



中华人民共和国金融行业标准

XX/T XXXXX—XXXX
代替

证券期货业网络安全能力成熟度模型

Cyber security capability maturity model of securities and futures
industry

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中国证券监督管理委员会

发布

目 次

前 言	2
1 范围	3
2 规范性引用文件.....	3
3 术语和定义	3
3.1 网络安全 cyber security	3
3.2 能力成熟度 capability maturity	3
3.3 能力成熟度模型 capability maturity model	3
3.4 安全过程 security process	4
3.5 能力域 capability domain	4
3.6 基本实践 base practice	4
4 缩略语	4
5 证券期货业网络安全能力成熟度模型.....	4
5.1 模型架构	4
5.2 能力成熟度等级维度.....	5
5.3 安全能力维度.....	6
5.4 安全过程维度.....	6
5.5 评分规则	7
6 网络安全能力成熟度评估.....	7
6.1 攻击预防能力（CD01）	7
6.2 安全加固能力（CD02）	11
6.3 事件检测能力（CD03）	20
6.4 事件响应能力（CD04）	25
6.5 诱捕溯源能力（CD05）	29
6.6 关联分析能力（CD06）	31
6.7 安全运营能力（CD07）	32
6.8 人员管理能力（CD08）	34
附 录 A	37
参 考 文 献	40

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。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国证券监督管理委员会科技监管司、郑州商品交易所、上海证券交易所、深圳证券交易所、中证信息技术服务有限责任公司、中信建投证券股份有限公司、国金证券股份有限公司、北京长亭科技有限公司、国泰君安期货有限公司、华安基金管理有限公司。

本文件主要起草人：.....。

证券期货业网络安全能力成熟度模型

1 范围

本文件规定了证券期货业网络安全能力成熟度模型，规定了攻击预防能力、安全加固能力、事件检测能力、事件响应能力、诱捕溯源能力、关联分析能力、安全运营能力和人员管理能力的成熟度等级要求，提出了能力成熟度等级核验方法。

本文件适用于证券期货行业机构（以下简称行业机构）进行实战化网络安全防护能力评估，也可作为行业机构开展网络安全防护能力建设时的依据。

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。

GB/T 25069-2010 信息安全技术 术语
GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南
JR/T 0171-2020 个人金融信息保护技术规范

3 术语和定义

GB/T 25069-2010和GB/T 37988—2019界定的术语和定义以及下列术语和定义适用于本文件。

3.1 网络安全 *cyber security*

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019，3.1]

3.2 能力成熟度 *capability maturity*

对一个行业机构有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

[来源：GB/T 37988-2019，3.6]

3.3 能力成熟度模型 *capability maturity model*

对一个行业机构的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或者模式。

能力成熟度模型为行业机构衡量其当前的实践、流程、方法的能力水平提供参考基准，并设置明确的提升目标。

[来源：GB/T 37988-2019, 3.7]

3.4 安全过程 security process

用于实现某一安全目标的完整过程，该过程包含输入和输出。

[来源：GB/T 37988-2019, 3.8]

3.5 能力域 capability domain

实现同一安全目标的相关网络安全基本实践的集合。

[来源：GB/T 37988-2019, 3.9]

3.6 基本实践 base practice

实现某一安全目标的网络安全相关活动。

[来源：GB/T 37988-2019, 3.10]

4 缩略语

下列缩略语适用于本文件。

CD：能力域（Capability Domain）

CSD：能力子域（Capability Sub-Domain）

SFI-CSMM模型：证券期货业网络安全能力成熟度模型（Cyber Security Capability Maturity Model of Securities and Futures Industry）

IT：信息技术（Information Technology）

VLAN：虚拟局域网（Virtual Local Area Network）

DMZ：非军事化区域（Demilitarized Zone）

5 证券期货业网络安全能力成熟度模型

5.1 模型架构

证券期货业网络安全能力成熟度模型 SFI-CSMM 架构见图1。

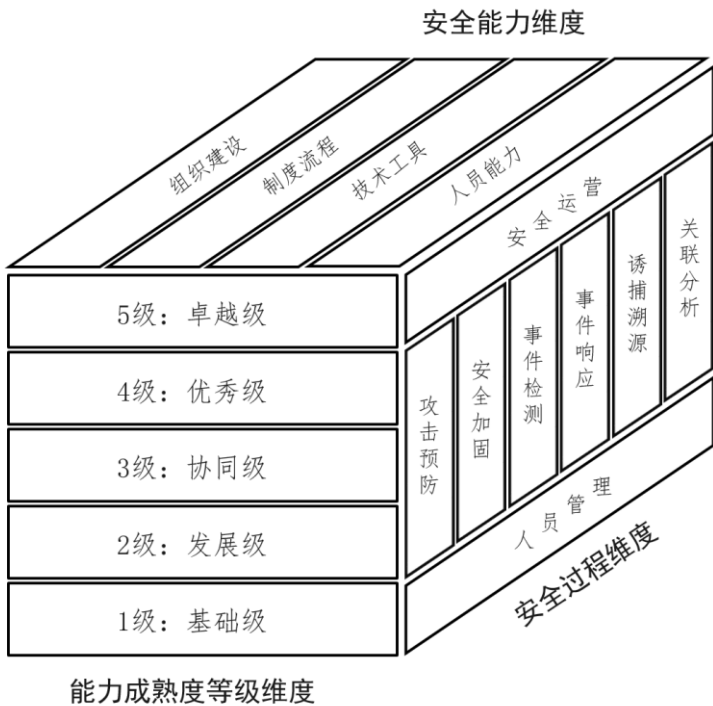


图1 证券期货业网络安全能力成熟度模型 SFI-CSMM 架构图

SFI-CSMM模型的架构由以下三个维度构成：

（1）能力成熟度等级维度

证券期货业网络安全能力成熟度划分为五级，具体包括：1级基础级，2级发展级，3级协同级，4级优秀级，5级卓越级。

（2）安全能力维度

明确行业机构应具备的四个方面能力，具体包括组织建设、制度流程、技术工具和人员能力。

（3）安全过程维度

明确行业机构网络安全生命周期安全管控的八个方面，具体包括攻击预防、安全加固、事件检测、事件响应、诱捕溯源、关联分析、安全运营、人员管理八个方面。

5.2 能力成熟度等级维度

行业机构网络安全能力成熟度共分为五级，各等级特征见表1。

表1 网络安全能力成熟度等级特征

能力成熟度等级	能力成熟度等级特征
等级1：基础级（L1）	行业机构在满足国家及行业法律法规要求的基础上，对于关键节点及重要环境仅通过实施有限的安全防护措施，做到应对已知风险的基础防护，但安全防护体系化不足，难以应对复杂问题。在发生重要业务运营中断事件后，能够快速恢复。
等级2：发展级（L2）	行业机构初步形成网络安全防护架构，检测和防护手段能做到因地制宜，开展规范化的安全防护工作，能够有效处置大部分业务的运营中断事件。

等级3：协同级（L3）	行业机构已具备较为完善的安全防护体系架构，并建立健全配套的组织架构、制度流程、技术工具和安全人员能力支撑，具备风险的自动化检测和纵深防御能力，能够有效处置绝大部分业务的运营中断事件。
等级4：优秀级（L4）	行业机构主动实施网络安全风险检测与分析，自动化的工作全面替代手工执行，侧重攻击方法学习和威胁情报收集，通过渗透测试、攻防演练、特征分析等以攻促防，积极参与国家与行业间安全风险防范联防联控。
等级5：卓越级（L5）	行业机构持续对网络安全防护能力现状进行分析评估，及时消除安全防护体系存在的问题和不足，持续提升网络安全能力，具备极限环境下的响应与恢复能力。

能力成熟度等级与能力域、能力子域、安全能力、基本实践的关系如下：

- 1) 将行业机构在每个网络安全能力子域的能力成熟度划分为五级，针对每个等级下应具备的基本实践要求，从4个安全能力（组织建设、制度流程、技术工具及人员能力）提出具体的基本实践要求；
- 2) 3级要求应包含全部4个安全能力，其他等级要求可不包含完整的4个网络安全能力；
- 3) 对于每个网络安全能力子域，高等级能力要求应包括所有低等级能力要求。针对某一具体网络安全能力子域，如果5级能力要求中未涉及某一关键能力的内容，则默认应达到4级能力要求中该关键能力的内容，如果4级能力要求中依旧未涉及该关键能力，则默认应达到3级能力要求中该关键能力的内容，以此类推。

5.3 安全能力维度

通过对行业机构在网络安全过程中应具备安全能力的量化，进而评估机构网络安全过程的实现能力，具体包括四个方面：

组织建设：行业机构内网络安全组织的设立、职责分工和沟通协作；

制度流程：行业机构内网络安全领域的制度和流程执行；

技术工具：通过技术手段和产品工具落实安全要求或自动化实现安全工作；

人员能力：行业机构内网络安全工作人员的安全意识及相关专业能力。

5.4 安全过程维度

安全过程是围绕网络安全生命周期的过程管控，具体分为以下八个方面：

攻击预防：预测可能的攻击方式和攻击者可能会利用的漏洞，采取措施减少被攻击的风险，具体包括漏洞预防能力、漏洞评估能力、漏洞修复能力、威胁预警能力、威胁评估能力和威胁抵御能力。

安全加固：针对系统和网络进行深入的安全配置和优化，以提高其抵御攻击的能力，具体包括账户与权限管理能力、安全配置管理能力、隔离技术、加密与签名管理能力、数据备份管理能力、功能简化能力、黑白名单管理能力、网络访问控制管理能力、认证管理能力、安全域管理能力、基线管理能力、日志管理能力、软件更新管理能力。

事件检测：利用各种工具和技术手段实时监控网络流量和系统活动，及时发现潜在的安全威胁，具体包括边界入侵检测能力、应用攻击检测能力、未知威胁发现能力、病毒与恶意软件检测能力、端点行为检测能力、流量检测能力。

事件响应：当检测到安全事件时，迅速启动预先制定的应急响应计划，以最小化损害并尽快恢复正常运行，具体包括边界入侵防御能力、应用攻击防护能力、防病毒与反恶意软件能力、端点行为防护能力、流量过滤能力。

诱捕溯源：在确保合法合规的前提下，对攻击源头进行追踪，确定攻击者的身份和位置，必要时采取法律行动，具体包括攻击诱捕能力、溯源取证能力。

关联分析：对收集到的各种安全事件数据进行综合分析以便更准确地判断攻击者的意图和下一步可能的动作，为后续的防御策略提供依据，具体包括策略分析能力和情报分析能力。

安全运营：持续不断地管理和优化组织的安全状况，确保所有安全措施的有效性和适应性，具体包括安全培训能力、安全对抗能力、安全运营规划能力。

人员管理：建立有效的人员安全意识培训、权限管理等制度，防止内部人员因疏忽或恶意行为导致的安全问题，具体包括人员安全策略管理能力、人员安全审计和监督能力、人员离职安全管理能力。

5.5 评分规则

整体评分框架总分100分，每项CSD能力成熟度分为L1-L5，分别对应0.5、1.0、1.5、2.0、2.5分。将所有单项CSD得分汇总相加后得到整体能力评分，整体级别与得分对应关系如下：

整体级别	得分范围
基础级（L1）	0分-30分
发展级（L2）	30.5分-50分
协同级（L3）	50.5分-70分
优秀级（L4）	70.5分-90分
卓越级（L5）	90.5分-100分

6 网络安全能力成熟度评估

6.1 攻击预防能力（CD01）

6.1.1 漏洞预防能力（CSD01.01）

漏洞预防能力是指通过采取措施避免系统中出现安全漏洞，以降低被攻击风险的能力。

能力等级标准如下：

a) 基础级（L1）

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的漏洞预防工作。

b) 发展级（L2）

1) 组织建设方面：具备专人或专岗负责漏洞预警工作的实施与跟进，并设定具体的职责。

2) 制度流程方面：

i. 建立基础性的漏洞预警识别机制和漏洞管理制度，包括但不限于从公开社区及第三方供应商处获取相关的漏洞信息；

ii. 初步构建获取最新漏洞情报的信息渠道，确保漏洞信息的来源多样化。

c) 协同级（L3）

1) 组织建设方面：组建专门的团队以专职承担漏洞预警工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：完善并维护获取最新漏洞情报的有效渠道，确保漏洞信息的及时性和有效性。

3) 技术工具方面：采用自动化的技术手段，对发布的漏洞预警信息进行集中管理和监控。

4) 人员能力方面：熟悉漏洞发现与评估、补丁管理与修复、安全开发与设计、访问控制与隔离威胁情报与监控、安全策略与培训等知识和技术，具备实施漏洞预防工作的能力。

d) 优秀级（L4）

- 1) 制度流程方面：建立包括社区、研究机构、知名安全厂商、互联网漏洞发布平台在内的多渠道获取最新漏洞信息的机制，确保漏洞信息的全面性和时效性。
 - 2) 技术工具方面：实现漏洞预警对组织内所有IT资产的全覆盖，且这些资产均来源于组织内正式的资产台账，确保预警的全面性和准确性。
- e) 卓越级 (L5)
- 1) 人员能力方面：人员具备根据漏洞情报分析出漏洞的影响面、特征和利用方式的能力，并可在安全设备上配置对应规则进行告警或拦截。

6.1.2 漏洞评估能力 (CSD01.02)

漏洞评估能力是指对系统、网络或应用程序中的潜在安全漏洞进行全面检测、分析和评级，以确定其严重性和优先级，为后续修复和管理提供依据的能力。

能力等级标准如下：

- a) 基础级 (L1)
- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的漏洞评估工作。
- b) 发展级 (L2)
- 1) 组织建设方面：具备专人或专岗负责漏洞评估工作，并设定具体的职责。
 - 2) 制度流程方面：建立初步的漏洞评估策略和标准，确保评估工作的规范化。
 - 3) 技术工具方面：采用标准化的管理工具，实现部分自动化评估功能。
- c) 协同级 (L3)
- 1) 组织建设方面：建立专门团队，获取最新漏洞的时效性信息，确保评估信息的及时性和准确性。
 - 2) 制度流程方面：建立较为完备的漏洞评估策略、标准以及机制，确保评估工作的全面性和有效性。
 - 3) 技术工具方面：采用自动化的技术手段，对漏洞信息进行集中管理和漏洞验证。
 - 4) 人员能力方面：熟悉漏洞发现与识别、风险评级与优先级划分、影响范围分析等知识和技术，具备实施漏洞评估工作的能力。
- d) 优秀级 (L4)
- 1) 组织建设方面：设定明确的工作目标，可严格按照漏洞修复时效性要求完成漏洞修复工作，并实施量化管理，如采用评估覆盖率、评估准确性等指标。
 - 2) 制度流程方面：新上线应用系统，在内部团队完成初次漏洞评估后，引入至少一家第三方厂商进行复核评估，确保评估结果的可靠性和准确性。
- e) 卓越级 (L5)
- 1) 技术工具方面：在漏洞评估过程中，具备依据原有的策略结合业务影响度、漏洞修复的难易程度及所需成本等因素建立定量评估模型的功能。
 - 2) 人员能力方面：团队成员具备丰富的安全攻防经验，能够准确判断漏洞的实际危害性和价值，并具备防御绕过的技能。

6.1.3 漏洞修复能力 (CSD01.03)

漏洞修复能力是指及时修复系统或软件中的安全漏洞，以消除安全隐患，确保系统安全稳定运行的能力。

能力等级标准如下：

- a) 基础级 (L1)
- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的漏洞修复工作。

b) 发展级 (L2)

- 1) 组织建设方面：具备专人或专岗负责漏洞修复工作，并设定具体的职责。
- 2) 制度流程方面：建立漏洞修复时效性的标准要求，确保漏洞修复的及时性。

c) 协同级 (L3)

- 1) 组织建设方面：建立专业的团队来负责或支持业务组的漏洞修复工作，且该团队具备相应的漏洞修复能力，确保修复工作的专业性和有效性。
- 2) 制度流程方面：建立完善的漏洞修复的流程机制，确保修复工作的规范化。
- 3) 技术工具方面：采用自动化的技术手段，对漏洞修复信息进行集中管理和监控。
- 4) 人员能力方面：具备实施关闭高危端口、限制应用访问权限、部署安全补丁等常见漏洞修复手段的能力，并能进行修复后验证，确保漏洞修复的有效性。

d) 优秀级 (L4)

- 1) 组织建设方面：建立漏洞修复的定期回顾和总结机制，持续改进修复策略，能够确保漏洞修复的有效性。

e) 卓越级 (L5)

- 1) 技术工具方面：基于业务需求，具备结合软件补丁、安全功能、安全设备、安全配置、人员意识等因素选择合适的修复方式及相应的组合措施的功能。
- 2) 人员能力方面：团队成员具备一定的攻防经验和软件开发能力，以及丰富的运维经验，能够深入理解和解决复杂的漏洞问题。

6.1.4 威胁预警能力 (CSD01.04)

威胁预警能力是指实时监测和分析潜在威胁，及时发出警报，以便采取应对措施的能力。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的威胁预警工作。
- 2) 人员能力方面：理解威胁预警的基本概念和方法，具备基本的威胁信息获取能力，可以从公开社区或第三方供应商处等获取相关的威胁信息。

b) 发展级 (L2)

- 1) 组织建设方面：具备专人或专岗负责威胁预警工作的实施与跟进，并设定具体的职责。
- 2) 制度流程方面：初步构建获取最新威胁情报的信息渠道，确保威胁信息的来源多样化。
- 3) 技术工具方面：采用标准化的威胁信息获取工具，实现部分自动化威胁预警功能。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队以专职承担威胁预警工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：完善并维护获取最新威胁情报的有效渠道，确保威胁信息的准确性和可靠性。
- 3) 技术工具方面：采用自动化的技术手段，对威胁信息进行集中管理和监控。
- 4) 人员能力方面：熟悉多源情报整合、实时数据采集等知识和技术，具备实施威胁预警工作的能力。

d) 优秀级 (L4)

- 1) 技术工具方面：能够实现威胁预警对组织内所有IT资产的全覆盖，且这些资产均来源于组织正式的资产台账，确保预警的全面性和准确性。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展安全威胁研究，并具备威胁分析与研究的能力，不断优化威胁预警方法和工具。

- 2) 制度流程方面：建立包括社区、研究机构、知名安全厂商、互联网威胁发布平台在内的多渠道获取最新威胁情报的机制，确保威胁信息的全面性和时效性。

6.1.5 威胁评估能力（CSD01.05）

威胁评估能力是指对检测到的威胁进行分析和评估，确定其严重性和潜在影响，为决策提供依据的能力。

能力等级标准如下：

a) 基础级（L1）

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的威胁评估工作。

b) 发展级（L2）

- 1) 组织建设方面：具备专人或专岗负责威胁预警工作的实施与跟进，并设定具体的职责。
- 2) 制度流程方面：建立初步的威胁评估策略和标准，确保评估工作的规范化。
- 2) 技术工具方面：采用标准化的威胁评估工具，实现部分自动化威胁评估功能。

c) 协同级（L3）

- 1) 组织建设方面：建立专门团队来负责威胁评估工作，且该团队具备相应的威胁评估能力，确保评估工作的专业性和有效性。
- 2) 制度流程方面：建立包含威胁评估分级分类标准、评估过程要求、评估频率要求等内容的威胁评估策略、标准和机制，确保评估工作的全面性和规范性。
- 3) 技术工具方面：采用自动化的技术手段，对威胁评估信息进行集中管理和监控。
- 4) 人员能力方面：熟悉情报管理分析、风险量化评级等知识和技术，具备实施威胁评估工作的能力。

d) 优秀级（L4）

- 1) 制度流程方面：将威胁评估常态化，并建立相应的评价体系，以动态评价评估效果，确保评估工作的持续改进。

e) 卓越级（L5）

- 1) 组织建设方面：团队成员具备丰富的安全攻防经验，精通二进制漏洞分析及调试技术，能够深入理解和应对复杂的威胁。
- 2) 技术工具方面：在威胁评估过程中，具备依据原有的策略结合业务影响度、威胁应对的难易程度及所需成本等因素建立定量评估模型的功能。

6.1.6 威胁防御能力（CSD01.06）

威胁防御能力是指采取措施阻止或减轻威胁对系统或网络的攻击，保护资源免受损害的能力。

能力等级标准如下：

a) 基础级（L1）

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的威胁防御工作。

b) 发展级（L2）

- 1) 制度流程方面：建立评估威胁防御效果的基本标准要求，确保抵御措施的有效性。
- 2) 技术工具方面：采用标准化的威胁防御工具，如防火墙、入侵检测系统等，实现部分自动化威胁防御功能。

c) 协同级（L3）

- 1) 组织建设方面：组建专门的团队以专职承担威胁防御工作的职责，且该团队具备常见威胁的知识、安全防护产品的使用能力，确保威胁防御工作的专业性和有效性。
- 2) 制度流程方面：建立威胁防御的流程机制，确保抵御工作的规范化。

3) 技术工具方面：采用自动化的技术手段，对威胁进行集中管理和监控。

4) 人员能力方面：熟悉防火墙、攻击检测与阻断、应急响应与恢复、安全管理与培训、物理安全等知识和技术，具备实施威胁防御工作的能力。

d) 优秀级 (L4)

1) 制度流程方面：与安全预防和加固能力建立联动机制，形成综合防御体系，确保安全措施协调性和一致性。

2) 技术工具方面：具备常见威胁的自动处置功能，如IP自动封禁与解封、恶意后门自动隔离与阻断。

e) 卓越级 (L5)

1) 技术工具方面：具备基于业务需求结合软件补丁、安全功能、安全设备、安全配置、人员意识等因素选择合适抵御方式的功能，确保抵御的全面性和有效性。

2) 人员能力方面：具备一定的攻防经验和软件开发能力，精通安全架构设计、安全功能设计及安全措施实现，能够应对复杂的威胁。

6.2 安全加固能力 (CD02)

6.2.1 账户与权限管理能力 (CSD02.01)

账户与权限管理能力是指对用户账户或权限进行创建、修改、删除和分配等操作，以确保账户与权限安全性和合规性的能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的账户与权限管理工作。

b) 发展级 (L2)

1) 组织建设方面：具备专人或专岗负责账户管理工作，并设定具体的职责。

2) 制度流程方面：建立账户管理的机制，同一级系统应采用统一的管理策略，确保账户与权限管理的标准化和规范化。

3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级 (L3)

1) 组织建设方面：组建专门的团队以专职承担账户与权限管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 建立包括申请审批、开设、审计、销毁等在内的账户与权限管理机制，确保账户与权限管理的全流程覆盖；

ii. 定期对账户的操作和权限情况进行审核与评估，确保账户与权限管理的合规性和安全性。

3) 技术工具方面：采用自动化的技术手段，对账户与权限信息进行监控和批量管理，实现账户与权限管理的自动化审批、分配和审计。

4) 人员能力方面：熟悉常见的合规监管标准、身份和访问管理工具、基本的安全协议、功能级权限管理、数据级权限管理等知识和技术，具备实施账号权限管理和定期审查工作的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如审批时间、审计覆盖率等指标。

2) 制度流程方面：建立账户与权限管理的持续改进机制，定期评估和优化管理策略。

3) 技术工具方面: 采用的账号与权限管理平台具备如自动化分析与总结功能, 可持续改进管理策略。

e) 卓越级 (L5)

- 1) 组织建设方面: 团队成员具备丰富的网络系统及信息系统账户与权限管理经验, 精通各种IT设备及系统的账户配置与管理。
- 2) 技术工具方面: 采用智能化账户与权限管理工具, 实现对账户的实时监控和动态调整, 对账户行为进行分析和预警。

6.2.2 安全配置管理能力 (CSD02.02)

安全配置管理能力是指对系统、网络设备等进行安全相关的参数设置和调整, 以确保其符合安全策略和最佳实践的能力。

能力等级标准如下:

a) 基础级 (L1)

- 1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展基础的安全配置工作。

b) 发展级 (L2)

- 1) 组织建设方面: 具备专人或专岗负责安全配置管理工作, 并设定具体的职责。
- 2) 制度流程方面: 建立资产基础信息及资产配置信息台账, 确保台账信息与实际情况相符。
- 3) 技术工具方面: 使用标准化的管理工具, 实现部分自动化管理功能。

c) 协同级 (L3)

- 1) 组织建设方面: 组建专门的团队以专职承担安全配置管理工作的职责, 确保职责匹配到人员或岗位, 并得到有效执行。
- 2) 制度流程方面:
 - i. 对安全配置信息进行统一管理, 涵盖各类资产设备、操作系统、软件类型、版本及配置信息等;
 - ii. 制定安全配置定期评估策略, 重点定义安全配置审计与评估的频率和实施方式, 以确保资产的安全配置策略处于最佳状态。
- 3) 技术工具方面: 采用自动化的技术手段, 对安全配置信息进行监控和批量管理, 实现安全配置自动化审批、变更管理和审计功能。
- 4) 人员能力方面: 具备对信息系统、网络设备等实施安全基线制定与标准化、配置变更控制、合规性管理等能力。

d) 优秀级 (L4)

- 1) 组织建设方面: 对人员的工作目标和绩效提出具体要求, 并实施量化管理, 如采用配置审计频率、配置变更成功率等指标。
- 2) 制度流程方面: 建立安全配置管理的持续改进机制, 定期评估和优化管理策略。

e) 卓越级 (L5)

- 1) 组织建设方面: 配备专业团队, 开展安全配置策略的研究, 不断优化安全配置管理方法和工具。
- 2) 技术工具方面: 具备如安全基线检查系统、安全有效性验证平台等自动化分析与总结功能。

6.2.3 隔离技术 (CSD02.03)

隔离技术是指通过将潜在有害的应用程序或进程隔离在安全环境中运行, 防止其对系统造成损害。

能力等级标准如下:

a) 基础级 (L1)

- 1) 组织建设方面：具备人员依据经验或借助第三方工具开展基础的信息化隔离工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责隔离工作，并设定具体的职责。
 - 2) 技术工具方面：使用标准化的管理工具，实现部分自动化管理功能。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担安全隔离工作的职责，并明确安全域、VLAN隔离管理职责。
 - 2) 制度流程方面：
 - i. 对隔离工作建立管理策略和实施策略，明确不同IT环境下的隔离技术采用策略；
 - ii. 明确区域间的逻辑和物理隔离要求及措施，例如生产环境与测试环境必须严格隔离，禁止相互访问。
 - 3) 技术工具方面：采用自动化的技术手段，对隔离信息进行监控和批量管理。
 - 4) 人员能力方面：熟悉网络隔离、容器隔离、进程隔离、微隔离等常见隔离手段和技术，具备实施常见隔离技术的能力。
- d) 优秀级（L4）
 - 1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如隔离配置的准确性、隔离策略的覆盖率等指标。
 - 2) 制度流程方面：建立隔离技术的持续改进机制，定期评估和优化隔离策略。
 - 3) 技术工具方面：具备如通过打通流程和隔离平台对接，全面落实自动化开通、回收隔离规则机制等功能。
- e) 卓越级（L5）
 - 1) 组织建设方面：配备专业团队，开展隔离技术的研究，并具备隔离技术研发与隔离工具开发能力。
 - 2) 技术工具方面：引入如零信任网络访问、微隔离等隔离技术，并具备成熟落地实践。

6.2.4 加密与签名管理能力（CSD02.04）

加密与签名管理能力是指对数据进行加密保护和数字签名验证，确保数据的保密性、完整性和可用性的能力。

能力等级标准如下：

- a) 基础级（L1）
 - 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的数据加密与签名管理工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责加密与签名工作，并设定具体的职责。
 - 2) 技术工具方面：使用标准化的管理工具，实现部分自动化管理功能。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担数据加密与签名管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 制定数据分级分类标准，确保不同级别的数据采用不同的加密与签名策略；
 - ii. 建立密钥管理机制，对密钥进行管理，确保密钥的安全性和有效性。
 - 3) 技术工具方面：采用自动化的技术手段，对加密与签名信息进行监控和批量管理。

4) 人员能力方面：熟悉加密算法、密钥生命周期管理、签名验签、证书体系管理、身份鉴别与认证等基础知识和实现方法，具备实施加密与签名管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如密钥管理的准确性、加密操作的成功率等指标。

2) 制度流程方面：建立加密与签名管理的持续改进机制，定期评估和优化管理策略。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展加密技术的研究，并具备加密技术研发与加密工具开发能力。

6.2.5 数据备份管理能力 (CSD02.05)

数据备份管理能力是指定期复制和存储重要数据，以便在数据丢失或损坏时能够快速恢复的能力。能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的数据管理工作，包括数据的备份与恢复。

b) 发展级 (L2)

1) 组织建设方面：具备专人或专岗负责数据备份工作，并设定具体的职责。

2) 技术工具方面：使用标准化的管理工具，实现部分数据自动化备份功能。

c) 协同级 (L3)

1) 组织建设方面：组建专门的团队以专职承担数据管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 建立包括数据备份、恢复机制在内的数据安全机制，确保数据备份的标准化和规范化；

ii. 制定应急预案，明确数据备份与恢复失败时的处置措施，确保业务的连续性和稳定性。

3) 技术工具方面：采用自动化的技术手段，对数据备份信息进行监控和批量管理。

4) 人员能力方面：熟悉常见数据库的快照与日志管理、加密与权限控制等知识和技术，具备实施数据备份和恢复验证工作的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如备份频率、恢复时间等指标。

2) 制度流程方面：建立数据备份管理的定期回顾和总结机制，定期评估和优化备份策略。

3) 技术工具方面：能够全面落实自动化备份机制，可基于不同类型数据实施差异化数据备份策略，如全量备份、增量备份、差异备份等，提高备份效率。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展数据管理技术的研究，并具备数据智能备份与恢复技术的研发能力。

2) 制度流程方面：建立“两地三中心”的数据备份机制，以确保数据的高可用性和灾难恢复能力。

6.2.6 功能简化能力 (CSD02.06)

功能简化能力是指通过评估边缘或非重要业务，并且对一些非必要对外暴露的资产进行收敛，使其更易于管理的能力。

能力等级标准如下：

a) 基础级（L1）

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的功能简化工作。

b) 发展级（L2）

1) 组织建设方面：具备专人或专岗负责功能简化工作，并设定具体的职责。

2) 技术工具方面：采用基本的功能简化工具，提高功能简化的效率和准确性。

c) 协同级（L3）

1) 组织建设方面：组建专门的团队以专职承担功能简化工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 明确功能简化的涉及范围及审批流程，如在重要时期保障期间关停非必要服务；

ii. 建立功能简化策略，明确应对安全风险所采用的功能简化项目，确保简化措施的有效性和合理性。

3) 技术工具方面：引入功能简化技术，如自动化脚本、配置管理工具等，提升整体能力。

4) 人员能力方面：熟悉暴露面识别收敛相关知识和技术，具备对外暴露资产的风险评估能力，具备实施功能简化工作的能力。

d) 优秀级（L4）

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如功能简化的审批时间、简化操作的成功率等指标。

2) 制度流程方面：制定相关应急预案，明确功能简化后的应急处置措施及替代方案，确保业务的连续性和稳定性。

e) 卓越级（L5）

1) 组织建设方面：配备专业团队，开展功能简化技术的研究，团队成员具备功能简化自动化实现的开发能力。

2) 制度流程方面：建立功能简化管理的定期回顾和总结机制，定期评估和优化简化策略。

6.2.7 黑白名单管理能力（CSD02.07）

黑白名单管理能力是指通过技术手段和策略，明确禁止或允许特定对象访问网络资源的能力。

能力等级标准如下：

a) 基础级（L1）

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的黑白名单管理工作。

b) 发展级（L2）

1) 组织建设方面：具备专人或专岗负责黑白名单管理工作，并设定具体的职责。

2) 制度流程方面：建立黑白名单的管理机制，确保黑白名单使用的标准化和规范化。

3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级（L3）

1) 组织建设方面：组建专门的团队以专职承担黑白名单管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 建立黑白名单管理策略，包括但不限于IP地址、账号、关键词、网址、邮箱地址、软件等，确保策略的合规性和有效性；

ii. 明确添加黑白名单的标准、流程及审计措施，确保黑白名单管理的全面性和安全性。

3) 技术工具方面：采用自动化的技术手段，对黑白名单信息进行监控和批量管理。

4) 人员能力方面：熟悉如防火墙等常用黑白名单管理工具和系统，了解常见的网络攻击手段和安全漏洞，具备实施黑白名单管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如审批时间、审计覆盖率等指标。

2) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于黑白名单管理工作。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展黑白名单策略的研究，不断优化黑白名单管理方法和工具。

2) 制度流程方面：具备黑白名单管理的反馈收集和持续改进机制，定期评估和优化管理策略。

6.2.8 网络访问控制管理能力 (CSD02.08)

网络访问控制管理能力是指通过技术手段和策略，对网络资源的访问进行限制、监控和管理的能力。能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的网络访问管理工作。

b) 发展级 (L2)

1) 组织建设方面：具备专人或专岗负责网络访问控制管理工作，并设定具体的职责。

2) 制度流程方面：建立网络访问控制管理机制，确保访问控制的开通、关闭等管理归口到相应专人。

3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级 (L3)

1) 组织建设方面：组建专门的团队以专职承担网络访问控制管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：通过管理制度明确安全域、VLAN、主机间的访问关系，确保访问控制的合规性和有效性。

3) 技术工具方面：采用自动化的技术手段，对网络访问控制信息进行监控和批量管理。

4) 人员能力方面：熟悉常用网络访问控制管理工具和系统，如防火墙、路由器、交换机等；了解常见的访问行为风险分析的知识，具备实施网络访问控制管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如审批时间、控制准确性等指标。

2) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于网络访问控制管理工作。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展网络访问控制技术的研究和实验。

2) 制度流程方面：具备网络访问控制的反馈收集和持续改进机制，定期评估和优化控制策略。

6.2.9 身份认证管理能力 (CSD02.09)

身份认证管理能力是指通过验证用户或设备的身份信息，确认其合法身份并据此授予相应访问权限的能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的身份认证管理工作。

b) 发展级 (L2)

- 1) 组织建设方面：具备专人或专岗负责认证管理工作，并设定具体的职责。
- 2) 制度流程方面：建立身份认证管理机制，确保用户或设备的访问权限管理归口到相应专人。
- 3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队以专职承担认证管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：能够明确身份注册的认证策略、重要操作的认证策略、账户口令丢失找回的认证策略等，确保认证管理的合规性和有效性。
- 3) 技术工具方面：采用自动化的技术手段，对身份认证信息进行监控和批量管理，提高网络访问控制的效率和准确性。
- 4) 人员能力方面：熟悉常见的如密码认证、多因素认证、单点登录、生物识别等身份认证技术，具备根据场景需要实施身份认证管理和定期权限审查工作的能力。

d) 优秀级 (L4)

- 1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如认证成功、认证响应时间等指标。
- 2) 制度流程方面：自研或采购系统在设计时需遵守组织制定的身份认证策略，重要系统的登录和操作需要在统一认证的基础上进一步的身份认证。
- 3) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于身份认证管理工作。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展身份认证管理技术的研究和实验。
- 2) 制度流程方面：具备认证管理的反馈收集和持续改进机制，定期评估和优化认证策略。

6.2.10 安全域管理能力 (CSD02.010)

安全域管理能力是指通过将网络划分为多个逻辑区域，对各区域实施针对性安全策略和访问控制的能力。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的安全域管理工作。

b) 发展级 (L2)

- 1) 组织建设方面：具备专人或专岗负责安全域管理工作，并设定具体的职责。
- 2) 制度流程方面：对网络进行基础的域划分，例如内网、外网、DMZ区域等，确保安全域划分归口到相应专人。
- 3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队以专职承担安全域管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：
 - i. 建立安全域划分、虚拟局域网划分、IP地址规划原则及申请流程，确保安全域管理的合规性和有效性；
 - ii. 明确安全域间整体访问规则，网络访问控制策略需严格遵守整体的访问规则。
- 3) 技术工具方面：采用自动化的技术手段，对安全域信息进行监控和批量管理，提高安全域管理的效率和准确性。

4) 人员能力方面：熟悉虚拟局域网划分、物理隔离等安全域管理的基础知识和实现方法，具备实施安全域管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如审批时间、规划准确性等指标。

2) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于安全域管理工作。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展安全域管理的研究和实验，不断优化安全域管理方法和工具。

2) 制度流程方面：具备安全域管理的反馈收集和持续改进机制，定期评估和优化管理策略。

6.2.11 基线管理能力 (CSD02.11)

基线管理能力是指通过设定、监控和维护网络或系统的基准安全运行配置和状态的能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的基线配置管理工作。

b) 发展级 (L2)

1) 组织建设方面：具备专人或专岗负责基线配置工作，并设定具体的职责。

2) 制度流程方面：对核心IT资产建立规范化配置基线库，确保基线配置归口到相应专人。

3) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。

c) 协同级 (L3)

1) 组织建设方面：组建专门的团队以专职承担基线配置管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 建立全面的安全配置管理基线库，覆盖操作系统、数据库、应用中间件等，确保基线配置的合规性和有效性；

ii. 建立安全操作基线，例如安全操作手册、安全配置标准及指南和各类工作流程等。

3) 技术工具方面：采用自动化的技术手段，对基线配置信息进行监控和批量管理，提高基线管理的效率和准确性。

4) 人员能力方面：熟悉各类操作系统配置、网络参数设置、应用程序配置等的基础知识和实现方法，具备实施基线管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如基线配置的覆盖率、配置准确性等指标。

2) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于基线管理工作。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队，开展基线管理的研究和实验，不断优化基线管理方法和工具。

2) 制度流程方面：具备基线配置管理的反馈收集和持续改进机制，定期评估和优化管理策略。

6.2.12 日志管理能力 (CSD02.12)

日志管理能力是指通过对网络或系统的日志进行收集、存储，并进行监控和管理的能力。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的日志管理工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责日志管理工作，并设定具体的职责。
 - 2) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担日志管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 建立日志管理机制，包括设备日志功能的开设、功能审查、日志异常处理等，确保日志管理的合规性和有效性；
 - ii. 建立日志生命周期管理机制，确保日志的生成、存储、分析、归档、销毁等各个环节得到管理。
 - 3) 技术工具方面：采用自动化管理工具和技术手段，对日志信息进行集中管理和监控。
 - 4) 人员能力方面：熟悉日志的分类、索引、备份等操作的基础知识和实现方法，具备实施日志管理的能力。
- d) 优秀级（L4）
 - 1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如日志收集的覆盖率、日志处理的及时性等指标。
 - 2) 人员能力方面：能够对日志管理建立分析模型，包括日志关联分析、场景分析、行为分析等，提升日志管理的智能化和高效性。
- e) 卓越级（L5）
 - 1) 组织建设方面：配备专业团队开展日志管理的研究和实验，不断优化日志管理方法和工具。
 - 2) 制度流程方面：具备日志管理的反馈收集和持续改进机制，定期评估和优化管理策略。

6.2.13 软件更新管理能力（CSD02.13）

软件更新管理能力是指通过对软件版本进行更新、部署和维护，以修复漏洞、提升性能或增加功能的能力。

能力等级标准如下：

- a) 基础级（L1）
 - 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的软件更新管理工作。
 - 2) 制度流程方面：要求生产用软件符合正版化要求且可更新，确保软件的合法性。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责软件更新管理工作，并设定具体的职责。
 - 2) 技术工具方面：采用标准化的管理工具，实现部分自动化管理功能。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担软件更新管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 制定软件更新管理策略，将软件更新流程纳入日常运维的变更流程，确保更新过程的合规性和有效性；
 - ii. 建立软件生命周期管理机制，包括软件安装、更新、卸载等，确保软件管理的全面性。
 - 3) 技术工具方面：采用自动化的技术手段，对软件更新信息进行监控和批量管理，提升软件更新管理的效率和准确性。

4) 人员能力方面：熟悉软件更新中的功能测试、性能测试、兼容性测试等的基础知识和实现方法，具备实施软件更新管理的能力。

d) 优秀级 (L4)

1) 组织建设方面：对人员的工作目标和绩效提出具体要求，并实施量化管理，如更新覆盖率、更新成功率等指标。

2) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于软件更新管理工作。

e) 卓越级 (L5)

1) 组织建设方面：配备专业团队开展软件更新管理的研究，不断优化软件更新管理方法和工具。

2) 制度流程方面：具备软件更新管理的反馈收集和持续改进机制，定期评估和优化管理策略。

6.3 事件检测能力 (CD03)

6.3.1 边界入侵检测能力 (CSD03.01)

边界入侵检测能力是指组织识别、分析攻击者在重要区域的网络入口是否正进行未经授权的访问或恶意活动的能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的入侵检测工作。

b) 发展级 (L2)

1) 组织建设方面：具备专人或专岗负责入侵检测工作，并设定具体的职责。

2) 制度流程方面：建立入侵检测工作流程及策略，明确入侵检测的目标和方法。

3) 技术工具方面：在关键区域部署并使用第三方或开源的入侵检测工具，提高入侵检测分析能力。

c) 协同级 (L3)

1) 组织建设方面：组建专门的团队以专职承担入侵检测管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 制定详细的入侵检测工作流程、操作规范及策略，包含入侵检测工具使用方式如升级频率等；

ii. 根据公司网络架构及安全需求，制定入侵检测工具部署架构。

3) 技术工具方面：在重要网络区域部署使用基于流量和基于日志的网络入侵检测工具，确保入侵检测的覆盖率和准确性；

4) 人员能力方面：

i. 入侵检测专岗人员熟悉工作流程，能够按需配置、调整策略，确保检测措施的有效落实；

ii. 入侵检测专岗人员熟悉整体网络安全部署架构和工具操作方式，能够按需调整入侵检测部署位置，进行设备的日常操作及故障处理。

d) 优秀级 (L4)

1) 组织建设方面：明确团队工作目标，制定检测告警时间、检测准确率等具体的绩效指标，并实施量化管理。

2) 技术工具方面：采用自动化的技术手段，对入侵事件进行集中管理和监控，并将入侵检测信息上报关联安全管理中心或行业态势感知平台，进行入侵行为的综合分析并给出处置方案。

3) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于入侵检测工作。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展入侵检测技术的研究，不断优化检测方法和工具。
- 2) 制度流程方面：建立入侵检测反馈机制和持续改进机制，持续改进检测内容和策略，确保检测质量。

6.3.2 应用攻击检测能力（CSD03.02）

应用攻击检测能力是指组织识别、分析针对应用系统的恶意行为的能力。

能力等级标准如下：

a) 基础级（L1）

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的应用攻击检测工作。

b) 发展级（L2）

- 1) 组织建设方面：具备专人或专岗负责应用攻击检测工作，并设定具体的职责。
- 2) 制度流程方面：建立初步的应用攻击检测工作流程及策略，明确检测的目标和方法。
- 3) 技术工具方面：具备基本的应用攻击检测工具，如Web应用防火墙（WAF）。

c) 协同级（L3）

- 1) 组织建设方面：组建专门的团队以专职承担应用攻击检测管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：
 - i. 制定详细的应用攻击检测的工作流程、操作规范及策略，包含应用攻击检测工具使用方式如升级频率等；
 - ii. 根据公司网络架构及安全需求，制定应用攻击检测工具部署架构。
- 3) 技术工具方面：使用标准化的检测工具，提高应用攻击检测的效率和准确性。
- 4) 人员能力方面：
 - i. 应用攻击检测专岗人员熟悉工作流程，能够按需配置、调整策略，确保检测措施的有效落实；
 - ii. 应用攻击检测专岗人员熟悉整体网络安全部署架构及工具操作方式，能够按需调整部署位置和检测工具的日常操作及故障处理；
 - iii. 岗位人员具备较强的应用攻击检测分析能力，能够按需调整应用攻击检测方式、策略，提高检测工具的有效性。

d) 优秀级（L4）

- 1) 组织建设方面：明确团队工作目标，制定检测告警时间、检测准确率等具体的绩效指标，并实施量化管理。
- 2) 技术工具方面：采用自动化工具和技术手段，对应用攻击事件进行集中管理和监控，并将应用攻击检测信息上报关联安全管理中心或行业态势感知平台，进行应用攻击的总体分析并给出处置方案。
- 3) 人员能力方面：了解新出现的网络攻击手段和安全漏洞，并能够用于应用攻击检测。

e) 卓越级（L5）

- 1) 组织建设方面：配备专业团队，开展应用攻击检测技术的研究，不断优化检测方法和工具。
- 2) 制度流程方面：建立应用攻击检测的反馈机制和持续改进机制，持续改进检测内容和策略，确保检测质量。

6.3.3 未知威胁发现能力（CSD03.03）

未知威胁发现能力是指组织识别、分析和应对尚未被已知特征或规则定义的潜在安全威胁的能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展未知威胁信息接收工作。

b) 发展级 (L2)

1) 组织建设方面: 具备信息技术人员负责未知威胁发现工作, 可以凭借经验开展基础的未知威胁识别与评估工作。

c) 协同级 (L3)

1) 组织建设方面: 具备专人或专岗负责未知威胁管理工作, 并设定具体的职责。

2) 制度流程方面:

i. 制定详细的未知威胁发现的工作流程和策略, 包含未知威胁检测工具使用方式如升级频率等;

ii. 根据公司网络架构及安全需求, 制定未知威胁检测工具部署架构。

3) 技术工具方面: 使用标准化的未知威胁发现工具, 提高未知威胁识别的效率和准确性。

4) 人员能力方面: 具备检测工具的日常操作及故障处理能力, 确保未知威胁工具的有效性。

d) 优秀级 (L4)

1) 组织建设方面:

i. 建立专门的团队来负责未知威胁管理工作, 确保职责匹配到人员或岗位;

ii. 明确团队工作目标, 并实施量化管理。

2) 技术工具方面:

i. 综合利用入侵检测、应用攻击、病毒与恶意软件等检测能力, 及时发现未知威胁;

ii. 采用自动化工具和技术手段, 对未知威胁事件进行集中管理和监控, 并将未知攻击检测信息上报关联安全管理中心或行业态势感知平台, 进行未知攻击的总体分析并给出处置方案。

3) 人员能力方面: 具备一定的未知威胁攻击研判分析能力。

e) 卓越级 (L5)

1) 组织建设方面: 配备专业团队, 开展未知威胁识别技术的研究, 不断优化检测方法和工具。

2) 制度流程方面: 建立未知威胁的定期回顾和总结机制, 定期评估未知威胁识别质量。

3) 人员能力方面: 具备一定的攻防经验和软件开发能力, 以及丰富的二进制逆向分析经验, 深入优化未知威胁识别能力。

6.3.4 病毒与恶意软件检测能力 (CSD03.04)

病毒与恶意软件检测能力是指组织识别、分析和应对计算机病毒、恶意软件 (如木马、勒索软件、间谍软件等) 的能力。

能力等级标准如下:

a) 基础级 (L1)

1) 组织建设方面: 具备信息技术人员依据经验或第三方工具开展基础的病毒与恶意软件检测工作。

b) 发展级 (L2)

1) 组织建设方面: 具备专人或专岗负责病毒与恶意软件管理工作, 并设定具体的职责。

2) 制度流程方面: 建立初步的病毒与恶意软件检测工作流程及策略, 明确病毒与恶意软件检测目标和方法。

3) 技术工具方面: 具备标准化的病毒与恶意软件检测工具, 如防病毒软件、EDR等。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队以专职承担病毒与恶意软件管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：
 - i. 制定完善的病毒与恶意软件工作流程、操作规范及策略，包含检测工具的使用方式如升级频率，确保检测的标准化和规范化，建立对病毒与恶意软件事件的分析管理机制，确保事件的及时处理和总结；
 - ii. 根据公司网络架构及安全需求，制定病毒与恶意软件检测工具部署区域和数量。
- 3) 技术工具方面：使用成熟化较高的检测工具，提高病毒与恶意软件检测的效率和准确性。
- 4) 人员能力方面：
 - i. 熟悉工作流程，能够按需配置、调整策略，确保管理措施的有效落实；
 - ii. 熟悉病毒与恶意软件工具操作方式，能够对检测工具进行日常操作及故障处理；
 - iii. 熟悉病毒与恶意软件攻击原理，能够按需调整检测方式、策略，确保管理的及时性和有效性。
- d) 优秀级（L4）
 - 1) 组织建设方面：明确团队工作目标，制定病毒查杀率、恶意软件检测率等指标，并实施量化管理。
 - 2) 技术工具方面：采用自动化的技术手段，对病毒与恶意软件事件进行集中管理和监控，并将病毒与恶意软件检测信息上报关联安全管理中心或行业态势感知平台，进行病毒或恶意软件的综合分析并给出处置方案。
- e) 卓越级（L5）
 - 1) 组织建设方面：配备专业团队，开展病毒与恶意软件识别与防范技术的研究，不断优化检测方法和工具。
 - 2) 制度流程方面：建立病毒与恶意软件的定期回顾和总结机制，定期评估检测质量。

6.3.5 端点行为检测能力（CSD03.05）

端点行为检测能力是指组织监控、分析和识别端点设备上用户和应用程序行为的异常或潜在恶意活动的的能力。

能力等级标准如下：

- a) 基础级（L1）
 - 1) 组织建设方面：具备信息技术人员依据经验或第三方工具开展基础的端点行为检测工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责端点行为检测工作，并设定具体的职责。
 - 2) 制度流程方面：建立初步的端点行为检测工作流程及策略，明确检测的目标和方法。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担端点行为检测管理工作的职责，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 制定完善的端点行为检测工作流程、操作规范及策略，包含检测工具的使用方式如升级频率，确保检测的标准化和规范化，建立对端点异常行为事件的分析管理机制，确保事件的及时处理和总结；
 - ii. 根据公司网络架构及安全需求，制定端点行为检测工具部署方式和区域。
 - 3) 技术工具方面：使用标准化的工具，提高端点行为的分析效率和准确性；根据人员类型、访问对象建立端点行为台账，记录端点行为数据。

- 4) 人员能力方面:
 - i. 熟悉工作流程, 能够按需配置、调整策略, 确保检测措施的有效落实;
 - ii. 熟悉端点行为检测工具操作方式, 能够对检测工具进行日常操作及故障处理;
 - iii. 熟悉本单位组织架构、人员类型及端点安全管理规定内容, 能够有针对性的开展具体工作, 确保检测的及时性和有效性。
- d) 优秀级 (L4)
 - 1) 组织建设方面: 明确团队工作目标, 制定端点行为异常检测率等指标, 并实施量化管理。
 - 2) 技术工具方面:
 - i. 建立身份行为模型, 模型组成涵盖访问行为、访问频率、访问时间、访问内容等相关性要素, 能够基于行为模型检测端点异常行为;
 - ii. 采用自动化的技术手段, 对端点异常行为事件进行集中管理和监控并实现端点行为检测信息上报关联安全管理中心或行业态势感知平台, 进行端点行为的综合分析并给出处置方案。
- e) 卓越级 (L5)
 - 1) 组织建设方面: 配备专业团队, 开展端点行为检测技术的研究, 不断优化检测方法和工具。
 - 2) 制度流程方面: 建立端点行为检测反馈机制和持续改进机制, 持续改进检测内容和策略, 确保检测质量。

6.3.6 流量检测能力 (CSD03.06)

流量检测能力是指组织监控分析和识别所有网络区域中关键网络节点中的异常或潜在恶意活动的能
力。

能力等级标准如下:

- a) 基础级 (L1)
 - 1) 组织建设方面: 具备信息技术人员依据经验或第三方工具开展基础的流量检测工作。
- b) 发展级 (L2)
 - 1) 组织建设方面: 具备专人或专岗负责流量检测工作, 并设定具体的职责。
 - 2) 制度流程方面: 建立初步的流量检测工作流程及策略, 明确检测的目标和方法。
- c) 协同级 (L3)
 - 1) 组织建设方面: 组建专门的团队以专职承担网络流量管理工作的职责, 确保职责匹配到人员或岗位, 并得到有效执行。
 - 2) 制度流程方面:
 - i. 制定详细的流量检测的工作流程、操作规范及策略, 包含应用流量检测工具使用方式如升级频率等;
 - ii. 根据公司网络架构及安全需求, 制定流量检测工具部署架构, 对流量管理进行合理规划, 确保流量检测的标准化和规范化。
 - 3) 技术工具方面: 使用标准化的流量检测工具, 提高流量检测的分析效率和准确性。
 - 4) 人员能力方面:
 - i. 熟悉工作流程, 能够按需配置、调整策略, 确保检测措施的有效落实;
 - ii. 熟悉整体网络安全部署架构及工具操作方式, 能够按需调整流量检测工具部署和检测工具的日常操作及故障处理;
 - iii. 具备较强的流量检测分析能力, 能够按需调整流量检测方式、策略, 提高检测工具的有效性。
- d) 优秀级 (L4)

- 1) 组织建设方面：明确团队工作目标，制定检测响应时间、检测准确率等指标，并实施量化管理。
- 2) 技术工具方面：
 - i. 对流量进行实时检测，能够及时发现异常流量并开展分析处置，采用自动化的技术手段，对流量异常事件进行集中管理和监控；
 - ii. 将流量检测信息上报关联安全管理中心或行业态势感知平台，进行流量异常的综合分析并给出处置方案。
- e) 卓越级（L5）
 - 1) 组织建设方面：配备专业团队，开展流量检测技术的研究，不断优化检测方法和工具。
 - 2) 制度流程方面：建立流量检测的定期回顾总结和持续改进机制，持续改进检测策略，提升检测质量。

6.4 事件响应能力（CD04）

6.4.1 边界入侵防御能力（CSD04.01）

边界入侵防御能力是指组织通过技术、策略和流程的结合，主动预防、检测和阻止在重要区域的网络入口未经授权的访问或恶意活动的能力。

能力等级标准如下：

- a) 基础级（L1）
 - 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的入侵防御工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责入侵防护工作，并设定具体的职责。
 - 2) 制度流程方面：建立标准化的入侵处置流程，可以对入侵行为进行规范化防御。
 - 3) 技术工具方面：具备专用的入侵防护工具，可以对不同类型的入侵行为进行响应与处置。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队以专职承担入侵防护管理工作，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 制定入侵事件响应处理机制、工作流程、操作规范及策略，包含应入侵防御工具使用方式如升级频率等，可以在入侵事件发生时根据预案进行流程化处置，并对处置流程进行存档记录；
 - ii. 根据公司网络架构及安全需求，制定入侵防御工具部署架构。
 - 3) 技术工具方面：采用自动化的主机、网络等多层次入侵防护工具，对入侵事件进行集中管理和监控。
 - 4) 人员能力方面：
 - i. 熟悉整体网络安全部署架构和设备操作方式，能够按需调整入侵防护部署位置，进行设备的日常操作及故障处理；
 - ii. 具备较强的入侵防护能力，能够利用入侵防护工具对入侵事件进行防护并按需调整入侵防护工具方式、策略。
- d) 优秀级（L4）
 - 1) 组织建设方面：对团队及人员的工作目标和绩效实施量化管理，如响应时间、处置成功率等。
 - 2) 技术工具方面：

- i. 建立统一的网络安全管理平台，关联多种攻击行为，对入侵行为的监测与响应进行集中管理；
 - ii. 可自定义入侵防护规则，针对性地制定入侵防护监测机制与响应手段。
- e) 卓越级 (L5)
- 1) 组织建设方面：配备专业团队，开展入侵防护技术的研究，持续对入侵防护体系进行评估并优化，不断优化防护方法和工具。
 - 2) 制度流程方面：建立入侵防御流程的反馈和持续改进机制，定期评估现有防御策略并优化改进。

6.4.2 应用攻击防护能力 (CSD04.02)

应用攻击防护能力是指组织通过技术、策略和流程的结合，识别、阻止和缓解针对应用系统的恶意行为的能力。

能力等级标准如下：

- a) 基础级 (L1)
- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的应用攻击响应与处置（如封禁等）工作。
- b) 发展级 (L2)
- 1) 组织建设方面：具备专人或专岗负责应用攻击防护工作，并设定具体的职责。
 - 2) 制度流程方面：建立标准化的应用攻击处置流程，可以对应用攻击行为进行规范化处置。
 - 3) 技术工具方面：具备专用的应用攻击防护工具，可以对常见的应用攻击行为（如注入攻击、跨站脚本攻击等）进行响应。
- c) 协同级 (L3)
- 1) 组织建设方面：组建专门的团队以专职承担应用攻击防护管理工作，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：
 - i. 建立应用攻击事件响应处理机制、工作流程、操作规范及策略，包含应用攻击防护工具使用方式如升级频率等，可以在应用攻击事件发生时根据预案进行流程化处置，并对处置流程进行存档记录；
 - ii. 根据公司网络架构及安全需求，制定应用攻击防护工具部署架构。
 - 3) 技术工具方面：采用自动化的技术手段，对应用攻击事件进行集中管理和监控。
 - 4) 人员能力方面：
 - i. 熟悉整体网络安全部署架构和设备操作方式，能够按需调整应用攻击防护工具部署位置，进行设备的日常操作及故障处理；
 - ii. 具备较强的应用攻击防护能力，能够利用应用攻击防护工具对应用入侵事件进行防护并按需调整应用入侵防护工具方式、策略。
- d) 优秀级 (L4)
- 1) 组织建设方面：对团队及人员的工作目标和绩效实施量化管理，如响应时间、处置成功率等。
 - 2) 技术工具方面：
 - i. 建立统一的网络安全管理平台，关联多种攻击行为，对应用攻击行为的监测与响应进行集中管理；
 - ii. 可自定义应用攻击防护规则，针对性地制定应用攻击防护监测机制与响应手段。
- e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展应用攻击防护技术的研究，持续对应用攻击防护体系进行评估并优化，不断优化防护方法和工具。
- 2) 制度流程方面：建立应用攻击防护流程的持续改进机制，定期评估现有防护策略并优化改进。

6.4.3 防病毒与反恶意软件能力（CSD04.04）

防病毒与反恶意软件能力是指组织通过技术、策略和流程的结合，检测、阻止和清除计算机病毒、恶意软件（如木马、勒索软件、间谍软件等）的能力。

能力等级标准如下：

a) 基础级（L1）

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方资源开展基础的防病毒与反恶意软件工作。
- 2) 人员能力方面：理解防病毒与反恶意软件的基本概念和方法，可开展基础的防病毒与反恶意软件工作。

b) 发展级（L2）

- 1) 组织建设方面：具备专职人员负责防病毒与反恶意软件工作，并设定具体的职责。
- 2) 制度流程方面：具备标准化的防病毒与反恶意软件处置流程，在发生病毒或恶意软件入侵时进行规范处置。
- 3) 技术工具方面：具备标准化的病毒与反恶意软件工具，可以开展完善的病毒查杀工作。

c) 协同级（L3）

- 1) 组织建设方面：组建专门的团队开展防病毒与反恶意软件工作，确保职责匹配到人员或岗位。
- 2) 制度流程方面：
 - i. 建立病毒与恶意软件管理与响应机制、工作流程、操作规范及策略，包含病毒与恶意软件防护工具使用方式如升级频率等，可以在发生病毒与恶意软件入侵事件时根据预案进行流程化处置，并对处置流程进行存档记录；
 - ii. 根据公司网络架构及安全需求，制定病毒与反恶意软件工具部署方式和区域。
- 3) 技术工具方面：采用自动化的和技术手段，对病毒和恶意软件进行集中管理和监控。
- 4) 人员能力方面：
 - i. 熟悉病毒与恶意软件防护工具操作方式，能够对防护工具进行日常操作及故障处理；
 - ii. 熟悉病毒与恶意软件攻击和防护原理，能够针对该类攻击开展防护工作并调整检测方式、策略，确保管理的及时性和有效性。

d) 优秀级（L4）

- 1) 组织建设方面：对团队及人员的工作目标和绩效实施量化管理，如病毒查杀率、恶意软件检测率等。
- 3) 技术工具方面：建立统一的网络安全管理平台，关联多种攻击行为，对恶意软件攻击行为的监测与响应进行集中管理。

e) 卓越级（L5）

- 1) 组织建设方面：配备专业团队，开展病毒与恶意软件识别与防范技术的研究，持续对防病毒与反恶意软件体系进行评估，不断优化防护方法与工具。
- 2) 制度流程方面：建立病毒与恶意软件防护流程的持续改进机制，定期评估现有防护策略并优化改进。

6.4.4 端点行为防护能力（CSD04.05）

端点行为防护能力是指组织通过技术、策略和流程的结合，监控、分析和保护端点设备上的用户 和应用程序行为，防止恶意活动或未经授权的操作的能力。

能力等级标准如下：

a) 基础级（L1）

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的端点行为防护工作。

b) 发展级（L2）

1) 组织建设方面：具备专职人员负责端点行为防护工作，并设定具体的职责。

2) 制度流程方面：具备标准化的端点异常行为处置流程，在发现异常端点行为时可以进行规范处置。

3) 技术工具方面：具备标准化的端点行为防护工具，可以对端点异常行为进行规范化防范。

c) 协同级（L3）

1) 组织建设方面：组建专门的团队以专职承担端点行为防护管理工作，确保职责匹配到人员或岗位，并得到有效执行。

2) 制度流程方面：

i. 建立端点异常行为响应处理机制、工作流程、操作规范及策略，包含端点行为防护工具的使用方式如升级频率等，可以在异常行为发生时根据预案进行流程化处置，并对处置流程进行存档记录；

ii. 根据公司网络架构及安全需求，制定端点行为防护工具部署方式和区域。

3) 技术工具方面：采用自动化的技术手段，对端点异常行为进行集中管理和监控。

4) 人员能力方面：

i. 熟悉端点行为防护工具操作方式，能够对防护工具进行日常操作及故障处理；

ii. 熟悉本单位组织架构、人员类型及端点安全管理规定内容，能够利用防护工具开展防护工作。

d) 优秀级（L4）

1) 组织建设方面：对团队及人员的工作目标和绩效实施量化管理，如响应时间、处置成功率等。

2) 技术工具方面：

i. 可通过建立用户行为模型进行端点异常行为响应工作，模型组成涵盖访问行为、访问频率、访问时间、访问内容等相关性要素；

ii. 建立统一的网络安全管理平台，关联多种攻击行为，对端点异常行为的监测与响应进行集中管理。

e) 卓越级（L5）

1) 组织建设方面：配备专业团队，开展端点行为防护技术的研究，建立异常行为模型用于端点异常行为响应工作。

2) 制度流程方面：建立端点异常行为防护流程的持续改进机制，定期评估现有防护策略与行为模型并持续优化改进。

6.4.5 流量过滤能力（CSD04.03）

流量过滤能力是指组织对所有网络区域中关键网络节点的流量进行检查、分析和筛选，以阻止恶意流量、未经授权的访问或不符合安全策略的数据传输的能力。

能力等级标准如下：

a) 基础级（L1）

1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的流量过滤工作。

b) 发展级（L2）

- 1) 组织建设方面：具备专人或专岗负责流量过滤工作，并设定具体的职责。
- 2) 制度流程方面：建立标准化的异常流量处置流程，可以对异常流量事件进行规范化处置。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队以专职承担网络流量管理工作，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：
 - i. 具备采取流量过滤措施的工作流程、操作规范及策略，包含流量过滤工具操作方式如升级频率等，明确流量过滤措施的启用、实施及回收流程，并对处置流程进行存档记录；
 - ii. 根据公司网络架构及安全需求，制定流量过滤工具部署架构。
- 3) 技术工具方面：具备多层次（网络层、传输层、应用层等）的自动化流量过滤能力，可依据多种流量管理工具实现纵深防护。
- 4) 人员能力方面：
 - i. 熟悉整体网络安全部署架构和设备操作方式，能够按需调整流量过滤工具部署位置，进行设备的日常操作及故障处理；
 - ii. 具备较强的流量过滤防护能力，能够利用多种流量管理工具开展流量过滤工作并按需调整流量过滤工具方式、策略。

d) 优秀级 (L4)

- 1) 组织建设方面：对团队及人员的工作目标和绩效实施量化管理，如流量过滤的覆盖率、准确率等。
- 3) 技术工具方面：可以通过统一流量管理平台开展实时的流量监控，对多层次的流量管理工具进行集中管控并开展响应处置工作。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展流量检测技术的研究，持续对流量过滤体系进行评估，不断优化检测方法和工具。
- 2) 制度流程方面：建立流量过滤的持续改进机制，定期评估现有过滤策略并优化改进。

6.5 诱捕溯源能力 (CD05)

6.5.1 攻击诱捕能力 (CSD05.01)

攻击诱捕能力是指组织通过部署诱饵环境主动吸引攻击者并监控其行为，以收集攻击信息、分析攻击手法并增强整体防御能力的的能力。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的攻击诱捕工作。

b) 发展级 (L2)

- 1) 组织建设方面：具备专人或专岗负责攻击诱捕工作，并设定具体的职责。
- 2) 制度流程方面：制定初步的攻击诱捕系统的实施计划，明确目标、范围，并开展必要的调研。

c) 协同级 (L3)

- 1) 组织建设方面：组建专门的团队负责攻击诱捕工作，确保职责匹配到人员或岗位，并得到有效执行。
- 2) 制度流程方面：
 - i. 制定详细的攻击诱捕操作流程和指南，明确工具使用方式和策略；
 - ii. 根据公司的网络架构和安全需求，制定攻击诱捕工具的部署架构。

- 3) 技术工具方面：部署不同类型的诱捕系统（如高交互蜜罐、低交互蜜罐、蜜网等），提高捕获攻击样本和行为的能力。
- 4) 人员能力方面：
 - i. 熟悉整体网络安全部署架构和设备操作方式，能够按需调整诱捕系统部署位置，开展设备的日常操作及故障处理；
 - ii. 具备一定的诱捕分析能力，能够对潜在的攻击手法进行分析，并按需调整诱捕系统的策略，提高诱捕系统分析能力。
- d) 优秀级（L4）
 - 1) 组织建设方面：明确团队工作目标，制定诱捕告警分析时间等具体的绩效指标，并实施量化管理。
 - 2) 技术工具方面：与其他安全组件（如防火墙、入侵检测系统、日志分析工具等）进行集成和联动，实现信息共享和协同作战。
- e) 卓越级（L5）
 - 1) 组织建设方面：配备专业团队，开展诱捕检测技术的研究，定期评估和分析攻击趋势、攻击手法和诱捕效果，不断调整和优化诱捕策略并结合组织情况自定义诱捕系统。
 - 2) 制度流程方面：定期对攻击诱捕系统的运营进行合规性审查和评估，持续改进诱捕内容和策略，确保诱捕质量。

6.5.2 溯源取证能力（CSD05.02）

溯源取证能力是指组织通过技术手段和数据分析，追踪网络攻击的来源、路径和攻击者身份并留存证据的能力。

能力等级标准如下：

- a) 基础级（L1）
 - 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的攻击溯源取证工作。
- b) 发展级（L2）
 - 1) 组织建设方面：具备专人或专岗负责攻击溯源取证工作，并设定具体的职责。
 - 2) 制度流程方面：制定基本的网络攻击溯源取证的管理规范，明确其合法性和规范性条件。
- c) 协同级（L3）
 - 1) 组织建设方面：组建专门的团队负责攻击溯源取证工作，确保职责匹配到人员或岗位，并得到有效执行。
 - 2) 制度流程方面：制定详细的溯源取证操作流程和指南，包括数据收集、分析、报告和处置等各个环节。
 - 3) 技术工具方面：
 - i. 具备多层次（网络层、应用层）的流量获取能力，实现攻击溯源全方位覆盖；
 - ii. 采用自动化工具和技术手段（如SIEM系统），对相关信息进行集中管理和监控，对收集到的攻击数据进行处理和分析。
 - 4) 人员能力方面：具备较强的攻击溯源取证能力，了解情报收集、攻击者漏洞探测、攻击利用等知识和技术，可利用组织现有的攻击溯源取证工具开展攻击溯源取证工作。
- d) 优秀级（L4）
 - 1) 组织建设方面：制定攻击溯源取证响应时间等具体的绩效指标，并实施量化管理。
 - 2) 技术工具方面：引入威胁情报系统，实现信息共享和协同作战，并可在取证方面实现自动化或半自动化功能。

3) 人员能力方面：具备较强的溯源取证能力，理解Web渗透、内网横向渗透、二进制逆向等技术，同时对行业特性有充分的认识。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，开展攻击溯源取证技术的研究，建立威胁预测模型和分析机制，不断优化溯源取证方法和工具。
- 2) 制度流程方面：建立攻击溯源取证的反馈机制和持续改进机制，定期评估现有攻击溯源策略并优化改进。
- 3) 技术工具方面：在组织内部具备网络靶场，持续训练并提升溯源取证的攻防水平。

6.6 关联分析能力 (CD06)

6.6.1 策略分析能力 (CSD06.01)

策略分析能力是指通过集中化的管理和控制进而优化定义、配置、执行网络安全策略。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员开展基本的策略分析概念的研究。

b) 发展级 (L2)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的策略管理工作。
- 2) 制度流程方面：初步制定策略分析的相关规定，包括策略的制定、更新和应用的基本流程。

c) 协同级 (L3)

- 1) 组织建设方面：具备专人或专岗负责策略分析工作，并设定具体的职责。
- 2) 制度流程方面：制定详细的策略分析流程，初步实现策略分析的标准化和流程化。
- 3) 技术工具方面：部署标准化的专用策略管理工具，用于记录和跟踪策略的执行情况。
- 4) 人员能力方面：具备策略管理能力，可利用组织现有的策略管理工具参照策略管理流程开展策略管理工作。

d) 优秀级 (L4)

- 1) 组织建设方面：
 - i. 建立专业的团队专职负责安全策略分析工作，确保职责匹配到人员或岗位，并得到有效执行；
 - ii. 明确团队工作目标，制定策略分析范围等具体的绩效指标，并实施量化管理。
- 2) 技术工具方面：实现策略分析与日志管理、入侵检测等系统的联动，建立关联的安全数据库，涵盖攻击预防、防御加固、事件检测与响应等多个方面内容，提高策略分析的效率和准确性。

e) 卓越级 (L5)

- 1) 组织建设方面：配备专业团队，深入开展策略分析的研究，不断优化策略分析和执行方法。
- 2) 制度流程方面：建立策略分析的持续改进机制，通过定期评估和优化策略，提升策略分析的有效性和适应性。

6.6.2 情报分析能力 (CSD06.02)

情报分析能力是指通过收集、分析、整合和分发与网络安全相关的威胁情报，从而有效支持组织的安全决策和快速响应。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员开展基本的情报分析概念的研究。

b) 发展级 (L2)

- 1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展基础的情报管理工作。
- 2) 制度流程方面: 初步制定情报分析的相关规定, 包括情报收集、整理和处理的基本流程。

c) 协同级 (L3)

- 1) 组织建设方面: 具备专岗或专人负责情报分析工作, 并设定具体的职责。
- 2) 制度流程方面: 制定详细的情报分析流程, 初步实现情报管理的标准版和流程化。
- 3) 技术工具方面: 部署专用的情报管理平台, 对于情报信息进行集中管理、分析和分发。
- 4) 人员能力方面: 具备情报分析能力, 可利用组织现有的情报管理工具参照情报管理流程开展情报管理工作。

d) 优秀级 (L4)

- 1) 组织建设方面:
 - i. 组建专业团队专职负责情报分析工作, 确保职责匹配到人员或岗位, 并得到有效执行;
 - ii. 明确团队工作目标, 制定情报分析范围等具体的绩效指标, 并实施量化管理。
- 2) 技术工具方面:
 - i. 建立统一的情报分析中心, 整合来自互联网、社区、企业、个人、机构等多渠道的情报资源, 形成集中管理并对获取的情报进行全生命周期管理, 涵盖情报的获取、分析、应用、共享和清理等环节;
 - ii. 实现情报管理与安全运营、威胁情报共享等系统的联动, 提高情报分析的效率和准确性。

e) 卓越级 (L5)

- 1) 组织建设方面: 配备专业团队, 深入开展情报分析的研究, 不断优化情报管理和分析方法。
- 2) 制度流程方面: 建立情报分析的持续改进机制, 定期评估情报的质量和时效性, 优化情报的分析流程。

6.7 安全运营能力 (CD07)

6.7.1 安全培训能力 (CSD07.01)

安全培训能力是指组织通过系统化的培训计划、课程和实践活动, 提升员工、团队和管理层在网络安全领域的知识、技能和意识的能力。

能力等级标准如下:

a) 基础级 (L1)

- 1) 组织建设方面: 具备信息技术人员开展基本的安全培训方法的研究。

b) 发展级 (L2)

- 1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展基础的网络安全培训工作, 如网络安全基础知识培训。
- 2) 制度流程方面: 建立基本的网络安全培训机制, 如年度网络安全意识培训。

c) 协同级 (L3)

- 1) 组织建设方面: 具备专人或专岗负责网络安全培训工作, 并设定具体的职责。
- 2) 制度流程方面: 建立详细的网络安全培训制度, 定期开展网络安全意识培训、网络安全技能培训等。
- 3) 技术工具方面: 采用在线学习平台并具备完整详细的网络安全培训视频和模拟演练环境, 提高培训的互动性和实效性。
- 4) 人员能力方面: 具备进行基础的网络安全培训宣讲的能力, 如开展网络安全意识培训。

d) 优秀级 (L4)

- 1) 组织建设方面：组建专门的团队承担网络安全培训管理工作的职责，确保职责匹配到人员或岗位，并制定网络安全培训方式等具体的绩效指标。
- 2) 制度流程方面：建立完整的网络安全攻防培训体系，包括建立网络安全攻防培训课程，涵盖理论知识和实操技能。
- 3) 人员能力方面：具备制定网络安全培训试题的能力，对培训效果进行考核，确保培训目标的达成。

e) 卓越级（L5）

- 1) 组织建设方面：配备专业团队，开展针对网络安全培训体系的研究，对培训效果进行智能分析，不断优化培训内容和方法。
- 2) 制度流程方面：建立认证体系和教务体系，建立培训反馈机制，提供专业的网络安全培训认证和资格证书。

6.7.2 安全对抗能力（CSD07.02）

安全对抗能力是指组织在面对网络攻击时，通过技术、策略和流程的结合，主动或被动地抵御、干扰、反击攻击者，以保护网络、系统和数据安全的能力。

能力等级标准如下：

a) 基础级（L1）

- 1) 组织建设方面：具备信息技术人员开展基本的安全对抗概念的研究。

b) 发展级（L2）

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的安全对抗工作。
- 2) 制度流程方面：初步制定网络安全对抗的相关流程，如定期检查安全设备的日志。

c) 协同级（L3）

- 1) 组织建设方面：具备专人或专岗负责网络安全对抗工作，并设定具体的职责。
- 2) 制度流程方面：
 - i. 制定详细完善的网络安全对抗流程和操作方式，如攻击对抗手册；
 - ii. 建立网络安全对抗机制，定期开展对抗演练，提高团队的实战能力。
- 3) 技术工具方面：具备多层次多维度的网络安全对抗工具，可实现部分自动化网络安全对抗。
- 4) 人员能力方面：了解常见漏洞利用、攻防对抗的知识和技术，可在第三方网络安全公司协助下开展网络安全对抗工作。

d) 优秀级（L4）

- 1) 组织建设方面：组建专门的团队以承担网络安全对抗管理工作的职责，确保职责匹配到人员，明确团队工作目标，制定网络安全对抗频率等具体的绩效指标，并实施量化管理。
- 2) 技术工具方面：实现安全日志、入侵检测等系统与主动防御工作的动态联动，提高对抗的效率和准确性。
- 3) 人员能力方面：具备一定的网络安全对抗能力，可独立开展网络安全对抗工作。

e) 卓越级（L5）

- 1) 组织建设方面：配备专业团队，开展网络安全对抗技术的研究，不断优化对抗策略和方法。
- 2) 制度流程方面：建立对抗效果评估机制，定期评估对抗效果，持续完善对抗策略。

6.7.3 安全运营规划能力（CSD07.03）

安全运营规划能力是指组织通过系统化的流程、技术工具和人员协作，对自身安全运营工作持续评估、总结、完善的规划能力。

能力等级标准如下：

a) 基础级 (L1)

1) 组织建设方面: 具备信息技术人员开展基本的安全运营方法的研究。

b) 发展级 (L2)

1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展基础的安全运营规划工作, 如通过定期安全评估发现存在的安全运营工作短板问题等。

2) 制度流程方面: 初步制定安全运营规划的相关机制, 如定期进行网络安全防御能力评估。

c) 协同级 (L3)

1) 组织建设方面: 具备专人或专岗负责安全运营规划工作, 并设定具体的职责。

2) 制度流程方面: 建立安全运营规划机制, 明确规划工作节奏, 开展安全运营协作流程建设。

3) 技术工具方面:

i. 部署安全运营工具如态势感知平台, 实现对资产、漏洞、安全设备等全面集中管理;

ii. 实现安全运营平台和漏洞扫描、入侵防御、应用攻击检测工具等联动, 实现对安全运营全过程管理。

4) 人员能力方面:

i. 熟悉安全运营平台操作方式, 可管理各类安全设备;

ii. 具备较强的安全分析能力, 可依托平台开展安全运营优化工作, 确保运营流程的顺利进行。

d) 优秀级 (L4)

1) 组织建设方面:

i. 组建专门的团队以承担安全运营规划工作的职责, 确保职责匹配到人员或岗位, 并得到有效执行;

ii. 明确团队工作目标, 制定网络安全运营效率等具体的绩效指标, 并实施量化管理。

2) 技术工具方面: 实现安全运营平台同组织工单系统、统一权限系统等联动, 便于安全运营运转的持续优化。

e) 卓越级 (L5)

1) 组织建设方面: 配备专业团队, 开展安全运营的研究, 不断优化运营策略, 寻找安全与业务的平衡点。

6.8 人员管理能力 (CD08)

6.8.1 人员安全策略管理能力 (CSD08.01)

人员安全策略管理能力是指通过制定的一系列规则和措施明确员工在信息安全中应承担的义务和角色、规范员工的行为、降低人为因素导致安全风险的能力。

能力等级标准如下:

a) 基础级 (L1)

1) 组织建设方面: 具备信息技术人员开展基本的人员安全政策及责任的研究。

b) 发展级 (L2)

1) 组织建设方面: 具备信息技术人员依据经验或借助第三方工具开展基础的人员安全政策管理工作, 如定期对员工进行安全政策培训。

2) 制度流程方面:

i. 制定基础的人员安全管理制度, 如入职管理、保密协议等;

ii. 制定较为详细的安全操作流程, 包括密码管理、设备管理等, 并制定培训计划, 有序开展网络安全政策培训。

c) 协同级 (L3)

- 1) 组织建设方面：具备专人或专岗负责安全政策管理工作，并设定具体的职责。
- 2) 制度流程方面：
 - i. 制定详细且完善的安全操作流程，搭建安全操作流程体系，覆盖组织的所有岗位和人员；
 - ii. 制定员工安全责任书，明确员工在信息安全方面的权利和义务。
- 3) 技术工具方面：
 - i. 使用信息化工具记录组织的管理制度、安全策略和岗位职责内容和变更记录；
 - ii. 使用信息化工具监督员工对安全策略的执行情况，对非预期行为及时记录并告警。

d) 优秀级 (L4)

- 1) 制度流程方面：
 - i. 将人员绩效和安全违规行为进行有效关联，确保组织的管理制度、安全策略具备较强的约束力；
 - ii. 建立包括但不限于安全政策审查、合规性检查在内的监督机制，确保政策的有效性和适应性。
- 2) 技术工具方面：使用信息化工具开展安全政策及岗位职责的学习、考试等。

e) 卓越级 (L5)

- 1) 组织建设方面：配备人员安全政策及责任研究团队，定期评估现有政策的有效性和前瞻性，并根据评估结果进行必要的调整。
- 2) 制度流程方面：建立持续开展安全文化制度建设、不断提升员工安全意识的制度，建立与外部监管机构、行业组织的合作交流机制。

6.8.2 人员安全审计和监督能力 (CSD08.02)

人员安全审计和监督能力是指通过对员工的安全背景、行为和权限进行持续监控、审查、评估和管理，确保其符合安全要求的能力。

能力等级标准如下：

a) 基础级 (L1)

- 1) 组织建设方面：具备信息技术人员开展基本的人员安全审计和监督的研究。

b) 发展级 (L2)

- 1) 组织建设方面：具备信息技术人员依据经验或借助第三方工具开展基础的人员安全审计和监督工作。
- 2) 制度流程方面：制定较为详细的安全审计操作流程和指南，包括审计计划、审计报告等。

c) 协同级 (L3)

- 1) 组织建设方面：具备专人或专岗负责安全审计和监督工作，并设定具体的职责。
- 2) 制度流程方面：
 - i. 制定详细且完善的安全审计操作流程和指南，并将安全审计的结果和绩效考核相结合；
 - ii. 建立安全事件响应机制，明确安全审计过程中发现问题的处理流程。
- 3) 技术工具方面：采用了标准化的人员安全审计和监督工具，能够和人员绩效管理系统做对接，并对审计数据进行集中管理和展示，直观化人员安全审计和督查结果。
- 4) 人员能力方面：
 - i. 具备自动化工具使用能力，确保IT工具的使用效果；
 - ii. 具备安全事件响应能力，当在安全审计时发现问题时可及时有效处置。

d) 优秀级 (L4)

- 1) 制度流程方面：定期对安全审计和监督流程进行合规性审查和风险评估，持续优化和完善安全审计操作流程和指南。
 - 2) 技术工具方面：采用自动化的技术手段开展审计和监督工作，人员安全审计与监督系统实现与安全审计与日志管理、入侵检测等系统的联动，提高审计效率和准确性。
- e) 卓越级 (L5)
- 1) 组织建设方面：配备专业团队，定期评估和分析安全审计和监督的效果，持续调整和优化审计策略。
 - 2) 技术工具方面：具备对人员安全审计和监督进行智能分析的功能，提前识别潜在的安全风险。

6.8.3 人员离职安全管理能力 (CSD08.03)

人员离职管理能力是指通过系统化的流程和措施，确保员工离职过程的顺利进行，同时保护组织利益和员工权益。

能力等级标准如下：

- a) 基础级 (L1)
- 1) 组织建设方面：具备信息技术人员可依据零散经验处理离职员工的相关事宜，包括账户注销和资产回收。
- b) 发展级 (L2)
- 1) 组织建设方面：具备信息技术人员依据经验或第三方工具开展基础的人员离职管理工作。
 - 2) 制度流程方面：制定初步的离职管理操作流程和指南，包括离职检查清单、资产回收确认流程等。
- c) 协同级 (L3)
- 1) 组织建设方面：具备专人或专岗负责人员离职管理工作，并设定具体的职责。
 - 2) 制度流程方面：
 - i. 制定详细且完善的人员离职操作流程和指南，根据岗位职责制定保密协议并约束员工签署和遵从；
 - ii. 制定离职员工信息泄露应急预案，明确发生信息泄露时的处理步骤。
 - 3) 技术工具方面：
 - i. 采用自动化工具和技术手段，对离职流程进行集中管理和监控；
 - ii. 同组织的统一权限管理等系统联动，自动清除离职人员相关权限。
 - 4) 人员能力方面：具备离职管理自动化工具使用能力，确保人员离职有序开展，各项权限及时回收。
- d) 优秀级 (L4)
- 1) 制度流程方面：
 - i. 定期对人员离职流程进行合规性审查和风险评估，持续优化和完善人员离职操作流程和指南；
 - ii. 对离职管理工作的目标和绩效提出具体要求，并实施量化管理。
 - 2) 技术工具方面：使用技术工具对组织的互联网敏感信息进行持续监控，及时发现离职员工泄漏有关组织的敏感信息。
- e) 卓越级 (L5)
- 1) 组织建设方面：配备专业团队对离职员工的行为数据进行智能分析，定期评估和分析离职管理的效果，不断调整和优化管理策略。
 - 2) 制度流程方面：建立全面的人员离职员工信息安全管理体系统，包括离职后一段时间内的相关信息持续监控，确保无任何信息泄露风险。

附 录 A

(资料性附录)

网络安全能力成熟度评估程序与方法示例

一、访谈调研阶段。

首先需确定评估范围及评估对象，调查并了解组织网络安全组织架构、管理流程和技术环境，确定评估范围的边界以及范围内的所有信息化资产；然后与接口人员确定访谈内容及访谈对象，制定访谈计划；其次针对制定的访谈计划开展访谈工作，详细记录访谈内容并保存为电子记录。

二、结果分析阶段。

整理访谈电子记录并输出访谈记录表；依托攻防能力成熟度评估工具进行初次成熟度评定；针对初次评定的结果在内部由专家组进行审核形成最终结论。

三、目标引入阶段。

选取并基于行业基线形成目标参考，确定具体的初步量化目标；基于选取的量化目标，针对自身的业务特点以及具体需求进行量化目标修正，形成最终的量化目标。

四、差距分析阶段。

针对成熟度评定结果，对比最终的量化目标进行差距分析，筛选出不符合的指标项；将指标项进行整合，确定要推进的工作内容以及立项建议。

五、评估汇报阶段。

整合访谈记录，成熟度评估结果，量化目标选取结果，工作内容以及立项需求出具完整的攻防能力成熟度评估报告；通过汇报的方式向组织输出项目成果。

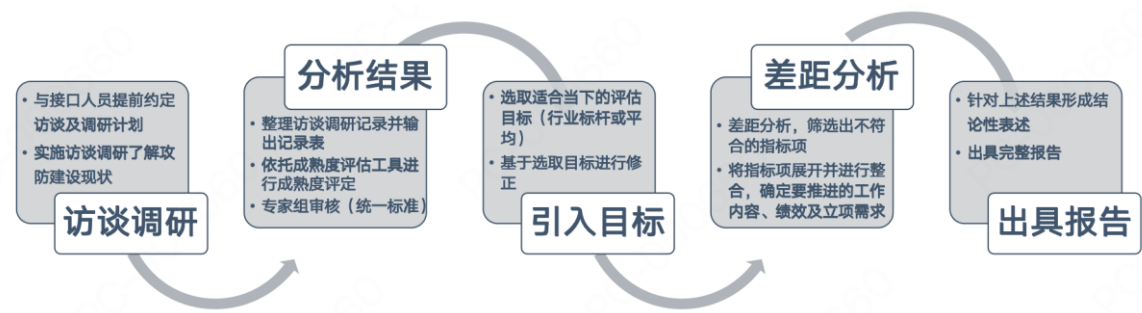


图2 证券期货业网络安全能力成熟度评估流程示意图

打分表可参考如下模板：

序号	能力模块	能力项	现状记录	得分
1	攻击预防能力 (CD01)	CD01.01 漏洞预防能力	示例：专门的团队负责具体的漏洞预警工作，设计了标准化的模板进行漏洞预警。在整体流程中定义了高危漏洞响应的规则以及时间要求。	

2		CD01.02 漏洞评估能力	示例：具备专人负责扫描器以定期评估（未建立基线），评级机制按照扫描器进行，未做标准化评级。定期引入厂商的渗透测试。采购了扫描器。	
3		CD01.03 漏洞修复能力	示例：具备专人负责，建立了漏洞修复的标准。人员的能力和技能良好	
4		CD01.04 威胁预警能力	示例：具备专人负责，但并未设置标准化的模板即统一的渠道	
5		CD01.05 威胁评估能力		
6		CD01.06 威胁抵御能力		
7	安全加固能力 (CD02)	CD02.01 账户与权限管理能力		
8		CD02.02 安全配置管理能力		
9		CD02.03 隔离技术		
10		CD02.04 加密与签名管理能力		
11		CD02.05 数据备份管理能力		
12		CD02.06 功能简化能力		
13		CD02.07 黑白名单管理能力		
14		CD02.08 网络访问控制管理能力		
15		CD02.09 身份认证管理能力		
16		CD02.10 安全域管理能力		
17		CD02.11 基线管理能力		
18		CD02.12 日志管理能力		
19		CD02.13 软件更新管理能力		
20	事件检测能力 (CD03)	CD03.01 边界入侵检测能力		
21		CD03.02 应用攻击检测能力		
22		CD03.03 未知威胁发现能力		
23		CD03.04 病毒与恶意软件检测能力		
24		CD03.05 端点行为检测能力		
25		CD03.06 流量检测能力		
26	事件响应能力 (CD04)	CD04.01 边界入侵防御能力		
27		CD04.02 应用攻击防护能力		
28		CD04.03 防病毒与反恶意软件能力		
29		CD04.04 端点行为防护能力		
30		CD04.05 流量过滤能力		
31	诱捕溯源能力 (CD05)	CD05.01 攻击诱捕能力		
32		CD05.02 溯源取证能力		
33	关联分析能力 (CD06)	CD06.01 策略分析能力		
34		CD06.02 情报分析能力		
35	安全运营能力 (CD07)	CD07.01 安全培训能力		
36		CD07.02 安全对抗能力		

37		CD07.03 安全运营规划能力		
38	人员管理能力 (CD08)	CD08.01 人员安全政策管理能力		
39		CD08.02 人员安全审计和监督能力		
40		CD08.03 人员离职安全管理能力		
平均成熟度评分				

参 考 文 献

- [1] 中华人民共和国网络安全法
- [2] GB/T 25069-2010 信息安全技术 术语
- [3] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
- [4] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
- [5] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南
- [6] JR/T 0171-2020 个人金融信息保护技术规范
- [7] 《中国信息安全体系机构基本框架与构想》，计算机安全，DOI:
10.3969/j.issn.1671-0428.2002.01.011
- [8] MITRE ATT&CK: Design and Philosophy,
<https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy>
- [9] 自适应安全框架ASA2.0,
<https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/>