ICS 35.030
CCS L 70

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T XXXXX—XXXX

电信网和互联网网络安全能力成熟度评价方法

Maturity assessment method for cybersecurity capability of telecom network and internet

(点击此处添加与国际标准一致性程度的标识)

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中电信数智科技有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、上海观安信息技术股份有限公司、长扬科技（北京）股份有限公司、北京长亭未来科技有限公司、华为技术有限公司。

本文件主要起草人：孟楠、赵泰、张思齐、蒋敏慧、赵爽、孙念、邱勤、李海明、王娜、徐赵虎、张静、欧阳周婷、谢江、张亚京、全政、邵萌。

电信网和互联网网络安全能力成熟度评价方法

1 范围

本文件规定了电信网和互联网网络安全能力成熟度的评价流程、评价方法和成熟度等级判定方法。

本文件适用于指导电信网和互联网网络运营者和第三方安全评价机构开展电信网和互联网网络安全能力成熟度评价活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T XXXXX 电信网和互联网网络安全能力成熟度评价模型

3 术语和定义

YD/T XXXXX界定的术语和定义适用于本文件。

4 概述

4.1 基本原则

4.1.1 分级递进原则

电信网和互联网网络安全能力成熟度评价应按照YD/T XXXXX中定义的5个成熟度等级，实施分等级、累计递进的网络安全能力成熟度评价。

4.1.2 全面参与原则

电信网和互联网网络安全能力成熟度评价应由各利益相关者全面参与，包括受评价方负责资源分配和风险管理的高层管理者、负责各能力域相关资源运作的负责人、协调人以及相关的安全管理人员、实施人员和各类支撑人员等。

4.1.3 经济性原则

测评结果可复用原则，电信网和互联网网络安全能力成熟度评价可采信符合性评测的结果，涉及企业层面的测评项，如已针对其他网络类型开展过成熟度评价，部分测评项结果可复用。

4.2 基本流程

电信网和互联网网络安全能力成熟度评价流程包括评价准备、评价计划、评价实施、评价分析、评价报告五个环节，基本评价流程如图1所示。

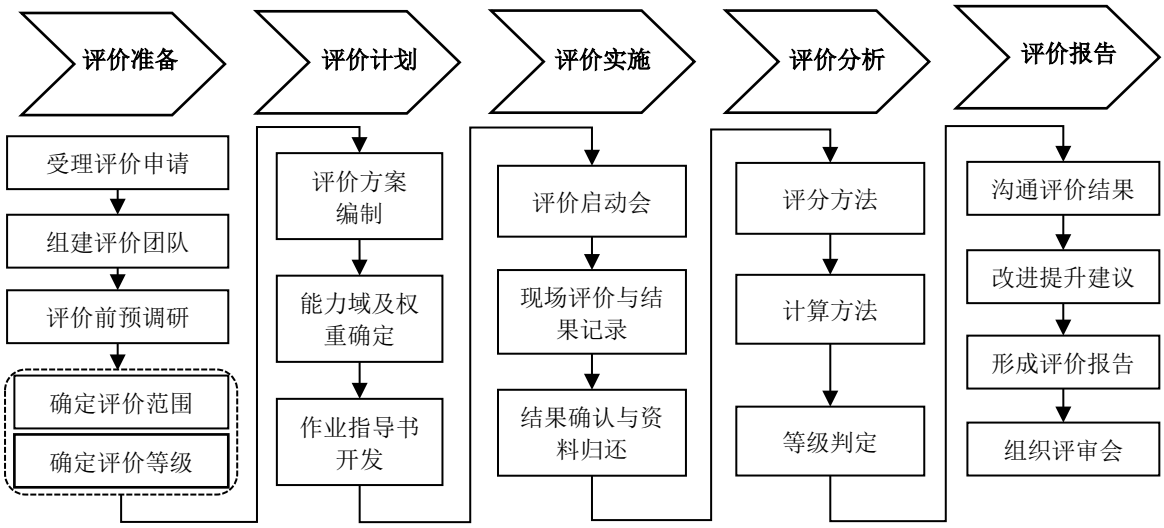


图1　电信网和互联网网络安全能力成熟度评价流程

4.3　相关角色

为确保网络安全能力成熟度评价工作的顺利有效进行，应采用合理的管理机制，其中主要相关角色和职责应与表1、表2相符合。

表1　评价方主要角色与职责说明

评价方 主要人员角色	工作职责
组长	作为网络安全能力成熟度评价实施方的管理者、责任人，具体工作职责包括： a)　根据受评价方所提交申请材料，组建评价团队； b)　根据受评价方所提交申请材料，与受评价方共同确定评价范围和评价等级，并组织评价团队成员对受评价方展开评价前预调研； c)　根据评价范围、评价等级及预调研情况，组织编写评价方案； d)　组织评价团队成员开展各阶段评价工作，并对实施过程进行监督、协调和控制，确保各阶段工作的有效实施； e)　与受评价方进行及时有效的沟通，及时商讨项目进展状况及可能发生问题的预测等； f)　组织评价团队成员将各阶段评价工作成果进行汇总，编写评价报告等项目成果物； g)　负责将项目成果物移交受评价方，向受评价方汇报项目成果，并提请验收。
评价人员	作为网络安全能力成熟度评价实施方负责技术方面评价工作的实施人员，具体工作职责包括： a)　根据确定的评价范围与评价等级参与评价前预调研，主要负责技术部分工作； b)　参与编写评价方案； c)　遵照评价方案实施各阶段具体的技术性评价工作； d)　对评价工作中遇到的问题及时向组长汇报，并提出需要协调的资源； e)　将各阶段的技术性评价工作成果进行汇总，参与编写评价报告等项目成果物； f)　负责向受评价方解答项目成果物中有关技术性细节问题。
专家团队	即专家组，针对大型复杂的评价项目，应考虑在评价期间聘请相关领域的专家对关键评价阶段进行工作指导，具体工作职责包括：

评价方 主要人员角色	工作职责
	a) 帮助受评价方和评价方规划总体工作思路和方向； b) 参与评价方案的确定； c) 对指标权重进行赋值； d) 对评价结果进行研判； e) 对出现的关键性难点问题进行决策。

表2 受评价方主要角色与职责说明

受评价方 主要人员角色	工作职责
负责人	作为网络安全能力成熟度受评价方的管理者、责任人，具体工作职责包括： a) 控制本组织的资源分配和风险管理工作； b) 与评价团队的组长进行工作协调； c) 组织本组织成员在各阶段评价活动中的配合工作； d) 组织本组织成员对提交给评价方的评价信息、数据及文档资料等进行确认，并对出现的偏离及时指正； e) 组织本组织成员对评价方提交的评价报告等项目成果物进行审阅； f) 组织对评价项目进行验收； g) 可授权协调人负责各阶段性工作，代理实施自己的职责。
协调人	作为网络安全能力成熟度受评价方的工作协调人员，具体工作职责是负责与受评价方各级部门之间的信息沟通，及时协调、调动相关部门的资源，包括工作场地、物资、人员等，以保障项目的顺利开展。
安全管理人员	通常为受评价方的安全管理人员，在评价活动中的具体工作职责包括： a) 在负责人的安排下，配合评价方在各阶段的评价工作； b) 参与对评价方提交的评价方案进行研讨； c) 参与对评价方提交的评价信息、数据及文档资料等进行确认，及时指正出现的偏离； d) 参与对评价方提交的评价报告等项目成果物进行审阅； e) 参与对评价项目的验收。
实施人员	包括业务人员、运维人员、开发人员等，具体工作职责包括： a) 在负责人的安排下，配合评价方在评价各阶段中的工作； b) 参与对评价方提交的评价方案进行研讨； c) 参与对评价方提交的评价信息、数据及文档资料等进行确认，及时指正出现的偏离； d) 参与对评价方提交的评价报告等项目成果物进行审阅； e) 参与对评价项目的验收。
其他支撑人员	包括行政人员、技术支持人员等，负责维护保障各阶段评价活动的顺利开展。

4.4 成熟度等级

成熟度模型定义了五个成熟度等级，成熟度等级独立适用于每个能力域。根据运营者能力实际情况，不同能力域的成熟度等级可能不同，例如，运营者可能在A能力域为成熟度二级、在B能力域为成熟度三级、在C能力域为成熟度四级。

成熟度等级在每个能力域是累积的。为了在给定能力域获得某成熟度等级，运营者必须满足该级别及其前面级别的所有要求，例如，运营者必须满足某能力域中成熟度一级和成熟度二级所有要求，才能获得该能力域成熟度二级的判定。

5 评价准备

5.1 受理评价申请

评价机构对运营者所提交的申请材料进行评审，确定运营者所从事的活动符合相关法律法规规定，根据运营者所申请的评价范围、评价等级及其他影响评价活动的因素，综合确定是否受理评价申请。

5.2 组建评价团队

应组建一个有经验、经过培训、具备评价能力的评价团队实施现场评价活动：

a） 评价团队应掌握《电信网和互联网网络安全能力成熟度评价模型》的评价内容和逐项评价方法；

b） 评价团队中应包含网络安全管理、网络安全技术和网络安全运营方面的专家；

c） 应确认一名评价组长及多名评价组员，评价人员数量应为奇数。

注：相关角色及职责说明见4.3。

5.3 评价前预调研

评价前预调研是了解、熟悉被评价对象的过程，评价团队应对运营者进行充分调研，以确定评价范围、评价等级等内容。调研活动应围绕运营者的需求：

a） 了解运营者基本情况；

b） 收集分析运营者可提供的直接或间接证据，如符合性评测结果等；

c） 确定正式评价实施的可行性。

评价前预调研可采用问卷调查、现场面谈等相结合的方式进行。

5.4 确定评价范围

网络安全能力成熟度评价的对象为网络运营者，评价范围包含运营单位内网络信息系统相关的所有物理机房、网络设备、安全设备、服务器/存储设备、终端/现场设备、系统管理软件/平台、业务应用系统/平台、数据、安全相关人员、安全管理文档等。

应结合评价前预调研情况，确定网络安全能力成熟度评价范围，分析各能力域的范围、特点及各设备或组件的主要功能，合理定义评价对象和评价范围边界，确定出本次评价的评价范围，可参考以下依据作为评价范围边界的划分原则：

a） 业务系统的业务逻辑边界；

b） 网络及设备载体边界；

c） 物理环境边界；

d） 组织管理权限边界；

e） 其他。

5.5 确定评价等级

根据运营者申请的评价等级，结合评价对象的业务重要性，社会影响力、规模和服务范围，评价双方共同确定评价等级。

6 评价计划

6.1 评价方案编制

评价方案是评价工作实施的基础，用于指导开展评价实施活动，使评价各阶段工作可控，应在评价活动实施前编制评价方案，并与运营者确认。评价方案的内容应包括：

a) 评价工作框架：包括评价目标、评价范围、评价任务等；
b) 评价团队组成：包括评价团队成员、角色及职责，如有必要还应包括专家组介绍等；
c) 评价工作计划：包含各阶段评价工作内容、工作形式、工作成果以及评价日程安排等；
d) 工具测试方法：介绍测试工具，包括漏洞扫描工具、渗透测试工具、协议分析工具等，结合实际网络拓扑结构，描述测试工具的接入点、测试目的、测试路径、测试对象等内容；
e) 风险规避措施：包括保密协议、评价工作环境要求、评价方法选择、应急预案等。

6.2 能力域及权重确定

根据运营者评价目标，结合评价前预调研情况，分析受评价方管理流程、业务流程、数据流程、技术措施、应急措施、处置措施、监管措施等实际情况，对10个网络安全关键能力域进行裁剪，从中确定出本次评价的能力域并确定权重。

能力域权重应根据评价前预调研情况，合理分析受评价方所涉及的能力域及各域的重要程度，确定不同能力域的权重。能力域不同评价对象也应根据网络位置、安全功能、业务重要性等确定不同的评价指标权重。能力域及推荐权重相关示例见附录A。

6.3 作业指导书开发

作业指导书是具体指导评价人员如何进行评价活动的文档，要求内容尽可能详实、充分。不同的评价对象应编制不同的作业指导书，作业指导书的内容应包括：

a) 适用范围；
b) 有关术语定义；
c) 评价内容；
d) 评价工作流程；
e) 评价工作的组织；
f) 评价中产生的相关文档和记录。

7 评价实施

7.1 评价启动会

本任务主要是与评价委托方充分沟通评价内容、配合需求及评价工作方式等内容，是保障评价工作顺利实施的前提，旨在确定工作目标、统一思想、协调各方资源，确保相关方对评价计划安排达成一致，并确保评价活动可执行。

输入：经过评审和确认的评价方案、风险规避实施方案、风险告知书、现场评价工作计划。

任务描述：

a) 评价启动会一般由评价组长组织召开，参与人员应包括评价团队全体成员、运营者高管、负责人、协调人等，如有必要可邀请相关专家组成员参加；
b) 运营者高管宣布此次评价工作的意义、目的、目标以及评价工作中的责任分工；
c) 运营者负责人说明此次评价工作的计划和各阶段工作任务，以及需配合的具体事项；

d) 评价团队组长介绍评价工作一般性方法和工作内容，确定评价日程以及明确其他需要提前沟通的事项，并签署现场评价授权书；

e) 运营者对风险告知书签字确认，了解评价过程中存在的安全风险，做好数据备份和应急响应等支撑工作。

输出/产品：会议记录、评价方案、现场评价工作计划、现场评价授权书、风险告知书等。

7.2 现场评价与结果记录

本任务主要是评价方按照工作计划和作业指导书开展实施评价，并将评价过程中获取的证据源进行详细、准确记录。现场评价工作方式主要包括访谈、核查和测试。

7.2.1 访谈

输入：现场评价工作计划、作业指导书、网络安全能力成熟度现场评价结果记录表格。

任务描述：评价人员与被定级对象有关人员(个人/群体)进行交流、讨论等活动，获取相关证据，了解有关信息。针对不同评价等级对象在访谈范围上有一定区别，一般应基本覆盖所有的安全相关人员类型,在数量上抽样。具体可参照《电信网和互联网网络安全能力成熟度评价模型》要求各部分标准中的各级要求。

输出/产品：网络安全能力成熟度现场评价结果记录。

7.2.2 核查

核查可细分为文档审查、实地察看和配置核查等几种具体方法。

7.2.2.1 文档审查

输入：现场评价工作计划、安全策略、安全方针文件、安全管理制度、安全管理的执行过程文,系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档、作业指导书、网络安全能力成熟度现场评价结果记录表格。

任务描述：

a) 核查《电信网和互联网网络安全能力成熟度评价模型》中确定的制度、策略、操作规程等文档是否齐备；

b) 核查是否有完整的制度执行情况记录,如机房出入登记记录、电子记录、关键设备的使用登记记录等；

c) 核查安全策略以及技术相关文档是否明确说明相关技术要求实现方式；

d) 对上述文档进行审核与分析,核查他们的完整性和这些文件之间的内部一致性。

输出/产品：网络安全能力成熟度现场评价结果记录。

7.2.2.2 实地察看

输入：作业指导书、网络安全能力成熟度现场评价结果记录表格。

任务描述：根据被评价定级对象的实际情况，评价人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况,评价其是否符合相应等级的安全要求。

输出/产品：网络安全能力成熟度现场评价结果记录。

7.2.2.3 配置核查

输入：作业指导书、网络安全能力成熟度现场评价结果记录表格。

任务描述：

a） 根据评价结果记录表格内容，利用上机验证的方式核查应用系统、主机系统、数据库系统以及各设备的配置是否正确，是否与文档、相关设备和部件保持一致,对文档审核的内容进行核实(包括日志审计等)；

b） 如果系统在输入无效命令时不能完成其功能，应测试其是否对无效命令进行错误处理；

c） 针对网络连接，应对连接规则进行验证。

输出/产品：网络安全能力成熟度现场评价结果记录。

7.2.3 测试

输入：现场评价工作计划、作业指导书、网络安全能力成熟度现场评价结果记录表格。

任务描述：

a） 根据作业指导书，利用技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透测试、功能测试、性能测试、入侵检测和协议分析等；

b） 备份测试结果。

输出/产品：网络安全能力成熟度现场评价结果记录。

7.3 结果确认与资料归还

本任务主要是将评价过程中得到的证据源记录进行确认，并将评价过程中借阅的文档归还。

输入：各类评价结果记录，工具测试完成后的电子输出记录。

任务描述：

a） 评价团队应首先汇总现场评价记录，对漏掉和需要进一步验证的内容实施补充评价；

b） 评价双方应对评价过程中得到的证据源记录进行现场沟通和确认；

c） 评价团队应归还评价过程中借阅的所有文档资料，并由运营者文档资料提供者签字确认。

输出/产品：经过运营者确认的评价证据和证据源记录。

8 评价分析

8.1 评分方法

评价团队应结合评价前预调研和现场评价情况，对照《电信网和互联网网络安全能力成熟度评价模型》中关于各等级能力成熟度要求，应按照表3给出的对应关系，对能力域每项要求的满足程度进行评分。

表3 成熟度要求满足程度与评分对应表

成熟度要求满足程度	评分
全部满足	1
大部分满足	0.8
部分满足	0.5
不满足	0

8.2 计算方法

能力子域得分(S)为该能力子域下每项具体要求得分的算术平均值，能力子域得分的计算见公式（1）：

$$S=\frac{1}{n}\sum_{1}^{n}X \qquad \cdots\cdots(1)$$

式中：

S——能力子域得分；

X——能力子域各项要求评分；

n——能力子域要求个数。

能力域得分(D)为该能力域下能力子域得分的加权求和，能力域得分的计算见公式（2）：

$$D=\sum(S\times\gamma) \qquad \cdots\cdots(2)$$

式中：

D——能力域得分；

S——能力子域得分；

γ ——能力子域权重。

能力成熟度等级得分(M)为该等级下各项能力域得分的加权求和，能力成熟度等级得分的计算见公式（3）：

$$M_i=\sum(D\times\alpha) \qquad \cdots\cdots(3)$$

式中：

M——能力成熟度等级得分；

D——能力域得分；

α——能力域权重。

能力成熟度等级赋值得分($\overline{\mathrm{M}}$)为能力成熟度等级得分(M)赋值后的得分。在计算过程中，为了客观反映某一级别(i)的成熟度得分，第i级别能力成熟度等级赋值得分为该级别实际得分，第i级别以下的第k级别(1,2,…,i-1)成熟度等级得分达到0.8赋值为1，反之取该级别实际得分，能力成熟度等级赋值得分的计算见公式（4）：

$$\overline{M_i}=M_{\mathrm{i}} \quad ; \quad \overline{M_k}=\begin{cases}1 & , M_k\geq 0.8\\ M_k & , M_k<0.8\end{cases} \qquad \cdots\cdots(4)$$

式中：

$\overline{M}$ ——能力成熟度等级赋值得分；

M——能力成熟度等级得分。

能力成熟度总体得分(T)为能力成熟度等级得分($\overline{\mathrm{M}}$)的累计求和，能力成熟度总体得分的计算见公式（5）：

$$T=\sum\overline{M_{\mathrm{i}}} \qquad \cdots\cdots(5)$$

式中：

T——能力成熟度总体得分；

$\overline{M}$——能力成熟度等级赋值得分。

8.3 等级判定

应按照表4给出的能力成熟度评分结果与成熟度等级的对应关系，根据成熟度总体得分(T)判断运营者当前所处的成熟度等级。成熟度总体得分计算与等级判定相关示例见附录B。

表4 成熟度等级与分数的对应关系

成熟度等级	分数区间(T)
一级（初始级）	[0.8,1.8)
二级（控制级）	[1.8,2.8)

成熟度等级	分数区间(T)
三级（规范级）	[2.8,3.8)
四级（优化级）	[3.8,4.8)
五级（卓越级）	[4.8,5.0]

9 评价报告

9.1 沟通评价结果

评价活动结束后，评价团队应对现场评价结果进行汇总分析，评价双方应对评价结果进行沟通和确认，确认无误后形成能力成熟度评价等级结论，评价团队编制形成评价报告中评价等级结论部分内容。

9.2 改进提升建议

针对评价对象当前能力与行业平均以及理想状态之间存在的差距，结合实际情况，提出相应改进建议，由运营者审核其可行性，经审核无异议，评价团队编制形成评价报告中改进提升建议部分内容。

9.3 形成评价报告

评价报告中可包括如下内容：

a) 网络安全能力成熟度评价等级结论；
b) 整体视图：直观展示运营者当前能力与行业平均、理想状态之间存在的差距，整体视图相关示例见附录C.1；
c) 对比视图：直观展示运营者在制度、人员、技术方面采取创新行动前后能力的变化，对比视图相关示例见附录C.2；
d) 能力域视图：直观展示运营者在各等级下个能力域表现情况；
e) 能力子域视图：直观展示运营者在能力域下各能力子域表现情况；
f) 改进提升建议。

9.4 组织评审会

组织评审会的目的包括：

a） 总结评价过程；
b） 发布评价发现和评价结果；
c） 对评价报告进行论证及评审。

评审会的内容至少应包括评价活动总结、评价结果、评价强项、评价弱项、改进方向以及后续相关能力提升建议等。

附 录 A
（资料性）
能力域及权重（示例）

表A.1给出了能力域及权重相关示例。

表A.1 能力域及权重（示例）

序号	能力域	能力域权重	能力子域	能力子域权重
1	制度管理	10%	网络安全规划	50%
			网络安全管理制度	50%
2	组织和人员管理	10%	组织机构及人员岗位	25%
			人力资源管理	25%
			教育培训及考核	25%
			沟通与合作	25%
3	资产管理	10%	资产清单管理	40%
			资产日常管理和维护	30%
			资产变更管理	30%
4	风险管理	10%	风险控制	50%
			风险识别和防范	50%
5	供应链安全管理	10%	供应链安全风险管理	50%
			采购情况管理	50%
6	系统和通信防护	10%	身份管理	30%
			访问控制	30%
			系统和边界防护	40%
7	运行维护	10%	安全运维	25%
			状态监控	25%
			日志及审计	25%
			备份和恢复	25%
8	检测评估	10%	检测评估	100%
9	安全态势分析	10%	漏洞管理	30%
			威胁信息管理	30%
			态势感知	40%
10	网络安全事件管理	10%	事件响应和处置	50%
			应急演练	50%

附 录 B
（资料性）
能力成熟度总体得分与等级判定（示例）

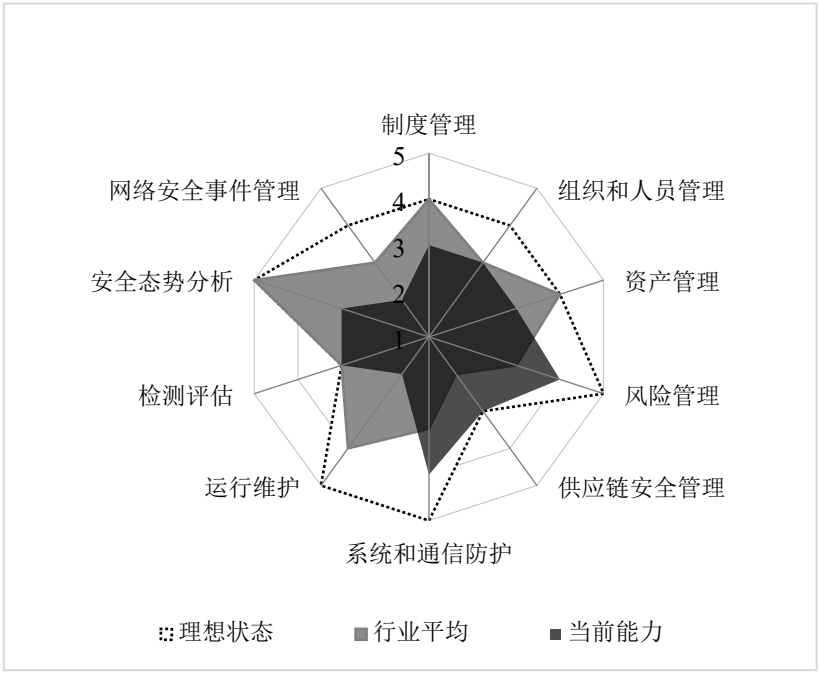
表B.1给出了能力成熟度总体得分与等级判定（示例）。如评价对象A的一、二、三级成熟度等级得分分别是0.9、0.85，0.6，该对象成熟度总分为1+1+0.6=2.6，判定该对象成熟度等级为二级（控制级）；评价对象B的一、二、三级成熟度等级得分分别是0.95、0.8，0.8，该对象成熟度总分为1+1+0.8=2.8，判定该对象成熟度等级为三级（规范级）。

表B.1 成熟度总体得分与等级判定（示例）

示例	能力成熟度等级得分(M)	成熟度总体得分(T)	等级判定
评价对象A （申请评价等级为三级）	能力成熟度一级得分为0.9 能力成熟度二级得分为0.85 能力成熟度三级得分为0.6	2.6（1+1+0.6）	二级（控制级）
评价对象B （申请评价等级为三级）	能力成熟度一级得分为0.95 能力成熟度二级得分为0.8 能力成熟度三级得分为0.8	2.8（1+1+0.8）	三级（规范级）

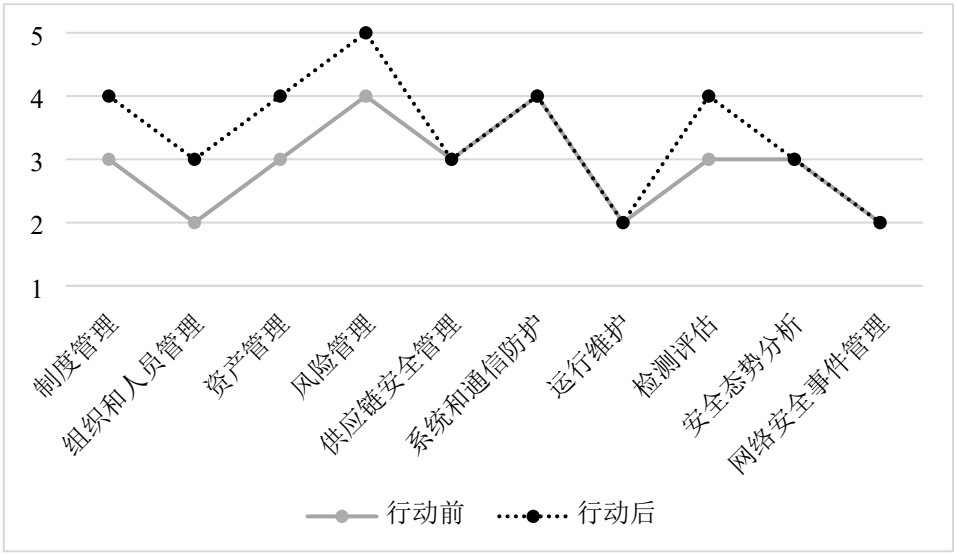
附 录 C
（资料性）
评价报告（示例）

图C.1给出了评价报告中整体视图相关示例。



图C.1 整体视图（示例）

图C.2给出了评价报告中对比视图相关示例。



图C.2 对比视图（示例）

参 考 文 献

[1] GB/T 20261-2020 信息技术 系统安全工程 能力成熟度模型

[2] GB/T 30271-2013 信息安全技术 信息安全服务能力评估准则

[3] GB/T 36073-2018 数据管理能力成熟度评估模型

[4] GB/T 37988-2019 数据安全能力成熟度模型

[5] GB/T 39116-2020 智能制造能力成熟度模型

[6] GB/T 39117-2020 智能制造能力成熟度评估方法

[7] Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC.Cybersecurity Maturity Model Certification.2020

[8] Office of Cybersecurity,Energy Security,and Emergency Response. Cybersecurity Capability Maturity Model.2021