云服务信息安全管理体系认证实施规则

编号：CTS/CHTC 0020-2022

云服务信息安全管理体系认证实施规则

（版本：V0.01）

2022 年 06 月 20 日发布　　2022 年 06 月 20 日实施

北京五洲恒通认证有限公司发布

前　言

本认证实施规则由北京五洲恒通认证有限公司（以下简称 CHTC）制定、发布，版权归北京五洲恒通认证有限公司所有。

制定单位：北京五洲恒通认证有限公司

参与起草单位：北京五洲恒通认证有限公司、北京五洲恒通认证有限公司广东分公司

主要起草人：李国秋、曲丽、马尧、陈波、谢明峰

目　录

1 目的和适用范围 4
3 认证的基本过程 4
4 认证依据 4
5 认证人员要求 4
6 初次认证程序 5
6.1 认证申请 5
6.2 审核策划 7
6.2.1 审核时间 7
6.2.2 业务范围 8
6.2.3 审核组 8
6.2.4 审核通知 8
6.2.5 审核计划 8
6.2.6 多现场 9
6.3 审核实施 10
6.4 审核报告 13
6.5 不符合、纠正和纠正措施的有效性 14
6.6 复核和认证决定 14
7 监督审核 15
8 再认证 17
9 认证证书和认证标识 17
9.1 认证证书要求 17
9.2 认证标志 18
9.3 认证证书处理 19
10 与其他管理体系的结合审核 20
11 信息报告 21

11.1 获证组织信息通报 21
11.2 认证变更 21
11.3 信息报送 21
12 受理组织的申诉 22
13 认证记录的管理 22
14 认证收费 22
附件 1 23
附件 2 24
附件 3 25

1 目的和适用范围

1.1根据《中华人民共和国认证认可条例》、《认证机构管理办法》和《国家认监委关于认证规则备案的公告》等认证认可相关法律法规，结合相关技术标准，对规范云服务信息安全管理体系认证活动过程作出具体规定，明确ISO/IEC 27017《基于ISO/IEC27002信息安全控制的云服务-—实施要求》过程的相关责任，确保认证活动的规范有效，特制定本规则。

1.2本规则旨在阐述申请、实施和保持云服务信息安全管理体系认证方面的要求，适用于所有申请CHTC云服务信息安全管理体系认证的申请方、获证组织，也同时适用于CHTC开展云服务信息安全管理体系认证。

1.3本规则适用于云服务信息安全管理体系认证活动。

2 认证模式

文件审查+初始审查+获证后监督

3 认证的基本过程

云服务管理体系认证主要过程包括：认证申请及申请评审；文件审核；现场审核；复核、认证决定；获证后监督；再认证。

4 认证依据

ISO\IEC 27017《云服务信息安全管理体系》

5 认证人员要求

5.1 云服务审核员应当取得国家认监委确定的认证人员注册机构颁发的管理体系审核员注册资格，并接受本实施规则及认证依据的培训。

5.2 从事云服务管理体系认证活动的其他认证人员，如认证申请评审人员、认证方案管理人员、认证决定人员应当接受过认证依据及本认证实施规则的培训，具备相应的知识和技能。

5.3 认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

5.4 认证人员不得是国家法律法规和国家政策禁止或者限制从事活动的人员。

6 初次认证程序

6.1 认证申请

6.1.1 CHTC 应向认证申请人至少应公开以下信息：

(1)本认证实施规则；

(2)CHTC 和认证申请方的权利与义务；

(3)CHTC 处理申诉、投诉和争议的程序；

6.1.2 申请人应具备云服务信息安全管理体系认证的条件

（1）取得国家、地方市场监督管理部门或有关机构注册登记的法人资格（或其组成部分）；

(2)已取得相关法规规定的行政许可（适用时）；

(3)已取得 ISO/IEC27001 认证证书，或同时申请 ISO/IEC27001 认证；

(4) 生产、加工及经营的产品或提供的服务符合相关法律、法规、标准和规范的要求；

(5)已建立和实施了云服务信息安全管理体系，且有效运行三个月以上；

(6)未列入严重违法失信名单。

6.1.3 认证申请人应提交的文件和资料

认证申请人申请认证时，应提交正式书面申请，如实填写认证申请书，并同时提交以下材料：

(1)具备相关法定资质资格的证据，如：营业执照、生产经营许可证等；

(2)云服务信息安全管理体系文件；

(3)提交产品或服务符合中华人民共和国相关法律、法规和有关规范的要求；

(4)风险评估报告（含风险评估方法描述）；

(5)残余风险报告。

6.1.4 申请评审

CHTC 应在 10 个工作日内对提交的申请文件和资料进行评审并做出是否受理的决定，保存评审记录。

对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，或在信用中国列为“严重失信”的认证委托人 CHTC 不应受理其认证申请。

如不受理申请方的认证申请，CHTC 应书面通知申请方，并说明不受理的理由。

6.1.5 认证协议

对于受理的申请，认证机构应与认证委托人签订认证协议，规定双方的权利和义务。

6.2 审核策划

CHTC 应与申请方约定在认证审查实施各环节的相关责任和安排，并根据受审查方实际情况，按照本规则的要求，确定云服务信息安全管理体系认证审查实施的具体方案。

6.2.1 审核时间

为确保认证审核的完整有效，CHTC 应以附录 1 所规定的时间为基础，根据申请组织合规管理体系覆盖的活动范围、特性、技术、过程管理等复杂程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成需要的时间。可以减少审核时间，但减少的时间不得超过附件 1 所规定的 30%。

确定风险等级的条件：

低风险\一般风险组织：

(1)IT 基础设施不涉及重大项目或基建项目；

(2)没有行业特定的风险或特定的法律法规；

(3)三年内无违反相关信息安全法律法规；

符合下述其中一个条件的情况，该组织可判断为云服务信息安全管理过程管理认证高风险组织：

(1)项目涉及基建或重大工程；

(2)有特定的法律法规规定的情况；

(3)三年内有违反信息安全管理法律法规的情况。

6.2.2 业务范围

CHTC 依据 CNAS-SC170:2017《信息安全管理体系认证机构认可方案》附录 A 进行业务范围划分，业务分类见附件 2。

6.2.3 审核组

CHTC 根据审核需要，组成审查组，CHTC 委派具有相应能力的审查员组成审查组。当审查员专业能力不足时，需安排技术专家支撑审查相关专业内容。

6.2.4 审核通知

CHTC 在现场审查前向审查组下达审核通知书及审查任务书，通知申请方以及审查组，审查通知书及任务书包含以下内容：

1）审查依据，包括认证标准、认证实施规则和其他规范性文件；

2）审查范围；

3）审查组组长和成员，计划实施审查的时间；

4）上年度认证机构提出的不符合项（适用时）

6.2.5 审核计划

审核组应制定书面的审核计划，经认证机构审定后交认证委托人并获得确认。审查组长应在现场评审前将审查计划发给受审查方确认，如受审核方有不同意见及合理要求，审核组长应对计划予以调整。

6.2.6 多现场

当申请方存在多现场时，由认证方案管理人员根据抽样原则确定抽样审查的场所和数量，并在审核方案中描述。监督审查发现多现场变更时，审查组长应及时通知审核部调整审查方案，确保审查有效。

6.2.5.1 抽样原则

不同场所存在相同或相似的活动的场所可以进行抽样审查，多现场需满足下面三个准则：

1）所有现场运行在同一个 ISMS 体系下，该 ISMS 体系被集中管理和内部审核，并集中统一进行管理评审；

2）所有现场被包括在组织的内部 ISMS 审核方案和程序中；

3）所有现场被包括在组织的内部 ISMS 管理评审方案和程序中；

6.2.5.2 抽样要求

场所数开平方根并向上取整数。其他需要调整的因素考虑信息如下：

1）总部和各分现场的内审结果；

2）各分现场的业务内容和规模；

3）各分现场的信息安全管理体系的复杂程度；

4）各分现场所从事的活动或组织的变化；

5）分现场的业务代表性；

6）法规的要求；

6.3 审核实施

6.3.1文件审核

在实施现场审查前，CHTC应安排人员对认证申请组织的管理文件进行审查，确认认证申请组织的服务管理文件符合云服务信息安全管理体系认证要求及有关法规要求。文件审查人员由审查组长负责，当组长不具备专业能力时，审查组内具备专业的人员（如审核组员或技术专家）协同完成文件审查。

6.3.2 现场审查

现场审查从首次会议开始至末次会议末次会议结束初次审核分成一阶段审核和二阶段审核。，现场审核至少包括以下过程：

（1）召开首次会议；

（2）现场审查，收集并验证审查证据；

（3）确认审查发现；

（4）末次会议。

6.3.2.1 一阶段审核

一阶段审核的目的和内容如下：

(1)组织的 27017 管理体系文件；

(2)审核组织对标准要求理解，特别是关键绩效、风险等级、关键云服务信息安全、过程、目标和管理体系运行情况；

(3)评估组织的场所、有效人数是否和认证申请保持一致；

(4)收集和确定必要的信息，包括范围、过程、场所以及相关法律法规的符合性；

(5)与认证委托人沟通二阶段的审核安排和准备情况，达成共识；

一阶段发现的不符合或关注事项应在 3 个月内完成整改并关闭，在组长推荐下，可进入二阶段审核。

6.3.2.2 二阶段审核

二阶段审核的目的是评价云服务信息安全管理体系实施的有效性，收集包括现场审核，包括且不限于：

（1）符合云服务信息安全管理体系的信息和证据；

（2）符合相关信息安全的法律法规的信息和证据；

（3）风险评估和绩效测量结果；

（4）运行控制情况；

（5）规范性要求和目标、指标达成情况；

(6)与适用的云服务信息安全管理体系要求或其他规范性文件的所有要求的符合情况及证据；

(7)依据关键绩效目标和指标对绩效进行的监视、测量、报告和评审；

(8)云服务信息安全管理过程风险评估及对应的控制措施适宜性和有效性；

(9)企业云服务信息安全管理过程管理能力以及在符合适用法律法规要求和合同要求方面的绩效；

(10)顾客投诉的处理。

6.3.2.3信息收集方法应包括：

(1)面谈；

(2)对过程和活动进行观察；

(3)审查文件和记录。

6.3.2.4确定和记录审核发现

(1)审核员在记录审查发现时应简述符合性评定，详细描述不符合以及为其提供支持的审查证据，并予以记录和报告，为认证决定或保持认证提供充分的信息。

(2)审核组长应尝试解决审查组与受审查组织之间关于审查证据或审查发现的任何分歧意见，未解决的分歧点应在审查报告中予以记录。

6.3.2.5准备审查结论

在末次会议前，由审核组长负责召集审核组准备审核结论。审核组应：

(1)对照审查目的审查发现和审查中收集的任何其他适用的信息；

(2)考虑审查过程中内在的不确定性，就审查结论达成一致；

(3)确定任何必要的跟踪活动；

现场评审结论通常有以下三种：

(1)推荐/保持申请认证注册：有充分的客观证据，证明申请组织满足云服务信息安全管理体系和相关法律法规要求时。

(2)验证后推荐/保持申请认证注册：审查结果发现有不符合，进行后续的验证通过后，推荐认证注册。

(3)不推荐/暂停、撤销认证注册：审查结果发现认证申请组织存在严重问题，经整改仍不能达不到要求的。

6.3.2.6 终止审查

发生以下情况时，审查组应向 CHTC 报告，经同意后终止审查：

(1)客户对审查活动不予配合，审查活动无法进行；

(2)客户实际情况与申请材料有重大不一致；

(3)三年内，客户有重大媒体负面曝光或行政处罚的情况；

(4)一年内，因违反信息安全相关法律法规遭遇执法机构处罚的情况；

(5)其他导致审查程序无法完成的情况；

6.4 审核报告

审核组应为每次审查结束后应形成书面审查报告。报告应详细描述审核证据并有可追溯性。审查组应根据云服务信息安全管理体系认证要求将审查的结果形成审查结论，可以识别改进机会，但不应提出具体解决办法的建议。

6.4.1 审查报告编写

审查组长负责编写审查报告，审查报告应准确、简明和清晰地描述审查活动的主要内容，至少包括以下内容：

(1)申请组织的名称和地址；

(2)申请组织活动范围和场所；

(3)审查的类型、准则和目的；

(4)审查组组长、审查组成员及其个人注册信息；

(5)审查活动的实施日期和地点，包括固定现场和临时现场；

(6)审核实施的情况，审核证据、审核发现、不符合项及审核结论；

(7)对偏离审查计划情况的说明，包括对审查风险及影响审查结论的不确定性的客观陈述；

(8)审查组对是否通过或保持认证的意见。

6.4.2审核组长应将完整的审查报告提交CHTC，审查组长对审查报告中所有内容负责，审查报告所有权属于CHTC。

6.5 不符合、纠正和纠正措施的有效性

6.5.1审核组组长负责应在末次会前进行内部汇总，对照审核准则评价审核证据以形成审核发现。形成的《不符合报告单》应与受审核组织沟通并得到确认。

6.5.2对于审查中发现的不符合，审查组组长应根据不符合的性质要求受审查方在规定期限内进行原因分析并采取有效的纠正和纠正措施，以消除不符合。

6.5.3审查组组长应审查受审核组织提交的纠正和纠正措施，验证所采取的任何纠正和纠正措施的有效性，以确定其是否可被接受。对原因分析不到位或纠正/纠正措施有效性差的，应要求受申请方重新进行原因分析并采取有效的措施，直至被接受为止。

6.5.4对不符合纠正措施的验证方式可以是书面验证或现场验证。

6.6 复核和认证决定

6.6.1 复核

6.6.1.1 检查审核过程中产生的所有信息（如记录、数据、报告等）及结果，确保其完整性和准确性。

6.6.1.2 验证审核过程，确保其符合 CHTC 相关程序和相关标准要求。

6.6.2 认证决定

6.6.2.1 便于进行认证评定，审查组长负责提交完整的审查资料为认证评定提供信息，审查资料包括：

(1)认证申请及评审资料；

(2)审查通知任务书；

(3)文件审查报告；

(4)审查计划；

(5)首末次会议记录；

(6)现场审查记录或证据；

(7)不符合报告单及不符合纠正、纠正措施；

(8)审核报告；

(9)证书制作确认表。

6.6.2.2 认证决定结论如下：

(1)符合要求，颁发认证证书；

(2)需提供补充证据后确定是否认证注册颁发认证证书；

(3)对经评定不合格的认证申请组织，应做出不予以认证注册的决定，并将不能注册的原因书面通知认证申请组织。

7 监督审核

为确保客户云服务信息安全管理体系持续满足认证要求，在证书有效期内进行二次例行的监督审查；初次认证后，监督审查跟踪监督审核的最长时间间隔不超过十二个月；特殊情况可以适当延长，但两次监督审查的时间间隔不能超过十五个月；监督审核的时间不少于初次审核人日数的三分之一。

7.1 当发生下述情况时，可考虑增加监督频次：

(1)客户出现被执法机关处罚、媒体曝光或顾客投诉并造成较大影响；

(2)客户发生重大变更，包括法人、组织机构、相关职能等；

(3)认证依据发生变化时；

(4)发生其他特殊情况时。

7.2 监督审查至少包括以下内容：

(1)上次审核中确定的不符合采取的措施以及其有效性；

(2)客户投诉的接受和及时处理；

(3)目标的实现和调整情况，云服务信息安全管理体系有效性及管理绩效；

(4)云服务信息安全管理体系覆盖的活动所涉及法律法规的持续符合性；

(5)组织的任何变更；

(6)组织开展的持续改进活动；

(7)认证证书、标志的使用情况。

7.3 监督审查结果

(1)审查结果满足要求时，推荐保持认证。

(2)在监督审查中发现不符合，客户应分析原因，并按规定时限要求完成纠正和纠正措施，并提供纠正和纠正措施有效性的证据。审查组应采用适宜的方式验证客户对扣分项进行处置的效果后给出最终的推荐结论：

——整改后满足已获级别要求时保持认证资格。

——整改后不能满足要求，暂停证书。

——证书暂停六个月内，持证人整改仍不能满足要求时，撤销证书。

8 再认证

8.1 获证组织应在认证证书有效期结束前三个月向 CHTC 提出再认证申请，再认证程序与初次认证程序一致。当获证组织的云服务过程和范围未发生变更时，可适当减少评审程序，CHTC 应根据再认证审查结果，做出再认证决定。

8.2 云服务信息安全管理体系再认证审核的时间，根据云服务信息安全管理体系审核时间规定的相关要求进行确定，不少于初次审核人日数的三分之二。

8.3 CHTC 根据再认证审核组提交的审核资料，做出再认证决定；

9 认证证书和认证标识

9.1 认证证书要求

9.1.1 认证证书的有效期为三年。有效期内，认证证书的有效性依据的获证后定期监督结果获得保持。 认证证书内容至少应标明：

(1)客户/经营场所名称

(2)地址

(3)认证范围

(4)认证标准

(5)证书编号

(6)发证机构名称

(7)发证日期

(8)证书有效期

9.1.2 认证证书的管理

获证后，当涉及认证证书内容或认证依据发生变化时，客户应向 CHTC 提出变更申请，经 CHTC 评定后通过后换发证书。换发证书应注明发证日期和换证日期。

扩大认证范围和场所时，应安排现场审查，有关要求同初次认证；符合要求的，换发证书。

9.2 认证标志

9.2.1 准许使用的标志样式

获证组织可在广告、宣传品、信笺、名片、展销会或其他业务洽谈会场合等使用认证标识或认证证书，以宣传企业的管理体系认证状态，不得暗示该范围之外的业务也获得了认证。若获证组织的名称、地址、认证标准、认证范围发生变化，需向认证机构提出变更申请。

根据认证结果允许客户使用的认证标志如下所示，标志的制作和使用应符合 CHTC 的相关规定。

认证标志可等比例放大、缩小、变色使用，不得变形。

9.2.2 获证组织不能利用管理体系认证标识和相关文字、符号，误导公众认为其产品、服务通过认证。

9.2.3 当认证证书被暂停、注销或撤销认证时，应立即停止使用认证证书和带有认证标志的所有文件和宣传资料。

9.3 认证证书处理

对不符合认证要求的获证组织，CHTC 应对其认证证书进行处理，认证证书处理包含暂停、撤销和注销三种方式。

9.3.1 暂停认证证书

客户有下列情况之一的，将暂停其认证资格，暂停期最长不超过六个月，并以适当的方式进行公布：

(1)客户不按期接受认证监督的，或客户联系方式变更未及时通知 CHTC，导致无法联系不能实施监督审查时；

(2)监督审查发现客户云服务信息安全管理体系达不到认证要求的；

(3)认证证书和认证标志使用不当的；

(4)客户出现违反中华人民共和国保守国家秘密法事件；

(5)未按时交纳认证费用的；

(6)主动申请暂停认证证书；

CHTC 应根据上述不符合产生的原因，对客户的证书进行部分暂停或全部暂停的处置，必要时应缩小证书范围。

9.3.2 撤销认证证书

客户有下列情况之一的，将撤销其认证资格：

(1)被注销或撤销法律地位证明文件或有关的行政许可证明；

(2)暂停证书期满，但导致暂停的问题未能得到解决或纠正；

(3)出现违反中华人民共和国保守国家秘密法事件，且未能采取有效处理措施的；

(4)隐瞒、虚报或者所需信息，或其他不当方式获取认证证书的情况；

(5)不当使用认证证书、认证标志的；

(6)拒不交纳认证费用的；

9.3.3 注销认证证书

客户有下列情况之一的，将注销其认证注册资格：

(1)由于认证依据和技术条件的变更，客户达不到新要求的；

(2)认证有效期届满，客户不再提出再次认证申请的；

(3)客户主动申请注销证书；

9.3.4 恢复认证证书

当暂停原因得到消除后，CHTC 对暂停认证证书予以恢复。

10 与其他管理体系的结合审核

10.1 对云服务管理体系和其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，并易于识别。

10.2 结合审核的审核时间，不得少于多个单独体系所需审核时间之和的三分之二。

11 信息报告

11.1 获证组织信息通报

为确保云服务管理体系认证持续有效，获证组织应建立信息通报制度，及时向认证机构通报以下信息：

（1）有关组织机构变化的信息；

（2）消费者投诉的信息；

（3）有关质量、环境、安全等重大事故的信息；

（4）被有关执法监管部门责令停业整顿的信息；

（5）监督或行业主管部门抽查不合格的信息；

（6）受到行政部门相关处罚信息；

（7）其他违反法律法规行为的信息；

（8）顾客重大投诉；

（9）其他重要信息。

11.2 认证变更

当获证方名称、地址、产品、标准发生变更时，应及时向 CHTC 提交书面的变更申请，经机构评价和确定是否同意实施变更。

11.3 信息报送

CHTC 遵照国家认监委的相关要求报送认证信息。

12 受理组织的申诉

申请组织或获证组织对认证决定有异议时，应在认证决定后 30 日内提出，CHTC 接受其申诉并及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。认证决定 30 日后提出的申诉 CHTC 可不予受理。

13 认证记录的管理

13.1CHTC 应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

13.2 记录应当真实准确以证实认证活动得到有效实施，归档留存的时间为认证证书有效期届满或者被注销、撤销之日起 2 年以上，认证记录应当使用中文。

14 认证收费

14.1 收费标准

申请费：¥1000.00 元

审核费：¥3000.00 元/人日

注册费：¥2000.00 元

年　金：¥2000.00 元

14.2 收费要求

初次/再认证：认证申请+审查费+注册费

监督：审核费+年金 1

（一）现场最少审核时间表（适用于低/一般风险组织）

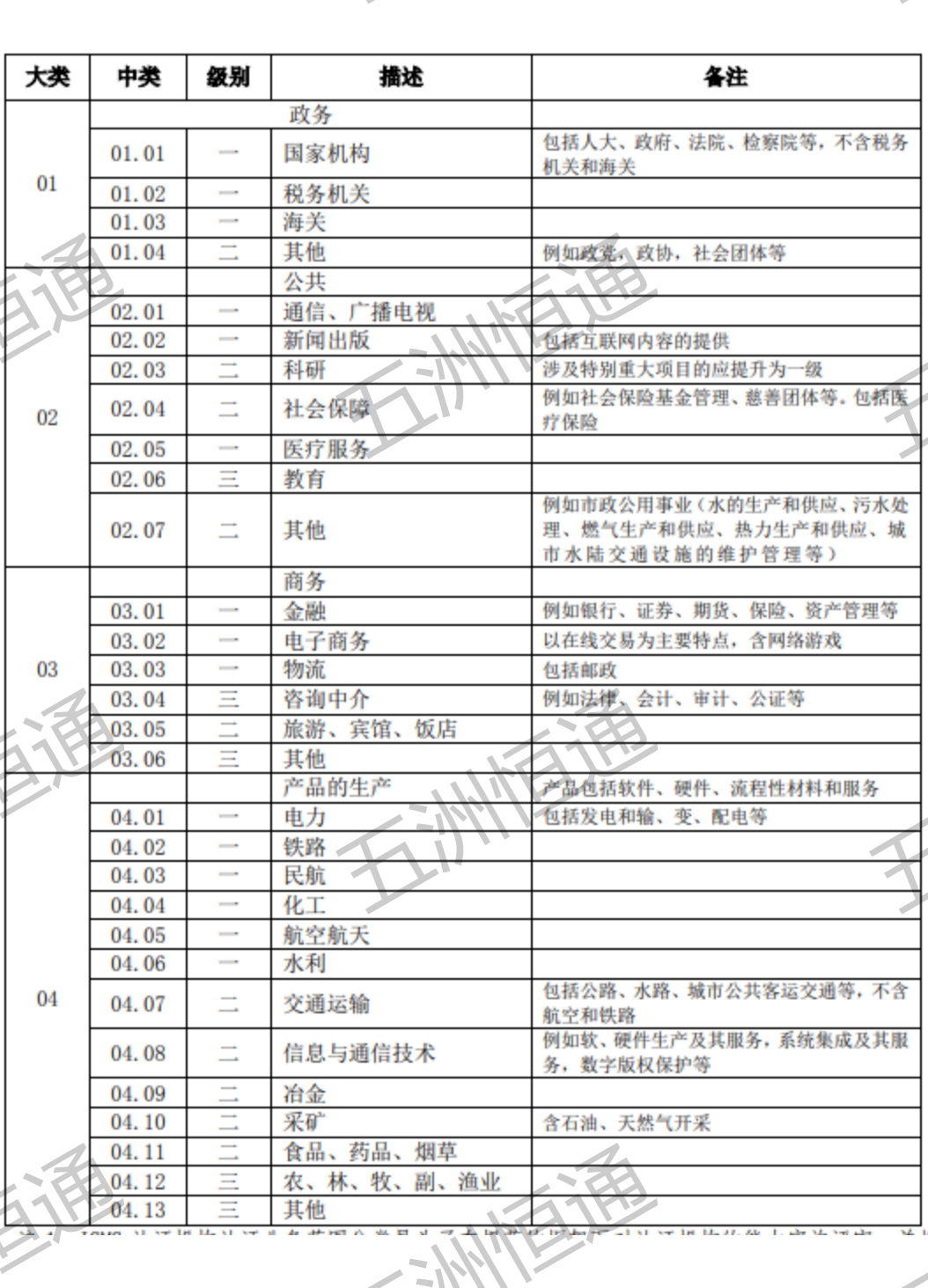
云服务信息安全管理体系覆盖人数	初次现场审查　（人日数）		监督现场审查人日数	再认证现场审查人日数
	第一阶段	第二阶段		
1-75	0.5	1.5	1	2
76-150	0.5	2.5	2	3
151-600	1	4	3	4
601-1000	1	5	3	5
1001-2000	2	5	4	5
2001-3000	2	6	4	6
3001-4000	2	7	5	7
4001-8000	2	8	5	8
8001-15000	3	8	6	8
15001 以上	3	9	6	9

（二）现场最少审核时间（适用于高风险组织）

云服务信息安全管理体系	初次现场审查　人日数		监督现场审查人日数	再认证现场审查人日数
	第一阶段	第二阶段		
1-75	1	2	2	3
76-150	1	3	3	4
151-600	1	5	4	5
601-1000	2	5	5	5
1001-2000	2	6	5	6
2001-3000	2	7	6	7
3001-4000	2	8	7	8
4001-8000	3	9	7	9
8001-15000	3	9	8	9
15001 以上	4	10	9	10

附件 2

业务范围分类



大类	中类	级别	描述	备注
01			政务	
	01.01	一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党、政协，社会团体等
02			公共	
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等，包括医疗保险
	02.05	一	医疗服务	
	02.06	三	教育	
	02.07	二	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03			商务	
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	二	旅游、宾馆、饭店	
	03.06	三	其他	
04			产品的生产	产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	