等级保护

01 等保基础

1.1 等级保护概念

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、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。
——《关于信息安全等级保护工作的实施意见》（公通字［2004］66号）

等保1.0指的是2007年的《信息安全等级保护管理办法》和2008年的《信息安全技术信息系统安全等级保护基本要求》。

2019年5月10日，等保2.0相关国家标准正式发布，同年12月1日开始实施，标志着我国正式进入等保2.0时代。

等保2.0将原来的标准《信息安全技术信息系统安全等级保护基本要求》改为《信息安全技术网络安全等级保护基本要求》，并对旧有内容进行调整。

本次课程的所有内容基于等保2.0进行讲解。

1.2 等级保护依据

等级保护工作开展的依据是《中华人民共和国网络安全法》：

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：
（一）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；
（二）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；
（三）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；
（四）采取数据分类、重要数据备份和加密等措施；
（五）法律、行政法规规定的其他义务。

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。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

伴随着《中华人民共和国网络安全法》的正式发布和实施，等级保护制度从一个规范性动作上升到了法律层面，确立了其在网络安全领域的基础、核心地位。简而言之，关键信息基础设施相关单位不按要求履行等保测评工作即是违法行为。

1.3 为什么要强制实行等级保护

国家强制推进实行等保制度的原因来自内、外两个部分：
内部因素：随着信息化建设工作的发展和推进，网络安全工作也需要同步推进，以此来保障国家重要行业和关键环节的安全系数。
外部因素：攻击技术不断发展和迭代，境外敌对势力的入侵形势日益严峻。

1.4 等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网(IoT)、工业控制系统和采用移动互联技术的系统等。

等级保护对象根据其在国家安全，经济建设，社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

1.5 安全保护等级

安全等级保护遵循分等级保护、分等级监管的原则，将信息系统按照重要性和危害性划分为五个安全保护等级，实行分等级保护：

等级	定义	安全保护能力
第一级：用户自主保护级	等级保护对象受到破坏后，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。	应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。
第二级：系统审计保护级	等级保护对象受到破坏后，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。	应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。
第三级：安全标记保护级	等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者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。	应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。
第四级：结构化保护级	等级保护对象受到破坏后，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。	应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击，严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。
第五级：访问验证保护级	等级保护对象受到破坏后，会对国家安全造成特别严重损害。	略

测评周期：
第一级：无要求。
第二级：一般每两年开展一次测评，时间上没有强制要求，部分行业有行业标准要求。
第三级：每年进行一次等级测评。
第四级：每半年进行一次等级测评。
第五级：应当依据特殊安全需求进行等级测评。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，不在《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》标准文件中，因此仅作了解即可。

1.6 等级保护角色&职责

等级保护对象实施网络安全等级保护过程中涉及的各类角色和职责如下：

1.6.1 等级保护管理部门

等级保护管理部门依照等级保护相关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

1.6.2 主管部门

负责依照国家网络安全等级保护的管理规范和技术标准，督促、检查和指导本行业、本部门或者本地区等级保护对象运营、使用单位的网络安全等级保护工作。

1.6.3 运营、使用单位

负责依照国家网络安全等级保护的管理规范和技术标准，确定其等级保护对象的安全保护等级，有主管部门的，应报其主管部门审核批准；根据已经确定的安全保护等级，到公安机关办理备案手续；按照国家网络安全等级保护管理规范和技术标准，进行等级保护对象安全保护的规划设计；使用符合国家有关规定，满足等级保护对象安全保护等级需求的信息技术产品和网络安全产品，开展安全建设或者改建工作；制定、落实各项安全管理制度，定期对等级保护对象的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的等级测评机构，定期进行等级测评；制定不同等级网络安全事件的响应、处置预案，对网络安全事件分等级进行应急处置。

1.6.4 网络安全服务机构

负责根据运营、使用单位的委托，依照国家网络安全等级保护的管理规范和技术标准，协助运营、使用单位完成等级保护的相关工作，包括确定其等级保护对象的安全保护等级、进行安全需求分析、安全总体规划、实施安全建设和安全改造、提供服务支撑平台等。

1.6.5 网络安全等级测评机构

负责根据运营、使用单位的委托或根据等级保护管理部门的授权，协助运营、使用单位或等级保护管理部门，按照国家网络安全等级保护的管理规范和技术标准，对已经完成等级保护建设的等级保护对象进行等级测评；对网络安全产品供应商提供的网络安全产品进行安全测评。

1.6.6 网络安全产品供应商

负责按照国家网络安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的网络安全产品，接受安全测评；按照等级保护相关要求销售网络安全产品并提供相关服务。

1.7 等级保护规定动作

首先需要说明的是，“等级保护规定动作”的概念并不等同于“等级保护实施基本流程”。完整的等保工作流程覆盖面非常广泛，需要所有角色各司其职，协同完成。不同角色所负责的工作内容当然也有所不同，因此在等保课程的学习过程中，“等级保护实施基本流程”能达到了解的程度即可，“等级保护规定动作”涉及到开展测评工作的必备技能，属于本次课程的重点。

《信息安全等级保护管理办法》（公通字[2007]43号）中将等级保护工作主要划分成了5个规定动作：定级、备案、安全建设或整改、等级测评和监督检查。

1.7.1 定级

信息系统运营、使用单位依据《信息安全等级保护管理办法》（公通字[2007]43号）和《网络安全等级保护定级指南》确定信息系统的安全保护等级。跨省或者全国统一联网运行的信息系统由主管部门统一确定安全保护等级。

1.7.2 备案

定级工作完成后，经过专家评审、行业主管部门审核后，报送所在地公安机关进行备案。

1.7.3 安全建设或整改

信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

1.7.4 等级测评

信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。

1.7.5 监督检查

信息系统运营、使用单位及其主管部门定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。受理备案的公安机关定期对备案系统的等级保护工作情况进行检查，若存在违规项，下发整改通知，必要时会采取规定处罚措施。

1.8 等级测评&差距分析

1.8.1 等级测评

等级保护测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对未涉及国家秘密的信息系统安全等级保护状况进行检测评估的活动。等级测评是标准符合性评判活动，即依据信息安全等级保护的国家标准或行业标准，按照特定方法对信息系统的安全保护能力进行科学公正的综合评判过程。

1.8.2 差距分析

等级保护服务安全建设机构及相关产品/服务厂商，依据网络安全等级保护的国家标准或行业标准，对信息系统进行全面的安全评估，了解信息系统的安全现状，找出现状与相应保护等级要求之间的差距，明确不满足项并提出对应的整改建议。

”差距分析“的概念并未在国标文件的等保工作流程中被提及，却是推进等保工作实践落地过程中必不可少的环节。

1.9 等保2.0变化解读

2019年5月13日，网络安全等级保护制度2.0标准正式发布，同年12月1日正式实施，标志着我国迈入等保2.0时代。相较于等保1.0，等保2.0标准在很多方面都做了调整，解读如下：

1.9.1 名称变化

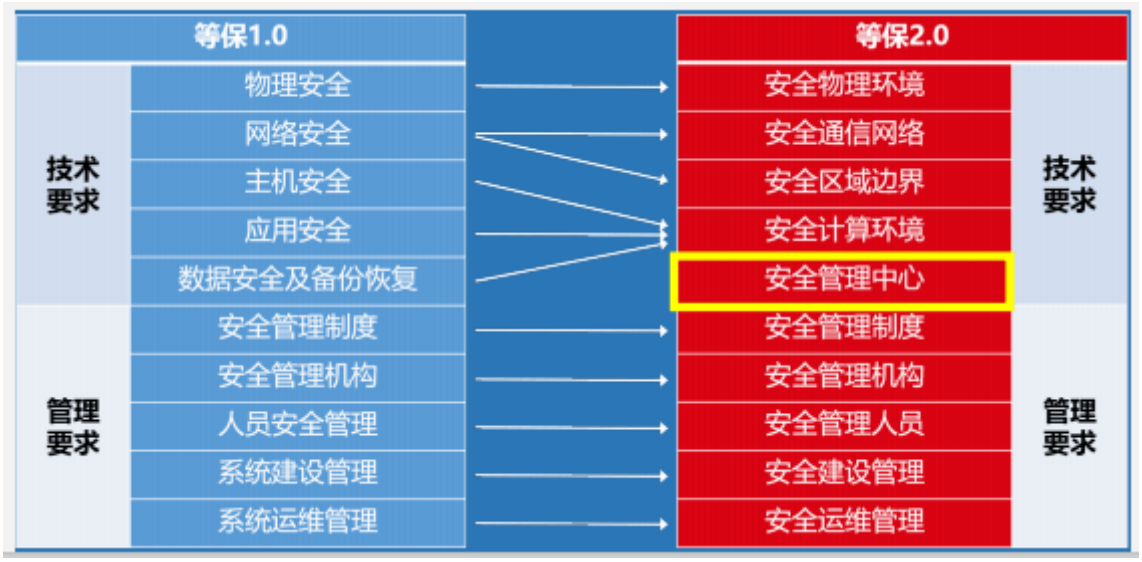
等保的标准名称由以前《信息系统安全等级保护基本要求》改为：《网络安全等级保护基本要求》，与《网络安全法》保持一致。

1.9.2 覆盖范围变化

等保1.0主要针对体制内的单位，参加测评的大部分都是一些计算机信息系统，到了等保2.0保护对象开始向全社会扩展，不在是以前单纯的计算机信息系统，现在的等保覆盖范围更广，更加严格。等保2.0在1.0的基础上，注重全方位主动防御、安全可信、动态感知和全面审计，实现了对传统信息系统、基础信息网络、云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象的全覆盖。

1.9.3 基本结构变化

1、技术要求中增加了安全管理中心，安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。
2、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、安全通信网络。



1.9.4 要求项变化

等保1.0只是要求信息系统安全等级保护基本要求，而等保2.0由一个单独的基本要求演变为“通用安全 + 安全扩展要求”两大要求，其中安全通用要求是不管等级保护对象形态如何都必须满足的要求，针对云计算、移动互联、物联网和工业控制系统提出了特殊要求，称为安全扩展要求。

2.0对基本要求项进行了优化精炼，通用安全要求中测评指标比之前减少了。

等保1.0	控制类	二级	三级	四级	等保2.0	控制类	二级	三级	四级
技术要求	物理安全	19	32	32	技术要求	安全物理环境	15	22	24
	网络安全	18	33	32		安全通信网络	4	8	11
	主机安全	19	32	36		安全区域边界	11	20	21
	应用安全	19	31	36		安全计算环境	23	34	36
	数据安全及备份恢复	4	8	11		安全管理中心	4	12	13
安全管理	安全管理制度	7	11	14	安全管理	安全管理制度	6	7	7
	安全管理机构	9	20	20		安全管理机构	9	14	15
	人员安全管理	11	16	18		安全管理人员	7	12	14
	安全建设管理	28	45	48		安全建设管理	25	34	35
	安全运维管理	42	62	70		安全运维管理	31	48	52
合计		176	290	317			135	211	228

安全通用要求变化对比表

1.9.5 测评结论变化

等保1.0测评结论：符合、基本符合、不符合（三个等级）；
等保2.0测评结论：优、良、中、差（四个等级）。其中测评结论“差”的判别依据是被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于70分。
注意：存在一个高风险项，即便分数是90分以上，评价也为”差“。

测评结论	等保1.0判断依据
符合	信息系统中未发现安全问题，等级测评结果中所有测评项得分均为5分。(100分)
基本符合	信息系统中存在安全问题，但不会导致信息系统面临高等级安全风险。(60分以上(含60分))
不符合	信息系统中存在安全问题，而且会导致信息系统面临高等级安全风险。(60分以下或具有高等级风险)

变化

测评结论	等保2.0判断依据
优	被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分90分以上(含90分)。
良	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险,且系统综合得分80分以上(含80分)。
中	被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险,且系统综合得分70分以上(含70分)。
差	被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于70分。

1.9.6 定级要求变化

对公民、法人和其他组织的合法权益的侵害程度为特别严重损害的时候，系统应该定为第三级。 *(定级内容在下一章会做详细解读，这里先了解一下即可)*

原标准

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

新标准

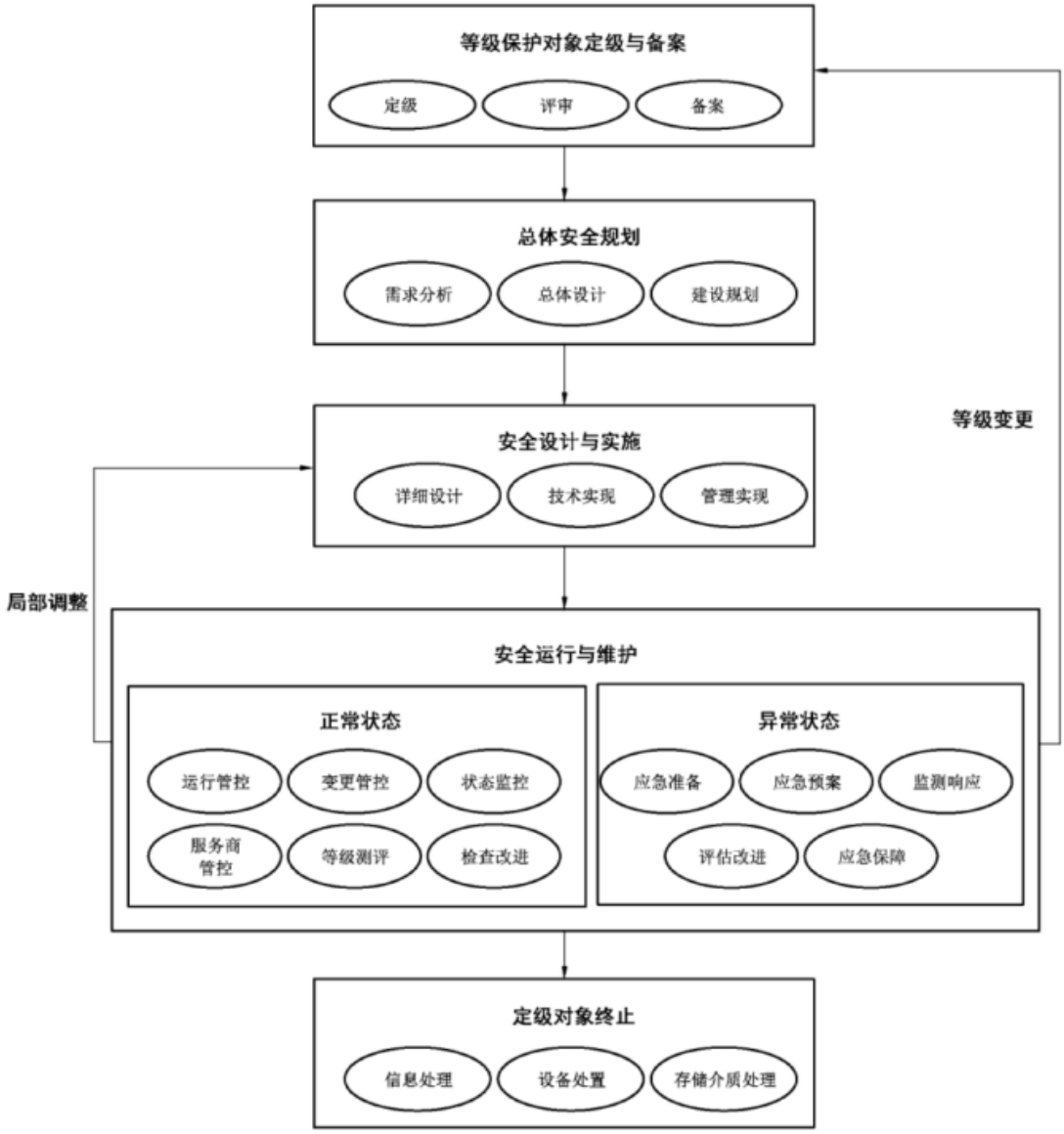
受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

02 等保要求

介绍等级保护的基本实施流程，解读定级要求和测评要求。

2.1 基本实施流程

对等级保护对象实施等级保护的基本流程包括等级保护对象定级与备案阶段、总体安全规划阶段、安全设计与实施阶段、安全运行与维护阶段和定级对象终止阶段。



在安全运行与维护阶段，等级保护对象因需求变化等原因导致局部调整，而其安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计，调整和实施安全措施，确保满足等级保护的要求。

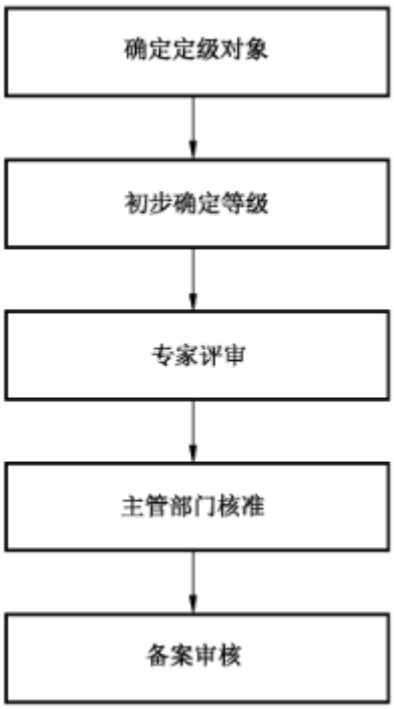
当等级保护对象发生重大变更导致安全保护等级变化时，应从安全运行与维护阶段进入等级保护对象定级与备案阶段，重新开始一轮网络安全等级保护的实施过程。

2.2 定级要求

2.2.1 定级准备工作

2.2.1.1 定级流程

等级保护对象定级工作的一般流程如下图所示：



2.2.1.2 定级范围

1、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。
2、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。
3、市（地）级以上党政机关的重要网站和办公信息系统。
4、涉及国家秘密的信息系统（简称“涉密信息系统”）。

2.2.1.3 定级原则

自主定级、专家评审、主管部门审批、公安机关审核监督。

2.2.2 确定定级对象

2.2.2.1 信息系统

1、定级对象的基本特征
作为定级对象的信息系统应具有如下基本特征：
a）具有确定的主要安全责任主体；
b）承载相对独立的业务应用；
c）包含相互关联的多个资源。

> 注1：主要安全责任主体包括但不限于企业，机关和事业单位等法人，以及不具备法人资格的社会团体等其他组织。
> 注2：避免将某个单一的系统组件，如服务器、终端或网络设备作为定级对象。

在确定定级对象时，云计算平台/系统、物联网、工业控制系统以及采用移动互联技术的系统在满足以上基本特征的基础上，还需分别遵循下述的相关要求。

2、云计算平台/系统
在云计算环境中，云服务客户侧的等级保护对象和云服务商侧的云计算平台/系统需分别作为单独的定级对象定级，并根据不同服务模式将云计算平台/系统划分为不同的定级对象。
对于大型云计算平台，宜将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

3、物联网
物联网主要包括感知、网络传输和处理应用等特征要素，需将以上要素作为一个整体对象定级，各要素不单独定级。

4、工业控制系统
工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行，现场控制和过程控制等要素需作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级。
对于大型工业控制系统，可根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

5、采用移动互联技术的系统
采用移动互联技术的系统主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

2.2.2.2 通信网络设施

对于电信网、广播电视传输网等通信网络设施，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。
跨省的行业或单位的专用通信网可作为一个整体对象定级，或分区域划分为若干个定级对象。

2.2.2.3 数据资源

数据资源可独立定级。
当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体对象定级；当安全责任主体不同时，大数据应独立定级。

2.2.3 初步确定等级

2.2.3.1 定级要素（就高不就低）

等级保护的定级要素包括以下两个要素：受侵害的客体、对客体的侵害程度

定级要素一：受侵害的客体
a）公民、法人和其他组织的合法权益
b）社会秩序、公共利益
c）国家安全

> 侵害国家安全的事项包括以下方面：
> ——影响国家政权稳固和领土主权、海洋权益完整；
> ——影响国家统一、民族团结和社会稳定；
> ——影响国家社会主义市场经济秩序和文化实力；
> ——其他影响国家安全的事项。
>
> 侵害社会秩序的事项包括以下方面：
> ——影响国家机关、企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序；
> ——影响公共场所的活动秩序、公共交通秩序；
> ——影响人民群众的生活秩序；
> ——其他影响社会秩序的事项。
>
> 侵害公共利益的事项包括以下方面：
> ——影响社会成员使用公共设施；
> ——影响社会成员获取公开数据资源；
> ——影响社会成员接受公共服务等方面；
> ——其他影响公共利益的事项。

侵害公民、法人和其他组织的合法权益是指受法律保护的公民、法人和其他组织所享有的社会权利和利益等受到损害。

确定受侵害的客体时，首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公共利益，最后判断是否侵害公民、法人和其他组织的合法权益。

定级要素二：对客体的侵害程度
a）一般损害
b）严重损害
c）特别严重损害

在针对不同的受侵害客体进行侵害程度的判断时，参照以下不同的判别基准：
--如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；
--如果受侵害客体是社会秩序、公共利益或国家安全，则以整个行业或国家的总体利益作为判断侵害程度的基准。

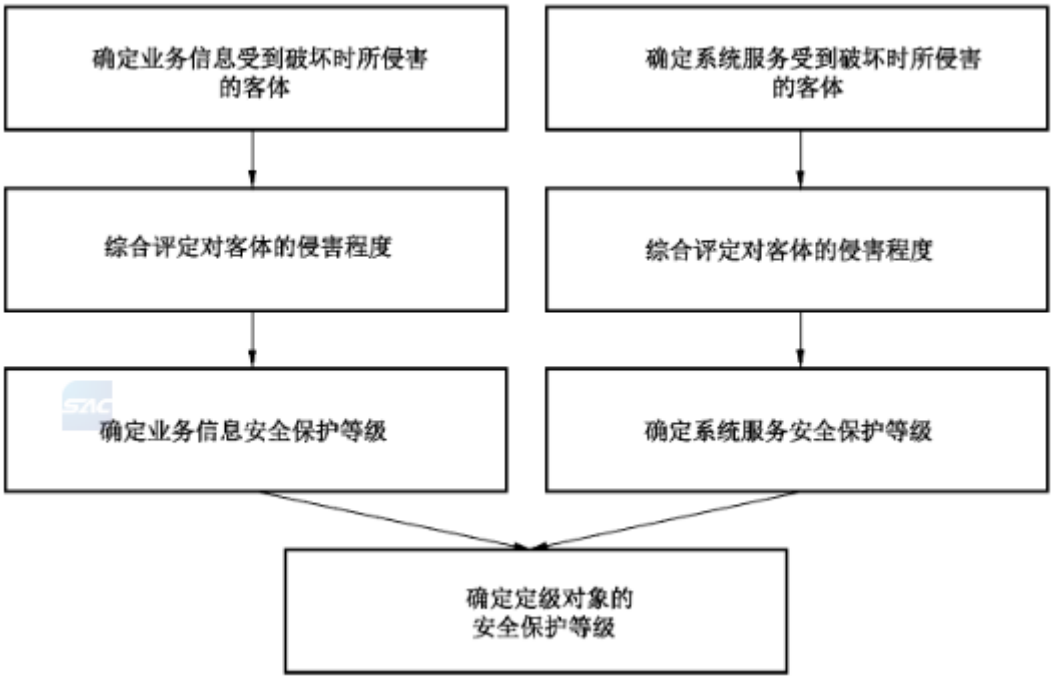
不同侵害后果的三种侵害程度描述如下：
--一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害；
--严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较高损害；
--特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常高损害。

定级要素与安全保护等级的关系：

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

2.2.3.2 定级方法

定级对象的安全主要包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同。因此，安全保护等级由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的定级对象安全保护等级称为业务信息安全保护等级，从系统服务安全角度反映的定级对象安全保护等级称为系统服务安全保护等级。
定级方法流程示意图如下所示：



简单理解，业务信息泛指应用，系统服务泛指基础架构。
业务信息安全：确保定级对象中信息的保密性、完整性和可用性等。
系统服务安全：确保定级对象可以及时、有效地提供服务，以完成预定的业务目标。

业务信息安全被破坏：可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。
系统服务安全被破坏：可以从定级对象服务覆盖的区域范围、用户人数或业务量等不同方面确定。

2.2.3.3 综合判定等级

根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据下表可得到业务信息安全保护等级：

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据下表可得到系统服务安全保护等级：

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级对象的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定：
业务信息安全保护等级（S）
系统服务安全保护等级（A）
通用安全保护等级（G）＝MAX（S，A）

安全等级	定级组合的结果
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4
第五级	S1A5G5，S2A5G5，S3A5G5，S4A5G5，S5A4G5，S5A3G5，S5A2G5，S5A1G5

2.2.3.4 定级参考

第一级信息系统：一般适用于小型私营、个体企业、中小学，乡镇所属信息系统，县级单位中一般的信息系统。
第二级信息系统：一般适用于县级某些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。
第三级信息系统：一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息以及这类信息以及这类信息在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省连接的网络系统等。
第四级信息系统：一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统。
第五级信息系统：一般适用于国家重要领域、重要部门中的极端重要系统。

2.2.4 专家评审&主管部门核准

对定级结果的合理性进行评审，并出具专家评审意见。有行业主管（监管）部门的，还需将定级结果报请行业主管（监管）部门核准，并出具核准意见。
对于通信网络设施、云计算平台 / 系统等定级对象，需根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上不低于其承载的等级保护对象的安全保护等级。
对于数据资源，综合考虑其规模、价值等因素，及其遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度确定其安全保护等级。涉及大量公民个人信息以及为公民提供公共服务的大数据平台 / 系统，原则上其安全保护等级不低于第三级。

上述工作全部完成后，输出《安全保护等级定级报告》。
报告模板详见《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）

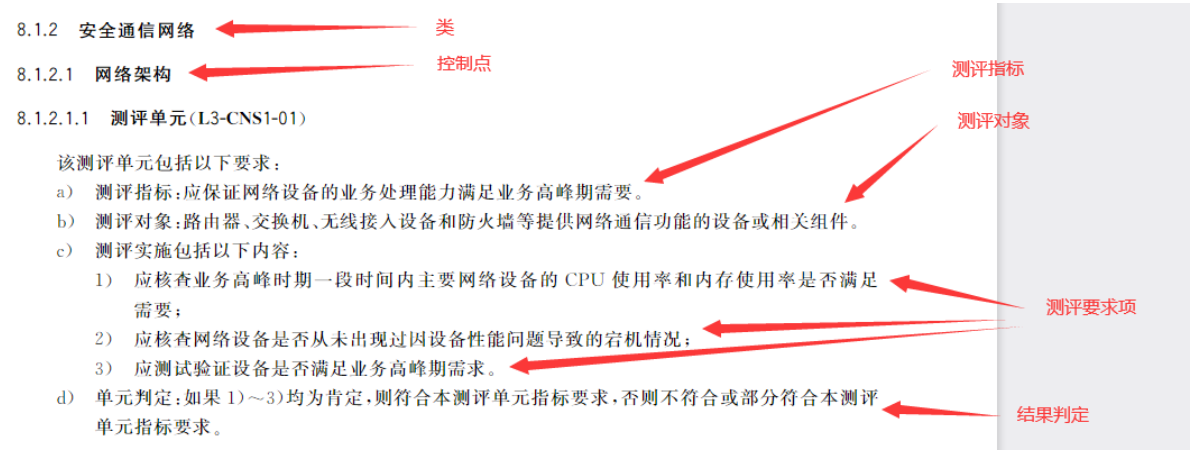
2.2.5 备案审核

网络运营者按照相关管理规定，将定级结果提交公安机关进行备案审核。审核不通过，其网络运营者需组织重新定级；审核通过后最终确定定级对象的安全保护等级。

2.3 测评要求

2.3.1 测评概述

等级保护对象整体测评应从安全控制点、安全控制点间和区域间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制点间测评和区域间测评，测评方法包括访谈、文档审查、实地察看、配置核查、工具测试等。



a）安全控制点测评：对单个控制点中所有要求项的符合程度进行分析和判定。如果该安全控制点下的所有要求项为符合，则该安全控制点符合，否则为不符合、部分符合或者不适用。

b）安全控制点间安全测评：对同一区域同一类内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。
在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行安全控制点间测评，应分析在同一类内，是否存在其他安全控制点对该安全控制点具有补充作用（如物理访问控制和防盗窃、身份鉴别和访问控制等）。同时，分析是否存在其他的安全措施或技术与该要求项具有相似的安全功能。
根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则对该测评指标的测评结果予以调整。

c）区域间安全测评：对互连互通的不同区域之间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。
在单项测评完成后，如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合，应进行区域间安全测评，重点分析等级保护对象中访问控制路径（如不同功能区域间的数据流流向和控制方式等）是否存在区域间的相互补充作用。
根据测评分析结果，综合判断该安全控制点所对应的系统安全保护能力是否缺失，如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，则对该测评指标的测评结果予以调整。

2.3.2 要求解读

为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护测评要求分为安全通用要求和安全扩展要求：
a）安全通用要求：针对共性化保护需求提出，等级保护对象无论以何种形式出现，应根据安全保护等级实现相应级别的安全通用要求，包括10个部分：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。
b）安全扩展要求：针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求，包括云计算扩展要求、物联网扩展要求、移动互联网扩展要求、工业控制系统扩展要求。

在定级工作中，一旦涉及到国家安全，至少定为第三级，因此三级系统是一个"分水岭"，也是在实际工作中最常遇到的系统。因此，下述内容基于三级要求项进行解读。

2.3.2.1 安全物理环境

控制点	测评指标	测评对象	测评实施
8.1.1.1 物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内	记录类文档和机房	1) 应核查所在建筑物是否具有建筑物抗震设防审批文档； 2) 应核查机房是否不存在雨水渗漏； 3) 应核查门窗是否不存在因风导致的尘土严重； 4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。
	b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施	机房	1) 应核查是否不位于所在建筑物的顶层或地下室，如果否，则核查是否采取了防水和防潮措施。
8.1.1.2 物理访问控制	a)机房出入口应配量电子门禁系统，控制、鉴别和记录进入的人员	机房电子门禁系统	1) 应核查出入口是否配置电子门禁系统； 2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。
8.1.1.3 防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标识	机房设备或主要部件	1) 应核查机房内设备或主要部件是否固定； 2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标记。
	b)应将通信线缆铺设在隐蔽安全处	机房通信线缆	1)应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。
	c)应设置机房防盗报警系统或设置有专人值守的视频监控系统	机房防盗报警系统或视频监控系统	1) 应核查机房内是否配置防盗报警系统或专人值守的视频监控系统； 2) 应核查防盗报警系统或视频监控系统是否启用。
8.1.1.4 防雷击	a)应将各类机柜、设施和设备等通过接地系统安全接地	机房	1)应核查机房内机柜、设施和设备等是否进行接地处理。
	b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等	机房防雷设施	1) 应核查机房内是否设置防感应雷措施； 2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。
8.1.1.5 防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火	机房防火设施	1) 应核查机房内是否设置火灾自动消防系统； 2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。

控制点	测评指标	测评对象	测评实施
	b)机房及相关的工作房间和辅助房应采用具有耐灭等级的建筑材料	机房验收类文档	1)应核查机房验收文档是否明确相关建筑材料的耐火等级。
	c)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施	机房管理员和机房	1) 应访谈机房管理员是否进行了区域划分； 2) 应核查各区域间是否采取了防火措施进行隔离。
8.1.1.6 防水和防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透	机房	1)应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施。
	b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透	机房	1) 应核查机房内是否采取了防止水蒸气结露的措施； 2) 应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。
	c)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警	机房防水检测设施	1) 应核查机房内是否安装了对水敏感的检测装置；2) 应核查防水检测和报警装置是否启用。
8.1.1.7 防静电	a)应采用防静电地板或地面并采用必要的接地防静电措施	机房	1) 应核查机房内是否安装了防静电地板或地面； 2) 应核查机房内是否采用了接地防静电措施。
	b)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等	机房	1)应核查机房内是否配备了防静电设备。
8.1.1.8 温湿度控制	a)应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内	机房温湿度调节设施	1) 应核查机房内是否配备了专用空调； 2) 应核查机房内温湿度是否在设备运行所允许的范围之内。
8.1.1.9 电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备	机房供电设施	1)应核查供电线路上是否配置了稳压器和过电压防护设备。
	b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求	机房备用供电设施	1) 应核查是否配备UPS等后备电源系统。 2) 应核查UPS等后备电源系统是否满足设备在断电情况下的正常运行要求。

控制点	测评指标	测评对象	测评实施
	c)应设置冗余或并行的电力电缆线路为计算机系统供电	机房	1)应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。
8.1.1.10 电磁防护	a)电源线和通信线缆应隔离铺设，避免互相干扰	机房线缆	1)应核查机房内电源线缆和通信线缆是否隔离铺设。
	b)应对关键设备实施电磁屏蔽	机房关键设备	1)应核查机房内是否为关键设备配备了电磁屏蔽装置。

2.3.2.2 安全通信网络

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

控制点	测评指标	测评对象	测评实施
8.1.2.1 网络架构	a)应保证网络设备的业务处理能力满足业务高峰期需要	路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件	1) 应核查业务高峰时期一段时间内主要网络设备的CPU使用率和内存使用率是否满足需要； 2) 应核查网络设备是否从未出现过因设备性能问题导致的宕机情况； 3)应测试验证设备是否满足业务高峰期需求
	b)应保证网络各个部分的带宽满足业务高峰期需要	综合网管系统等	1)应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量； 2)应测试验证网络带宽是否满足业务高峰期需求。
	c)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址	路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件	1) 应核查是否依据重要性、部门等因素划分不同的网络区域； 2) 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。
	d)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段	网络拓扑	1) 应核查网络拓扑图是否与实际网络运行环境一致； 2) 应核查重要网络区域是否未部署在网络边界处； 3) 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL)等。
	e)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性	网络管理员和网络拓扑	1)应核查系统是否有关键网络设备、安全设备和关键计算设备的硬件冗余（主备或双活等)和通信线路冗余。

控制点	测评指标	测评对象	测评实施
8.1.2.2 通信传输	a)应采用校验技术或密码技术保证通信过程中数据的完整性	提供核验技术或密码技术功能的设备或组件	1) 应核查是否在数据传输过程中使用校验码技术或密码技术来保证其完整性；2) 应测试验证密码技术设备或组件能否保证通信过程中数据的完整性。
	b)应采用密码技术保证通信过程中数据的保密性	提供密码技术功能的设备或组件	1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施； 2) 应测试验证在通信过程中是否对数据进行加密。
8.1.2.3 可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	提供可信验证的设备或组件、提供集中审计功能的系统	1) 应核查是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证； 2) 应核查是否在应用程序的关键执行环节进行动态可信验证； 3) 应测试验证当检测到通信设备的可信性受到破坏后是否进行报警； 4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

2.3.2.3 安全区域边界

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

控制点	测评指标	测评对象	测评实施
8.1.3.1 边界防护	a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件	1) 应核查在网络边界处是否部署访问控制设备； 2) 应核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口配置并启用了安全策略； 3) 应采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等)核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信。
	b)应能够对非授权设备私自联到内部网络的行为进行检查或限制	终端管理系统或相关设备	1) 应核查是否采用技术措施防止非授权设备接入内部网络； 2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
	c)应能够对内部用户非授权联到外部网络的行为进行检查或限制	终端管理系统或相关设备	1)应核查是否采用技术措施防止内部用户存在非法外联行为。
	d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络	网络拓扑和无线网络设备	1) 应核查无线网络的部署方式，是否单独组网后再连接到有线网络； 2) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。
8.1.3.2 访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件	1) 应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略； 2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
	b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件	1) 应核查是否不存在多余或无效的访问控制策略； 2) 应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。

控制点	测评指标	测评对象	测评实施
	c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件	1)应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数； 2)应测试验证访问控制策略中设定的相关配置参数是否有效。
	d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力	网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件	1)应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力； 2)应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。
	e)应对进出网络的数据流实现基于应用协议和应用内容的访问控制	第二代防火墙等提供应用层访问控制功能的设备或相关组件	1) 应核查是否部署访问控制设备并启用访问控制策略； 2) 应测试验证设备访问控制策略是否能够对进出网络的数据流实现基于应用协议和应用内容的访问控制。
8.1.3.3 入侵防范	a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1) 应核查相关系统或组件是否能够检测从外部发起的网络攻击行为； 2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本； 3) 应核查相关系统或组件配置信息或安全策略是否能够覆盖网络所有关键节点。 4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。

控制点	测评指标	测评对象	测评实施
	b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1) 应核查相关系统或组件是否能够检测到从内部发起的网络攻击行为； 2) 应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本； 3) 应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点。 4) 应测试验证相关系统或组件的配置信息或安全策略是否有效。
	c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析	抗APT攻击系统、网络回溯系统和威胁情报检测系统或相关组件	1) 应核查是否部署相关系统或组件对新型网络攻击进行检测和分析； 2) 应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。
	d)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1) 应核查相关系统或组件的记录是否包括攻击源IP、攻击类型、攻击目的、攻击时间等相关内容； 2) 应测试验证相关系统或组件的报警策略是否有效。
8.1.3.4 恶意代码和垃圾邮件防范	a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	防病毒网关和UTM等提供防恶意代码功能的系统或相关组件	1) 应核查在关键网络节点处是否部署防恶意代码功能的系统或相关组件； 2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新； 3) 应测试验证相关系统或组件的安全策略是否有效。
	b)应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新	防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件	1) 应核查在关键网络节点处是否部署了防垃圾邮件产品等技术措施； 2) 应核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新； 3) 应测试验证相关系统或组件的安全策略是否有效。

控制点	测评指标	测评对象	测评实施
8.1.3.5 安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	综合安全审计系统等	1) 应核查是否部署了综合安全审计系统或类似功能的系统平台； 2) 应核查安全审计范围是否覆盖到每个用户； 3) 应核查是否对重要的用户行为和重要安全事件进行了审计。
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	综合安全审计系统等	1)应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	综合安全审计系统等	1) 应核查是否采取了技术措施对审计记录进行保护； 2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
	d)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	上网行为管理系统或综合安全审计系统	应核查是否对远程访问用户及互联网访问用户行为单独进行审计分析。
8.1.3.6 可信验证	a)可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	提供可信验证的设备或组件、提供集中审计功能的系统	1) 应核查是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证； 2) 应核查是否在应用程序的关键执行环节进行动态可信验证； 3) 应测试验证当检测到边界设备的可信性受到破坏后是否进行报警； 4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

2.3.2.4 安全计算环境

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

控制点	测评指标	测评对象	测评实施
8.1.4.1 身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查用户在登录时是否采用了身份鉴别措施； 2) 应核查用户列表确认用户身份标识是否具有唯一性； 3) 应核查用户配置信息或测试验证是否不存在空口令用户； 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否配置并启用了登录失败处理功能； 2) 应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等； 3) 应核查是否配置并启用了登录连接超时及自动退出功能。

控制点	测评指标	测评对象	测评实施
	c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别； 2)应核查其中一种鉴别技术是否使用密码技术来实现。

控制点	测评指标	测评对象	测评实施
8.1.4.2 访问控制	a)应对登录的用户分配账户和权限	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应检查是否为用户分配了账户和权限及相关设置情况； 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。
	b)应重命名或删除默认账户，修改默认账户的默认口令	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否已经重命名默认账户或默认账户已被删除； 2) 应核查是否已修改默认账户的默认口令。

控制点	测评指标	测评对象	测评实施
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应；2) 应测试验证多余的、过期的账户是否被删除或停用。
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否进行角色划分； 2) 应核查管理用户的权限是否已进行分离； 3) 应核查管理用户权限是否为其工作任务所需的最小权限。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否由授权主体（如管理用户）负责配置访问控制策略； 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则； 3) 应测试验证用户是否有可越权访问情形。

控制点	测评指标	测评对象	测评实施
	f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级。
	g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否对主体、客体设置了安全标记； 2) 应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。
8.1.4.3 安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否开启了安全审计功能； 2) 应核查安全审计范围是否覆盖到每个用户； 3) 应核查是否对重要的用户行为和重要安全事件进行审计。

控制点	测评指标	测评对象	测评实施
	b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查是否采取了保护措施对审计记录进行保护； 2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

控制点	测评指标	测评对象	测评实施
	d)应对审计进程进行保护，防止未经授权的中断	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否受到保护。
8.1.4.4 入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等	1) 应核查是否遵循最小安装原则； 2) 应核查是否未安装非必要的组件和应用程序。
	b)应关闭不需要的系统服务、默认共享和高危端口	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等	1) 应核查是否关闭了非必要的系统服务和默认共享； 2) 应核查是否不存在非必要的高危端口。

控制点	测评指标	测评对象	测评实施
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等	1)应核查配置文件是否对终端接入范围进行限制。
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求	业务应用系统、中间件和系统管理软件及系统设计文档等	1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块； 2) 应测试验证是否对人机接口或通信接口输入的内容进行有效性检验。
	e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件等	1) 应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2) 应核查是否在经过充分测试评估后及时修补漏洞。

控制点	测评指标	测评对象	测评实施
	f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统)、网络设备（包括虚拟网络设备)、安全设备（包括虚拟安全设备)、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备和控制设备等	1) 应访谈并核查是否有入侵检测的措施； 2) 应核查在发生严重入侵事件时是否提供报警。
8.1.4.5 恶意代码防范	a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断	终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统)、移动终端、移动终端管理系统、移动终端管理客户端和控制设备等	1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代码库； 2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为； 3) 应核查当识别入侵和病毒行为时是否将其有效阻断。
8.1.4.6 可信验证	a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	提供可信验证的设备或组件、提供集中审计功能的系统	1) 应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证； 2) 应核查是否在应用程序的关键执行环节进行动态可信验证； 3) 应测试验证当检测到计算设备的可信性受到破坏后是否进行报警； 4) 应测试验证结果是否以审计记录的形式送至安全管理中心。

控制点	测评指标	测评对象	测评实施
8.1.4.7 数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等	1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性； 2) 应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
	b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备中等	1) 应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性； 2) 应核查是否采用技术措施（如数据安全保护系统等)保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性； 3) 应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
8.1.4.8 数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等	业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1) 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性； 2) 应通过嗅探等方式抓取传输过程中的数据包，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。
	b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限千鉴别数据、重要业务数据和重要个人信息等	业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备中的重要配置数据	1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性； 2) 应核查是否采用技术措施（如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性； 3) 应测试验证是否对指定的数据进行加密处理。

控制点	测评指标	测评对象	测评实施
8.1.4.9 数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	配置数据和业务数据	1) 应核查是否按照备份策略进行本地备份； 2) 应核查备份策略设置是否合理、配置是否正确； 3) 应核查备份结果是否与备份策略一致； 4) 应核查近期恢复测试记录是否能够进行正常的数据恢复。
	b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地	配置数据和业务数据	1)应核查是否提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。
	c)应提供重要数据处理系统的热冗余，保证系统的高可用性	重要数据处理系统	1)应核查重要数据处理系统（包括边界路由器、边界防火墙、核心交换机、应用服务器和数据库服务器等)是否采用热冗余方式部署。
8.1.4.10 剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等	1)应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。
8.1.4.11 个人信息保护	a)应仅采集和保存业务必需的用户个人信息	业务应用系统和数据库管理系统等	1) 应核查采集的用户个人信息是否是业务应用必需的； 2) 应核查是否制定了有关用户个人信息保护的管理制度和流程。
	b)应禁止未授权访问和非法使用用户个人信息	业务应用系统和数据库管理系统等	1) 应核查是否采用技术措施限制对用户个人信息的访问和使用； 2) 应核查是否制定了有关用户个人信息保护的管理制度和流程。

2.3.2.5 安全管理中心

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域。

控制点	测评指标	测评对象	测评实施
8.1.5.1 系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计	提供集中系统管理功能的系统	1) 应核查是否对系统管理员进行身份鉴别； 2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作； 3) 应核查是否对系统管理的操作进行审计。
	b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等	提供集中系统管理功能的系统	1)应核查是否通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
8.1.5.2 审计管理	a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计	综合安全审计系统、数据库审计系统等提供集中审计功能的系统	1) 应核查是否对审计管理员进行身份鉴别； 2) 应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作； 3) 应核查是否对安全审计操作进行审计。
	b)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等	综合安全审计系统、数据库审计系统等提供集中审计功能的系统	1)应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

控制点	测评指标	测评对象	测评实施
8.1.5.3 安全管理	a)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计	提供集中安全管理功能的系统	1) 应核查是否对安全管理员进行身份鉴别； 2) 应核查是否只允许安全管理员通过特定的命令或操作界面进行安全审计操作； 3) 应核查是否对安全管理操作进行审计。
	b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等	提供集中安全管理功能的系统	1)应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
8.1.5.4 集中管控	a)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控	网络拓扑	1) 应核查是否划分出单独的网络区域用于部署安全设备或安全组件； 2) 应核查各个安全设备或安全组件是否集中部署在单独的网络区域内。
	b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理	路由器、交换机和防火墙等设备或相关组件	1) 应核查是否采用安全方式（如SSH、HTTPS、IPSec VPN等)对安全设备或安全组件进行管理； 2) 应核查是否使用独立的带外管理网络对安全设备或安全组件进行管理。
	c)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测	综合网管系统等提供运行状态监测功能的系统	1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； 2) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阀值（或默认阀值)实时报警。

控制点	测评指标	测评对象	测评实施
	d)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求	综合安全审计系统、数据库审计系统等提供集中审计功能的系统	1) 应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部集中安全审计系统中； 2) 应核查是否部署统一的集中安全审计系统，统一收集和存储各设备日志，并根据需要进行集中审计分析； 3)应核查审计记录的留存时间是否至少为6个月。
	e)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理	提供集中安全管控功能的系统	1) 应核查是否能够对安全策略（如防火墙访问控制策略、入侵保护系统防护策略、WAF安全防护策略等)进行集中管理； 2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现对防恶意代码病毒规则库的升级进行集中管理； 3) 应核查是否实现对各个系统或设备的补丁升级进行集中管理。
	f)应能对网络中发生的各类安全事件进行识别、报警和分析	提供集中安全管控功能的系统	1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警； 2) 应核查监测范围是否能够覆盖网络所有关键路径。

2.3.2.6 安全管理制度

控制点	测评指标	测评对象	测评实施
8.1.6.1 安全策略	a)应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等	总体方针策略类文档	1)应核查信息安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。
8.1.6.2 管理制度	a)应对安全管理活动中的各类管理内容建立安全管理制度	安全管理制度类文档	1)应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容。
	b)应对管理人员或操作人员执行的日常管理操作建立操作规程	操作规程类文档	1)应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。
	c)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系	总体方针策略类文档、管理制度类文档、操作规程类文档和记录表单类文档	1)应核查总体方针策略文件、管理制度和操作规程、记录表单是否全面且具有关联性和一致性。
8.1.6.3 制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定	部门/人员职责文件等	1)应核查是否由专门的部门或人员负责制定安全管理制度。
	b)安全管理制度应通过正式、有效的方式发布，并进行版本控制	管理制度类文档和记录表单类文档	1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容； 2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。
8.1.6.4 评审和修订	a)应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定； 2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。

2.3.2.7 安全管理机构

控制点	测评指标	测评对象	测评实施
8.1.7.1 岗位设置	a)应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权	信息/网络安全主管、管理制度类文档和记录表单类文档	1) 应访谈信息/网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组； 2) 应核查相关文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责； 3) 应核查委员会或领导小组的最高领导是否由单位主管领导担任或由其进行了授权。
	b)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责	信息/网络安全主管和管理制度类文档	1) 应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门； 2) 应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责； 3) 应核查岗位职责文档是否有岗位划分情况和岗位职责。
	c)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责	信息/网络安全主管和管理制度类文档	1) 应访谈信息/网络安全主管是否进行了安全管理岗位的划分； 2) 应核查岗位职责文档是否明确了各部门及各岗位职责。
8.1.7.2 人员配备	a)应配备一定数量的系统管理员、审计管理员和安全管理员等	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否配备系统管理员、网络管理员和安全管理员； 2) 应核查人员配备文档是否明确各岗位人员配备情况。
	b)应配备专职安全管理员，不可兼任	记录表单类文档	1)应核查人员配备文档是否配备了专职安全管理员。
8.1.7.3 授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	管理制度类文档和记录表单类文档	1) 应核查部门职责文档是否明确各部门审批事项； 2) 应核查岗位职责文档是否明确各岗位审批事项。
	b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度	操作规程类文档和记录表单类文档	1) 应核查系统变更、重要操作、物理访问和系统接入等事项的操作规范是否明确建立了逐级审批程序； 2) 应核查审批记录、操作记录，审批结果是否与相关制度一致。

控制点	测评指标	测评对象	测评实施
	c)应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否对各类审批事项进行更新； 2) 应核查是否具有定期审查审批事项的记录。
8.1.7.4 沟通和合作	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制； 2) 应核查会议记录是否明确各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通。
	b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制； 2) 应核查会议记录是否明确与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。
	c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息	记录表单类文档	1)应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。
8.1.7.5 审核和检查	a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否定期进行了常规安全检查； 2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
	b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	信息/网络安全主管和记录表单类文档	1) 应访谈信息/网络安全主管是否定期进行了全面安全核查； 2) 应核查全面安全检查记录是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
	c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报	记录表单类文档	1)应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录。

2.3.2.8 安全管理人员

控制点	测评指标	测评对象	测评实施
8.1.8.1 人员录用	a)应指定或授权专门的部门或人员负责人员录用	信息/网络安全主管	1)应访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作。
	b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核	管理制度类文档和记录表单类文档	1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）； 2) 应核查是否具有人员录用时对录用人身份、安全背景、专业资格和资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等； 3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
	c)应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议	记录表单类文档	1) 应核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容； 2) 应核查岗位安全协议是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。
8.1.8.2 人员离岗	a)应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备	记录表单类文档	1)应核查是否具有离岗人员终止其访问权限、交还身份证件、软硬件设备等的登记记录。

控制点	测评指标	测评对象	测评实施
	b)应办理严格的调离手续，并承诺调离后的保密义务后方可离开	管理制度类文档和记录表单类文档	1) 应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等； 2) 应核查是否具有按照离岗程序办理调离手续的记录； 3) 应核查保密承诺文档是否有调离人员的签字。
8.1.8.3 安全意识教育和培训	a)应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施	管理制度类文档	1) 应核查信息安全教育及岗位技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容； 2) 应核查安全责任和惩戒措施管理文档或培训文档是否包含具体的安全责任和惩戒措施。
	b)应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训	记录表单类文档	1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划； 2) 应核查培训内容是否包含安全基础知识、岗位操作规程等； 3) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等的描述。
	c)应定期对不同岗位的人员进行技能考核	记录表单类文档	1)应核查是否具有针对各岗位人员的技能考核记录。

控制点	测评指标	测评对象	测评实施
8.1.8.4 外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案	管理制度类文档和记录表单类文档	1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等； 2) 应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等； 3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
	b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案	管理制度类文档和记录表单类文档	1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程； 2) 应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等； 3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。

控制点	测评指标	测评对象	测评实施
	c)外部人员离场后应及时清除其所有的访问权限	管理制度类文档和记录表单类文档	1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限； 2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
	d)获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息	记录表单类文档	1)应核查外部人员访问保密协议是否明确人员的保密义务(如不得进行非授权操作，不得复制信息等)。

2.3.2.9 安全建设管理

控制点	测评指标	测评对象	测评实施
8.1.9.1 定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由	记录表单类文档	1)应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。
	b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定	记录表单类文档	1)应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见。
	c)应保证定级结果经过相关部门的批准	记录表单类文档	1应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。
	d)应将备案材料报主管部门和相应公安机关备案	记录表单类文档	1)应核查是否具有公安机关出具的备案证明文档。
8.1.9.2 安全方案设计	a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施	安全规划设计类文档	1)应核查安全设计文档是否根据安全等级选择安全措施，是否根据安全需求调整安全措施。

控制点	测评指标	测评对象	测评实施
	b)应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件	安全规划设计类文档	1)应核查是否有总体规划和安全设计方案等配套文件，设计方案中应包含密码技术相关内容。
	c)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施	记录表单类文档	1)应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。
8.1.9.3 产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定	记录表单类文档	1)应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等。
	b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求	建设负责人和记录表单类文档	1) 应访谈建设负责人是否采用了密码产品及其相关服务； 2) 应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。

控制点	测评指标	测评对象	测评实施
	c)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单	记录表单类文档	1)应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。
8.1.9.4 自行软件开发	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制	建设负责人	1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试，与实际运行环境分开； 2) 应核查测试数据和结果是否受控使用。
	b)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则	管理制度类文档	1)应核查软件开发管理制度是否明确软件设计、开发、测试和验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权和审批。
	c)应制定代码编写安全规范，要求开发人员参照规范编写代码	管理制度类文档	1)应核查代码编写安全规范是否明确代码安全编写规则。
	d)应具备软件设计的相关文档和使用指南，并对文档使用进行控制	软件开发类文档	1)应核查是否具有软件开发文档和使用指南，并对文档使用进行控制。
	e)应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测	记录表单类文档	1)应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码。

控制点	测评指标	测评对象	测评实施
	f)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制	记录表单类文档	1)应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字。
	g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查	建设负责人	1)应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等。
8.1.9.5 外包软件开发	a)应在软件交付前检测其中可能存的恶意代码	记录表单类文档	1)应核查是否具有交付前的恶意代码检测报告。
	b)应保证开发单位提供软件设计文档和使用指南	操作规程类文档和记录表单类文档	1)应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。

控制点	测评指标	测评对象	测评实施
	c)应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道	建设负责人和记录表单类文档	1) 应访谈建设负责人委托开发单位是否提供软件源代码； 2) 应核查软件测试报告是否审查了软件可能存在的后门和隐蔽信道。
8.1.9.6 工程实施	a)应指定或授权专门的部门或人员负责工程实施过程的管理	记录表单类文档	1)应核查是否指定专门部门或人员对工程实施进行进度和质量控制。
	b)应制定安全工程实施方案控制工程实施过程	记录表单类文档	1)应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。
	c)应通过第三方工程监理控制项目的实施过程	记录表单类文档	1)应核查第三方工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容。
8.1.9.7 测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告	记录表单类文档	1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容； 2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。

控制点	测评指标	测评对象	测评实施
	b)应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容	记录表单类文档	1)应核查是否具有上线前的安全测试报告，报告应包含密码应用安全性测试相关内容。
8.1.9.8 系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点	记录表单类文档	1)应核查交付清单是否说明交付的各类设备、软件、文档等。
	b)应对负责运行维护的技术人员进行相应的技能培训	记录表单类文档	1)应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等。
	c)应提供建设过程文档和运行维护文档	记录表单类文档	1)应核查交付文档是否包括建设过程文档和运行维护文档等，提交的文档是否符合管理规定的要求。
8.1.9.9 等级测评	a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改	运维负责人和记录表单类文档	1) 应访谈运维负责人本次测评是否为首次，若非首次，是否根据测评结果进行相应的安全整改； 2) 应核查是否具有以往等级测评报告和安全整改方案。

控制点	测评指标	测评对象	测评实施
	b)应在发生重大变更或级别发生变化时进行等级测评	运维负责人和记录表单类文档	1) 应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评； 2) 应核查是否具有相应情况下的等级测评报告。
	c)应确保测评机构的选择符合国家有关规定	等级测评报告和相关资质文件	1)应核查以往等级测评的测评单位是否具有等级测评机构资质。
8.1.9.10 服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定	建设负责人	1)应访谈建设负责人选择的安全服务商是否符合国家有关规定。
	b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务	记录表单类文档	1)应核查与安全服务商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容。

控制点	测评指标	测评对象	测评实施
	c)应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制	管理制度类文档和记录表单类文档	1) 应核查是否具有服务供应商定期提交的安全服务报告； 2) 应核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告； 3) 应核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。

2.3.2.10 安全运维管理

控制点	测评指标	测评对象	测评实施
8.1.10.1 环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;	物理安全负责人和记录表单类文档	1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等)进行定期维护； 2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员； 3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息； 4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
	b)应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定;	管理制度类文档和记录表单类文档	1) 应核查机房安全管理制度是否覆盖机房物理访问、物品进出和环境安全等方面内容； 2) 应核查物理访问、物品进出和环境安全等相关记录是否与制度相符。
	c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	管理制度类文档和办公环境	1) 应核查机房安全管理制度是否明确来访人员的接待区域； 2) 应核查办公桌面上等位置是否未随意放置了含有敏感信息的纸档文件和移动介质等。
8.1.10.2 资产管理	a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容;	记录表单类文档	1)应核查资产清单是否包括资产类别（含设备设施、软件、文档等)、资产责任部门、重要程度和所处位置等内容。
	b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施;	资产管理员、管理制度类文档和设备	1) 应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同； 2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求； 3) 应核查资产清单中的设备是否具有相应标识，标识方法是否符合2)相关要求。
	c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	管理制度类文档	1) 应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类)； 2) 应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。

控制点	测评指标	测评对象	测评实施
8.1.10.3 介质管理	a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点	资产管理员和记录表单类文档	1) 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理； 2) 应核查介质管理记录是否记录介质归档、使用和定期盘点等情况。
	b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录	资产管理员和记录表单类文档	1) 应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制； 2) 核查是否对介质的归档和查询等进行登记记录。
8.1.10.4 设备维护管理	a)应对各种设备（包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理	设备管理员和管理制度类文档	1) 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护； 2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
	b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等	管理制度类文档和记录表单类文档	1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容； 2) 应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
	c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密	设备管理员和记录表单类文档	1) 应访谈设备管理员含有重要数据的设备带出工作环境是否有加密措施； 2) 应访谈设备管理员对带离机房的设备是否经过审批； 3) 应核查是否具有设备带离机房或办公地点的审批记录。

控制点	测评指标	测评对象	测评实施
	d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用	设备管理员	1)应访谈设备管理员含有存储介质的设备在报废或重用前，是否采取措施进行完全清除或被安全覆盖。
8.1.10.5 漏洞和风险管理	a)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补	记录表单类文档	1) 应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和安全通报等）； 2) 应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。
	b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题	安全管理员和记录表单类文档	1) 应访谈安全管理员是否定期开展安全测评； 2) 应核查是否具有安全测评报告； 3) 应核查是否具有安全整改应对措施文档。
8.1.10.6 网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限	记录表单类文档	1)应核查网络和系统安全管理文档，系统管理员是否划分了不同角色，并定义各个角色的责任和权限。
	b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制	运维负责人和记录表单类文档	1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理； 2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。

控制点	测评指标	测评对象	测评实施
	c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定	管理制度类文档	1)应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等)，配置文件的生成及备份，变更审批、授权访问，最小服务，升级与打补丁，审计日志管理，登录设备和系统的口令更新周期等方面。
	d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等	操作规程类文档	1)应核查重要设备（如操作系统、数据库、网络设备、安全设备、应用和组件)的配置和操作手册是否明确操作步骤、参数配置等内容。
	e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容	记录表单类文档	1)应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。
	f)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为	系统管理员和记录表单类文档	1) 应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计； 2) 应核查是否具有对日志、监测和报警数据等进行分析统计的报告。
	g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库	系统管理员和记录表单类文档	1) 应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本； 2) 应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动； 3) 应核查是否具有变更运维的操作过程记录。

控制点	测评指标	测评对象	测评实施
	h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据	系统管理员和记录表单类文档	1) 应访谈系统管理员使用运维工具结束后是否删除工具中的敏感数据； 2) 应核查是否具有运维工具接入系统的审批记录； 3) 应核查运维工具的审计日志记录，审计日志是否不可以更改。
	i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道	系统管理员和记录表单类文档	1) 应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立即关闭了接口或通道； 2) 应核查开通远程运维的审批记录； 3) 应核查针对远程运维的审计日志是否不可以更改。
	j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为	安全管理员和记录表单类文档	1) 应访谈系统相关人员网络外联连接（如互联网、合作伙伴企业网、上级部门网络等)是否都得到授权与批准； 2) 应访谈网络管理员是否定期核查违规联网行为； 3) 应核查是否具有外联授权的记录文件。
8.1.10.7 恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等	运维负责人和管理制度类文档	1) 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识； 2) 应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。
	b)应定期验证防范恶意代码攻击的技术措施的有效性	安全管理员和记录表单类文档	1) 若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件； 2) 若采用防恶意代码产品，应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件； 3) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。

控制点	测评指标	测评对象	测评实施
8.1.10.8 配置管理	a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等	系统管理员	1)应访谈系统管理员是否对基本配置信息进行记录和保存。
	b)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库	系统管理员和记录表单类文档	1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库； 2) 应核查配置信息的变更流程是否具有相应的申报审批程序。
8.1.10.9 密码管理	a)应遵循密码相关国家标准和行业标准	安全管理员	1)应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。
	b)应使用国家密码管理主管部门认证核准的密码技术和产品	安全管理员	1)应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。
8.1.10.10 变更管理	a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施	记录表单类文档	1) 应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容； 2) 应核查是否具有变更方案评审记录和变更过程记录文档。
	b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程	记录表单类文档	1) 应核查变更控制的申报、审批程序其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容； 2) 应核查是否具有变更实施过程的记录文档。
	c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练	运维负责人和记录表单类文档	1) 应访谈运维负责人变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练； 2) 应核查是否具有变更恢复演练记录； 3) 应核查变更恢复程序是否规定变更中止或失败后的恢复流程。

控制点	测评指标	测评对象	测评实施
8.1.10.11 备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等	系统管理员和记录表单类文档	1) 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统； 2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
	b)应规定备份信息的备份方式、备份频度、存储介质、保存期等	管理制度类文档	1)应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。
	c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等	管理制度类文档	1)应核查备份和恢复的策略文档是否根据数据的重要程度制定相应备份恢复策略和程序等。
8.1.10.12 安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件	运维负责人和记录表单类文档	1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； 2) 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。
	b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等	管理制度类文档	1)应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。
	c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训	记录表单类文档	1)应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。

控制点	测评指标	测评对象	测评实施
	d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序	运维负责人和记录表单类文档	1) 应访谈运维负责人不同安全事件的报告流程； 2) 应核查针对重大安全事件是否制定不同安全事件报告和处理流程，是否明确具体报告方式、报告内容、报告人等方面内容。
8.1.10.13 应急预案管理	a)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容	管理制度类文档	1)应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面。
	b)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容	管理制度类文档	1)应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各个方面)。
	c)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练	运维负责人和记录表单类文档	1) 应访谈运维负责人是否定期对相关人员进行应急预案培训和演练； 2) 应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等； 3) 应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。
	d)应定期对原有的应急预案重新评估，修订完善	记录表单类文档	1)应核查应急预案修订记录是否定期评估并修订完善等。
8.1.10.14 外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定	运维负责人	1) 应访谈运维负责人是否有外包运维服务情况； 2) 应访谈运维负责人外包运维服务单位是否符合国家有关规定。
	b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容	记录表单类文档	1)应核查外包运维服务协议是否明确约定外包运维的范围和工作内容。

控制点	测评指标	测评对象	测评实施
	c)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确	记录表单类文档	1)应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力。
	d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等	记录表单类文档	1)应核查外包运维服务协议是否包含可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等内容。

2.3.2.11 云计算扩展

类	控制点	测评指标	测评对象	测评实施
8.2.1 安全物理环境	8.2.1.1 基础设施位置	a)应保证云计算基础设施位于中国境内	机房管理员、办公场地、机房和平台建设方案	1)应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内； 2)应核查云计算平台建设方案，云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件是否均位于中国境内。
8.2.2 安全通信网络	8.2.2.1 网络架构	a)应保证云计算平台不承载高于其安全保护等级的业务应用系统	云计算平台和业务应用系统定级备案材料	1)应核查云计算平台和云计算平台承载的业务应用系统相关定级备案材料，云计算平台安全保护等级是否不低于其承载的业务应用系统安全保护等级。
		b)应实现不同云服务客户虚拟网络之间的隔离	网络资源隔离措施、综合网管系统和云管理平台	1)应核查云服务客户之间是否采取网络隔离措施； 2)应核查云服务客户之间是否设置并启用网络资源隔离策略； 3)应测试验证不同云服务客户之间的网络隔离措施是否有效。

类	控制点	测评指标	测评对象	测评实施
		c)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力	防火墙、入侵检测系统、入侵保护系统和抗APT系统等安全设备	1)应核查云计算平台是否具备为云服务客户提供通信传输、边界防护、入侵防范等安全防护机制的能力； 2)应核查上述安全防护机制是否满足云服务客户的业务需求。
		d)应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略	云管理平台、网络管理平台、网络设备和安全访问路径	1)应核查云计算平台是否支持云服务客户自主定义安全策略，包括定义访问路径、选择安全组件、配置安全策略；2)应核查云服务客户是否能够自主设置安全策略，包括定义访问路径、选择安全组件、配置安全策略。

类	控制点	测评指标	测评对象	测评实施
		e)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务	相关开放性接口和安全服务及相关文档	1)应核查接口设计文档或开放性服务技术文档是否符合开放性及安全性要求； 2)应核查云服务客户是否可以接入第三方安全产品或在云计算平台选择第三方安全服务。
8.2.3 安全区域边界	8.2.3.1 访问控制	a)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则	访问控制机制、网络边界设备和虚拟化网络边界设备	1)应核查是否在虚拟化网络边界部署访问控制机制，并设置访问控制规则； 2)应核查并测试验证云计算平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效； 3)应核查并测试验证云计算平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效； 4)应核查并测试验证不同云服务客户间访问控制规则和访问控制策略是否有效； 5)应核查并测试验证云服务客户不同安全保护等级业务系统之间访问控制规则和访问控制策略是否有效。

类	控制点	测评指标	测评对象	测评实施
		b)应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则	网闸、防火墙、路由器和交换机等提供访问控制功能的设备	1)应核查是否在不同等级的网络区域边界部署访问控制机制，设置访问控制规则； 2)应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效； 3)应测试验证不同安全等级的网络区域间进行非法访问时，是否可以正确拒绝该非法访问。

类	控制点	测评指标	测评对象	测评实施
	8.2.3.2 入侵防范	a)应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1)应核查是否采取了入侵防范措施对网络入侵行为进行防范，如部署抗APT攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件； 2)应核查部署的抗APT攻击系统、网络入侵保护系统等人侵防范设备或相关组件的规则库升级方式，核查规则库是否进行及时更新； 3)应核查部署的抗APT攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能，以及报警功能和清洗处置功能； 4)应验证抗APT攻击系统、网络入侵保护系统等入侵防范设备或相关组件对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证入侵防范设备或相关组件是否能记录攻击类型、攻击时间、攻击流量)； 5)应验证抗APT攻击系统、网络入侵保护系统等入侵防范设备或相关组件对云服务客户网络攻击行为的报警策略是否有效（如模拟产生攻击动作，验证抗APT攻击系统或网络入侵保护系统是否能实时报警)； 6)应核查抗APT攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否具有对SQL注入、跨站脚本等攻击行为的发现和阻断能力； 7)应核查抗APT攻击系统、网络入侵保护系统等入侵防范设备或相关组件是否能够检测出具有恶意行为、过分占用计算资源和带宽资源等恶意行为的虚拟机； 8)应核查云管理平台对云服务客户攻击行为的防范措施，核查是否能够对云服务客户的网络攻击行为进行记录，记录应包括攻击类型、攻击时间和攻击流量等内容； 9)应核查云管理平台或入侵防范设备是否能够对云计算平台内部发起的恶意攻击或恶意外连行为进行限制，核查是否能够对内部行为进行监控； 10)通过对外攻击发生器伪造对外攻击行为，核查云租户的网络攻击日志，确认是否正确记录相应的攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者IP和攻击流量规模等内容； 11)应核查运行虚拟机监控器(VMM)和云管理平台软件的物理主机，确认其安全加固手段是否能够避免或减少虚拟化共享带来的安全漏洞。

类	控制点	测评指标	测评对象	测评实施
		b)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1)应核查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量等； 2)应核查网络攻击行为检测设备或相关组件的规则库是否为最新； 3)应测试验证网络攻击行为检测设备或相关组件对异常流量和未知威胁的监控策略是否有效。

类	控制点	测评指标	测评对象	测评实施
		c)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量	虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1)应核查是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能； 2)应测试验证对异常流量的监测策略是否有效。

类	控制点	测评指标	测评对象	测评实施
		d)应在检测到网络攻击行为、异常流量情况时进行告警	虚拟机、宿主机、抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统和入侵保护系统或相关组件	1)应核查检测到网络攻击行为、异常流量时是否进行告警； 2)应测试验证其对异常流量的监测策略是否有效。

类	控制点	测评指标	测评对象	测评实施
	8.2.3.3 安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启	堡垒机或相关组件	1)应核查云服务商（含第三方运维服务商)和云服务客户在远程管理时执行的远程特权命令是否有相关审计记录；2)应测试验证云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
		b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计	综合审计系统或相关组件	1)应核查是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作)可被云服务客户审计； 2)应测试验证云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。

类	控制点	测评指标	测评对象	测评实施
8.2.4 安全计算环境	8.2.4.1 身份鉴别	a)当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制	管理终端和云计算平台	1)应核查当进行远程管理时是否建立双向身份验证机制；2)应测试验证上述双向身份验证机制是否有效。
	8.2.4.2 访问控制	a)应保证当虚拟机迁移时，访问控制策略随其迁移	虚拟机、虚拟机迁移记录和相关配置	1)应核查虚拟机迁移时访问控制策略是否随之迁移； 2)应测试验证虚拟机迁移后访问控制措施是否随其迁移。
		b)应允许云服务客户设置不同虚拟机之间的访问控制策略	虚拟机和安全组或相关组件	1)应核查云服务客户是否能够设置不同虚拟机间访问控制策略； 2)应测试验证上述访问控制策略的有效性。

类	控制点	测评指标	测评对象	测评实施
	8.2.4.3 入侵防范	a)应能检测虚拟机之间的资源隔离失效，并进行告警	云管理平台或相关组件	1)应核查是否能够检测到虚拟机之间的资源隔离失效并进行告警，如CPU、内存和磁盘资源之间的隔离失效。
		b)应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警	云管理平台或相关组件	1)应核查是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
		c)应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警	云管理平台或相关组件	1)应核查是否能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

类	控制点	测评指标	测评对象	测评实施
	8.2.4.4 镜像和快照保护	a)应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务	虚拟机镜像文件	1)应核查是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。
		b)应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改	云管理平台和虚拟机镜像、快照或相关组件	1)应核查是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改； 2)应测试验证是否能够对镜像、快照进行完整性验证。

类	控制点	测评指标	测评对象	测评实施
		c)应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问	云管理平台和虚拟机镜像、快照或相关组件	1)应核查是否对虚拟机镜像或快照中的敏感资源采用加密、访问控制等技术手段进行保护，防止可能存在的针对快照的非法访问。
	8.2.4.5 数据完整性和保密性	a)应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定	数据库服务器、数据存储设备和管理文档记录	1)应核查云服务客户数据、用户个人信息所在的服务器及数据存储设备是否位于中国境内； 2)应核查上述数据出境时是否符合国家相关规定。

类	控制点	测评指标	测评对象	测评实施
		b)应只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限	云管理平台、数据库、相关授权文档和管理文档	1)应核查云服务客户数据管理权限授权流程、授权方式、授权内容； 2)应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查是否有相关授权证明。
		c)应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施	虚拟机	1)应核查在虚拟资源迁移过程中，是否采取校验技术或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

类	控制点	测评指标	测评对象	测评实施
		d)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	密钥管理解决方案	1)当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能保证云服务客户自行实现数据的加解密过程； 2)应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能保证云服务客户自行实现数据的加解密过程。
	8.2.4.6 数据备份恢复	a)云服务客户应在本地保存其业务数据的备份	云管理平台或相关组件	1)应核查是否提供备份措施保证云服务客户可以在本地备份其业务数据。
		b)应提供查询云服务客户数据及备份存储位置的能力	云管理平台或相关组件	1)应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。

类	控制点	测评指标	测评对象	测评实施
		c)云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致	云管理平台或相关组件	1)应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本； 2)应核查各副本内容是否保持一致。

类	控制点	测评指标	测评对象	测评实施
		d)应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程	相关技术措施和手段	1)应核查是否有相关技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统； 2)应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
	8.2.4.7 剩余信息保护	a)应保证虚拟机所使用的内存和存储空间回收时得到完全清楚	云计算平台	1)应核查虚拟机的内存和存储空间回收时，是否得到完全清除； 2)应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等)是否已清理。

类	控制点	测评指标	测评对象	测评实施
		b)云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除	云存储系统和云计算平台	1)应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。
8.2.5 安全管理中心	8.2.5.1 集中管控	a)应对物理资源和虚拟资源按照策略做统一管理调度与分配	资源调度平台、云管理平台或相关组件	1)应核查是否有资源调度平台等提供资源统一管理调度与分配策略； 2)应核查是否能够按照上述策略对物理资源和虚拟资源做统一管理调度与分配。
		b)应保证云计算平台管理流量与云服务客户业务流量分离	网络架构和云管理平台	1)应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离； 2)应测试验证云计算平台管理流量与业务流量是否分离。

类	控制点	测评指标	测评对象	测评实施
		c)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计	云管理平台、综合审计系统或相关组件	1)应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集； 2)应核查云服务商和云服务客户是否能够实现各自的集中审计。

类	控制点	测评指标	测评对象	测评实施
		d)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测	云管理平台或相关组件	1)应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

类	控制点	测评指标	测评对象	测评实施
8.2.6 安全建设管理	8.2.6.1 云服务商选择	a)应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力	系统建设负责人和服务合同	1)应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商； 2)应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。
		b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标	服务水平协议或服务合同	1)应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。

类	控制点	测评指标	测评对象	测评实施
		c)应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	服务水平协议或服务合同	1)应核查服务水平协议或服务合同中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

类	控制点	测评指标	测评对象	测评实施
		d)应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除	服务水平协议或服务合同	1)应核查服务水平协议或服务合同是否明确服务合约到期时，云服务商完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
		e)应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据	保密协议或服务合同	1)应核查保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据的规定。

类	控制点	测评指标	测评对象	测评实施
	8.2.6.2 供应链管理	a)应确保供应商的选择符合国家有关规定	记录表单类文档	1)应核查云服务商的选择是否符合国家的有关规定。
		b)应将供应链安全事件信息或安全威胁信息及时传达到云服务客户	供应链安全事件报告或威胁报告	1)应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户，报告是否明确相关事件信息或威胁信息。

类	控制点	测评指标	测评对象	测评实施
		c)应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制	供应商重要变更记录、安全风险评估报告和风险预案	1)应核查供应商的重要变更是否及时传达到云服务客户，是否对每次供应商的重要变更都进行风险评估并采取控制措施。

类	控制点	测评指标	测评对象	测评实施
8.2.7 安全运维管理	8.2.7.1 云计算环境管理	a)云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定	运维设备、运维地点、运维记录和相关管理文档	1)应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。

2.3.2.12 物联网扩展

类	控制点	测评指标	测评对象	测评实施
8.4.1 安全物理环境	8.4.1.1 感知节点设备物理防护	a)感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动	感知节点设备所处物理环境和设计或验收文档	1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致； 2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
		b)感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域)	感知节点设备所处物理环境和设计或验收文档	1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态 所处物理环境的说明，是否与实际情况一致； 2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域)。
		c)感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等	感知节点设备所处物理环境和设计或验收文档	1) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致； 2) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。
		d)关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力)	关键感知节点设备的供电设备（关键网关节点设备的供电设备)和设计或验收文档	1) 应核查关键感知节点设备（关键网关节点设备)电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施（关键网关节点设备持久稳定的电力供应措施); 2) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。
8.4.2 安全区域边界	8.4.2.1 接入控制	a)应保证只有授权的感知节点可以接入	感知节点设备和设计文档	1) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述； 2) 应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。

类	控制点	测评指标	测评对象	测评实施
	8.4.2.2 入侵防范	a)应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为	感知节点设备和设计文档	1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求； 3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
		b)应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为	网关节点设备和设计文档	1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求； 3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
8.4.3 安全计算环境	8.4.3.1 感知节点设备安全	a)应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更	感知节点设备	1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更； 2) 应通过试图接入和控制传感网访问未授权的资源，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
		b)应具有对其连接的网关节点设备（包括读卡器)进行身份标识和鉴别的能力	网关节点设备（包括读卡器)	1) 应核查是否对连接的网关节点设备（包括读卡器)进行身份标识与鉴别，是否配置了符合安全策略的参数； 2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
		c)应具有对其连接的其他感知节点设备（包括路由节点)进行身份标识和鉴别的能力	其他感知节点设备（包括路由节点)	1) 应核查是否对连接的其他感知节点设备（包括路由节点)设备进行身份标识与鉴别，是否配置了符合安全策略的参数； 2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
	8.4.3.2 网关节点设备安全	应设置最大并发连接数	网关节点设备	应核查网关节点设备是否配置了最大并发连接数参数。

类	控制点	测评指标	测评对象	测评实施
		a)应具备对合法连接设备（包括终端节点、路由节点、数据处理中心)进行标识和鉴别的能力	网关节点设备	1) 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能； 2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。
		b)应具备过滤非法节点和伪造节点所发送的数据的能力	网关节点设备	1) 应核查是否具备过滤非法节点和伪造节点发送的数据的功能； 2) 应测试验证是否能够过滤非法节点和伪造节点发送的数据。
		c)授权用户应能够在设备使用过程中对关键密钥进行在线更新	感知节点设备	1)应核查感知节点设备是否对其关键密钥进行在线更新。
		d)授权用户应能够在设备使用过程中对关键配置参数进行在线更新	感知节点设备	1)应核查是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。
	8.4.3.3 抗数据重放	a)应能够鉴别数据的新鲜性，避免历史数据的重放攻击	感知节点设备	1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放； 2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。
		b)应能够鉴别历史数据的非法修改，避免数据的修改重放攻击	感知节点设备	1) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施； 2) 应测试验证是否能够避免数据的修改重放攻击。
	8.4.3.4 数据融合处理	a)应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用	物联网应用系统	1) 应核查是否提供对来自传感网的数据进行数据融合处理的功能； 2) 应测试验证数据融合处理功能是否能够处理不同种类的数据。

类	控制点	测评指标	测评对象	测评实施
8.4.4 安全运维管理	8.4.4.1 感知节点管理	a)应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护	维护记录	1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护， 由何部门或何人负责，维护周期多长； 2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
		b)应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理	感知节点和网关节点设备安全管理文档	1)应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
		c)应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维 护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	感知节点设备、网关节点设备部署环境的管理制度	1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容； 2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。

2.3.2.13 移动互联网扩展

类	控制点	测评指标	测评对象	测评实施
8.3.1 安全物理环境	8.3.1.1 无线接入点的物理位置	a)应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰	无线接入设备	1) 应该查询物理位置与无线信号的覆盖范围是否合理； 2) 应测试验证无线信号是否可以避免电磁干扰。
8.3.2 安全区域边界	8.3.2.1 边界防护	a)应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备	无线接入网关设备	1)应核查有线网络与无线网络边界之间是否部署无线接入网关设备。
	8.3.2.2 访问控制	a)无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证	无线接入设备	1)应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证。
	8.3.2.3 入侵防范	a)应能够检测到非授权无线接入设备和非授权移动终端的接入行为	终端准入控制系统、移动终端管理系统或相关组件	1) 应核查是否能够检测非授权无线接入设备和移动终端的接入行为； 2) 应测试验证是否能够检测非授权无线接入设备和移动终端的接入行为。
		b)应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为	抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件	1) 应核查是否能够对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测； 2) 应核查规则库版本是否及时更新。
		c)应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态	无线接入设备或相关组件	1)应核查是否能够检测无线接入设备的SSID广播、WPS等高风险功能的开启状态。
		d)应禁用无线接入设备和无线接入网关存在风险的功能，如： SSID广播、WEP认证等	无线接入设备和无线接入网关设备	1)应核查是否关闭了SSID广播、WEP认证等存在风险的功能。
		e)应禁止多个AP使用同一个认证密钥	无线接入设备	1)应核查是否分别使用了不同的鉴别密钥。

类	控制点	测评指标	测评对象	测评实施
		f)应能够阻断非授权无线接入设备或未授权移动终端	终端准入控制系统、移动终端管理系统或相关组件	1)应核查是否能够阻断非授权无线接入设备或非授权移动终端接入； 2)应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入。
8.3.3 安全计算环境	8.3.3.1 移动终端管控	a)应保证移动终端安装、注册并运行终端管理客户端软件	移动终端和移动终端和管理系统	1)应核查移动终端是否安装、注册并运行移动终端客户端软件。
		b)移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等	移动终端和移动终端管理系统	1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略； 2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。
	8.3.3.2 移动应用管控	a)应具有选择应用软件安装、运行的功能	移动终端管理客户端	1)应核查是否具有选择应用软件安装、运行的功能。
		b)应只允许指定证书签名的应用软件安装和运行	移动终端管理客户端	1)应核查全部移动应用是否由指定证书签名。
		c)应具有软件白名单功能，应能根据白名单控制应用软件安装、运行	移动终端管理客户端	1) 应核查是否具有软件白名单功能； 2) 应测试验证白名单功能是否能够控制应用软件安装、运行。
8.3.4 安全建设管理	8.3.4.1 移动应用软件采购	a)应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名	移动终端	1)应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。
		b)应保证移动终端安装、运行的应用软件由指定的开发者开发	移动终端	1)应核查移动应用软件是否经由指定的开发者开发。
	8.3.4.2 移动应用软件开发	a)应对移动业务应用软件开发者进行资格审查	系统建设负责人	1)应访谈系统建设负责人，是否对开发者进行资格审查。
		b)应保证开发移动业务应用软件的签名证书合法性	软件的签名证书	1)应核查开发移动业务应用软件的签名证书是否具有合法性。

类	控制点	测评指标	测评对象	测评实施
8.3.5 安全运维管理	8.3.5.1 配置管理	a)应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别	记录表单类文档、移动终端管理系统或相关组件	1)应核查是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备。

2.3.2.14 工业控制系统扩展

类	控制点	测评指标	测评对象	测评实施
8.5.1 安全物理环境	8.5.1.1 室外控制设备物理防护	a)室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等	室外控制设备	1) 应核查是否放置于采用铁板或其他防火材料制作的箱体或装置中并紧固； 2) 应核查箱体或装置是否具有透风 、散热、防盗、防雨和防火能力等。
		b)室外控制设备放置应远离强电磁干扰 、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行	室外控制设备	1) 应核查放置位置是否远离强电磁干扰和热源等环境； 2) 应核查是否有应急处置及检修维护记录。
8.5.2 安全通信网络	8.5.2.1 网络架构	a)工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段	网闸、路由器、交换机和防火墙等提供访问控制功能的设备	1) 应核查工业控制系统和企业其他系统之间是否部署单向隔离设备； 2) 应核查是否采用了有效的单向隔离策略实施访问控制； 3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。
		b)工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段	路由器、交换机和防火墙等提供访问控制功能的设备	1) 应核查工业控制系统内部是否根据业务特点划分了不同的安全域； 2) 应核查各安全域之间访问控制设备是否配置了有效的访问控制策略。
		c)涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网 ，在物理层面上实现与其他数据网及外部公共信息网的安全隔离	工业控制系统网络	1)应核查涉及实时控制和数据传输的工业控制系统是否在物理层面上独立组网。
	8.5.2.2 通信传输	a)在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输	加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备	1)应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。

类	控制点	测评指标	测评对象	测评实施
8.5.3 安全区域边界	8.5.3.1 访问控制	a)应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务	网闸、防火墙、路由器和交换机等提供访问控制功能的设备	1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略； 2) 应核查设备安全策略，是否禁止E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
		b)应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警	网闸、防火墙、路由器和交换机等提供访问控制功能的设备，监控预警设备	1) 应核查设备是否可以在策略失效的时候进行告警； 2) 应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。
	8.5.3.2 拨号使用控制	a)工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施	拨号服务类设备	1)应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户 / 口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。
		b)拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施	拨号服务类设备	1)应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
	8.5.3.3 无线使用控制	a)应对所有参与无线通信的用户（人员 、软件进程或者设备)提供唯一性标识和鉴别	无线通信网络及设备	1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施； 2) 应核查用户身份标识是否具有唯一性。
		b)应对所有参与无线通信的用户（人员 、软件进程或者设备)进行授权以及执行使用进行限制	无线通信网络及设备	1)应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理，核查未授权的使用是否可以被发现及告警。
		c)应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护	无线通信网络及设备	1)应核查无线通信传输中是否采用加密措施保证传输报文的机密性。

类	控制点	测评指标	测评对象	测评实施
		d)对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为	无线通信网络及设备和监测设备	1)应核查在工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出警告并可以对试图接入的无线设备进行屏蔽。
8.5.4 安全计算环境	8.5.4.1 控制设备安全	a)控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制	控制设备	1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等功能，如控制设备具备上述功能，则按照通用要求测评；2) 如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		b)应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作	控制设备	1) 应核查是否有测试报告或测试评估记录； 2) 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。
		c)应关闭或拆除控制设备的软盘驱动 、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理	控制设备	1) 应核查控制设备是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等； 2) 应核查保留的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等是否通过相关的措施实施严格的监控管理。
		d)应使用专用设备和专用软件对控制设备进行更新	控制设备	1)应核查是否使用专用设备和专用软件对控制设备进行更新。
		e)应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序	控制设备	1)应核查由相关部门出具或认可的控制设备的检测报告，明确控制设备固件中是否不存在恶意代码程序。
8.5.5 安全建设管理	8.5.5.1 产品采购和使用	a)工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用	安全管理员和检测报告类文档	1) 应访谈安全管理员系统使用的工业控制系统重要设备及网络安全专用产品是否通过专业机构的安全性检测； 2) 应核查工业控制系统是否有通过专业机构出具的安全性检测报告。

类	控制点	测评指标	测评对象	测评实施
	8.5.5.2 外包软件和开发	a)应在外包开发合同中规定针对开发单位，供应商的约束条款，包括设备及系统在生命周期内有关保密，禁止关键技术扩散和设备行业专用等方面的内容	外包合同	1)应核查是否在外包开发合同中规定针对开发单位，供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。