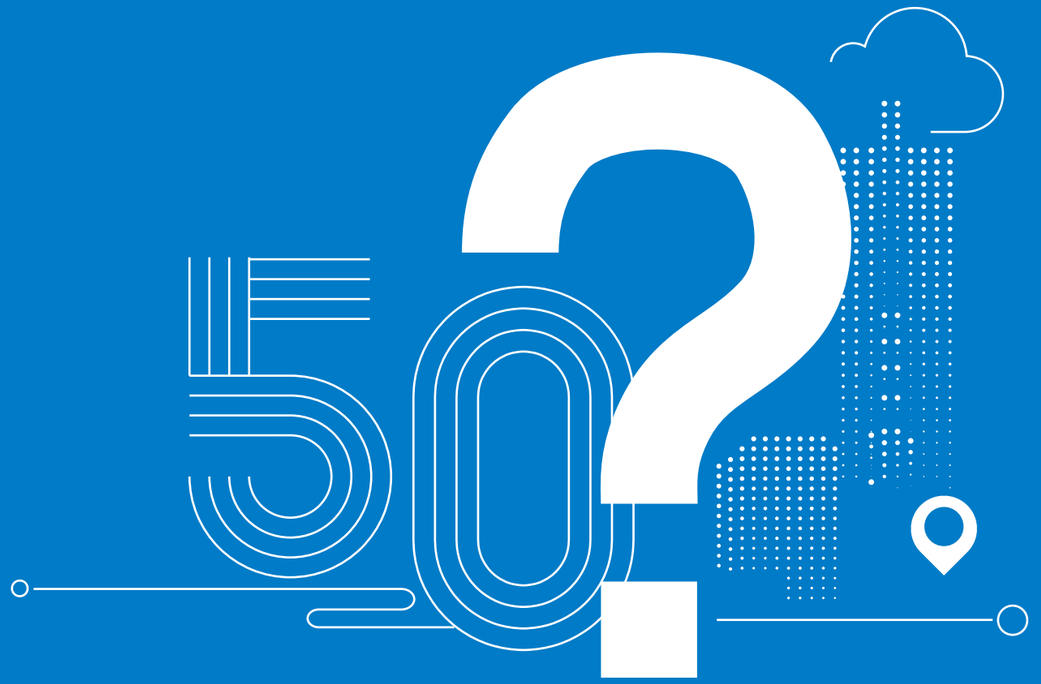
保卫·保护·保障

关基50问

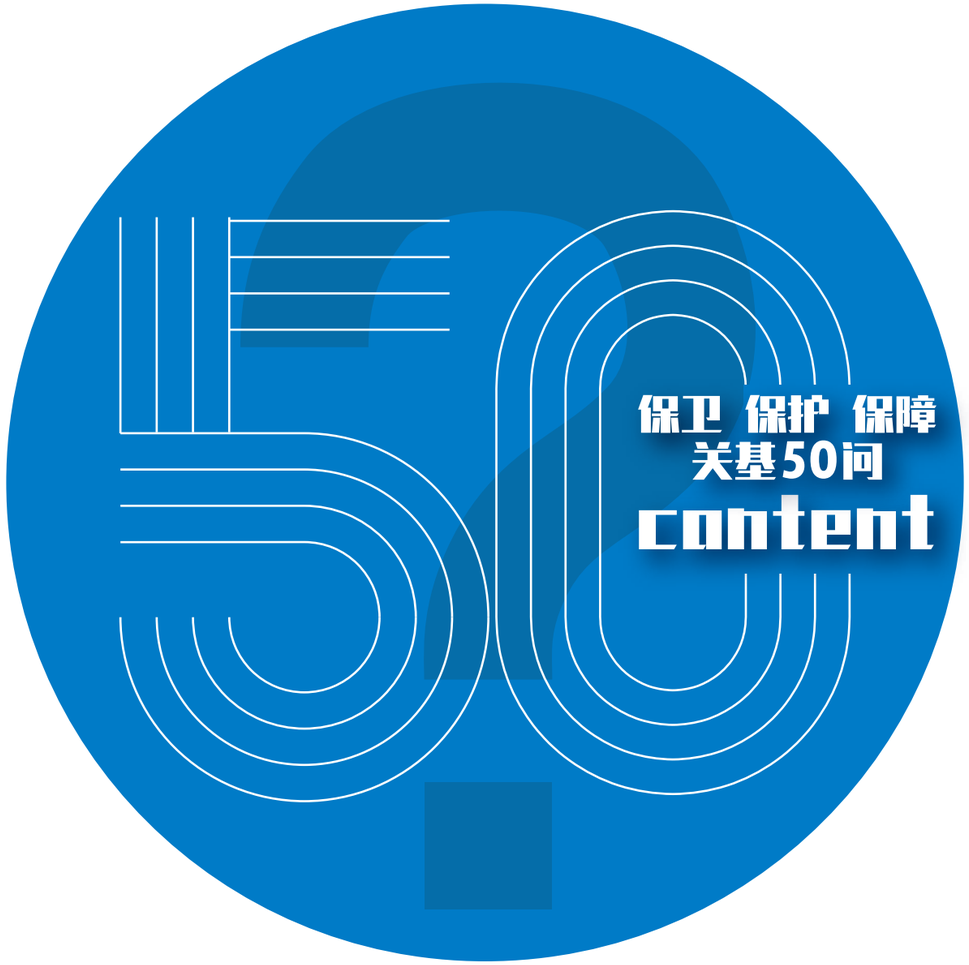


前言

2020年7月，公安部研究制定了1960号《贯彻落实网络安全等保制度和关保制度的指导意见》，明确指出各单位、各部门深入开展网络安全等级保护工作，建立并实施关键信息基础设施安全保护制度。2021年7月30日，李克强总理签发第745号国务院令《关键信息基础设施安全保护条例》，并于2021年9月1号开始实施，标志着我国关键信息基础设施安全保护工作迈入新的阶段。

本手册依据下列标准整理，后续将持续跟踪行业动态并进行问题集更新。

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



01问 什么是关键信息基础设施?

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指出：金融、能源、电力、通信、交通等领域的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。

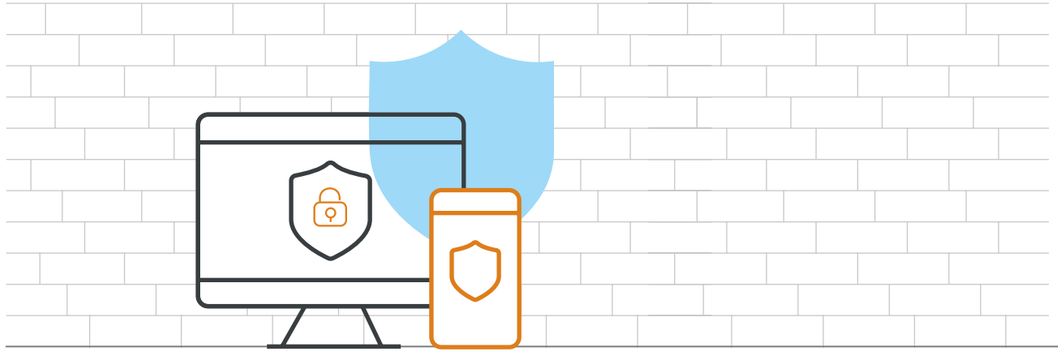
在《国家网络安全检查操作指南》、《网络安全法》和《关键信息基础设施安全保护条例》等法律法规或政策文件中基本都采用了“特定行业范围 + 严重危害后果”的方式对关键信息基础设施进行了定义。

发布日期	法律法规或政策文件	关键信息基础设施定义
2016年6月	《国家网络安全检查操作指南》	关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。
2016年11月	《中华人民共和国网络安全法》	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。
2021年7月	《关键信息基础设施安全保护条例》	本条例所称关键信息基础设施，是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

02问 如何认识关键信息基础设施?

关键信息基础设施涉及的要素有：关键业务、关键业务信息、关键业务信息流、关键信息基础设施元素等。认识关键信息基础设施需了解关键信息基础设施涉及的基本要素。

- **关键业务（Critical Business）：**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；
- **关键业务信息（Critical Business Information）：**业务核心功能正常运行所必需的信息数据的统称；
- **业务信息流（Critical Business Information Flow）：**关键业务信息从产生到终止，在整个生命周期内的流动轨迹；
- **关键信息基础设施元素（Critical Information Infrastructure Elements）：**构成关键信息基础设施的网络设施、信息系统的统称，其中网络设施是指连接通信信息网络（互联网、物联网、工控网、专用网等）的基础性网络设施，以及在上述网络中对信息数据进行发送、传输、控制等操作的网络设备；信息系统是指由计算机软硬件、数据、规章制度等组成的按照一定规则运行的功能单元。



03问 如何开展关键信息基础设施保护工作?（主要环节及活动）

关键信息基础设施安全保护工作的开展主要包括分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置六个环节。

在国家目前已有的关键信息基础设施安全保护标准体系内，规定关键信息基础设施安全保护工作在各环节开展以下工作：

- **分析识别：**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分析和识别活动，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；
- **安全防护：**运营者根据已识别的关键业务和资产、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；
- **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；
- **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，建立威胁情报和信息共享机制，落实相关措施，提高关键信息基础设施主动防御能力；
- **技术对抗：**运营者以对攻击行为的监测发现为基础，主动采取诱捕、溯源、干扰和阻断等措施，提升对网络威胁与攻击行为的识别、分析和攻防对抗能力；
- **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。

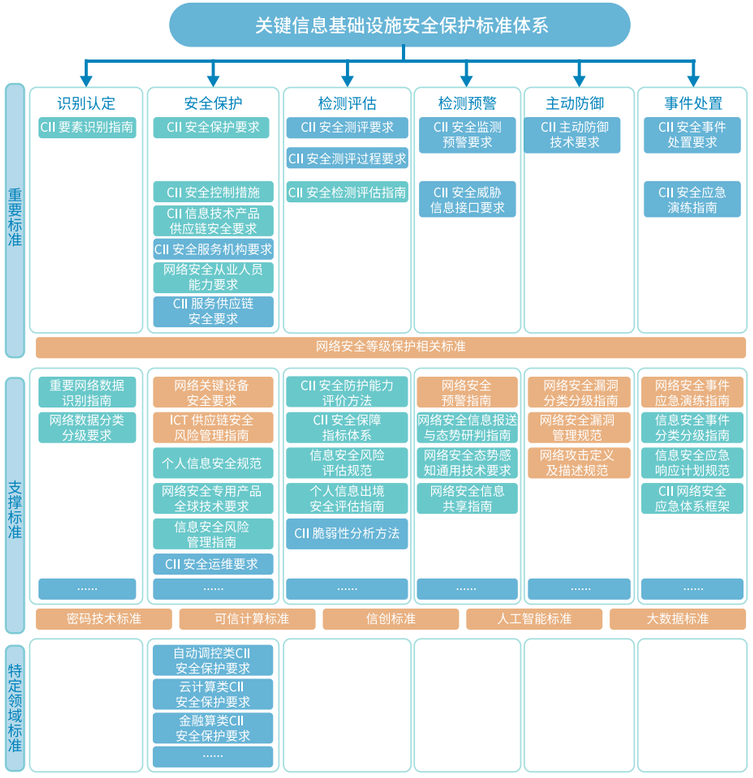
04 问 关键信息基础设施安全保护政策体系？

我国正在逐步建立并完善关键信息基础设施安全保护政策体系，如图所示。

- **上层**是《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》等上位法。
- **中层**法规政策包括《关键信息基础设施安全保护条例》《网络安全等级保护条例》，以及公安部发布的《贯彻落实网络安全等保制度和关键信息基础设施安全保护制度的指导意见》等。
- **下层**是用来指导关键信息基础设施安全防护各参与者开展工作的网络安全标准规范。

05问 关键信息基础设施相关的标准有哪些?

关键信息基础设施安全保护标准体系主要用于明确关基安全保护的标准化需求、环节和范围，指导国家关基安全保护标准体系建设。根据公安部信息安全等级保护评估中心文章显示，关键信息基础设施安全保护标准体系框架如下图所示：



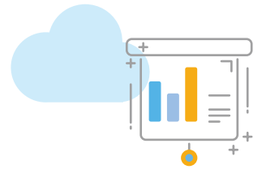
根据上图所示，关基安全保护标准按照标准定位可分为重要标准、支撑标准以及特殊领域标准，按照标准应用的关基保护工作环节划分可分为识别认定类、安全保护类、检测评估类、监测预警类、主动防御类和事件响应处置类等标准。其中橙色模块为已发布的国家标准，绿色模块标准为已立项尚未发布的国家标准，蓝色模块为未立项标准。

目前，已掌握的部分立项制定的关键信息基础设施安全保护国家标准标准状态如下：

序号	标准名称	标准内容	标准状态
1	《信息安全技术 关键信息基础设施安全保护要求》	规定了关键信息基础设施分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置等环节的安全要求	报批稿
2	《信息安全技术 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
3	《信息安全技术 信息技术产品供应链安全要求》	规定了信息技术产品供应方和需求方应满足的供应链安全要求	征求意见稿
4	《信息安全技术 网络安全从业人员能力基本要求》	规定了网络安全从业人员分类和各类从业人员具备的知识和技能要求	征求意见稿
5	《信息技术 关键信息基础设施安全检查评估指南》	给出了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
6	《信息安全技术 关键信息基础设施安全保障指标体系》	规定了用于开展关键信息基础设施安全保障的指标及其释义	报批稿
7	《信息安全技术 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	送审稿
8	《信息安全技术 关键信息基础设施网络安全应急体系框架》	提出了关键信息基础设施网络安全应急体系框架，包括目标、原则、方式、角色、职责和协同机制等	草案

06问 关键信息基础设施安全保护各重要标准的定位是什么？

序号	标准名称	使用范围	标准定位
1	《信息安全技术 关键信息基础设施要素识别指南》	关基运营者	该标准用于关基确定之后，指导运营者划定关基的重点保护范围、确定关键资产、涉及多责任方的保护责任识别等。
2	《信息安全技术 关键信息基础设施安全保护要求》	关基保护工作部门及运营者	为通用性的保护指导标准，规定关基在分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求，是各CII开展安全保护工作时，需在等级保护要求基础上增强的最低要求。
3	《信息安全技术 关键信息基础设施安全控制措施》	关基保护工作部门及运营者	为《关基安全保护要求》提出的各项要求提供实施落地指导，该标准内容力求全面，针对《关基安全保护要求》的每一项安全要求，力争写出不同实现强度的安全控制措施，供关基保护工作部门及运营者在落地实施时选择参考。
4	《信息安全技术 关键信息基础设施安全测评要求》	关基评估机构	该标准与《关基安全保护要求》为姊妹篇，定位类似于等保测评要求，从第三方评估机构开展安全评估的角度，而非监管部门的安全检查角度，提出相应的安全评估方法。针对《关基安全保护要求》的各项要求内容，描述对应的测评方法。
5	《信息安全技术 关键信息基础设施安全测评过程指南》	关基评估机构	该标准与《关基安全测评要求》共同指导关键信息基础设施安全检测评估工作，定位类似于等保测评过程指南，从第三方评估机构开展安全评估的角度，提出相应的安全评估过程及工作任务。
6	《信息安全技术 关键信息基础设施安全检查评估指南》	关基保护工作部门	该标准明确关基检查评估的方法、流程和内容，用于保护工作部门开展关基安全检查评估。
7	《信息安全技术 关键信息基础设施安全监测预警要求》	关基运营者、监测服务机构、产品提供者	该标准针对关基安全监测预警工作提出规范要求，包括监测点的部署、监测数据的汇总及分析技术要求、监测数据的管理要求等等。
8	《信息安全技术 关基信息基础设施安全威胁信息接口要求》	关基运营者、网络安全服务机构、其他科研机构以及有关部	规定漏洞信息、威胁信息进行安全共享时所采用的格式、接口、索引标签要求等，在此基础上开展威胁漏洞评级。
9	《信息安全技术 关基信息基础设施主动防御技术要求》	关关基保护工作部门、运营者、安全服务机构	该标准针对《关基安全保护要求》中的主动防御类条款，指导关键信息基础设施保护工作部门及运营者如何具体落实。
10	《信息安全技术 关基信息基础设施安全事件处置要求》	关基运营者	该标准指导关基运营者将其运营关基可能发生的安全事件分类分级，为不同类别不同级别事件的处置奠定基础。指导关基运营者不同类别和级别的事件如何进行处置，包括何种情况向保护工作部门汇报、何种情况向国家相关管理部门汇报等等。
11	《信息安全技术 关基信息基础设施安全应急演练指南》	关基保护主管部门、保护工作部门、运营	该标准规范关基的应急演练，尤其是跨部门、跨单位、跨行业的演练指导。



07问 关键信息基础设施安全保护各重要标准与其他相关标准的关系？

- **《信息安全技术 关键信息基础设施要素识别指南》与《关基安全保护要求》：**可用于指导保护工作部门及运营者落实《关基安全保护要求》中分析识别环节的工作；与《关基安全测评要求》：可用于指导评估机构对被评估关基的业务、业务链以及资产的分析识别工作。

- **《信息安全技术 关键信息基础设施安全保护要求》与《网络安全等级保护基本要求》：**在 GB/T 22239 第三级安全通用要求基础上的增强要求，不重复第三级安全通用要求；与《关基安全控制措施》：《关基安全控制措施》依据本标准中各要求项提出落地措施；与《关基安全测评要求》：《关基安全测评要求》给出本标准中提出的各要求项的具体测评方法。

- **《信息安全技术 关键信息基础设施安全测评要求》与《关基安全保护要求》：**对于要求条款给出测评方法；与《关基安全测评过程指南》：共同指导关基检测评估活动；与《网络安全等级保护测评要求》：在 GB/T 28448 单项测评结果基础上加强测评深度，评价融合等级测评结果；与《信息安全风险评估方法》：风险评估思路与其保持一致；与《关基安全防护能力评价方法》和《关基安全检查评估指南》：作为评价防护能力及检查评估结果的输入。

- **《信息安全技术 关键信息基础设施安全测评过程指南》与《关基安全测评要求》：**共同指导 CII 检测评估活动。

- **《信息安全技术 关键信息基础设施安全检查评估指南》与《关基安全测评要求》：**《关基安全测评要求》作为本标准测评证据的输入。

- **《信息安全技术 关键信息基础设施安全监测预警要求》与《关基安全保护要求》：**为《关基安全保护要求》中监测预警相关要求内容的细化。

- **《信息安全技术 关键信息基础设施安全威胁信息接口要求》与《网络安全信息共享指南》：**为《网络安全信息共享指南》在关键信息基础设施保护领域的特殊要求，相同内容应保持一致。

- **《信息安全技术 关基信息基础设施主动防御技术要求》与《关基安全保护要求》：**为《关基安全保护要求》中相关要求内容的细化。

- **《信息安全技术 关基信息基础设施安全事件处置要求》与《信息安全事件分类分级指南》：**基于已有国标《GB/Z 20986-2007 信息安全事件分类分级指南》，着眼在 CII 面临的安全事件；与《网络安全预警指南》：与《网络安全预警指南》中的报送内容及方式保持一致。

- **《信息安全技术 关基信息基础设施安全应急演练指南》与《网络安全事件应急演练通用指南》：**在《网络安全事件应急演练通用指南》的基础上提出关键信息基础设施的应急演练相关内容，包括机构组织、工作方案、脚本、流程、评估方案、保障措施等演练方案内容等，尤其应加强跨部门、跨单位、跨行业的演练指导内容。

08问 关键信息基础设施运营者的安全保护义务及责任？

针对关键信息基础设施安全保护，作为运营者来说必须承担相应的法律保护义务和责任，而不同的法律从立法角度不同，规定了运营者不同的义务和责任。

- **《中华人民共和国网络安全法》**

  《中华人民共和国网络安全法》第三章第一节第二十一条明确指出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：

  - 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
  - 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
  - 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
  - 采取数据分类、重要数据备份和加密等措施；
  - 法律、行政法规规定的其他义务。

除第二十一条的规定外，《中华人民共和国网络安全法》在第三章第二节第三十四条明确指出关键信息基础设施的运营者还应当履行下列安全保护义务：

- 设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；
- 定期对从业人员进行网络安全教育、技术培训和技能考核；
- 对重要系统和数据库进行容灾备份；
- 制定网络安全事件应急预案，并定期进行演练；
- 法律、行政法规规定的其他义务。

此外，在《中华人民共和国网络安全法》第三章第二节第三十五到第三十八条中针对一些特殊情况对运营者提出了要求：

- 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。
- 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。
- 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；法律、行政法规另有规定的，依照其规定。
- 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。

《中华人民共和国密码法》

《中华人民共和国密码法》第二十七条明确指出法律、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。

《关键信息基础设施安全保护条例》

《关键信息基础设施安全保护条例》第三章“运营者责任义务”第十二条到第二十一条对关基运营者需要承担的责任和义务做出了明确的规定。

第十二条　安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条　运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条　运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条　专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

- 建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；
- 组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；
- 按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；
- 认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；
- 组织网络安全教育、培训；
- 履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；
- 对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
- 按照规定报告网络安全事件和重要事项。

第十六条　运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条　运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条　关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条　运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

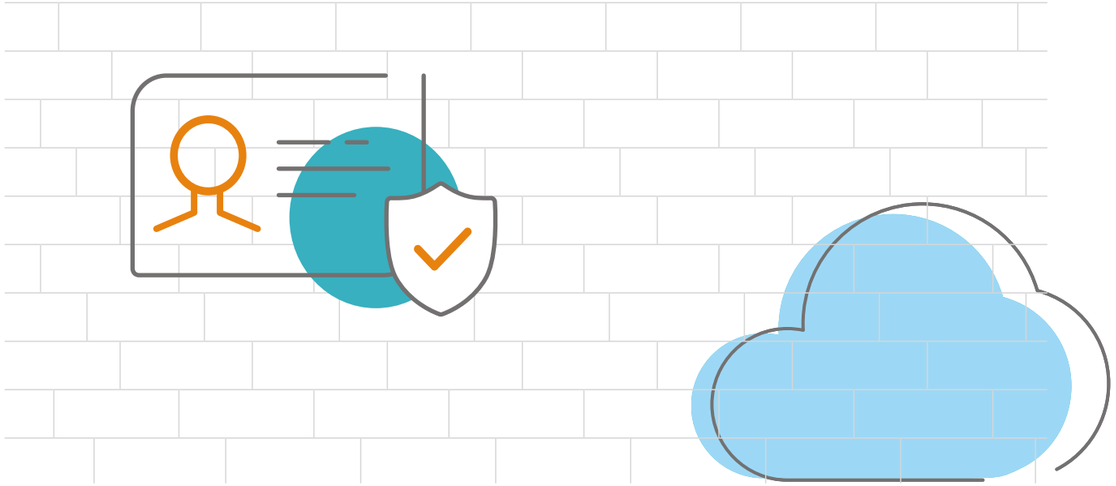
第二十条　运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

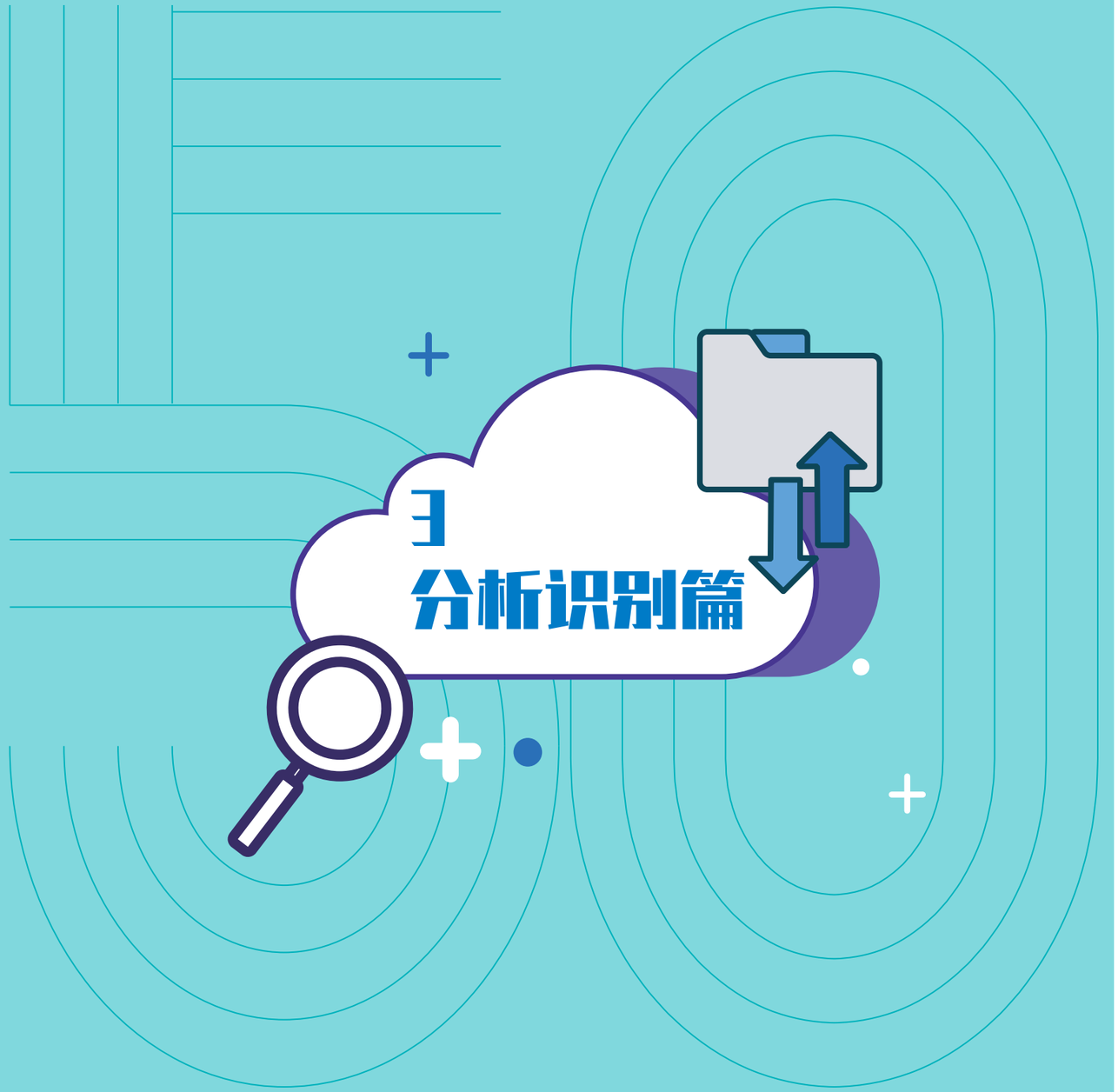
第二十一条　运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

09问 关键信息基础设施安全保护基本原则是什么？

关键信息基础设施的安全保护应遵循重点保护、整体防护、动态风控、协同参与的基本原则，建立网络安全综合防御体系。

- **重点保护**是指关键信息基础设施网络安全保护应首先符合网络安全等级保护政策及 GB/T 22239-2019 等标准相关要求，在此基础上加强关键信息基础设施关键业务的安全保护。
- **整体防护**是指基于关键信息基础设施承载的业务，对业务所涉及的多个网络和信息系统（含工业控制系统）等进行全面防护。
- **动态风控**是指以风险管理为指导思想，根据关键信息基础设施所面临的安全风险对其安全控制措施进行调整，以及时有效的防范应对安全风险。
- **协同参与**是指关键信息基础设施安全保护所涉及的利益相关方，共同参与关键信息基础设施的安全保护工作。





10问 关键信息基础设施范围有哪些?

《国家网络安全检查操作指南》指出关键信息基础设施范围包括:

- 网站类，如党政机关网站、企事业单位网站、新闻网站等;
- 平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台;
- 生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

《关键信息基础设施安全保护条例》指出关键信息基础设施保护范围包括: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、国防科技工业等重要行业和领域的。综上，可将关键信息基础设施保护范围归纳为:国家关键行业和领域内重要单位运行、管理的一旦遭到破坏、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和信息系统，涵盖网站类、平台类、生产业务类等相关的网络设施、信息系统及数据资产。

《关键信息基础设施安全保护条例》第二章第九条明确指出由保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。制定认定规则应当主要考虑下列因素:

- 网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度;
- 网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度;
- 对其他行业和领域的关联性影响。

11问 关键信息基础设施识别原则是什么?

关键信息基础设施边界识别是将关键业务持续、稳定运行所必需必备的网络设施、信息系统同关键信息基础设施运营者所运营的其他信息设施区分开来，CII 边界识别对 CIIP 明确保护对象、落实保护要求、实施控制措施具有重要意义，是开展 CIIP 的前提和基础。

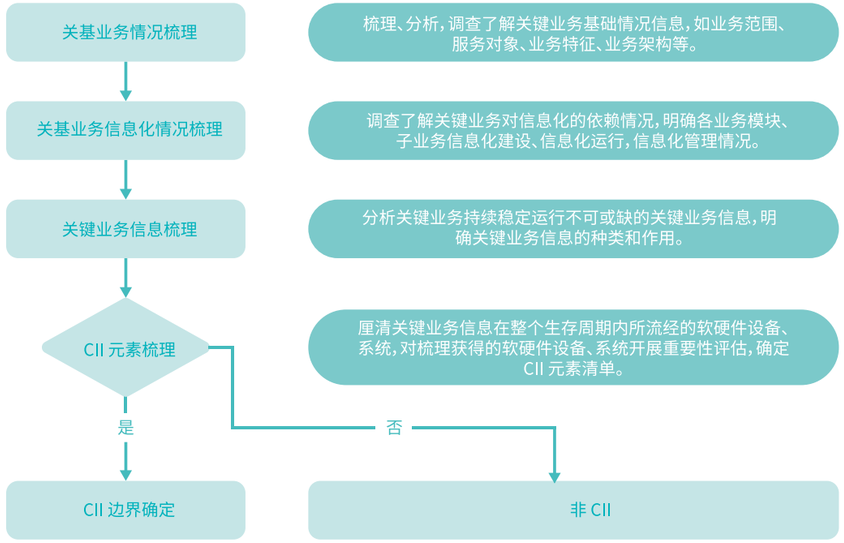
《信息安全技术 关键信息基础设施边界确定方法》（征求意见稿）描述了关键信息基础设施边界识别原则:

- **安全性原则:** 以保障关键业务安全为基本原则;
- **整体性原则:** 从保障整个关键业务安全的角度开展;

- **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；
- **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。

12问 关键信息基础设施识别流程是什么？

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》（征求意见稿）指出确定 CII 边界具体包括关键业务基础情况梳理、关键业务信息化情况梳理、关键业务信息梳理、CII 元素梳理和 CII 边界确定五个部分，如下所示。



关键信息基础设施边界识别的目的是为确定 CII 边界范围内网络设施、信息系统和数据资产，便于确定 CIIP 工作的保护对象。CII 边界识别流程如下：

- **关键业务识别：**梳理出 CII 运营者运行、管理的关键业务；
- **关键业务梳理：**摸清关键业务运行情况，包括业务范围、服务对象、业务特征及业务架构等；
- **关键业务信息化：**梳理支撑业务运行的网络拓扑结构、网络设施和信息系统部署情况；
- **关键业务信息：**梳理关键业务持续运行、稳定运行所必须的业务信息（BI）；
- **关键业务信息流：**梳理业务信息全生命周期的流动轨迹（BIF）以及 BIF 涉及的网络设施和信息系统部署详情，获得相应资产清单；
- **CII 元素梳理：**对上一阶段获得的资产清单进行归集处理，得到 CII 元素候选清单；
- **CII 元素清单：**分析 CII 元素候选清单内的资产受到破坏、丧失功能或者数据泄露对业务可用性、业务完整性和数据机密性所造成的影响，确定 CII 元素清单；
- **CII 边界确定：**根据 CII 元素梳理的清单，进一步厘清关键业务与 CII 元素之间的支撑作用、依赖关系和分布、部署情况，确定逻辑边界、物理边界、管理边界，该阶段是 CII 边界识别工作的最终目标。

13问 关键业务情况梳理包括哪些工作?

关键业务情况梳理是为了明确关键业务运行框架、组织结构、业务特征、业务范围等信息，具体工作内容及输出成果如下表。

序号	步骤名称	输出成果
1	基本信息梳理	● 关键业务信息化范围整体介绍
		● 各业务模块信息化情况介绍
		● 各子业务信息化情况介绍
		● 运营者网络安全管理部门介绍
		● 业务服务对象介绍
		● 业务服务区域介绍
		● 与其他业务的依赖性分析
2	业务特征梳理	○ 业务功能介绍
		○ 业务关键性分析
		○ 业务组织、管理架构介绍
3	业务架构梳理	● 业务运行架构介绍
		● 业务运行逻辑介绍
		● 各业务模块情况介绍
		● 各子业务情况介绍
4	业务范围描述	○ 业务整体范围概述
		○ 业务依赖性分析
		○ 业务完整性分析
5	基础情况描述	● 关键业务基础情况概述
		● 关键业务基本信息描述文件
		● 关键业务特征描述文件
		● 关键业务运行架构描述文件
		● 关键业务范围描述文件

14问 关键业务信息化梳理的定义及工作内容是什么?

通过关键业务信息化情况梳理，可以厘清关键业务信息化建设、信息化管理、信息化运维等信息，明确关键业务信息的种类和作用。具体工作内容及输出成果如下表。

步骤	名称	输出成果
1	信息化范围梳理	● 关键业务信息化范围整体介绍
		● 各业务模块信息化情况介绍
		● 各子业务信息化情况介绍
2	关键业务信息（CBI）梳理	○ CBI整体情况概述
		○ CBI类别介绍
		○ CBI功能介绍
		○ CBI关键性介绍
3	业务架构梳理	● 关键业务信息化整体情况概述
		● 关键业务信息化范围描述文件
		● CBI描述文件

15问 关键业务信息梳理的定义及工作内容是什么？

关键业务信息梳理是对关键业务持续、稳定运行不可或缺的信息进行整理，明确关键业务信息的类别、功能及其用途等。

以电力行业的电网运行稳态监视与控制系统为例，描述关键业务信息梳理的工作内容。首先将电网运行稳态监视与控制涉及的业务信息进行分类，分为监测信息、控制信息、辅助信息天气 / 水纹信息和共享信息四类，然后对各类信息进一步进行梳理和功能描述。

序号	业务信息类型	子类信息分类	功能
1	监测信息	电能量计量信息	用于监测实时用电量，为电力调度提供依据
		继电保护信息	实现对供电安全装置的运行状态、动作行为进行监测 在电网故障时则进行快速的故障分析
		相量测量信息和行波测距信息	用于对故障地点进行定位
2	控制信息	控制指令	用于开合刀闸、投切电容器
		发电计划指令	用于控制各发电机组的发电量
3	辅助信息天气、水纹信息	——	用于辅助下发控制指令
4	共享信息	——	用于各供电局实时掌握用电量 为制定行业发展规划提供依据

16问 关键信息基础设施元素梳理的定义及工作内容是什么？

关键信息基础设施元素梳理是分析关键业务信息（CBI）整个生存周期内的流动轨迹（CBIF），梳理 CBIF 上的网络设施、信息系统，确定 CII 候选元素。具体工作内容及输出成果如下表。

步骤	名称	输出成果
1	CBIF梳理	● CBIF梳理情况概述
		● 各CBIF介绍
		● 各CBIF网络设施、信息系统情况介绍
2	CII候选元素汇总去重	○ CII候选元素整体情况概述
		○ 网络设施介绍
		○ 信息系统介绍
		○ CII候选元素资产清单
3	CII候选元素描述	● CII候选元素整体情况概述
		● CBIF描述文件
		● CII候选元素清单描述文件
		● CII候选元素分布、部署详情

17问 关键信息基础设施边界如何确定?

将关键信息设施元素从 CII 运营者的其他信息基础设施组成元素中识别出来，是开展 CII 保护工作的第一步。基于关键信息基础设施的范围和识别原则，关键信息基础设施识别流程如下。

确定关键行业和领域

依据《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》等规定，关键行业和领域包括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、国防科技工业等；

确定核心业务

针对关键行业和领域的业务进行梳理、分析，基于业务规模、业务范围、业务影响及业务替代性等多个维度综合分析，确定出核心业务及其关联业务。

确定关键信息基础设施运营者

根据网络设施、信息系统和数字资产对本行业、本领域关键、核心业务的重要程度以及一旦遭到破坏可能带来的危害，指定本行业、本领域内的 CII 运营者；

确定边界

CII 运营者根据确定出的核心业务及其关联业务，对核心业务及其关联业务的信息化支撑元素进行枚举，并识别哪些网络设施、信息系统和数字资产是关键业务正常运营必不可少的，形成 CII 支撑元素列表。

信息报备

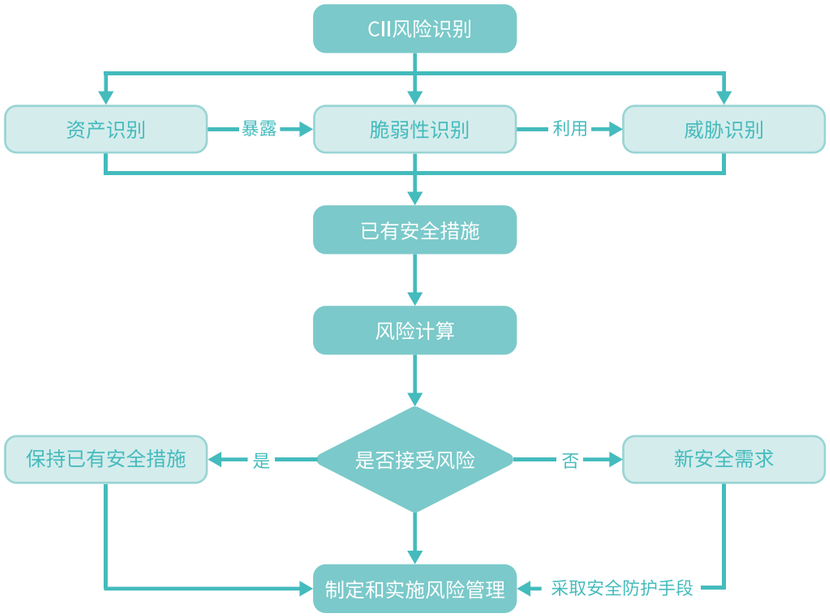
CII 运营者按照“功能”将纳入 CII 边界内的网络设施、信息系统和数字资产等 CII 支撑元素进行分类和分组，以便于管理和保护，并将分类分组后的数据表上报国家有关部门。

18问 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。具体工作内容如下表。

序号	识别类型	识别内容
1	资产识别	● 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； ● 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。



19问 关键信息基础设施风险评估的必要性是什么？

风险评估是 CIIP 识别环节对关键信息基础设施存在或潜在风险识别的主要方法，是关基分析识别环节一项主要工作内容。风险识别基于关键信息基础设施的威胁、脆弱性、已有安全控制措施及主要安全风险，确定风险处置的优先级。此外，风险评估是开展安全防护、检测评估、监测预警、技术对抗、事件处置相关环节工作的基础，是检测评估环节的核心内容。

20问 关键信息基础设施安全防护的要求有哪些?

工作内容	安全要求
网络安全等级保护制度	运营者应落实符合国家网络安全等级保护制度相关要求，开展定级、备案、相应等级的安全建设整改和等级测评工作。
安全管理制度	建立适合本组织的网络安全保护计划，明确关键信息基础设施安全保护工作的目标，从管理体系、技术体系、运营体系、保障体系等方面进行规划，加强机构、人员、经费、装备等资源保障，支撑关键信息基础设施安全保护工作。网络安全保护计划应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。
	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	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（以下简称“安全管理机构”），明确机构负责人及岗位，建立并实施网络安全考核及监督问责机制。
	将安全管理机构主要人员纳入本组织信息化决策体系。

工作内容		安全要求
安全管理人员		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审查和安全技能考核，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。
		要求安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到相关部门及人员。
		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，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。
		当安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化（例如取得非中国国籍）或必要时，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，收回与身份鉴别相关的软硬件设备，进行离职面谈并通知相关人员或角色。
		明确从业人员安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等。必要时，签订安全保密协议。
安全通信网络	互联安全	建立或完善不同网络安全等级系统、不同业务系统、不同区域、与其他运营者之间的安全互联策略。
		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网络安全等级系统、不同业务系统、不同区域中的一致性。
		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鉴别。
	边界防护	对不同网络安全等级系统、不同业务系统、不同区域、与其他运营者之间的互操作、数据交换和信息流向进行严格控制。
		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。

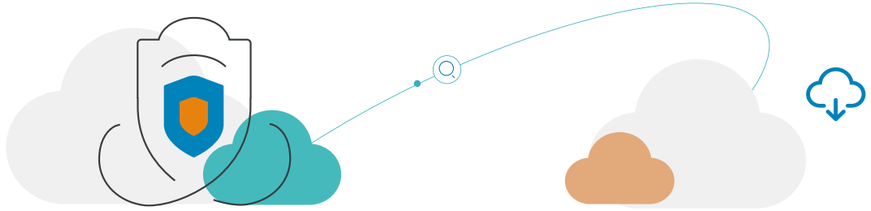
工作内容		安全要求
安全计算环境	鉴别与授权	运营者应明确重要业务操作或异常用户操作行为，并形成清单。
		对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别等方式。
		针对重要业务数据资源的操作，基于安全标记等技术实现访问控制。
	入侵防范	实现对新型网络攻击行为（如APT（高级可持续威胁，advanced persistent threat）攻击）的入侵防范。
		具备系统主动防护能力，及时识别并阻断入侵和病毒行为。
	自动化工具	运营者应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，应在经过验证后及时修补。
安全建设管理		运营者应在新建或改建、扩建关键信息基础设施时，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。
安全运维管理		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。
		要求维护人员签订安全保密协议。
		确保优先使用已在本组织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。
供应链安全保护		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。
		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。
		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。
		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。

工作内容	安全要求
供应链安全保护	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。
	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。
	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。
	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，应当通过国家网络安全审查。
	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相关部门报告。
	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。
数据安全防护	建立数据安全管理责任和评价考核制度，制定数据安全保护计划，实施数据安全技术防护，开展数据安全风险评估，制定数据安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。
	制定基于数据分类分级的数据安全保护策略，明确数据和个人信息保护的相应措施。
	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。
	严格控制重要数据的使用、加工、传输、提供和公开等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。
	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。
	业务数据安全性要求高的实现数据的异地实时备份。
	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。
	在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。

21问 关键信息基础设施安全控制措施分类有哪些?

在分析识别、安全防护、检测评估、监测预警、技术对抗、应急处置六个环节，关键信息基础设施运营者应采取的安全防护控制措施有下列几类。

- **分析识别：** 围绕关键信息基础设施承载的关键业务，识别关键信息基础设施的资产并分类，建立资产清单，标识重要系统和数据库；识别关键信息基础设施的威胁、脆弱性、已有安全措施，进行风险分析。
- **安全防护：** 根据已识别的安全风险，实施相应的安全控制措施，包括等级保护合规性要求、网络安全与信息化同步要求、网络安全责任制、个人信息和重要数据保护、数据境内存储与出境评估、人员与组织安全、人员安全审查、安全培训与考核、维护、供应链保护、重要系统和数据库的灾难备份等，确保关键信息基础设施的运行安全。
- **检测评估：** 通过建立健全关键信息基础设施检测评估制度，自行或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进行检测评估，并分析潜在安全风险可能引起的安全事件。
- **监测预警：** 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进行预警通报。
- **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。
- **应急处置：** 根据检测评估、监测预警环节发现的问题，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。



22问 关键信息基础设施运营者如何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》第十九条的规定，运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

同时，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	路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55万条
	交换机	整系统吞吐量(双向)≥30Tbps 整系统包转发率≥10Gpps
	服务器(机架式)	CPU数量≥8个 单CPU内核数≥14个 内存容量≥256GB
	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	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
	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
	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
	入侵检测系统(IDS)	满检速率≥15Gbps 最大并发连接数≥500万

	设备或产品类别	范围
网络安全专用产品	入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500万
	安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
	反垃圾邮件产品	连接处理速率（连接/秒）＞100 平均延迟时间＜100ms
	网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5万条/秒
	网络脆弱性扫描产品	最大并行扫描IP数量≥60个
	安全数据库系统	TPC-EtpsE（每秒可交易数量）≥4500个
	网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10级

列入该目录的设备或产品，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。关基运营者需优先选购信创类产品，以及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。

23问 关键信息基础设施相关个人信息和重要数据需出境，该如何处理？

《网络安全法》第三十一条规定，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。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；

《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。若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，则数据不得出境。

24问 关键信息基础设施安全防护能力等级如何划分？

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。

基安全防护能力等级	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。

25问 关键信息基础设施安全防护能力评价方法是什么？

关键信息基础设施安全防护能力评价包括能力域级别评价、等级保护测评和密码测评三部分。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密码测评。然后，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。

如：某关键信息基础设施满足 5 个能力域能力等级 1 的能力评价项，则该关键信息基础设施安全防护能力等级为 1。若某关键信息基础设施安全防护能力域能力等级没有达到能力等级 1，但是其检测评估能力达到能力等级 2 或 3，能够尽快发现风险并转移或缓解风险，能够使得关键信息基础设施不受损害，业务连续性不受影响，评估后关键信息基础设施安全防护能力为能力等级 1。

26问 关键信息基础设施安全防护能力评价实施流程？

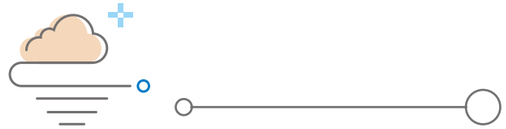
安全防护能力评价实施流程包括评价准备、方案编制、现场实施和分析评价四个阶段，与关基运营单位的沟通与洽谈会贯穿上述四个阶段。

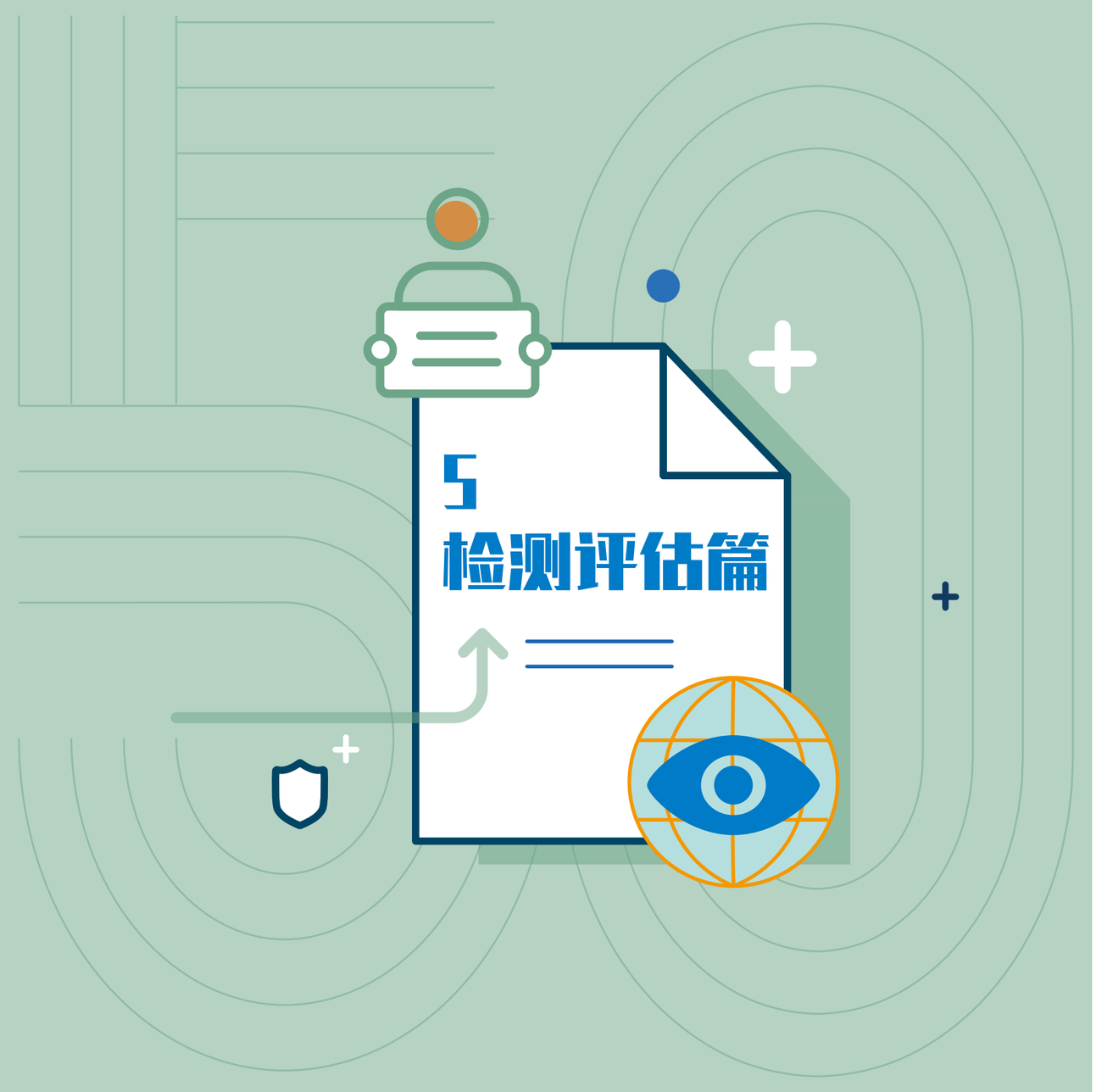
- **在评价准备阶段，**应明确被测对象、准备拟提供的证据、评价进度等相关信息，并组建评价实施团队。
- **在方案编制阶段，**应确定评价对象、评价内容和评价方法，确定评价边界和范围，了解关基运营单位的系统运行状况、安全机构、制度、人员等现状，并根据需要选择、调整、开发和优化测试用例，形成相应安全评价方案。
- **在现场实施阶段，**应根据评价操作方法进行审核，并根据需要进行测试。必要时，应补充相关证据，双方对现场实施结果进行确认。
- **在分析评价阶段，**应对现场实施阶段所形成的证据进行分析，给出对每项评价指标的判定结果和所处级别，得出每个能力域级别，从而判定关键信息基础设施安全防护能力级别。评价报告中应给出整体安全状况、每个能力域的安全状况、安全薄弱点、安全保护较好的方面等内容，便于关基运营单位全面了解自身安全防护状况和下一步提升方向。

27问 关键信息基础设施安全能力评价形式？

关键信息基础设施安全防护能力评价形式包括运营者自评和外部评价两种。

- **运营者自评**是由关基运营单位自行对其关键信息基础设施安全防护情况进行评价。通过自评，掌握其安全防护现状，并针对薄弱环节采取有效的改进措施，最终达到改善和提高关键信息基础设施安全防护能力的目的。
- **外部评价**是由网络安全服务机构等外部组织按照能力等级和评价方法对安全防护情况进行评价，最终达到为关基运营单位提供更客观、更详实、更专业的安全防护能力的目的。





28问 关键信息基础设施安全检测评估的要求有哪些?

关键信息基础设施安全防护能力评价形式包括运营者自评和外部评价两种。

- 在《网络安全法》中明确规定，关基运营单位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；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保护条例》第十五条条、第十七条条以及第二十六到二十八条，均对《网络安全法》中检测评估相关的规定内容进行了明确和丰富；《关键信息基础设施安全保护要求》（报批稿）在关键信息基础设施保护六个环节中的检测评估环节中，对检测评估制度以及检测评估方式和内容的相关要求进行了细化；《关键信息基础设施安全控制措施》（报批稿）中明确了检测评估的三种措施：自评估、安全检测和安全抽查。
- 《关键信息基础设施安全检查评估指南》（报批稿）给出了关键信息基础设施检查评估的方法、流程，定义了检查评估的主要内容。《关键信息基础设施安全保障指标体系》（报批稿）依据检查评估的结果对关键信息基础设施安全保障状况进行定量评价。
- 《关键信息基础设施安全防护能力评价方法》（征求意见稿）描述了关键信息基础设施安全防护能力评价模型，检测评估作为能力评价模型中的五个能力域之一，在这个标准中给出了检测评估具体的评价内容、评价操作方法和能力等级描述。

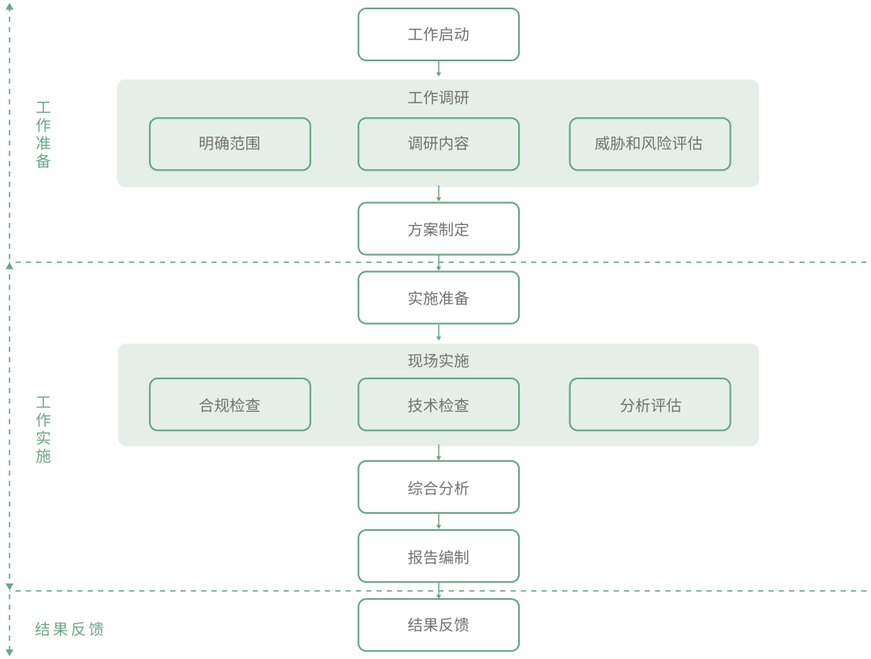
29问 关键信息基础设施安全检测评估内容包含什么?

《关键信息基础设施安全保护要求》（报批稿）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、攻防演练情况等，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。

30问 关键信息基础设施安全检查评估流程?

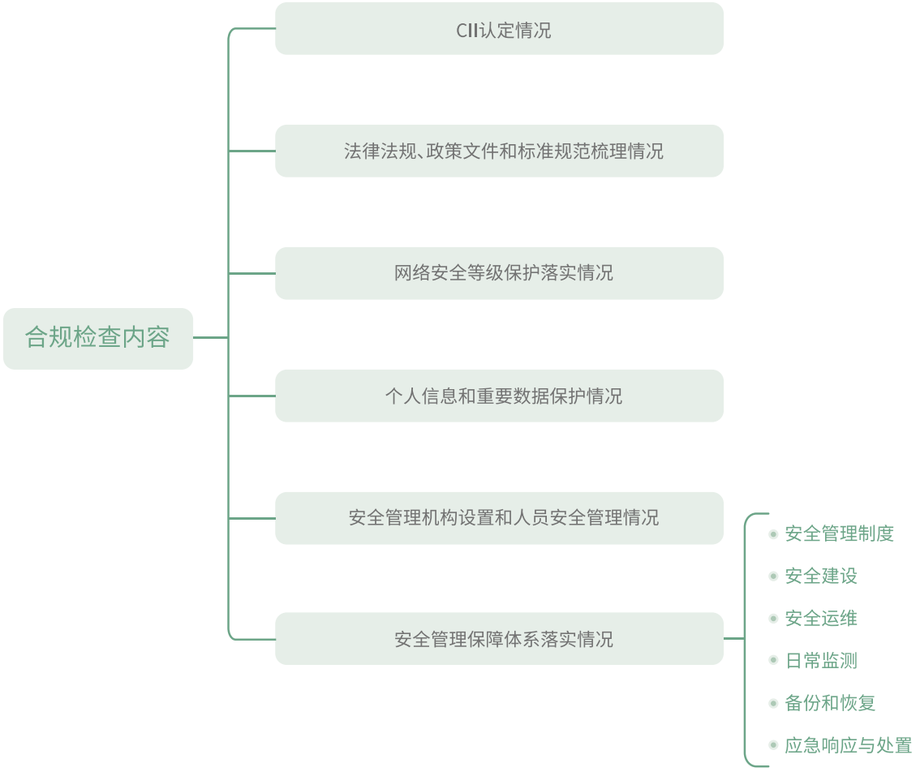
关键信息基础设施安全检查评估流程分为工作准备、工作实施和结果反馈三个阶段。

工作准备阶段是检查评估正式实施之前需要完成的准备工作，包括工作启动、工作调研和方案制定三个环节；工作实施阶段是检查评估方对被检查方开展正式的检查评估工作，包括实施准备、现场实施、综合分析和报告编制四个环节；结果反馈阶段主要是向检查评估委托方反馈检查结果和检查评估报告的过程。



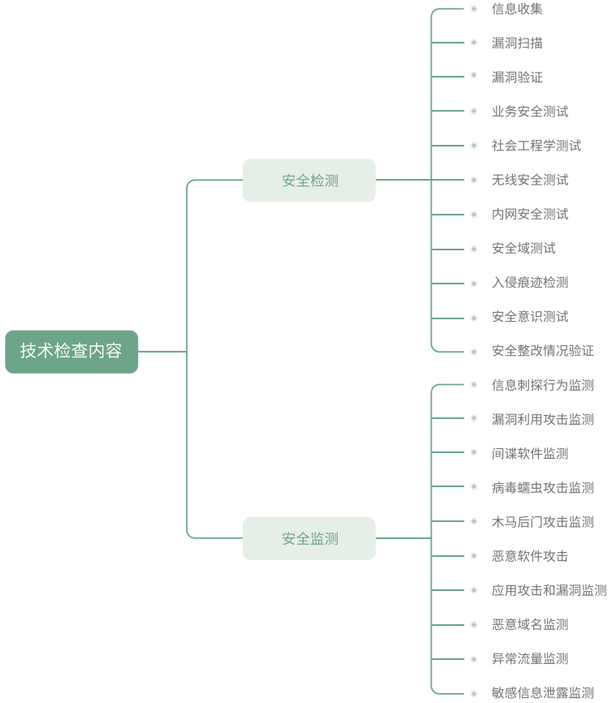
31问 关键信息基础设施合规检查的主要内容有哪些?

《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。其中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。其主要内容如下：



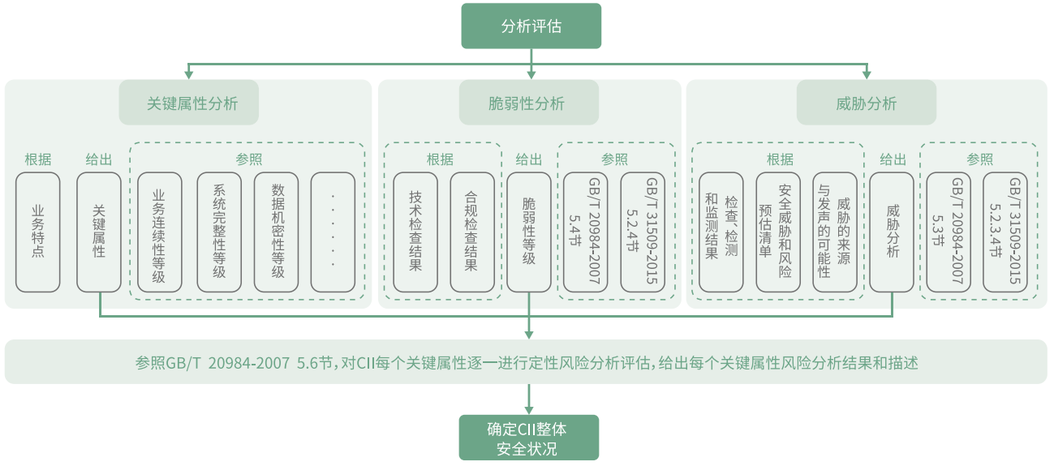
32问 关键信息基础设施技术检测的主要内容有哪些?

《关键信息基础设施安全检查评估指南》（报批稿）中将检查评估内容分为合规检查和技术检查两部分。其中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。其主要内容如下：



33问 关键信息基础设施如何进行分析评估?

《关键信息基础设施安全检查评估指南》中明确规定针对关键信息基础设施进行分析评估需要进行关键属性分析、脆弱性分析和威胁分析，再根据上述三种分析的结果综合确定 CII 整体安全状况。



此外，在《关键信息基础设施安全检查评估指南》中规定了六种应认定该 CII 的网络安全风险为高的情况：

- 合规检查部分有 5 项或以上明显不符的；
- CII 范围内的服务器（含其上运行的操作系统、数据库、中间件和后台管理软件）、运维管理终端（含其上运行的操作系统、远程运维管理软件）存在已公开的高危漏洞，或自查发现后未采取修补措施或制定修补计划的；
- CII 范围内存在被植入超过 1 个月的后门、木马，或重要管理账号密码被窃取 1 个月以上，导致 CII 范围内的服务器、运维管理终端、重要应用可被控，或个人信息和重要数据可被任意读取的；

- 对自查和主管监管部门检查发现的问题和提出的整改意见，有时限要求的，在时限要求内未完成的。无时限要求，在检查结束 1 个月后未制定整改计划的；
- 出现 2 起或以上未对发现或通报预警的网络安全高危漏洞、风险、威胁和事件等及时进行应对或处置，或未按要求反馈情况的；
- 出现 2 起或以上瞒报、漏洞、谎报网络安全事件的。

34问 关键信息基础设施检查评估结果如何输出？

根据合规检查、技术检查和分析评估得到的结果，输出正式的检查评估报告，报告内容应宜包括：

- **被检查方描述：**CII 运营单位基本情况、网络拓扑情况、核心资产情况、承载业务情况和安全防护现状；
- **合规检查结果说明：**合规检查项、检查结果及其详细描述；
- **技术检查结果说明：**技术检查内容、发现的主要问题（高风险安全漏洞和隐患、入侵情况等）及其详细描述；
- **安全风险分析：**通过对合规检查、技术检查中发现的安全问题及风险，汇总分析存在的安全隐患及造成的影响；
- **安全状况评价：**结合被检查方所承载业务重要性和威胁，综合评价 CII 的总体安全状况；
- **整改建议：**针对检查中发现的安全问题和风险，提出解决措施和整改建议，并对进一步提升被检查方、被检查行业网络安全水平提出建议。

35问 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；关键信息基础设施一定是等级测评和密评的评估对象；密评对象含关键信息基础设施、第三级等级保护对象和部分重要的信息系统。
- **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。

6 监测预警和事件处置篇

36问 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 关键信息基础设施安全保护要求》（报批稿）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，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。建立威胁情报和信息共享机制，落实相关措施，提高关键信息基础设施主动防御能力。

37问 关键信息基础设施安全对监测预警制度的要求是什么？

- 关基运营者要依据《信息安全技术 关键信息基础设施安全保护要求》（报批稿）开展关键信息基础设施安全监测预警工作，落实监测预警制度。
- 首先，要建立并落实常态化监测预警、快速响应机制。制定自身的监测预警和信息通报制度，确定网络安全预警分级准则，明确监测策略、监测内容和预警流程，对关键信息基础设施的网络安全风险进行监测预警；建立关键信息基础设施的预警信息响应处置程序，明确不同级别预警的报告、响应和处置流程；建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
- 其次，要关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及到的关键信息基础设施安全性进行研判分析，必要时发出预警；建立与外部组织之间、与其他运营者之间，以及运营者内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作机制，定期召开协调会议，共同研判、处置网络安全问题；建立网络安全信息共享渠道，例如建立与保护工作部门、同一关键信息基础设施的其他运营者、研究机构、网络安全服务机构、业界专家之间的沟通与合作机制，共享的信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。

38问 关键信息基础设施安全对事件管理制度的要求是什么?

- 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。
- 网络安全事件管理制度首先需要运营者具备网络安全事件的处理能力，建立网络安全事件管理制度，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等，制定应急预案等网络安全事件管理文档。事件处置制度应符合国家联防联控相关要求，及时将信息共享给相关方。
- 其次，要为网络安全事件处置提供相应资源，组织建立专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。
- 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、案件侦办等工作。

39问 关键信息基础设施安全对应急预案的要求是什么?

- 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。
- 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。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。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。
- 此外，在应急预案中包括非常规时期、遭受大规模攻击时等处置流程，要定期对网络安全应急预案进行评估修订，并持续改进。

40问 关键信息基础设施网络安全事件分类分级?

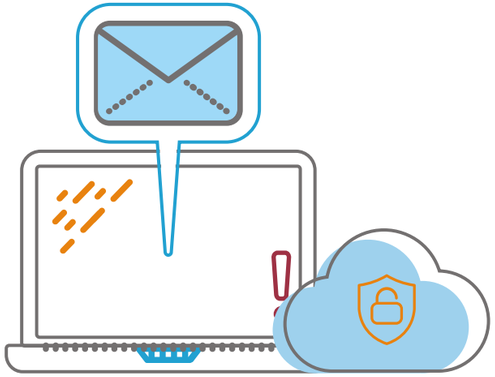
网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

- 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。
- 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。
- 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。
- 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。
- 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。
- 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。
- 其他事件是指不能归为以上分类的网络安全事件。

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

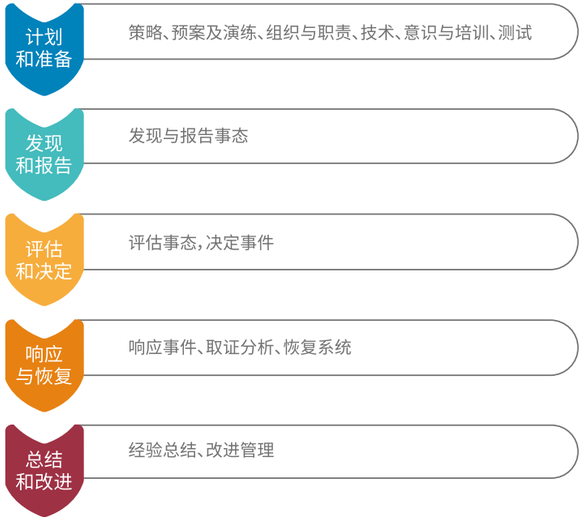
- 符合下列情形之一的，为特别重大网络安全事件：
  - 重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。
  - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。
  - 其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

- 符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：
  - 重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。
  - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。
  - 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。
- 符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：
  - 重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。
  - 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。
  - 其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。
- 除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。



41问 关键信息基础设施网络安全事件处置流程?

网络安全应急管理一般分为计划和准备、发现和报告、评估和决定、响应和恢复、总结和改进 5 个过程。



- 关基网络运营者在对安全事件进行处置时，首先应建立网络安全事件管理的相关制度，明确事件分类分级，制定安全应急预案和灾难恢复计划并开展应急演练，明确不同级别安全事件的应急处置流程，同时还要储备有力的安全应急支撑团队来有效处置安全事件。
- 当安全事件发生时，要及时通报可能受影响的内外部相关方，并向安全管理机构报备。按照事先的应急预案开展事件处置工作，尽快恢复关键业务和信息系统，进行取证分析并形成事件处理报告，将安全事件和处置结果通知内外部相关方及安全管理机构。
- 最后，针对安全事件和处置结果，需重新评估并更新现有安全策略。

42问 关键信息基础设施网络安全事件处置方法?

关键信息基础设施网络安全事件的处置方法如下:

- 按照事件处置流程、应急预案进行事件处理，恢复关键业务和信息系统到已知的状态。
- 在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的响应活动被适当记录，便于日后分析。
- 在进行取证分析时，应与业务连续性计划相协调。
- 在事件处理完成后，采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理。

  在恢复关键业务和信息系统后，对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键业务和信息系统遭受再次破坏、危害或故障。

  在进行事件处理活动时，协调组织内部多个部门和外部相关组织，以更好的对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

43问 关键信息基础设施网络安全应急目标及原则?

- **关键信息基础设施网络安全应急的目标有三个:**
  - 采取紧急措施，最快速度恢复业务到正常服务状态;
  - 调查安全事件发生的原因，避免同类安全事件再次发生;
  - 保存各种必要的证据，以方便日后追究责任。

- **网络安全应急遵循以下原则:**
  - 坚持统一领导、分级负责;
  - 坚持统一指挥、密切协同、快速反应、科学处置;
  - 坚持预防为主，预防与应急相结合;
  - 坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

44问 关键信息基础设施预警包括的内容?

- 在进行事件处理活动时，协调组织内部多个部门和外部相关组织，以更好的对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。
- 对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，按照相关部门要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、建议采取的应对措施等。
- 当内部预警信息发出之后，情况出现新的变化，运营者应向有关人员和组织及时补发最新内部预警信息。
- 能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案。获取的安全预警信息应按照规定通报给相关人员和相关部门。
- 采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程。

45问 如何建立并实施关键信息基础设施安全保护制度?

公网安〔2020〕1960 号《贯彻落实网络安全等保制度和关保制度的指导意见》明确指出在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。在 1960 号文中指出建立并实施关键信息基础设施安全保护制度。

深入贯彻实施国家网络安全等级保护制度	建立并实施关键信息基础设施安全保护制度	加强网络安全保护工作协作配合	加强网络安全工作各项保障
● 深化网络定级备案工作 ● 定期开展网络安全等级测评 ● 科学开展安全建设整改 ● 强化安全责任落实 ● 加强供应链安全管理 ● 落实密码安全防护要求	● 组织认定关键信息基础设施 ● 明确关键信息基础设施安全保护工作职能分工 ● 落实关键信息基础设施重点防护措施 ● 加强重要数据和个人信息保护 ● 强化核心岗位人员和产品服务的安全管理	● 加强网络安全立体化监测体系建设 ● 加强网络安全信息共享和通报预警 ● 加强网络安全应急处置机制建设 ● 加强网络安全事件处置和案件侦办 ● 加强网络安全问题隐患整改督办	● 加强组织领导 ● 加强经费政策保障 ● 加强考核评价 ● 加强技术攻关 ● 加强人才培养

46问 如何加强网络安全立体化监测体系建设?

全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置。要加强网络新技术研究和应用，研究绘制网络空间地理信息图谱（网络地图），实现挂图作战。行业主管部门、网络运营者要建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作，并与公安机关有关安全保卫平台对接，形成条块结合、纵横联通、协同联动的综合防控大格局。重点行业、网络运营者和公安机关要建设网络安全监控指挥中心，落实7x24 小时值班值守制度，建立常态化、实战化的网络安全工作机制。

47问 如何加强网络安全信息共享和通报预警?

行业主管部门、网络运营者要依托国家网络与信息安全信息通报机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。第三级以上网络运营者和关键信息基础设施运营者要开展网络安全监测预警和信息通报工作，及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。公安机关要加强网络与信息安全信息通报预警机制建设和力量建设，不断提高网络安全通报预警能力。

48问 如何加强网络安全应急处置机制建设?

行业主管部门、网络运营者要按照国家有关要求制定网络安全应急预案，加强网络安全应急力量建设和应急资源储备，与公安机关密切配合，建立网络安全事件报告制度和应急处置机制。关键信息基础设施运营者和第三级以上网络运营者应定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。行业主管部门、网络运营者应配合公安机关每年组织开展的网络安全监督检查、比武演习等工作，不断提升安全保护能力和对抗能力。