ICS 35.020
CCS L 70/84

# 团　　体　　标　　准

# 信息安全专员能力水平评价规范

Evaluation specification for the competence level of information security specialist

武汉企业信息化促进会
武汉市网络安全协会　　联合发布

# 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。

本文件主要参考中共中央办公厅国务院办公厅《关于分类推进人才评价机制改革的指导意见》中明确提出的健全以市场和出资人认可为重要标准的组织经营管理人才评价体系，在国标 GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求》基础上，面对企业的信息安全及数据安全的从业人员或即将上岗的信息安全从业人员，围绕工作者的工作学识、工作经验、工作技能、安全认证与评估、基础知识、安全事件处置等方面展开全方位的工作评定，目标是提升人员能力、提升企业或组织经营能力、实现信息安全赋能企业的战略目标，制定了相关评估细则和要求，最大程度的满足企业对数字安全需求的价值实现及安全的保障企业数字化系统持续服务目标。面向信息安全方向专业专职人才的培养目标，建立社会化的高端网络安全人才评价制度，发挥市场、社会等多元评价主体作用，突出对个人专业能力，个人管理能力，企业经营业绩和综合素质的评价和考核，积极培育发展各级信息安全人才评价社会组织和专业机构，逐步有序承接政府转移的人才评价职能，建立信息安全人才评价机构综合评估、动态调整机制的相关政策而制定的人才评价标准规范。

本文件由武汉市工业信息化中心指导，由武汉乾跃信息技术有限公司牵头起草。

本文件由武汉企业信息化促进会和武汉市网络安全协会提出并归口。

本文件起草单位（排名不分先后）：湖北省电子信息产品质量监督检验院、武汉大学国家网络安全学院、武汉工程大学计算机科学与工程学院、武汉职业技术学院信创学院、武昌船舶重工集团有限公司、长飞光纤光缆股份有限公司、武汉城市数字科技有限公司、武汉中科通达高新技术股份有限公司、湖北东贝机电集团股份有限公司、武汉烽火信息集成技术有限公司、深信服科技股份有限公司、武汉安恒信息科技有限公司、武汉观安信息技术有限公司、武汉鸿源信息化发展有限公司、武汉青牛智能科技有限公司、武汉华工正源光子技术有限公司、武汉创信博达信息技术有限公司、湖北星野科技发展有限公司、北京网御星云信息技术有限公司、湖北数智安信科技有限公司。

本文件主要起草人（排名不分先后）：刘浩、胡颸、刘悦恒、何德彪、吴静、徐文霞、徐银霞、邓小飞、冯希胤、胡成国、戴维娇、徐亚军、白玉东、梅蕊、王超、商哲旻、王开学、盛智标、朱博、罗伦文、陈烨、何双江、邱秋鹏、彭建军、童文茂、冯颖琼、周利斌、上官含章、李春、施兴海、杨泽渊、邵峰、刘泽洋、王冰、赵德宝、路炳华、张淑英、江玉至、龚臣、徐煦、乔奇、李媛。

# 信息安全专员能力水平评价规范

## 1 范围

本文件规定了信息安全专员的岗位定义、职业水平等级和信用等级、申报条件、申报流程和认定要求。

本文件适用于信息安全专员类人才的职业水平等级和信用等级评价、鉴定、管理、职业培训等。

本文件中所述信息安全包含但不限于网络安全、数据安全、工业互联网安全、智能网联汽车安全、云安全等内容。其中工业互联网安全可以细分为设备安全、控制安全和应用安全等专业性内容，对应的人员岗位为网络安全官、数据安全官、应用安全官；设备安全是指智能传感器、工业机器人、智能仪表、智能产品等安全；控制安全是指 SCADA（Supervisory Control And Data Acquisition，监视控制与数据采集系统）、DCS（Distributed Control System，分布式控制系统）/FCS（FieldBus Control System），现场总线控制系统）、PLC（Programmable Logic Controller，可编程序逻辑控制器 ）、HDMI（High Definition Multimedia Interface，高清多媒体接口）等安全；应用安全是指 CAx（CAD、CAM、CAE、CAPP、CIM、CIMS、CAS、CAT、CAI 等各项技术之综合叫法）、PLM（Product Lifecycle Management，产品生命周期管理）、ERP（Enterprise Resource Planning,企业资源计划）、MES（Manufacturing Execution System，制造执行系统）、CRM（Customer Relationship Management,客户关系管理系统）、SCM（Supply Chain Management,供应链管理系统）、BI（Business Intelligence，商业智能）等应用系统安全。

## 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—2022　信息安全技术　术语

GB/T 42446—2023　信息安全技术　网络安全从业人员能力基本要求

## 3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

### 3.1 网络空间安全 Cyberspace Security

是网络空间作为信息环境中一个整体域的安全性。网络空间安全本质上指在网络空间框架下的信息安全，完整定义是“所有类型的计算机系统和计算机网络环境、物理环境及相关人的安全”。

### 3.2 数据安全 Data Security

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.3 **安全从业人员** Security Workforce

从事安全工作，承担相应安全职责，并具有相应安全知识和技能的人员。

[**来源**：GB/T 42446-2023，3.1，有修改]

3.4 **信息安全专员** Information Security Specialist

在企业中负责企业的信息安全管理或信息安全防范措施的工作人员，可以是信息安全工程师、信息安全运维人员、信息安全管理者。能配合企业信息官完成相关的信息安全防护工作。本标准描述的信息安全专员，主要以技术为主，管理为辅，落实企业的信息安全防护措施。

3.5 **首席安全官** Chief security officer（CSO）

负责企业信息安全运行状态，保障企业的业务连续性，实施企业经营信息安全合规性和风险管理的目标。首席安全官岗位包含但不限于高级安全管理员、信息安全管理者、高层信息安全管理执行官。主要以管理为主，辅助技术实现和运营管理，施展组织及协调能力，理解企业的信息安全业务，保障企业的业务连续性。

3.6 **智能网联汽车** Connected and Automated Mobility(CAM)

是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与车、路、人、云端等智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等控制，可实现“安全、高效、舒适、节能”行驶的新一代汽车。

[**来源**：工业和信息化部关于加强车联网网络安全和数据安全工作的通知（工信部网安{2021}134 号）]

3.7 **工业互联网** Industrial Internet

是新一代信息通信技术与制造业深度融合的关键基础设施、新型应用模式和全新产业生态，通过人、机、物的全面互联，构建起全要素、全产业链、全价值链的全面连接、数据驱动的工业生产制造和服务体系，成为第四次工业革命的重要基石。

[**来源**：工业互联网综合标准化体系建设指南（2021 版）]

3.8 **知识** Knowledge

通过经验或教育获取的事实、信息、真理、原理或者领悟。

[**来源**：GB/T 42446-2023，3.2]

3.9 **技能** Skill

通过教育、培训、经验或其他方式完成任务的一种能力。

[**来源**：GB/T 42446-2023，3.3]

### 3.10 能力 Competence

综合运用知识和技能达到预期目的的本领。

[**来源**：GB/T 42446-2023，3.1]

## 4 信息安全专员职责和特征

### 4.1 信息安全专员职责

信息安全专员需要在国家规定的网络安全相关的法律法规的范围内对整个企业的安全运行状态负责，既包括物理安全又包括数字安全（包含网络安全、数据安全、工业控制系统信息网络安全、工业互联网安全、智能网联汽车安全、云安全）。信息安全专员具体职责包含但不限于以下内容：

a）负责监控、协调企业内部的信息安全工作，包括信息技术、人力资源、通信、数据资产、设备管理、应用安全管理、控制安全管理以及其他组织；

b）确定保护目标和保护制度与企业的战略计划保持一致，制定及执行企业的信息安全策略、信息安全标准、指导方针和执行程序，以保证持续解决信息安全问题；

c）需要经常举办或参加相关领域的活动，如参与和业务连续性、损失预防、诈骗预防和保护隐私等相关议题的活动，保持对新兴技术的学习和更新能力；

d）负责供应链安全，监控和跟踪供应链的全过程安全，保护企业资产、知识产权和计算机系统安全；

e）信息保护职责包括：完善网络安全结构，监控网络访问，跟踪政策变化，及时为企业普及更新后的政策要点，组织企业员工参加信息安全相关政策的培训，提升企业全员的网络安全意识等；

f）执行全面监控信息安全事件响应计划，及时应急响应并解决企业信息安全事件；

g）安全审计：监测、记录系统运行状态、日常操作、故障维护、远程运维等，并留存相关日志；

h）制定并执行全面的风险管理策略，并确保策略的执行，全面监控产品的内部使用，并且确保工程小组与操作小组保持沟通，以便在产品出现问题时及时发现并解决问题，进一步完善灾难恢复和业务连续性策略，通过每一个业务单元的共同努力，确保企业拥有一个整合性良好的安全计划和策略。

针对以上信息安全专员职责范围，根据不同的行业及企业实际情况，对初级、中级、高级信息专员职责，从工作关注点、组织机构、汇报对象三方面进行阐述，具体工作职责包括但不限于以下描述。

#### 4.1.1 初级信息安全专员

承担企业内部主机安全、网络安全、数据安全、云基础设施的日常安全巡检，安全维护和日常运营，保障企业内部的业务系统能连续性运行；能组织及协调供应商的信息安全人员完成安全策略配置和安全架构工作；能及时发现信息安全事件并及时上报信息化主管，对企业信息安全规划提出合理化建议；完成日常信息化系统中涉及的设备、系统、应用等安全日常运维工作。

无需成立专门的信息安全部门或小组，工作汇报对象为信息安全中心主管和分管领导。

整体工作以执行为主，不参与规划、设计、监督、检查等工作。

### 4.1.2 中级信息安全专员

承担企业的日常信息安全运维工作，保障企业的信息化系统及业务系统持续运行；发现信息安全事件并能及时响应和处置；能对企业的信息化系统及支撑环境做出一定的信息安全规划（围绕技术、管理、运营），提出满足企业需求的信息安全管理体系和信息安全策略，构建企业的信息安全防护体系；能组织或协调人员完成信息安全态势监测、漏洞管理、安全加固、安全评估、安全意识培训与教育、代码审查、渗透测试、应急攻防演练等安全活动，并能指导部门其他人员申请初级信息安全专员或对已经是信息安全专员的人员提供工作内容和能力上的指导。

可以组建信息安全小组或部门，汇报对象为信息安全中心负责人。

整体工作以执行为主，参与信息安全需求设计、信息安全实现、信息安全运营等工作。

### 4.1.3 高级信息安全专员

配合企业的经营战略，提出信息和网络安全的顶层设计，构建企业的网络和数据安全架构，形成一套行之有效的管理体系、技术体系、运营模式，保障企业的信息化系统零安全事故目标；建立信息安全部门，带领团队和成员完成企业的战略经营目标，每年的信息安全设备及产品、软件、服务、人员的财务支出小于信息安全创造的价值；完成企业的信息安全教育与培训，提升企业员工的信息安全技能和信息安全事件应急能力；规划中、建设中、已运行的系统需满足国家及行业监管部门的合规风险要求，及时制定应对策略。

组建信息安全部门设定专人专岗，与信息中心的 CIO、企业的 CTO 等管理者并列，一起听从企业 CEO 管理工作，落实企业的安全需求、安全设计与规划、安全建设、安全运营、安全全生命周管理；从管理、技术、运营等三方面构建企业的信息安全防护体系，制定企业的信息安全战略目标，组织和协调人员保障业务连续性的目标，信息安全风险控制在最小范围。

## 4.2 信息安全专员职业特质

从初级信息安全专员到高级信息安全专员，需满足以下职业特质：

### 4.2.1 具有良好的职业道德

维护国家、社会和公众的信息安全，保护基础设施。行为得体、诚实、公正、负责和守法，为委托人提供尽职的、合格的服务，持续发展自身，维护荣誉。

### 4.2.2 具有较强的信息安全专业素养

熟悉 ISO27000/27001 安全体系和标准，熟悉《网络安全法》《密码法》《民法典》《数据安全法》《个人信息保护法》等网络安全相关的国家级法律法规。

#### 4.2.3 具有一定的安全风险管理素质

熟悉《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》《GB/T31509-2015 信息安全技术 信息安全风险评估实施指南》《GB/T 36466-2018 信息安全技术 工业控制系统风险评估实施指南》等国家标准，并能灵活应用于实践工作。

#### 4.2.4 具有一定的信息安全专业知识和技术技能

理解并熟悉网络安全基础知识（OSI 七层模型、TCP/IP 协议及安全漏洞、计算机主机安全、数据库安全、恶意程序、计算机病毒、日志审计、web 安全等）、密码学知识、安全渗透测试知识、漏洞扫描技术、防火墙技术、入侵检测及防御技术、数据防泄漏技术、流量检测与分析技术、安全态势感知技术。

#### 4.2.5 具有一定的信息安全运营能力

结合企业业务及发展要求，应用安全技术和管理措施，保障企业的日常信息安全运营，建立信息安全运营管理体系、技术实现流程及制度、运营管理制度和流程，围绕数字安全展开日常工作，保障企业设备、系统、应用软件、网络通信环境、业务的正常运转，提升企业的服务能力。

#### 4.2.6 具有良好的身心素质

有健康的身体和职业心态，心理承受与调适能力较强，抗压能力强、适应高强度工作。

### 4.3 职业水平等级和信用等级

信息安全专员根据水平评价划分等级为：初级信息安全专员、中级信息安全专员、高级信息安全专员三个等级。其中，初级信息安全专员为入门级或预备级的信息安全人员，需具备基础信息安全知识和基础信息安全技能，满足企业正常运营的基本信息安全要求。

职业信用等级分为：C、B、A。针对每一等级信息安全专员，均可申请 C、B、A 信用等级，其中：C 等级为基本信用等级，但 C 级的信用风险较高；B 级是在满足基本信用等级基础上，在职员工持有信息安全领域国家级证书数量不低于 2 份，且持有时间不低于 2 年，持证证书的级别、企业的信息安全能力获得行业认可、具有行业领导力、信息安全事故年发生率低于 30%、信息安全事件损失低于 100 万元，B 级信用风险较低；A 级是满足基本等级基础上，在职员工持有信息安全领域国家级证书数量多于 2 份，且持有时间多于 2 年，持证证书级别均为高级、企业信息安全能力获得区域或国家认可、具有区域、省级或国家级领导力、信息安全事故发生率低于 5%、信息安全事件损失低于 50 万元、A 级信用等级风险最小。

初次申报信息安全专员资质认证注册证书者无职业信用等级，获取信息安全专员等级资质认证证书两年以上方可申报职业信用等级；或申请者能提供从职业开始完整履约周期忠于组织，信守合同，依法纳税，取信于客户和员工，讲求信誉，兑现承诺，维护组织和消费者利益，履约期间企业未出现重大信息安全事故的有关证据，并由任职企业出具相应的证明材料，可以直接申请职业信用等级。对于各个级别信息安全专员，信任等级申请从 C 级开始。

## 5 能力要求

信息安全专员均需具备良好的职业道德和职业素养，其能力按照三个等级（分别为初级信息安全专员、中级信息安全专员、高级信息安全专员）有不同的要求。

面对不同级别的申请人员，持有证书可证明申请人员拥有信息安全基础知识，工作经验可证明申请人员具备一定专业技能，基础知识和专业技能是评定申请者的基本考核指标。各个等级的具体能力要求描述参见以下表 1：

| 能力要求 | 初级信息安全专员 | 中级信息安全专员 | 高级信息安全专员 |
|---|---|---|---|
| 学历要求 | 高中以上学历 | 高职、专科以上学历 | 本科以上学历 |
| 知识基础要求 | 有一定的计算机科学与技术、网络工程、信息安全、软件工程，通信工程，数字媒体技术等相关知识的基础，且有意愿从事信息安全领域工作的，均可申请。 | 有计算机科学与技术、网络工程、信息安全、软件工程，通信工程，数字媒体技术，信息与计算科学，人工智能等相关知识基础 | 有计算机科学与技术、网络工程、信息安全、软件工程，通信工程，数字媒体技术，信息与计算科学，人工智能等相关知识基础 |
| 工作年限要求 | 1. 高中学历：必须在企业从事信息安全工作 5 年以上；<br>2. 高职、专科学历以上即将毕业的学生，无工作年限要求<br>3. 已经在网络安全行业从业 2 年以内的在职人员； | 网络安全行业<br>从业年限满 3 年 | 网络安全行业<br>从业年限满 5 年 |
| 证书要求 | 1. 无特定证书要求；未获得任何证书的人员将按照正常评价流程进行面试和笔试；<br>2. 如持有 CISAW 预备级证书、NISP 证书、CISP-CISE（工程师）或数据安全工程师（初级））一项或多项的，将免去笔试，通过专家组的面试即可； | CISP 系列证书、CISAW（专业级）、数据安全工程师（中级）等相关证书一项或多项；或各大网络安全厂商自行推出的网络安全技能类的证书达到 2 个以上。（符合条件的网络安全厂商名单将由评定机构另行公布） | CISP-CISO（管理方向）、CISAW（高级专业级）、数据安全工程师等证书一项或以上，或各大网络安全厂商自行推出的网络安全技能类的证书达到 3 个以上。（符合条件的网络安全厂商名单将由评定机构另行公布） |
| 信息安全技能 | 了解网络安全基础知识，具备一定的信息安全技术技能，如了解常见网络安全设备的工作原理，基本的网络安全巡检和基本运维方法等。 | 除具备初级网络安全专员的技能外，还需要熟悉网络安全合规要求、网络安全相关的法律法规和标准，了解组织的业务战略和目标，能为组织制定和规划网络安全战略，并指导监督网络安全战略的落地实施。面对网络安全事件或突发的灾害性的网络安全事件，能积极应对，高效处置，最大限度降低企业因为信息安全事件而造成较大损害。 | 除具备中级网络安全专员的技能外，高级信息安全专员的信息安全技能要达到信息安全行业内专家水平，并具备多年的信息安全运营管理经验。 |

| | | | |
|---|---|---|---|
| 组织工作能力 | 具备部门内部和部门之间的组织及协调能力，可支撑企业的正常经营，通过执行信息安全相关的管理措施、技术手段、运维策略等解决企业日常的信息安全问题，面对网络安全事件能简单的响应并有效处置，并能形成安全报告向主管及时汇报。 | 除具备初级信息安全专员的组织工作能力外，还需要具备组建信息安全部门，协调信息安全部门和企业内部各部门之间的关系，协调信息安全部门和外部供应商、服务商之间的关系的能力，并能定期形成信息安全报告向主管进行汇报。 | 熟悉组织的业务战略和目标，能制定组织的网络安全战略和规划，并指导监督网络安全战略规划的落地实施，确保组织的业务满足信息安全合规要求，实现网络安全风险管理闭环和持续优化。能制定信息安全事件的应急响应预案、应急演练、应急处置，面对重大或突发的重大事件有监测手段和处置机制及流程，规避重大或特别重大事件的发生或事件发生后能高效处置。 |

表 1：不同等级信息安全专员能力要求表

**注**：表 1 中的各项能力要求仅是初次申请时需要参考的要求，在取得了相应的等级证书后，可以按照第 6 条中 g)项中的升级方法来取得更高等级的证书。

## 6 申报条件

特别声明：

a）申报人员需是具备完全行为能力的自然人。

b）申报人员须持有信息安全证书，且必须是在国家颁发许可的有效期内；持有的证书必须是信息安全范畴或者与其相关的信息安全职业技能认证证书。

c）企业是中国境内注册、经营正常、无不良诚信记录，均可以支持员工申报。

d）申报者获得评定机构审批后由评定机构颁发信息安全专员证书，证书有效期三年，持证期间需要到评定机构持续学习或分享相关知识以积累学分（参加技术沙龙活动或线上培训学习或分享个人经验），总学分 60 分；持证期间完成学分后缴纳一定的评定费用，可续证或升级证书。

e）初级信息安全专员升级到中级信息安全专员和高级信息安全专员，必须参加评定机构的培训认证，获得认证后，自动升级为对应的级别。

f）综合考评，根据申报者“学历”、“工作经验”、“持有证书”、“工作岗位”、“企业安全人力需求”、“时间”等方面，按照不同的比率由评定机构进行最终评价并颁发证书，初级信息安全专员按照基础知识 80%、专业技能 20%；中级信息安全专员按照基础知识 60%、专业技能 40%；高级信息安全专员按照基础知识 30%、专业技能 70%；同等条件下，每具备一项可见显示性证书材料，加分并优先选择；所有条件具备则直接颁发相对应的等级证书；其中，“时间”是特指持有证书或工作经验的一个显示性证明；

g）申报人员如持有国内知名网络安全厂商颁发的相关技能证书，也可直接申请相应等级的信息安全专员，同样，获得信息安全专员证书的申报人员也将获得相应安全厂商的认可，具体符合条件的网络安全厂商名单由评定机构另行公布。

h）获得初级、高级、中级等证书的持有者，需要在持证时间完成一定的学时学分（通过在线学习、线下参加活动、技术沙龙、分享个人经验或知识等方式积累学分），然后在证书三年期满前 1-3 个月申报换证。初级持证人员在获得证书满一年后，在完成了学时学分的基础上，可以申请升级到中级证书；中级持证人员在获得证书满两年后，在完成了学时学分的基础上，可以申请升级到高级证书，在

升级到高级证书时，需要满足高级基本要求，还需做出书面的应答考核（比如书面、论文、工作业绩、重大奖项、重大信息安全事件的处理能力等等），具体细则需要遵循评定机构的要求。

### 6.1 申报初级信息安全专员个人应该具备的条件

--具有高中学历（在企业信息安全岗位工作 5 年以上）或大专以上且有意从事信息安全领域工作的应届毕业生可直接申报，并按照正常评价流程进行笔试和面试。

--若申请人员为大专以上应届毕业生且持有 CISAW 预备级或 NISP 证书等信息安全技能型的职业认证证书（证书须在国家颁发许可的有效期内），可免去笔试环节，通过面试即可获得初级信息安全专员证书；

--若申请人员在组织中的信息化职能部门或信息安全岗位工作经历满 1 年，具有一定的信息安全工作经验，具备 CISP-CISE（工程师）、CISAW（预备级或初级）、数据安全工程师（初级）、NISP 等证书中的一项以上，或者在没有获得任何证书的情况下，所在企业愿意提供详细的工作情况证明（包括但不限于技术能力、工作成绩等），可免去笔试环节，通过面试即可获得初级信息安全专员证书；

### 6.2 申报中级信息安全专员个人应该具备的条件

--在组织中从事信息安全工作满 3 年或行业信息化职能部门工作满 2 年；

--持有 CISP 系列证书，CISP-CISO（管理方向）、CISAW（专业级）、数据安全工程师（中级）等证书中的一项；或持有国内网络安全厂商自行推出的网络安全技能类的证书达到 2 个以上。（符合条件的网络安全厂商名单将由评定机构另行公布）

--具有高职、专科及以上学历，在组织中担任网络安全职能部门主管、副主管/经理级管理工作者，在信息化职能部门或信息安全岗位工作相关经历满 2 年。

以上三项中具备 2 项或以上，就可以申报中级信息安全专员。

### 6.3 申报高级信息安全专员个人应该具备的条件

--需持有中级信息安全专员证书；

--在组织中从事信息安全工作经验满 5 年或行业信息化工作 5 年或以上；

--持有 CISP-CISO（管理方向）、CISAW（高级专业级）、数据安全工程师等证书一项或以上；或持有国内网络安全厂商自行推出的网络安全技能类的证书达到 3 个以上。（符合条件的网络安全厂商名单将由评定机构另行公布）

--获得过国家级或省部级网络安全相关的奖励（发明专利、科研项目、发表高水平期刊、国际会议、参与组织团标或国标等）任何一项，在组织中担任网络安全职能部门主管、副主管/经理级管理工作者，在信息化职能部门或信息安全岗位工作相关经历满 5 年。

以上四项中，具备任意三项或以上，就可以申请高级信息安全专员。

## 7 认证要求

### 7.1 品德要求

a）遵纪守法，保密合规。

b）廉洁自律，不谋私利。

c）牢记职责，爱岗敬业。
d）客观严谨，公平公正。
e）流程规范，操作安全。
f）认真负责，团结协作。
g）挑战自我，勇于创新。

## 7.2 知识要求

### 7.2.1 通用知识要求

信息安全专员应该具备 GB/T 42446-2023 的 5.1 规定的通用知识要求。

### 7.2.2 各级信息安全专员网络安全知识要求

各级信息安全专员应该掌握的网络安全知识参见以下表 2：

| 级别 | 网络安全知识类别 | 具体的网络安全知识 |
| --- | --- | --- |
| 初级信息安全专员 | 网络安全基础 | 计算机基础知识、网络安全基础知识、密码学基础知识、TCP/IP 协议、数据库基础知识、OSI 七层模型及安全漏洞、操作系统基础知识；<br>熟悉网络安全设备工作原理及操作使用，网络安全设备包含但不限于防火墙、入侵检测、上网行为、堡垒机、日志审计、网闸、上网行为等设备；<br>了解网络安全攻防技术，比如终端安全、病毒查杀、补丁升级、恶意程序防范、漏洞防范；<br>了解主机安全、web 应用安全、数据库安全； |
| | 网络安全管理知识 | 信息安全运维管理，对设备、系统、账户、业务等进行信息安全保障，满足企业的信息系统的正常运行；<br>实施和落实信息安全技术实现，应用采购的技术、产品、服务等解决企业的信息安全问题和日常业务连续性需求<br>信息安全管理措施，配合企业信息安全主管，完成简单的信息安全标准、体系、流程、制度、文化等建设，满足企业的信息安全合规要求；<br>应急管理，能对企业发生的信息安全事件及时应对和处置，完成设备或系统的安全故障恢复；<br>漏洞管理，发现漏洞、识别漏洞、验证漏洞、升级补丁； |
| | 产品原理与应用知识 | 理解网络产品及信息安全设备功能原理、认知网络环境中信息安全防护对象和范围；<br>网络安全产品特指交换机、路由器、光传输设备、负载均衡、灾备等设备；安全设备特指防火墙、入侵检测/入侵防御、杀毒软件、堡垒机、安全管理系统、蜜罐、密码管理平台等网络安全等级保护中提到的 |

| | | |
|---|---|---|
| | | 20 余款信息安全产品； |
| | 教育培训 | 制定信息安全意识教育和培训计划、跟踪和落实教育培训管理、评估信息安全教育与培训、人员认证和企业认证的有效性保障； |
| 中级信息安全专员（包含具备初级信息安全专员的知识） | 专业知识 | 具备初级信息安全专员知识；熟悉信息安全保障框架模型、信息安全态势感知体系；<br>熟悉业务连续性、管理体系、认证认可和漏洞管理；熟悉 PKI/CA 体系、身份认证和访问控制等安全策略； |
| | 数据安全知识 | 数据相关的法律法规及政策标准指南；数据安全管理和技术；数据资产管理；数据风险评估；个人信息保护管理和技术；企业级数据安全防护策略和运营手段； |
| | 安全合规管理 | 等保、密评、关基、分级保护、攻防应急演练活动、数据分级分类、数据风险评估等保障企业持续经营的法律法规实施要求； |
| | 网络安全建模技术知识 | 构建企业级网络和数据安全风险模型，监测和告警，信息安全事件分析； |
| | 安全开发、测试及攻防技术知识 | 熟悉软件开发流程、应用 DevSecOps 模型监测和检查安全管理、安全编码规范管理、安全过程监测、安全发布验证管理和技术、安全评估（渗透测试、攻防验证、上线前评估）、网络攻防技术原理和实践流程； |
| | 网络安全监测分析技术知识 | 日志管理、事件管理、流量监测、网络安全分析方法和技术手段； |
| | 密码技术与应用知识 | 国际及国产密码体系、密码算法、协议、以及密码技术工作原理和技术手段、密码合规管理的风险管控、国产密码的应用法规要求； |
| | 云安全 | 理解无边界的云安全管理知识和应用场景、能实施云环境的安全防护及应用场景保护、规避云安全合规风险； |
| | 工业互联网安全 | 设备安全、控制安全、应用安全、通信及链路安全、安全监测与预警、应急响应； |
| | 车联网安全（可选） | 主机安全、通信协议安全、控制系统安全、供应链安全、组件安全、安全监测与预警、应急响应； |
| 高级信息安全专员（包含具备中级信息安全专员的知识） | 专业知识 | 安全管理、技术管理、运营管理、安全战略管理、安全驱动业务、项目管理的安全运营体系和标准、信息安全业务合规、风险管理、信息安全意识教育和培训管理、信息安全顶层设计、信息安全建设管理、优化和完善信息安全体系及流程、优化信息安全作业指导、应急管理、安全评估、安全业务和技术融合创新； |
| | 电子取证知识 | 日志分析、流量分析、业务异常分析、大数据关联性和一致性分析、取证调查方法和技术手段、取证调查管理体系； |
| | 新技术知识 | 零信任安全、人工智能、区块链、大数据、隐私安全和个人信息保护、云安全、数字安全、视频安全与防护、数据要素、移动安全、信创安全； |
| | 信创安全 | 熟悉和了解我国的硬件、软件、数据库、中间件、云平台、鸿蒙等信创设备及应用系统的安全；如何在实际应用环境中既要保障信创系统的正常运行又要保障信息安全策略的实施和落地。 |

表 2：各级信息安全专员应该掌握的网络安全知识

## 7.3 技能要求

### 7.3.1 通用技能要求

信息安全专员应该具备 GB/T 42446-2023 的 5.2 规定的通用技能要求。

### 7.3.2 各级信息安全专员网络安全技能要求

各级信息安全专员应该掌握的网络安全技能参见以下表 3：

| 级别 | 网络安全知识技能类别 | 具体的网络安全技能 |
| --- | --- | --- |
| 初级信息安全专员 | 网络安全管理 | 完成企业内的网络安全设备及系统的安全维护、安全支撑、技术实施协调工作；<br>能对网络安全设备进行操作并设定信息安全策略；<br>组织和协调人员，完成企业的信息安全规划、信息安全建设、信息安全使用；<br>账户安全管理、漏洞管理、应急管理、信息安全事件管理、终端安全管理、主机安全防护管理、制度及流程的简单管理； |
| 中级信息安全专员（包含具备初级信息安全专员的技能） | 网络安全应急 | 能识别网络威胁和信息安全事件进行跟踪响应和处置；能编制网络和数据安全事件应急预案；<br>能完成网络安全事件发现、研判和信息报送；能利用常见信息安全技术手段，对网络安全事件进行威胁抑制、入侵排查、追踪溯源；<br>能依据应急预案开展应急演练；<br>能根据数据安全风险评估标准进行数据安全攻防演练活动；<br>能组织人员参与内部或外部网络安全应急演练比赛； |
| | 信息安全运营 | 能构建信息安全运维体系，即制度、流程、人员、作业指导、标准化等技能；<br>能实施企业业务运营保障的考核指标，构建完善的信息安全 KPI 考量值，能定期进行信息安全运行评估； |
| | 网络安全测试 | 能组织人员或第三方人员对网络及数据系统进行渗透性测试，发现其安全风险；<br>能完成脆弱性测试和渗透性测试；<br>能对被测系统提出修复建议和防护措施； |
| | 信息安全建设 | 能识别企业中信息安全保护对象并分析其面临的安全风险能力；能理解网络安全需求；<br>能识别和评判供应商的信息安全产品技术能力；<br>能设计网络安全架构；<br>能完成网络安全及信息化设备选型； |
| | 数据安全 | 能带领团队完成组织级数据的全生命周期管理，构建企业级的数据安全成熟度模型，基于模型完善和优化安全能力、能力成熟度等级、数据安全过程等管理和技术体系能力； |

| | | |
|---|---|---|
| | | 能完成数据安全风险评估检查；<br>能进行数据合规风险管理；<br>有数据全生命周期的技术管控； |
| | 网络安全监测与分析 | 能收集、整理、管理威胁信息；<br>能识别并评估可能危及组织和/或合作伙伴利益的网络威胁和信息安全事件；<br>能使用各类方法和工具进行网络安全监测；<br>能监测数据安全风险并及时采取防护措施； |
| | 安全开发管理 | 能制定安全开发管理规范、软件开发安全编码制度、能管理代码安全漏洞、能设计和执行安全测试计划用例及方法； |
| | 供应链安全 | 能识别、评估、实施供应链安全； |
| | 信息安全评估 | 能建立一套信息安全风险评估系统、量化指标、风险值、风险预警值、风险分级分类； |
| | 工业互联网安全 | 了解工业互联网信息安全架构，熟悉组织内工业设备、应用、控制系统的安全漏洞及缺陷，能提出安全防护措施（技术、管理、运营），加强其安全防护能力； |
| 高级信息安全专员<br>（包含具备中级信息安全专员的技能） | 信息安全风险评估 | 能对组织内、组织外的系统进行安全风险评估，提升信息安全防护能力；<br>能识别资产、威胁、脆弱性和已有的信息安全控制措施；能使用或指导同事使用各类评估相关工具和方法，分析并评价信息安全风险；<br>能根据风险分析结构，提出风险处置建议，并编制评估报告； |
| | 信息安全审计 | 能管理、组织和实施审计；<br>能做出审计结论、提出审计建议、编制网络安全审计报告，并跟踪审计；<br>能结合标准及规范构建企业级的集中审计平台，汇聚数据进行安全审计；<br>对企业内部和外部的安全审计构建完善的体系、流程、标准、作业指导等； |
| | 信息安全认证 | 能对受审核方的信息进行收集和分析；<br>能按照审核准则编制审核计划；<br>能依据审核计划开展审核活动，发现不符项并编制审核报告；<br>能配合第三方机构完成企业的安全认证和评估，而不导致企业数据外泄或信息泄露；<br>能组织专家及服务厂商进行自我安全评估，为第三方机构认证审核提供基础条件； |
| | 信息安全创新 | 能结合组织实际情况开展信息安全技术、管理措施、运营机制等进行突破和创新；<br>能结合自身信息安全问题进行技术攻关和业务建模； |
| | 信息安全教育与培训 | 能组织相关人员及全员进行信息安全意识宣贯；<br>能对国家级的标准和政策进行学习；<br>能组织专业领域人员组织培训和认证考试； |
| | 信息安全咨询 | 能对企业战略发展，从信息安全角度提出合规、风险、业务增长的建议；<br>能结合政策和技术趋势，为组织构建动态的信息安全防护体系；<br>能对业务部门的信息安全需求提供合理的应对措施和防护解 |

| | | |
|---|---|---|
| | | 决手段；<br>能在管理会议上，提出网络通讯、数据全生命周期、终端设备、云设施、人员、制度、流程上的信息安全策略优化和完善；<br>能定期对企业的信息安全风险和预警进行通知和告警； |
| | 业务安全战略能力 | 基于信息安全专业知识和最佳实践经验，通过信息安全体系、标准、流程、制度、作业指导，能辅助企业在战略发展层面有新突破，实施信息安全保障能力提升企业的竞争力；<br>能通过信息安全创造价值，保障企业信息安全的同时让企业可持续经营；<br>具备战略眼光，能应用新技术、新模式，为企业的信息系统平台提升信息安全防护能力；<br>能实施零故障的信息安全防护管理要求； |
| | 数字安全素养提升 | 能对企业的数字化平台提供全方位的安全保障、提升全员信息安全防护意识、强化平台的持续安全稳定运行；能定期做风险评估、人员信息安全能力考核、信息安全素养检查等工作；定期进行信息安全考核和末位淘汰管理，一直保持信息安全组织及人员的高效率运作；<br>能做出详细地考核指标、量化考核、透明实施、零事故运营的管理模式； |
| | 学术研究 | 能结合组织及人员情况，把最佳实践形成方案或学术论文，对外发布；<br>能通过最佳实践提升企业竞争力，让信息安全变成增值业务；<br>能不断地融合和跨界，把业务、数据、网络基础设施形成一体化的平台，提升平台的运作效率，降低风险； |
| | 学习技能 | 能适应新技术和新业务模式的变革，如新漏洞的持续产生，AI 技术的发展带来的新的安全隐患等，基于这些变革，应具备快速学习和响应能力，提供及时有效的应对策略，通过不断学习解决新环境下的信息安全问题和信息安全需求。 |

**表 3**：各级信息安全专员应该掌握的网络安全技能

## 8 能力框架

a）初级信息安全专员，重点考核技术知识和基础工作执行能力。

b）中级信息安全专员，重点考核技术知识、项目管理能力、合规风险管理、应急管理、简单的信息安全业务（等保）。

c）高级信息安全专员，重点考核管理能力，通过管理技能提升企业的信息安全价值。

信息安全专员能力框架参见以下图 1：能力框架结构图

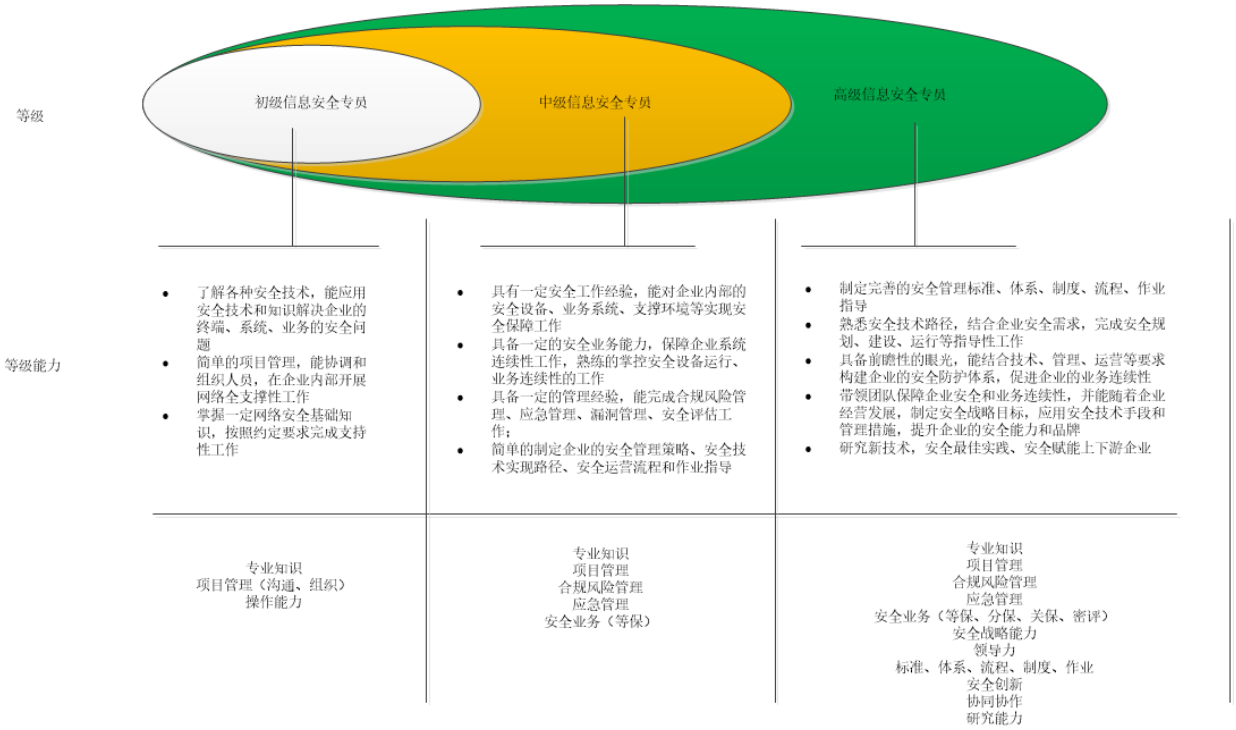


图 1：能力框架结构图

能力考核的维度，按照信息安全知识、信息安全技能、学习能力，评定不同信息安全专员的级别。能力考核维度参见以下图 2：能力考核维度

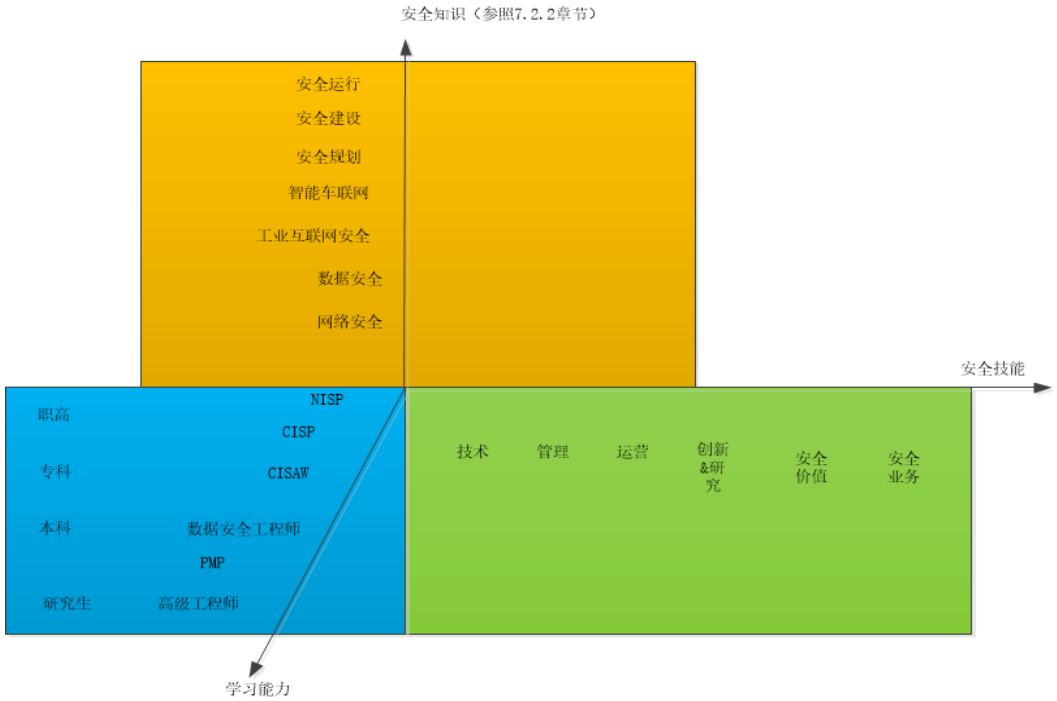


图 2：能力考核维度

## 9 评价方法

### 9.1 评价方法概述

分为理论知识考试、专业能力考核、管理能力素质测评。

### 9.2 理论知识考试

理论综合知识考试采用闭卷笔试方式，按百分制评分，60 分以上为合格。

a)初级信息安全专员:以信息安全技术为主,需掌握信息安全基本知识和基本工作技能，60 分合格；

b) 中级信息安全专员:以信息安全技术为主，辅以部分信息安全管理和信息安全运营的知识考点，60 分合格；

c) 高级信息安全专员：以信息安全管理为主，结合“信息安全基础知识+信息安全运营+信息安全管理”为内容进行考核，通过书面答题，70 分合格。

### 9.3 专业技能考核

分为业绩报告评估与综合评审两部分。

a）初级信息安全专员，已经工作的人员提供工作简历和企业推荐函即可；即将毕业的大学生需要学校提供就读专业证明和在校期间参加的网络安全相关的培训证明；已经毕业但尚未参加工作的学生需提供学历证明以及参加过的网络安全相关培训的证明。所有申请初级信息安全专员的若能提供 CISAW 预备级证书或 NISP 证书或 CISP-CISE（工程师）或数据安全工程师（初级）等信息安全技能型的职业认证证书（证书须在国家颁发许可的有效期内），则只需要参加面试即可。

b）业绩报告评估与综合评审：中级信息安全专员和高级信息安全专员学员按统一要求的格式提交工作业绩报告，由综合评审委员会进行综合评审。按百分制评分，60 分以上为合格。

### 9.4 管理能力素质测评

仅中、高级信息安全专员需要进行测评，采用管理能力测试软件进行测试与专家评估相结合的办法。学员在规定时间内完成测试，由测评机构为每位学员出具书面测评报告。测试时间 120 分钟，标准总分为 150 分。90 分为管理能力一级；100 分为管理能力二级；120 分为管理能力三级。

## 10 申报流程

a）个人向合格的评估机构获取《信息安全专员能力评定申请表》，并准备个人资质材料；

b）个人或企业为其员工发起申请；

c）评估机构对申请材料进行审核；

d）评估机构针对申请人员所在行业以及申请的级别进行汇总，确定评估考核时间，组织同类申报人员进行线下考核；

e）评估机构对考核合格的人员进行定级；

f）评估机构将考核和定级结果推荐上报；

注：个人申报流程图参见图 3：个人申报流程图

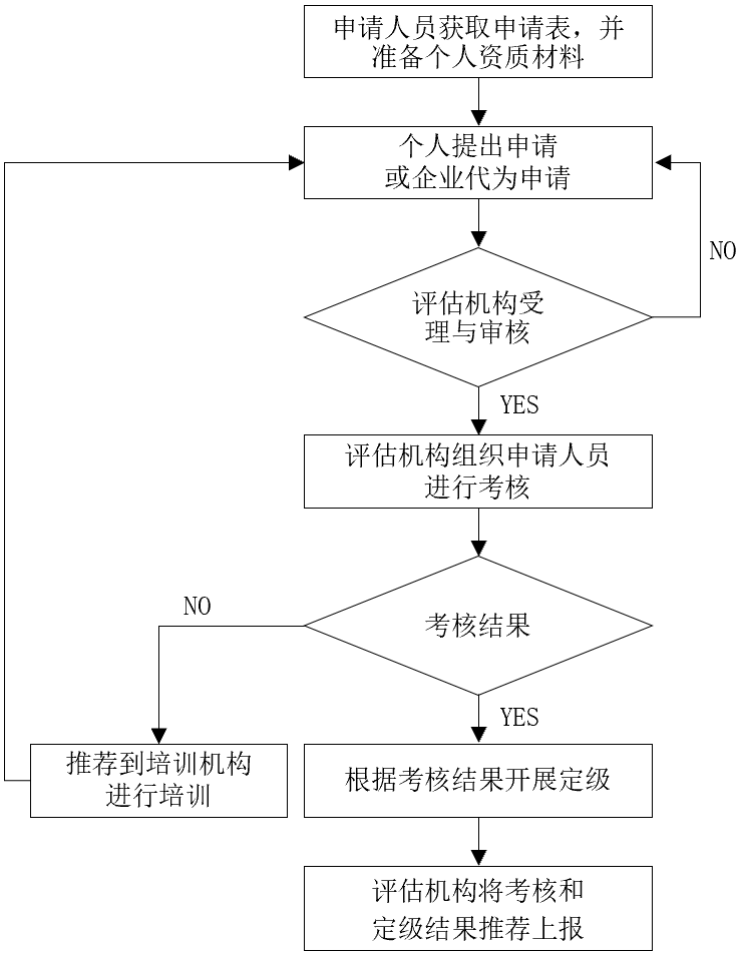


**图 3**：个人申报流程图

## 11 评估机构和评定机构

### 11.1 评估机构

#### 11.1.1 评估机构职能

评估机构主要负责：

a）面向市场宣传并推广本文件，引导更多人员申请信息安全专员证书；

b）接收申请人员的申请材料，组织申请人员进行考核，并将考核通过的人员情况及考核结果反馈给评定机构；

c）对于考核未通过的人员，引导该人员和经过认定的培训机构对接，帮助考核未通过的人员有效通过考核；

d）配合培训机构结合市场需求持续更新考核内容；

e）提交本单位专家人员材料，配合评定机构建设专家库。

#### 11.1.2 评估机构申请标准

a）申请机构须是在武汉市注册的独立法人单位；外地注册的法人单位须在武汉有分支机构；

b）申请机构应具有较好的社会诚信度，且近三年内无违纪、违法和不良信用等记录；

c） 申请机构所在行业应属于网络安全、数据安全或云安全领域，对于工业互联网和智能网联汽车行业的机构，机构内需设有专门的网络安全相关的部门；

d）申请机构人员规模应不少于 20 人，其中技术人员不少于 7 人，咨询人员不少于 3 人，机构应具备信息安全管理体系认证证书、信息技术服务管理体系认证证书、质量管理体系认证证书等资质；

e）申请机构在获得评估机构资格后，应每年引导不少于 100 人参与信息安全专员证书的申请；

f)每半年对获得评估机构资格的申请机构进行评估，评估维度包括对本文件的宣传工作情况；引导参与信息安全专员证书申请的人数；对申请人员进行考核的组织、管理、通报的情况等，年度总考核不合格的评估机构将有可能被取消评估资格。

### 11.2 评定机构

评定机构为本标准发布单位，评定规则另行规定。

# 参考文献

[1] GB/T 25069—2022　信息安全技术　术语

[2] GB/T 42446—2023　信息安全技术　网络安全从业人员能力基本要求

[3] 工业和信息化部关于加强车联网网络安全和数据安全工作的通知（工信部网安{2021}134 号）

[4] 工业互联网综合标准化体系建设指南（2021）