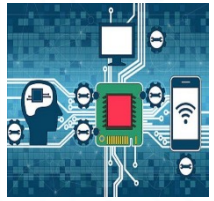

水利


金融

公共服务

电子政务


国防科技工业


重要行业和领域

什么是关键信息基础设施？

关键信息基础设施，简称“关基”或“CII”

2016年4月19日，习总书记在网信工作会议中指出:

关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。

关键信息基础设施安全可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。

在国家陆续发布的---

- **《国家网络安全检查操作指南》；**
- **《网络安全法》；**
- **《关键信息基础设施安全保护条例》。**

……

法律法规中对关键信息基础设施的定义基本都采用了**“特定行业范围+严重危害后果”**的方式。

习近平总书记对关键信息基础设施安全防护的指示

- 2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上强调：
  - 强调“加快构建关键信息基础设施安全保障体系”；
  - 提出“全天候全方位感知网络安全态势”。
- 2017年2月17日，习近平总书记在召开的国家安全工作座谈会强调：
  - 要构筑网络安全防线，提高网络安全保障水平；
  - 强化关键信息基础设施防护；
  - 加强网络安全预警监测，实现全天候全方位感知和有效防护。
- 2017年12月8日，习近平总书记在中共中央政治局第二次集体学习时强调：
  - 要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。

关键信息基础设施政策体系？

我国正在逐步建立完善关键信息基础设施保护政策体系，**上层、中层、下层**等法规政策。

《中华人民共和国网络安全法》
《中华人民共和国密码法》
《中华人民共和国数据安全法》

《关键信息基础设施保护条例》
《网络安全等级保护条例》
《国家网络安全检查操作指南》
《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

《关键信息基础设施网络安全框架》
《关键信息基础设施边界确定方法》
《关键信息基础设施安全保障指标体系》
《关键信息基础设施安全检查评估指南》
《关键信息基础设施安全保护要求》
《关键信息基础设施安全控制措施》
《关键信息基础设施安全防护能力评价方法》

《网络安全法》中对关基的要求

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。

第三十三条

建设关键信息基础设施应当确保其具有支持**业务稳定、持续运行**的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十八条

关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的**风险每年至少进行一次检测评估**，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条

国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行**抽查检测，提出改进措施**，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行**网络安全应急演练**，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的**网络安全信息共享**；

（四）对**网络安全事件的应急处置与网络功能**的恢复等，提供技术支持和协助。

《密码法》中对关基的要求

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。
- 关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

《数据安全法》中对关基的要求

中华人民共和国
数据安全法

第三十一条

- 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

《网络安全审查办法》中对关基的要求

- 第一条 为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，制定本办法。
- 第二条 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，数据处理者（以下称运营者）开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。
- 第五条 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

  关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。
- 第二十条 本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。

本办法所称网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

《关键信息基础设施安全保护条例》正式发布

启明星辰 领航信息安全

网络安全行业一直以来比较关注的《关键信息基础设施安全保护条例》（以下简称：“关保条例”），在国务院第133次常务会议上获得通过，总理李克强签署了国务院第745号令，条例总共六章五十一条，并将于2021年9月1号开始实施，预示着网络安全行业新的一波建设热潮即将到来，网络安全正式进入了“关保”时代。

中华人民共和国国务院令

第 745 号

《关键信息基础设施安全保护条例》已经2021年4月27日国务院第133次常务会议通过，现予公布，自2021年9月1日起施行。

总 理 李克强

2021年7月30日

《关键信息基础设施安全保护条例》章节结构

第一章 总则
第一到七条，总计7条

第二章 关键信息基础设施认定
第八到十一条，总计4条

第三章 运营者责任义务
第十二到二十一条，总计10条

第四章 保障和促进
第二十二到三十八条，总计17条

第五章 法律责任
第三十九条到第四十九条，总计11条

第六章 附则
第五十条和第五十一条，总计2条

- 关键信息基础设施范围和保护工作的原则目标
- 明确了监督管理体制
- 完善了关键信息基础设施认定机制
- 明确了运营者的责任义务
- 明确了保障和促进措施
- 明确了各方面的法律责任。

关键信息基础设施相关的标准有哪些？

目前，已立项制定的关键信息基础设施安全保护国家标准主要有：

序号	标准名称	标准内容	标准状态	保护环节
1	《信息技术 关键信息基础设施网络安全框架》	规范关键信息基础设施保护框架的基本要素及其关系，统一术语和定义	草案	五个环节
2	《信息技术 关键信息基础设施边界确定方法》	提出关键信息基础设施边界识别基本原则，给出了关键信息基础设施边界识别模型、方法和流程	征求意见稿	识别认定
3	《信息技术 关键信息基础设施安全保障指标体系》	提出关键信息基础设施安全保障指标及其释义	报批稿	五个环节
4	《信息技术 关键信息基础设施安全检查评估指南》	规定关键信息基础设施检查评估工作的方法、流程和内容	报批稿	识别认定、检查评估
5	《信息技术 关键信息基础设施安全保护要求》	规定关键信息基础设施分析识别、安全防护、检测评估、监测预警、事件处置等环节的安全要求	报批稿	五个环节
6	《信息技术 关键信息基础设施安全控制措施》	规定关键信息基础设施运营者在风险识别、安全防护、检测评估、监测预警、应急处置等环节应实现的安全控制措施	报批稿	五个环节
7	《信息技术 关键信息基础设施安全防护能力评价方法》	提出关键信息基础设施安全防护能力评价模型，给出能力评价方法	征求意见稿	五个环节

贰

关基工作流程

关基保护工作流程及内容

（主要环节及活动）

事件处置

对网络安全事件进行处置，并根据检测评估、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，恢复由于网络安全事件而受损的功能或服务。

分析认定

运营者配合保护工作部门，按照相关规定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，开展业务依赖性识别、风险识别等活动；

技术对抗

收敛互联网暴露面，加强攻击点管控，层层设防。在网络关键节点架设监测设备，发现并处置网络攻击和未知威胁。布设蜜罐、沙箱等设备，诱捕和溯源网络攻击，提升攻防对抗能力。

安全防护

运营者根据已识别的安全风险，实施安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面的安全控制措施，确保关键信息基础设施的运行安全；

监测预警

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；

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；

分析认定

开展CII边界识别是将关键业务持续、稳定运行所必须的网络设施、信息系统同其它信息基础设施区分开来，**明确保护对象，确定保护范围，识别风险**。

业务识别

业务依赖性识别
关基行业及业务的识别

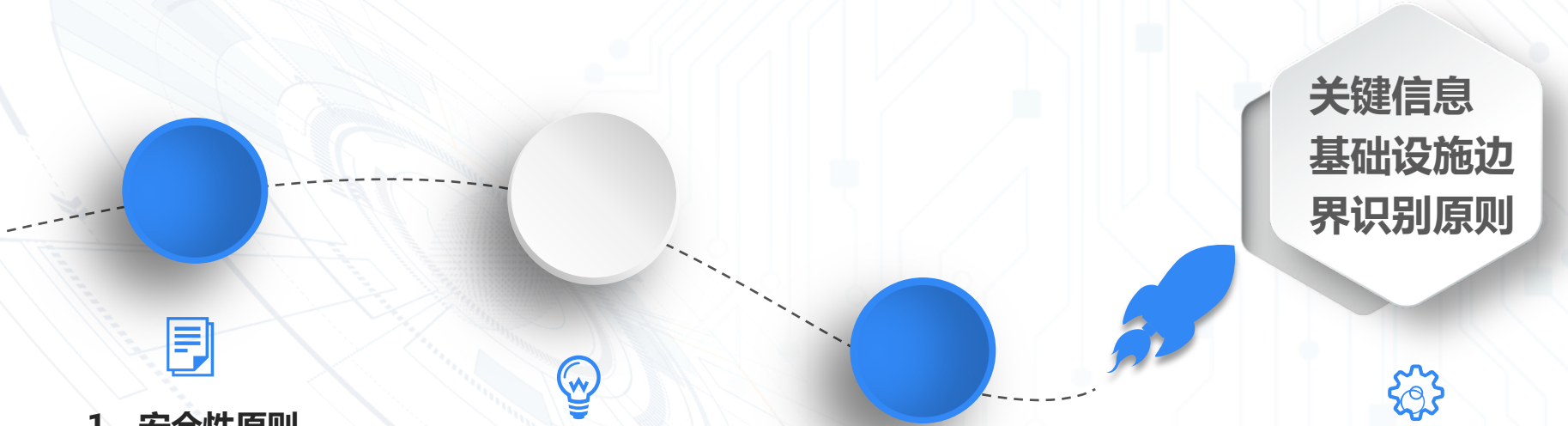
资产识别

对识别的关基业务进行边界识别与划定

风险识别

对关基业务及其关联业务相关的资产开展风险识别工作

关键信息基础设施识别原则



1、安全性原则

保障关键业务安全为基本原则；

2、整体性原则：

从保障整个关键业务安全的角度开展；

3、重要性原则：

CII边界识别应聚焦一旦遭到破坏、丧失功能或者发生数据泄露，会严重危害关键业务持续、稳定运行的软硬件设备、系统，严格控制范围；

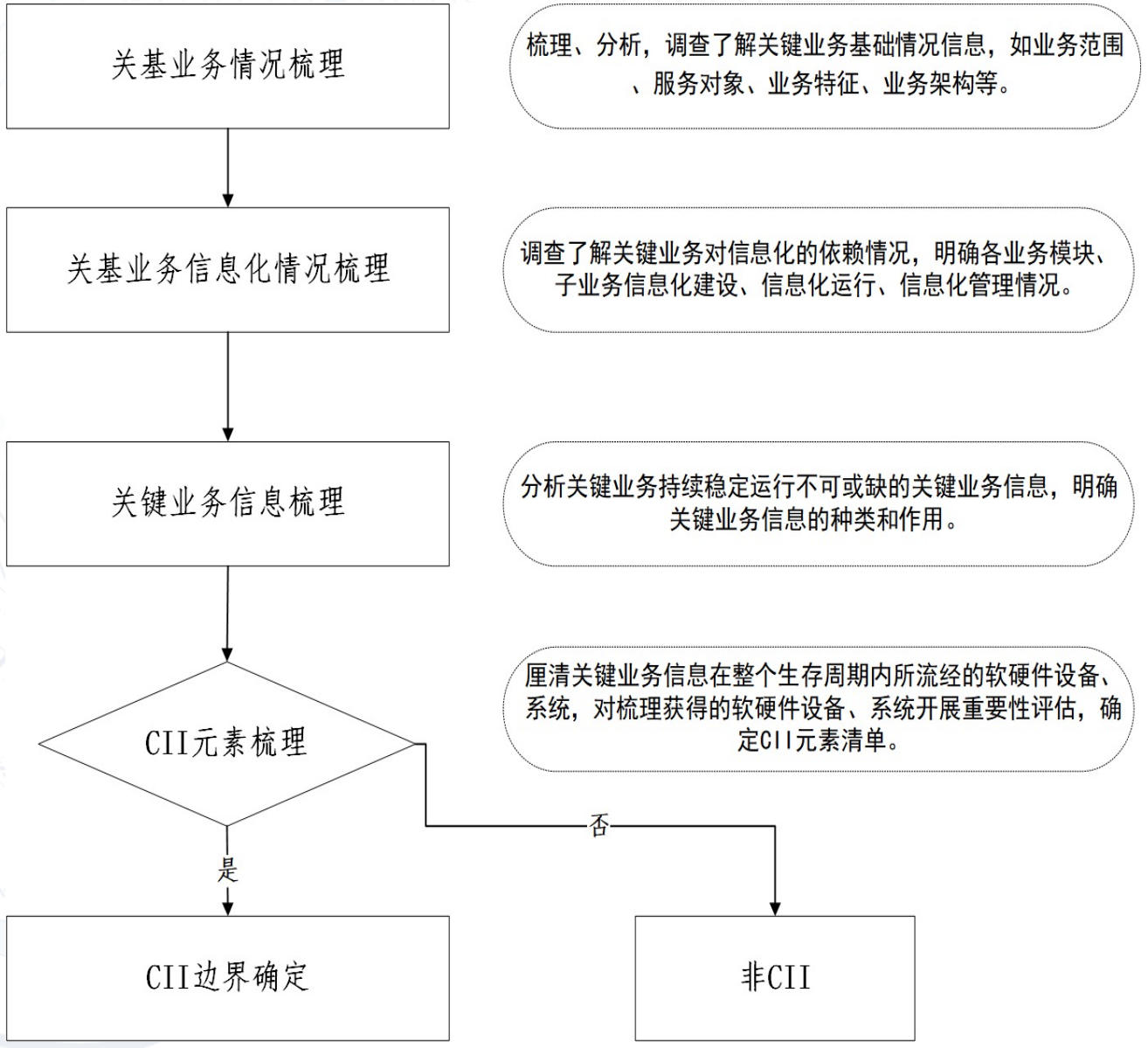
4、动态识别原则：

CII边界识别应采用动态工作方式，及时更新CII边界信息，当CII运营者的组织结构、业务架构、从属关系等**发生重大调整时**，应及时实施边界识别工作，确保CII边界**及时调整**。

关键信息基础设施识别流程

确定CII边界是完成关键信息基础设施识别认定的核心工作；

《信息安全技术·关键信息基础设施边界确定方法》指出确定CII边界具体包括关键业务基础情况 元素梳理和CII边界确定五个部分，如图所示：



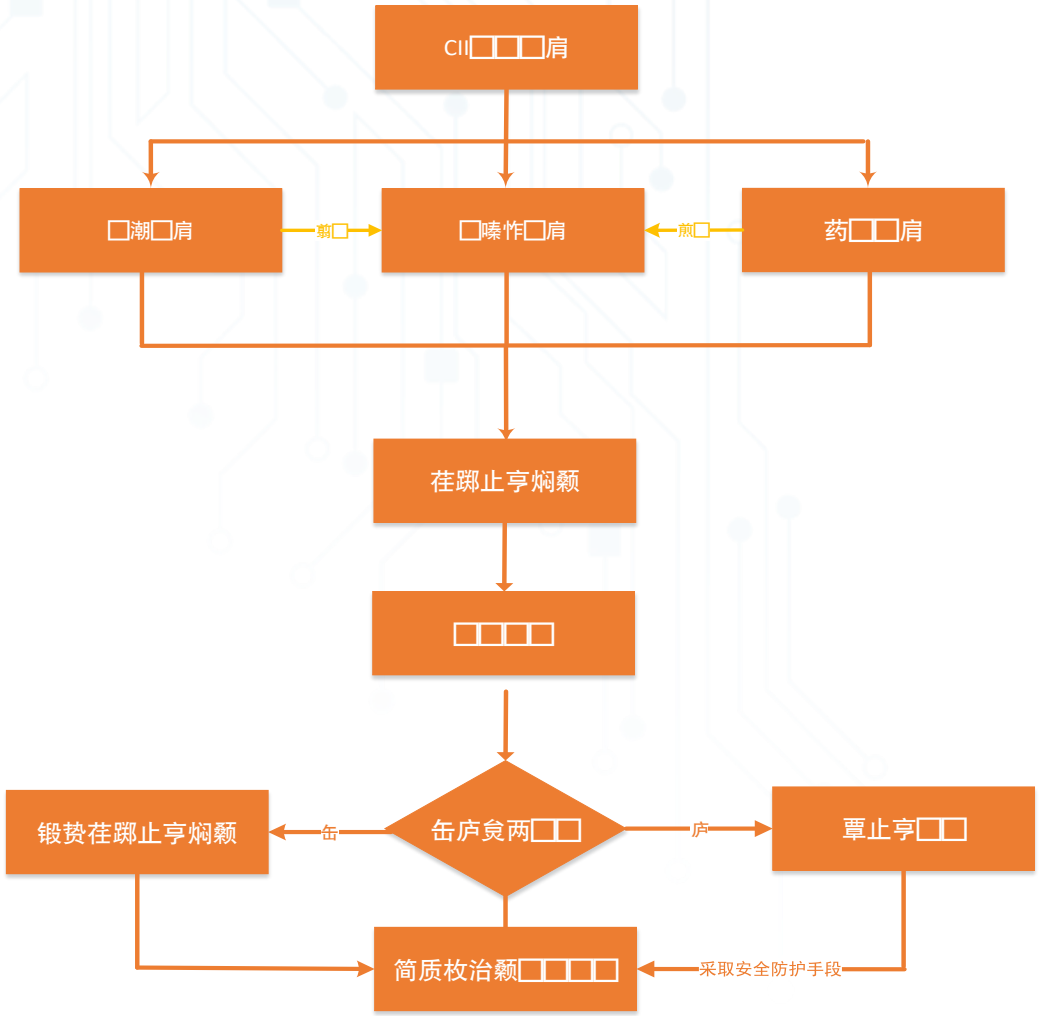
关键信息基础设施风险识别内容及方法

关基风险识别包括资产识别、威胁识别、脆弱性识别和已有安全措施识别与确认等内容。

具体工作内容及输出成果如图表：

序号	识别类型	识别内容
1	资产识别	1) 识别关键信息基础设施的资产并进行分类，包括数据、服务、信息系统、平台或支撑系统、基础设施、服务、人员管理等； 2) 识别资产价值及对机密性、完整性、可用性三个安全属性的要求。
2	威胁识别	识别关键信息基础设施可能面临的内部、外部威胁有哪些，并判断各种威胁出现的频率。
3	脆弱性识别	脆弱性识别以资产为核心，从技术和管理维度，针对每一项需要保护的资产,识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估。
4	已有安全措施识别	在识别脆弱性的同时，对已采取的安全措施的有效性进行确认。确认其有效性，对有效的安全措施继续保持，防止安全措施的重复实施。对不适当的安全措施取消或修正。

关基风险识别方法如下图所示：



安全防护

开展CII安全防护的目的是为了保障关键业务稳定、持续运行，支撑关键业务的网络设施、信息系统一旦发生安全事件都可能对关键业务造成重大影响，让其**网络设施、信息系统上面的保护措施成为了“马奇诺防线”**。

网络安全等级保护制度

开展网络安全等级保护工作

- 定级备案
- 相应等级的测评
- 安全建设
- 整改及自查工作

安全管理

- 安全管理制度
- 安全管理机构
- 安全管理人员
- 安全建设管理
  - 网络安全与信息化同步要求
  - 供应链安全保护
- 安全运维管理

安全技术

- 安全通信网络
  - 互联安全
  - 边界防护
  - 安全审计
- 安全计算环境
  - 鉴别与授权
  - 入侵防范
  - 数据安全防护
  - 自动化工具

关键信息基础设施安全防护的要求-1

工作内容	安全要求
网络安全等级保护制度	运营者应符合国家网络安全等级保护制度相关要求，开展定级备案、相应等级的测评、安全建设、整改及自查工作。
安全管理制度	a）建立适合本组织的网络安全保护计划，结合关键业务流的安全风险报告，明确关键信息基础设施网络安全保护工作的目标安全策略、组织架构、管理制度、技术措施、实施细则及资源保障等，形成文档并经审批后发布至相关人员。网络安全保护计划应至少每年修订一次，或发生重大变化时进行修订。
	b）基于关键业务链、供应链等安全需求建立或完善安全策略和制度，并根据关键信息基础设施面临的安全风险和威胁的变化相应调整。
安全管理机构	a）成立指导和管理网络安全工作的委员会或领导小组，由组织主要负责人担任其领导职务，设置专门的网络安全管理机构，建立首席网络安全官制度，建立并实施网络安全考核及监督问责机制。
	b）安全管理机构主要人员应参与本组织信息化决策。
	c）安全管理机构相关人员应参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到本组织。
安全管理人员	a）对安全管理机构的负责人和关键岗位的人员进行安全背景和安全技能审查，符合要求的人员方能上岗，关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应专人负责，并配备2人以上共同管理。
	b）运营者应建立网络安全教育培训制度，定期开展基于岗位的网络安全教育培训和技能考核，应规定适当的关键信息基础设施从业人员和网络安全关键岗位从业人员的年度培训时长，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等。
	c）在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份认证相关的软硬件设备，进行离职面谈并通知相关人员或角色。
	d）与从业人员签订安全保密协议，在安全保密协议中，应约定安全职责、奖惩机制，以及当离岗后的脱密期限。

关键信息基础设施安全防护的要求-2

工作内容		安全要求
安全通信网络	互联安全	a）建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略。
		b）保持相同的用户其用户身份、安全标记、访问控制策略等在不同等级系统、不同业务系统、不同区域中的一致性。例如，可以使用统一身份与授权管理系统/平台。
		c）对不同局域网之间远程通信时采取安全防护措施，例如在通信前基于密码技术对通信的双方进行验证或认证。
	边界防护	a）对不同网络安全等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流向进行严格控制。例如：采取措施限制数据从高网络安全等级系统流向低网络安全等级系统。
		b）应对未授权设备进行动态检测及管控，只允许通过运营者自身授权和安全评估的软硬件运行。
	安全审计	运营者应加强网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于12个月。

关键信息基础设施安全防护的要求-3

工作内容		安全要求
安全计算环境	鉴别与授权	a）运营者应明确重要业务操作或异常用户操作行为，并形成清单。
		b）对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别方式等。
		c）针对重要业务数据资源的操作，基于安全标记等技术实现访问控制。
	入侵防范	a）实现对新型网络攻击行为（如APT攻击）的入侵防范。
		b）具备系统主动防护能力，及时识别并阻断入侵和病毒行为。
	数据安全防护	a） 建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。
		b） 制定数据安全管理策略，明确数据和个人信息保护的相应措施。
		c） 将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定。对数据的全生命周期进行安全管理，基于数据分类分级实现相应的数据安全保护。
		d） 严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。
		e） 建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。
		f） 业务数据安全性要求高的实现数据的异地实时备份。
		g） 业务连续性要求高的实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。
	自动化工具	运营者应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，应在经过验证后及时修补。

关键信息基础设施安全防护的要求-4

工作内容		安全要求
安全建设管理	网络安全与信息化同步要求	a）在新建或改建、扩建关键信息基础实施设施时，充分考虑网络安全因素，在规划、建设和投入使用阶段保证安全措施的有效性，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境。
		b）当关键信息基础设施退役废弃时，按照数据安全管理策略对存储的数据进行处理。
	供应链安全保护	a）制定供应链安全管理策略，包括：风险管理策略、供应商选择和管理策略、产品开发采购策略、安全维护策略等。
		b）建立供应链安全管理制度，设置相应的供应链安全管理部门，提供用于供应链安全管理的资金、人员和权限等可用资源。
		c）保证产品的设计、研发、交付、使用、废弃等各阶段，以及制造设备、工艺等的供应链安全风险基本可控。
		d）选择有保障的供应商，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。
		e）在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。
		f）要求供应商承诺不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。
		g）采购、使用的网络关键设备和网络安全专用产品，应通过国家规定的检测认证。
		h）采购、使用的网络产品和服务，应符合法律、行政法规的规定和相关国家标准的要求，可能影响国家安全的，应当通过国家安全审查。
		i）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，涉及重大风险的应当按规定向保护工作部门报告。
		j）采购网络产品和服务时，明确提供者的安全责任和义务，要求提供者做出必要安全承诺，并签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等。
安全运维管理		a）保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，应当符合我国相关规定。
		b）应要求维护人员签订安全保密协议。
		c）确保优先使用已登记备案的运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。

关键信息基础设施运营者采购和使用网络安全设备

《网络安全法》的二十三条规定，网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求。

根据**《关键信息基础设施安全保护条例》第三十条的规定**，运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。

为加强网络关键设备和网络安全专用产品的安全管理，国家互联网信息办公室会同工业和信息化部、公安部、国家认监委等部门**依据《中华人民共和国网络安全法》制定了《网络关键设备和网络安全专用产品目录（第一批）》，并于2017年6月1日发布。**其中涉及5类网络关键设备和15类网络安全专用产品。

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量（双向）≥12Tbps 整系统路由表容量≥55 万条
	2. 交换机	整系统吞吐量（双向）≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器（机架式）	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时
	6. 防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统（IDS）	满检速率≥15Gbps 最大并发连接数≥500 万
	9. 入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500 万
	10. 安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率（连接/秒）＞100 平均延迟时间＜100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC－E tpsE（每秒可交易数量）≥4500 个
	15. 网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10 级

列入该目录的设备和产品，要按照相关国家标准的强制性标准要求进行安全认证或安全检测。

关基运营者需要选购安全认证合格或安全检测符合要求的网络关键设备和网络安全专用产品。

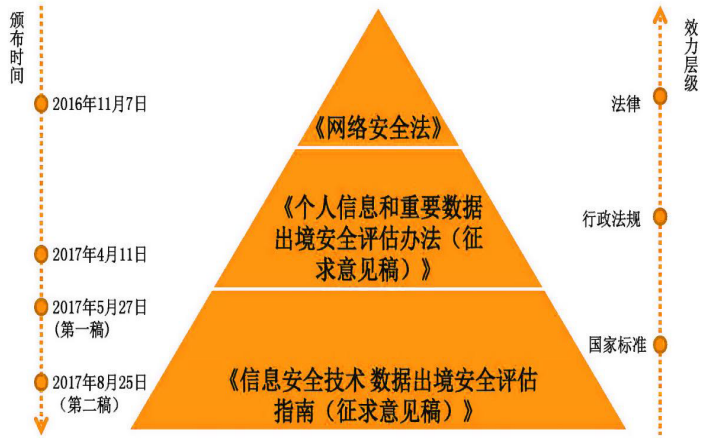
关键信息基础设施相关个人信息和重要数据出镜

《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；

《关键信息基础设施安全保护条例》第二十九条进一步明确，关基相关个人信息和重要数据因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；

《个人信息和重要数据出境安全评估办法》（征求意见稿）第五条、第六条、第九条、第十条、第十一条规定，国家网信部门指导行业主管或监管部门定期组织开展本行业数据出境安全检查。出境数据涉及关键信息基础设施的系统漏洞、安全防护等网络安全信息或关键信息基础设施运营者向境外提供个人信息和重要数据等情形的，**网络运营者应报请行业主管或监管部门组织安全评估，评估工作应当在六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。**当然出境数据存在未经个人信息主体同意、可能侵害个人利益或给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益等情形的，则数据不的出境。

数据出境安全评估制度配套法规金字塔



关键信息基础设施安全防护能力等级划分

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含所有低等级能力要求。能力等级及其特征如下：

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。

检测评估

检测评估制度

制定检测评估制度

检测评估方式

- 自行或委托安全服务机构
- 每年一次

检测评估内容

- 网络安全制度落实情况；
- 组织机构建设情况；
- 人员和经费投入情况；
- 教育培训情况；
- 网络安全等级保护工作落实情况；
- 密码应用安全性评估情况；
- 技术防护情况；
- 云服务安全评估情况；
- 风险评估情况；
- 应急演练情况；
- 攻防演练情况
- ……

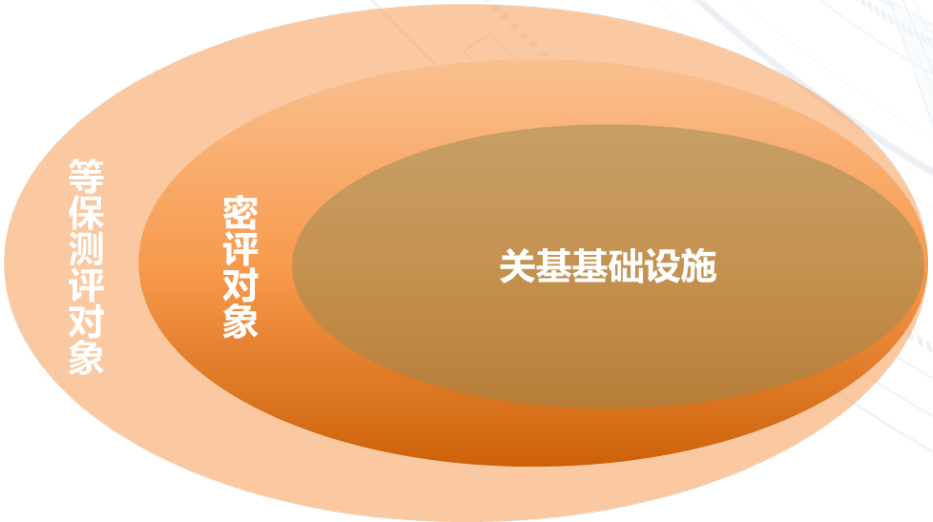
◆ 开展CII安全检查和检测的目的是为了有效落实保护方案，保障CII持续、稳定运行；

◆ CII安全检查和检测需聚焦在**关键业务安全运行至关重要的网络设施、信息系统**之上。

关键信息基础设施安全评估与密评、等级测评间的关系

- **从评估对象来说：**等级保护测评对象基本覆盖了全部的网络和信息系统，第三级以上的网络安全等级保护对象同时为关基和密评的评估对象；
- **关键基础设施：**一定是等级测评和密评的评估的对象；
- **密评对象：**含关键基础设施、第三级等级保护对象和部分重要的信息系统。

三者评估对象间的关系如下图所示：



从评估方式来说：要遵照商用密码应用安全性评估管理办法（试行）第十条规定，关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次，测评机构可将商用密码应用安全性评估与关键信息基础设施网络安全测评、网络安全等级保护测评**同步进行，相互衔接，避免重复评估、测评。**

关键信息基础设施安全检测评估的要求

在《网络安全法》中明确规定：

1）针对关基的运营者

应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

2）针对国家网信部门

应当统筹协调有关部门对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估。

关键信息基础设施安全检测评估内容

《关键信息基础设施网络安全保护基本要求》中明确指出“检测评估内容包括但不限于：

- 网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况；
- 组织机构建设情况；
- 人员和经费投入情况；
- 教育培训情况；
- 网络安全等级保护工作落实情况；
- 密码应用安全性评估情况；
- 技术防护情况、云服务安全评估情况；
- 风险评估情况；
- 应急演练情况；
- 攻防演练情况。

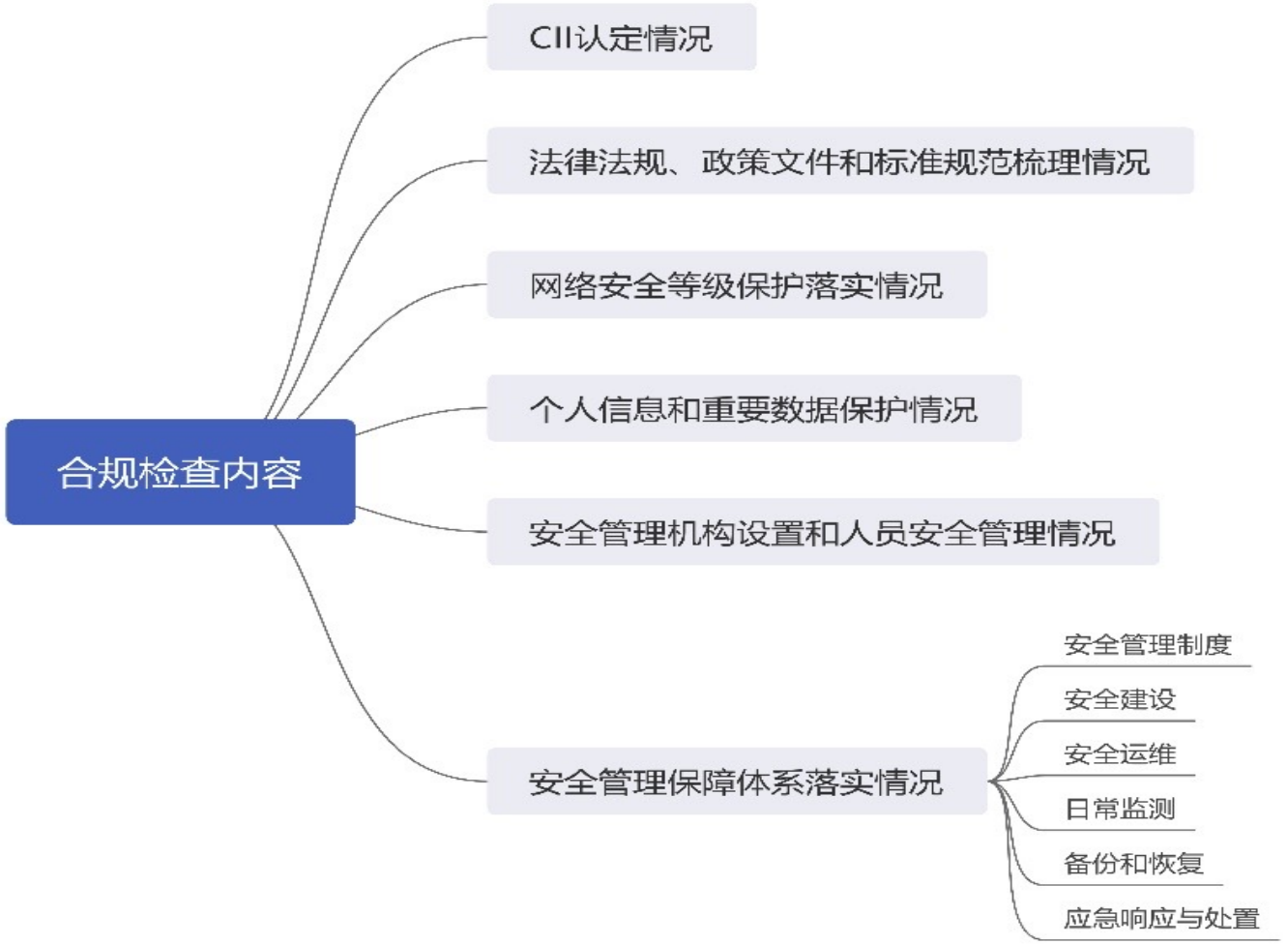
尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。”

关键信息基础设施合规检查的主要内容

《关键信息基础设施安全检查评估指南》中将检查评估内容分为：合规检查和技术检查两部分。

合规检查：

是指通过资料核实、人员访谈和技术验证等手段，检查被检查方是否遵从法律、法规和政策标准的相关要求。



关键信息基础设施技术检测的主要内容

《关键信息基础设施安全检查评估指南》中将检查评估内容分为：合规检查和技术检查两部分。

技术检查可分为：安全检测和安全监测两部分。

安全检测：是指检查人员在合适的检测接入点，通过漏洞扫描、渗透测试和社会工程学等安全测试方法，验证被检查方某种特定性能指标的技术手段。

安全监测：是指检查人员在合适的监测接入点部署监测工具，长时间获取网络实时流量，发现被检查方安全漏洞和安全隐患的技术手段。

监测预警

监测预警制度

- 制定自身的监测预警和信息通报制度；
- 对关键业务所涉及的信息系统实施监测的相关文档、实地查验。

监测

- 信息系统监测
- 物理访问监测
- 信息泄露监测
- 恶意代码检测

预警

- 预警信息接收
- 预警研判和通报
- 信息共享

中华人民共和国
国家安全法

第五十一条

国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条

负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的**网络安全监测预警和信息通报制度**，并按照规定报送网络安全监测预警信息。

关键信息基础设施安全监测预警包括的内容

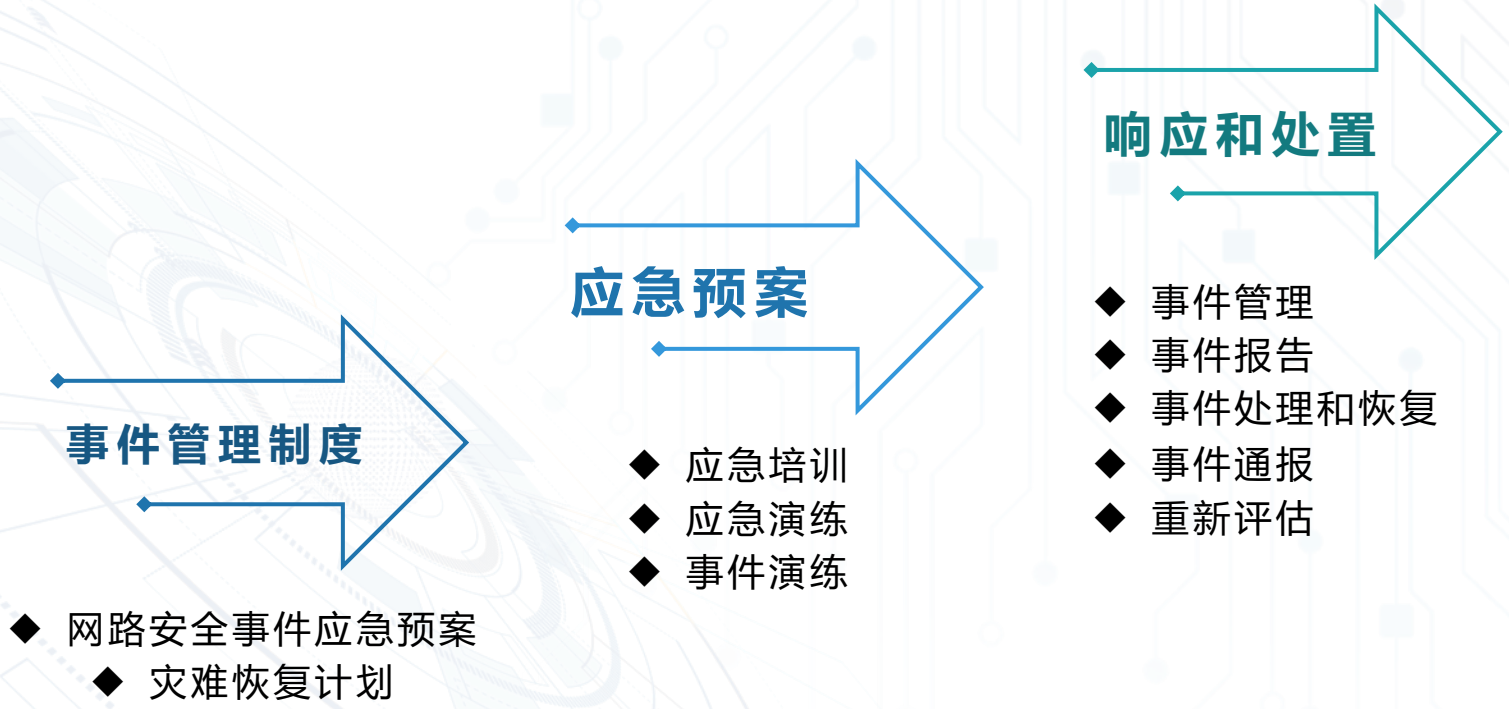
《信息安全技术·关键信息基础设施网络安全保护基本要求》

对监测预警方面提出了要求，关基运营者需制定并实施：

- **网络安全监测预警和信息通报制度，**
- **建立信息共享渠道，**
- **分析监测结果，**

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。

事件处置



CII网络安全应急目标：

a)联动处置：CII网络安全应急相关方可以信息共享、协同配合，实施联动应急处置，以尽可能快的速度和尽可能小的代将CII恢复到正常状态，保障跨运营者的关键业务持续、稳定运行。

b)提高应对网络安全事件的能力：建立健全CII网络安全事件应急体系，提高应对网络安全事件能力，预防、减少网络安全事件造成的损失和危害。

关键信息基础设施安全对事件管理制度的要求

随着关键信息基础设施互联互通的发展,各种网络安全事件时有发生。关基运营单位需建立网络安全事件管理制度，通过制度来保障安全事件的处置工作能落到实处。

网络安全事件分类分级

首先，需要明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程，按照事件级别制定应急预案、演练计划、回退措施等网络安全事件管理文档。

网络安全事件提供必要资源

其次，要为网络安全事件的处置提供必要的资源，指定专门网络安全应急支撑队伍、专家队伍，保障安全事件能得到及时有效处置。

网络安全应急演练

最后，要按规定参与和配合相关部门开展的网络安全应急演练、应急处置等工作

关键信息基础设施安全对应急预案的要求

在国家网络安全事件应急预案的框架下，关基运营单位需根据行业和地方的特殊要求，制定网络安全事件应急预案，并确保每年至少组织1次跨组织、跨地域的应急演练。

制定应急预案

在制定应急预案时，要明确一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间。

应急事件处理

应急预案不限于本组织应急事件的处理，如果涉及第三方的话，要包含联合其它单位共同开展的应急事件的处理工作的预案。

内部相关计划

同所涉及到的运营者内部相关计划（例如业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足。

网络安全应急预案评估

此外，要定期对网络安全应急预案进行评估修订，并持续改进。


叁
关基智能化安全运营服务体系

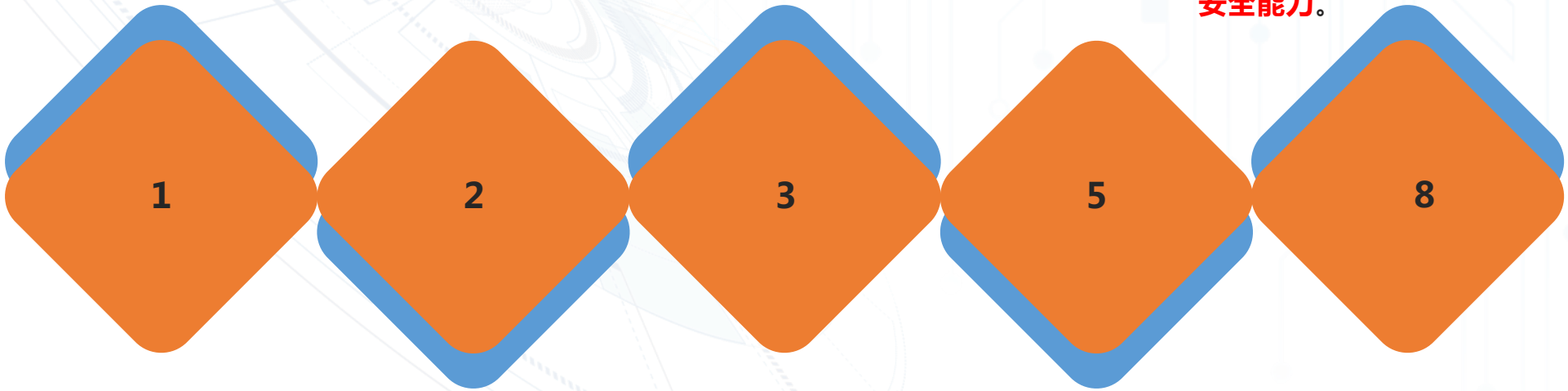
“启明星辰12358”智能化安全运营服务体系

为更好地服务政企用户，深入贯彻落实“两个制度”，“启明星辰12358”关键信息基础设施智能化安全运营服务体系应运而生。(启明星辰12358基本理念如下)：

以安全运营中心为**核心**的关键信息基础设施智能化安全运营服务体系。

立足“三位一体”，聚合“人员、流程、技术”，建立智能化安全运营中心，完善网络安全措施。

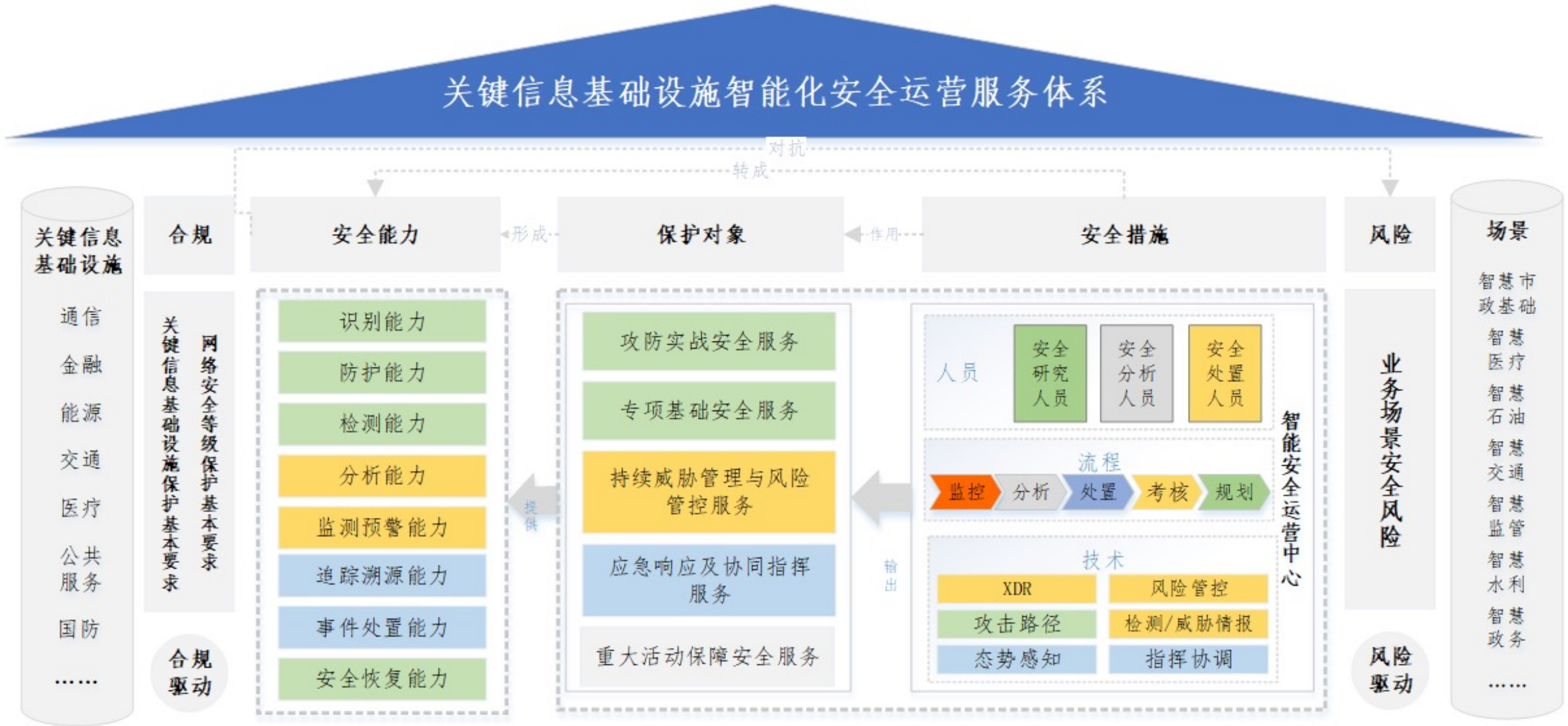
智能化安全运营服务体系通过安全服务的形式助力用户落实安全防护措施，构建关键信息基础设施安全、合规、稳定、高效运行所需的**八大安全能力**。



面向重要行业关键信息基础设施，积极推动两个制度落实，以安全**“合规”**和**“风险”**为驱动。

以“安全运营”为核心理念，通过智能化安全运营中心为客户提供**五个专项安全服务**.

“启明星辰12358”智能化安全运营服务体系基本框架如下图



关键信息基础设施保护工作中需要完成的工作

阶段	主要工作内容	涉及的安全服务
识别认定	资产识别、风险识别、业务识别、关基边界确定	资产梳理服务、安全评估服务、边界确定服务、攻防演练服务
安全防护	落实网络安全等级保护制度基础上强化安全防护措施	等保2.0合规性服务（安全咨询服务）、安全管理体系建设服务、安全体系建设服务、安全加固服务、安全评估服务、安全教育培训服务、攻防演练安全服务
检测评估	建立检测评估制度、开展检测评估工作	安全评估服务、渗透测试服务、漏洞检测服务
监测预警	监测预警体系建设、安全监测、安全信息预警	持续性威胁分析与防御服务、风险感知/遏制与响应服务、威胁情报服务、事件调查/溯源/跟踪服务、资产/漏洞安全监测服务
技术对抗	暴露面收敛、攻击溯源分析、攻防演练	安全评估服务、安全加固服务、攻防演练服务、红蓝对抗服务
事件处置	应急预案、应急响应、安全评估	应急管理体系咨询服务、事件应急响应服务、热点应急管理


谢谢观看
THANK YOU