c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.4.1.2 测评单元(L4-MMS4-02)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：感知节点和网关节点设备安全管理文档。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.4.4.1.3 测评单元(L4-MMS4-03)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度。

c) 测评实施：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5 工业控制系统安全测评扩展要求

9.5.1 安全物理环境

9.5.1.1 室外控制设备物理防护

9.5.1.1.1 测评单元(L4-PES5-01)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.1.1.2 测评单元(L4-PES5-02)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：室外控制设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)或 2)为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2 安全通信网络

9.5.2.1 网络架构

9.5.2.1.1 测评单元(L4-CNS5-01)

该测评单元包括以下要求：

a) 测评指标：应在工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用符合国家或行业规定的专用产品实现单向安全隔离。

b) 测评对象：网闸、防火墙和单向安全隔离装置等提供访问控制功能的设备。

c) 测评实施包括以下内容：

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；

4) 应核查所使用的专用产品是否符合国家规定，如有行业特殊规定的是否符合行业规定。

d) 单元判定：如果 1)～4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.1.2 测评单元(L4-CNS5-02)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.1.3 测评单元(L4-CNS5-03)

该测评单元包括以下要求:

a) 测评指标: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。

b) 测评对象:工业控制系统网络。

c) 测评实施: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。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.5.2.2 通信传输

9.5.2.2.1 测评单元(L4-CNS5-04)

该测评单元包括以下要求:

a) 测评指标: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。

b) 测评对象: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。

c) 测评实施: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。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.5.3 安全区域边界

9.5.3.1 访问控制

9.5.3.1.1 测评单元(L4-ABS5-01)

该测评单元包括以下要求:

a) 测评指标: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。

b) 测评对象:网闸、防火墙、路由器和交换机等提供访问控制功能的设备。

c) 测评实施包括以下内容:

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。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.5.3.1.2 测评单元(L4-ABS5-02)

该测评单元包括以下要求:

a) 测评指标: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。

b) 测评对象: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。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.3.2 拨号使用控制

9.5.3.2.1 测评单元(L4-ABS5-03)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：拨号服务类设备。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.2.2 测评单元(L4-ABS5-04)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：拨号服务类设备。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.2.3 测评单元(L4-ABS5-05)

该测评单元包括以下要求：

a) 测评指标：涉及实时控制和数据传输的工业控制系统禁止使用拨号访问服务。

b) 测评对象：拨号服务类设备。

c) 测评实施：应核查涉及实时控制和数据传输的工业控制系统内是否禁止使用拨号访问服务。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.3 无线使用控制

9.5.3.3.1 测评单元(L4-ABS5-06)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：无线通信网络及设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.3.3.2 测评单元(L4-ABS5-07)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：无线通信网络及设备。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.3.3 测评单元(L4-ABS5-08)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：无线通信网络及设备。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.3.4 测评单元(L4-ABS5-09)

该测评单元包括以下要求：

a) 测评指标：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行为。

b) 测评对象：无线通信网络及设备、监测设备。

c) 测评实施：应核查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告警并可以对试图接入的无线设备进行屏蔽。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.4 安全计算环境

9.5.4.1 控制设备安全

9.5.4.1.1 测评单元(L4-CES5-01)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)或 2)为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.4.1.2 测评单元(L4-CES5-02)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

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。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.4.1.3 测评单元(L4-CES5-03)

该测评单元包括以下要求：

a) 测评指标：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。

b) 测评对象：控制设备。

c) 测评实施包括以下内容：

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) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.4.1.4 测评单元(L4-CES5-04)

该测评单元包括以下要求：

a) 测评指标：应使用专用设备和专用软件对控制设备进行更新。

b) 测评对象：控制设备。

c) 测评实施：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。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.4.1.5 测评单元(L4-CES5-05)

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：控制设备。
c) 测评实施：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。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.5 安全建设管理

9.5.5.1 产品采购和使用

9.5.5.1.1 测评单元（L4-CMS5-01）

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：安全管理员和检测报告类文档。
c) 测评实施包括以下内容：
   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。
d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.5.2 外包软件开发

9.5.5.2.1 测评单元（L4-CMS5-02）

该测评单元包括以下要求：

a) 测评指标：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。
b) 测评对象：外包合同。
c) 测评实施：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。
d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

10 第五级测评要求

略。

11 整体测评

11.1 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。

安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。

安全控制点间安全测评是指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。

区域间安全测评是指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。

11.2 安全控制点测评

在单项测评完成后，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，否则为不符合或部分符合。

11.3 安全控制点间测评

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。

11.4 区域间测评

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。

12 测评结论

12.1 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对定级对象造成的安全风险。

12.2 等级测评结论

等级测评报告应给出等级保护对象的等级测评结论，确认等级保护对象达到相应等级保护要求的程度。

应结合各类的测评结论和对单项测评结果的风险分析给出等级测评结论：

a) 符合：定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。

b) 基本符合：定级对象中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于阈值。

c) 不符合：定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题会导致定级对象面临高等级安全风险，或者中低风险所占比例超过阈值。

附 录 A
（资料性附录）
测 评 力 度

A.1 概述

测评力度是在等级测评过程中实施测评工作的力度，体现为测评工作的实际投入程度，具体由测评的广度和深度来反映。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多。测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的工作投入。投入越多，测评力度就越强，测评效果就越有保证。

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法，涉及访谈、核查和测试等三种基本测评方法。三种基本测评方法的测评力度可以通过其测评的深度和广度来描述：

——访谈深度：分别为简要、充分、较全面和全面等四种。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。

——访谈广度：体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。

——核查深度：分别为简要、充分、较全面和全面等四种。简要核查主要是对功能性的文档、机制和活动，使用简要的评审、观察或核查以及核查列表和其他相似手段的简短测评；充分核查有详细的分析、观察和研究，除了功能性的文档、机制和活动外，还适当需要一些总体或概要设计信息；较全面核查有详细、彻底分析、观察和研究，除了功能性的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面核查有详细、彻底分析、观察和研究，除了功能性的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。

——核查广度：核查的广度体现在核查对象的种类（文档、机制等）和数量上。核查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。

——测试深度：测试的深度体现在执行的测试类型上，包括功能测试、性能测试和渗透测试。功能测试和性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入等级保护对象。

——测试广度：测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。

A.2 等级测评力度

为了检验不同级别的等级保护对象是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。测评的广度和深度落实到访谈、核查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、核查和测试的投入程度的不同。第一级到第四级等级保护对象的测评力度反映在访谈、核查和测试等三种基本测评方法的测评广度和深度上，落实在不同单项测评中具体的测评实施上。

表 A.1 从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同级别的等级保护对象安全测评中的具体体现。

表 A.1　不同级别的等级保护对象的测评力度要求

测评力度	测评方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

从表 A.1 可以看到，对不同级别的等级保护对象进行等级测评时，选择的测评对象的种类和数量是不同的，随着等级保护对象安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同级别的等级保护对象进行等级测评时，实际抽查测评对象的种类和数量，应当达到表 A.1 的要求，以满足相应等级的测评力度要求。在确定测评对象时，需遵循以下原则：

——重要性，应抽查对被测定级对象来说重要的服务器、数据库和网络设备等；

——安全性，应抽查对外暴露的网络边界；

——共享性，应抽查共享设备和数据交换平台/设备；

——全面性，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型；

——符合性，选择的设备、软件系统等应能符合相应等级的测评强度要求。

附 录 B
（资料性附录）
大数据可参考安全评估方法

B.1 第一级安全评估方法

B.1.1 安全通信网络

B.1.1.1 测评单元（BDS-L1-01）

该测评单元包括以下要求：

a） 测评指标：应保证大数据平台不承载高于其安全保护等级的大数据应用。

b） 测评对象：大数据平台和业务应用系统定级材料。

c） 测评实施：应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料，大数据平台安全保护等级是否不低于其承载的业务应用系统。

d） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

B.1.2 安全计算环境

B.1.2.1 测评单元（BDS-L1-01）

该测评单元包括以下要求：

a） 测评指标：大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。

b） 测评对象：数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。

c） 测评实施包括以下内容：

1） 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施；

2） 应测试验证身份鉴别措施是否能够不被绕过。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.1.3 安全建设管理

B.1.3.1 测评单元（BDS-L1-01）

该测评单元包括以下要求：

a） 测评指标：应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。

b） 测评对象：大数据应用建设负责人、大数据平台资质及安全服务能力报告和大数据平台服务合同等。

c） 测评实施包括以下内容：

1） 应访谈大数据应用建设负责人，所选择的大数据平台是否满足国家的有关规定；

2） 应查阅大数据平台相关资质及安全服务能力报告，是否大数据平台能为其所承载的大数

据应用提供相应等级的安全保护能力；

3） 应核查大数据平台提供者的相关服务合同，是否大数据平台提供了其所承载的大数据应用相应等级的安全保护能力。

d） 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2 第二级安全评估方法

B.2.1 安全物理环境

B.2.1.1 测评单元（BDS-L2-01）

该测评单元包括以下要求：

a） 测评指标：应保证承载大数据存储、处理和分析的设备机房位于中国境内。

b） 测评对象：大数据平台管理员和大数据平台建设方案。

c） 测评实施包括以下内容：

1） 应访谈大数据平台管理员大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件是否均位于中国境内；

2） 应核查大数据平台建设方案中是否明确大数据平台的存储节点、处理节点、分析节点和大数据管理平台等承载大数据业务和数据的软硬件均位于中国境内。

d） 单元判定：如果 1）和 2）均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

B.2.2 安全通信网络

B.2.2.1 测评单元（BDS-L2-01）

该测评单元包括以下要求：

a） 测评指标：应保证大数据平台不承载高于其安全保护等级的大数据应用。

b） 测评对象：大数据平台和业务应用系统定级材料。

c） 测评实施：应核查大数据平台和大数据平台承载的大数据应用系统相关定级材料，大数据平台安全保护等级是否不低于其承载的业务应用系统。

d） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

B.2.3 安全计算环境

B.2.3.1 测评单元（BDS-L2-01）

该测评单元包括以下要求：

a） 测评指标：大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。

b） 测评对象：数据采集终端、导入服务组件、业务应用系统、数据管理系统和系统管理软件等。

c） 测评实施包括以下内容：

1） 应核查数据采集终端、用户或导入服务组件、数据导出终端、数据导出服务组件在登录时是否采用了身份鉴别措施；

2） 应测试验证身份鉴别措施是否能够不被绕过。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.2 测评单元(BDS-L2-02)

该测评单元包括以下要求：

a) 测评指标：大数据平台应能对不同客户的大数据应用实施标识和鉴别。

b) 测评对象：大数据平台、大数据应用系统和系统管理软件等。

c) 测评实施包括以下内容：

1) 应核查大数据平台是否对大数据应用实施身份鉴别措施；

2) 应测试验证身份鉴别措施是否能够不被绕过。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.3 测评单元(BDS-L2-03)

该测评单元包括以下要求：

a) 测评指标：大数据平台应为大数据应用提供管控其计算和存储资源使用状况的能力。

b) 测评对象：大数据平台和大数据应用。

c) 测评实施包括以下内容：

1) 应核查大数据平台是否为大数据应用提供计算和存储资源管控的模块；

2) 应建立大数据应用测试账户，核查大数据平台是否支持计算和存储资源监测和管控功能。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.4 测评单元(BDS-L2-04)

该测评单元包括以下要求：

a) 测评指标：大数据平台应对其提供的辅助工具或服务组件，实施有效管理。

b) 测评对象：辅助工具、服务组件和大数据平台。

c) 测评实施包括以下内容：

1) 应核查提供的辅助工具或服务组件是否可以进行安装、部署、升级和卸载等；

2) 应核查提供的辅助工具或服务组件是否提供日志；

3) 应核查大数据平台是否采用技术手段或管理手段对辅助工具或服务组件进行统一管理，避免组件冲突。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.5 测评单元(BDS-L2-05)

该测评单元包括以下要求：

a) 测评指标：大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行。

b) 测评对象：设计文档、建设文档、计算节点和存储节点。

c) 测评实施包括以下内容：

1) 应核查设计文档或建设文档等是否具备屏蔽计算、内存、存储资源故障的措施和技术手段；

2) 应测试验证单一计算节点或存储节点关闭时，是否不影响业务正常运行。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.6 测评单元(BDS-L2-06)

该测评单元包括以下要求：

a) 测评指标：大数据平台应提供静态脱敏和去标识化的工具或服务组件技术。

b) 测评对象：设计或建设文档、大数据应用和大数据平台。

c) 测评实施包括以下内容：

1) 应核查大数据平台设计或建设文档是否具备数据静态脱密和去标识化措施或方案，如核查工具或服务组件是否具备配置不同的脱敏算法的能力；

2) 应核查静态脱敏和去标识化工具或服务组件是否进行了策略配置；

3) 应核查大数据平台是否为大数据应用提供静态脱敏和去标识化的工具或服务组件技术；

4) 应测试验证脱敏后的数据是否实现对敏感信息内容的屏蔽和隐藏，验证脱敏处理是否具备不可逆性。

d) 单元判定：如果 1)～4)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.3.7 测评单元(BDS-L2-07)

该测评单元包括以下要求：

a) 测评指标：对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理。

b) 测评对象：大数据平台、大数据应用系统、数据管理系统和系统设计文档等。

c) 测评实施包括以下内容：

1) 应核查是否由授权主体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) 应测试验证是否不存在可越权访问情形。

d) 单元判定：如果 1)～3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

B.2.4 安全建设管理

B.2.4.1 测评单元(BDS-L2-01)

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。

b) 测评对象：大数据应用建设负责人、大数据平台资质及安全服务能力报告和大数据平台服务合同等。

c) 测评实施包括以下内容：

1) 应访谈大数据应用建设负责人，所选择的大数据平台是否满足国家的有关规定；

2) 应查阅大数据平台相关资质及安全服务能力报告，是否大数据平台能为其所承载的大数据应用提供相应等级的安全保护能力；

3) 应核查大数据平台提供者的相关服务合同，是否大数据平台提供了其所承载的大数据应用相应等级的安全保护能力。