中部国际认证有限公司

信息安全管理体系认证实施规则

文件编号：CTS ZICC-GZ-ISMS-29

发布日期：2024-05-10

实施日期：2024-05-10

修订日期：2026-01-01

版　　本：A/2

编　　制：技术部

审　　核：郭魁娜

批　　准：王　华

修改记录

修改日期	修改人	修改次	修改内容	实施日期
2025.11.26	郭魁娜	1	调整一阶段不在申请组织现场进行的要求	2025.11.26
2026.01.01	郭魁娜	2	认证标准转换	2026.01.01

目录

1 目的和适用范围

1.1 为规范信息安全管理体系认证工作，根据《中华人民共和国认证认可条例》、《认证机构管理办法》等法规制定本规则。

1.2 本规则规定了本公司（或 ZICC）从事信息安全管理体系认证，实施信息安全管理体系认证的程序与管理的基本要求，是公司从事信息安全管理体系认证活动的基本依据。

1.3 本公司在中华人民共和国境内从事信息安全管理体系认证活动应遵守本规则。

2 认证依据

以 GB/T 22080—2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》为认证依据。

3 对认证人员的要求：

3.1 认证管理人员

包括机构主要业务主管负责人、认证规则和认证方案制定人员、申请评审人员、审核方案管理人员、人员能力评价人员、审核人员、认证决定人员等：

1）应通过 GB/T 22080—2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》标准基础知识及相关法律法规的学习，并经评价合格。

2）掌握相应管理岗位所涉及的知识和技能，经评价合格。

3.2 审核员

1）取得中国认证认可协会（CCAA）颁发的信息安全管理体系审核员注册资格。

2）认证人员应当遵守与从业相关的法律法规，对认证活动及做出的认证审核报告和认证结论的真实性承担相应的法律责任。

3）专业要求

(1)实施信息安全管理体系认证审核人员必须取得 CCAA 组织的信息安全管理体系认证注册资格，并得到 ZICC 的专业能力评价，以确定其能够胜任所安排的审核任务。认证业务范围分类及分级按附录 B 执行。

审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增强审核组的技术能力。

具有与管理体系相关的管理和法规等方面特定知识的技术专家可以成为审核组成员。技术专家应在审核员的指导下进行工作，可就受审核方或获证组织管理体系

中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员单独实施审核。

(2)信息安全管理体系审核人员应具备GB/T 19011 中 7.2所属的职业素质和通用知识和技能。

3.3 审核组长

信息安全管理体系组长应具备下述资格条件之一:

a、具备信息安全管理体系组长资格或经学习后评价合格。

b、参与两次的信息安全管理体系项目审核，见证一次并评价合格。

3.4 认证决定人员

为经本机构授权、对认证结果作出决定的人员。

3.4.1 审核人员应当取得中国认证认可协会（CCAA）的信息安全管理体系注册审核员，经过 GB/T 22080—2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》要求相关标准的培训，并考试合格。

3.4.2 认证人员应当遵守与从业相关的法律法规，对认证活动及做出的认证审核报告和认证结论的真实性承担相应的法律责任。

3.4.3 认证审核员还应具有以下方面特定的知识和技能：

与信息安全管理体系审核有关的方法和技术，能对信息安全管理体系进行评价并形成适当的结论，包括了解信息安全管理体系评价相关术语、信息安全管理体系基本要求和管理体系运行过程；能理解审核范围内的技术内容，包括信息安全管理体系证据的采集方式、信息安全管理体系运行过程实施、信息安全管理体系的关键资源、信息安全管理体系履行的知识和技能。

4 认证程序

4.1 认证申请

4.1.1 ZICC 应要求认证委托人具备以下条件：

（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）未列入严重违法失信名单；

（4）按照本规则规定的认证依据，建立和实施信息安全管理体系，且有效运行 3 个月以上；

（5）一年内未发生违反相关法律、法规的信息安全事故；

（6）三年内未违反相关法规或虚报、瞒报获证所需信息，而被 ZICC 撤销认证证书。

4.1.2 ZICC 应要求认证委托人提交以下文件和资料：

（1）认证申请；

（2）法律地位证明文件。当信息安全管理体系覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件；

（3）申请认证范围所涉及的法律法规要求的行政许可证明文件（适用时）；

（4）信息安全管理体系文件化信息；

（5）组织机构与职责说明；

（6）多场所清单、外包开发情况说明（适用时）；

（7）产品符合安全要求的相关证据；

（8）承诺遵守相关法律法规、ZICC 要求及提供材料真实有效的自我声明；

（9）其他需要的文件。

4.2 认证受理

4.2.1 ZICC 受理认证申请应至少公开以下信息：

（1）可开展认证业务的范围，以及获得相应认可的情况；

（2）开展认证活动所依据的认证标准；

（3）相关的认证方案、认证程序；

（4）批准、保持、变更、暂停、恢复、撤销认证证书的规定与程序；

（5）拟获取认证委托人的信息，以及对相关信息的保密规定；

（6）认证证书的使用规定；

（7）对认证过程的申诉、投诉规定；

（8）认证要求变更的规定。

4.2.2 申请评审

ZICC 应根据认证依据、程序等要求，对认证委托人提交的申请文件和资料进行评审并保存评审记录，以确保：

（1）认证要求规定明确、形成文件并得到理解；

（2）ZICC 和认证委托人之间在理解上的差异得到解决；

（3）对于申请的认证范围、认证委托人的工作场所和任何特殊要求，ZICC 均有能力开展认证服务。

4.2.3 评审结果处理

（1）申请材料齐全、符合要求的，予以受理认证申请；

（2）未通过申请评审的，应书面通知认证委托人在规定时间内补充、完善，不同意受理认证申请应明示理由。

4.3 签订认证合同

ZICC 应与认证委托人签订具有法律效力的书面认证合同。认证合同应明确信息安全管理体系覆盖的范围以及 ZICC 和认证委托人各自应当承担的责任、权利和义务。

4.4 审核方案和审核策划

4.4.1 ZICC 应对整个认证周期制定审核方案，确定适宜的审核时机，以使审核组能够在现场针对认证范围内有代表性的行业类别与子行业类别的典型产品/服务进行审核。

4.4.2 初次认证审核方案应包括两个阶段的初次审核、认证决定之后的监督审核及再认证审核。第一个三年的认证周期从初次认证决定算起，以后的周期从再认证决定算起。审核方案的确定和任何后续调整，应考虑认证委托人的规模，其信息安全管理体系的安全风险，以及经过证实的信息安全管理体系有效性水平和以前审核的结果。

4.4.3 初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核之间不应超过 15 个月。ZICC 应合理策划监督审核的时间间隔或频次。

4.4.4 当认证委托人的信息安全管理体系覆盖了多个场所时，ZICC 应对包括 ZICC 职能在内的所有场所实施认证审核，以确保审核的有效性。

4.4.5 如果认证委托人采用轮班作业，应在制定审核方案和编制审核计划时考虑在轮班工作中发生的活动。

4.4.7 审核时间

ZICC 按附录 A 中规定的审核时间为基础，并应至少考虑行业类别、产品/服务实现过程的复杂程度、涉及信息安全方面的员工数、场所数量等因素。

ZICC 应针对每个认证委托人确定策划和完成对其信息安全管理体系的完整有效审核所需的时间。

4.4.8 组建审核组

ZICC 应根据受审核方的行业、规模和业务复杂程度组建审核组，指派审核组长。审核组组建原则见第 3 章。

4.4.9 ZICC 应编制审核计划，审核计划中至少应包括以下内容：审核目的、审核准则、审核范围、审核日期、时间安排和场所、审核组成员及审核任务安排。

ZICC 应在现场审核活动开始前将审核计划提交给认证委托人进行确认，并留出足够的时间，以使认证委托人能够对某一审核组成员的任命表示反对，并在反对有效时使 ZICC 能够重组审核组。

4.5 初次认证

初次认证审核应分两个阶段实施：第一阶段审核和第二阶段审核。

4.5.1 第一阶段审核

4.5.1.1 第一阶段审核的目标是通过了解认证委托人的信息安全管理体系和认证委托人对第二阶段的准备状态，策划第二阶段审核的关注点。审核组应对受审核方开展一阶段审核，以确定：

1）受审核方的管理体系得到策划和实施；

2）受审核方的管理体系已运行，并有足够的证据证明其运行情况；

3）受审核方对运行的管理体系进行了监视、测量、分析和评价，并有充分的证据；

4）受审核方对管理体系进行了有效的持续改进；

5）受审核方是否识别并遵守了相关的法律法规；

6）受审核方有充足的资源保障现场审核的进行；

7）收集关于客户的管理体系范围、过程和场所的必要信息，包括：

a)客户的场所

b)使用的过程和设备

c)所建立的控制的水平（特别是客户为多场所时）

4.5.1.2 应告知认证委托人第一阶段审核的结果可能导致推迟或取消第二阶段审核。

4.5.1.3 对于第一阶段审核过的信息安全管理体系的相应部分，被确定为实施充分、有效并符合要求的，第二阶段可以不再对其审核。然而，ZICC 应确保信息安全管理体系已审核的部分持续符合认证要求。在这种情况下，审核报告应包含第一阶段审核中的审核发现，并且应清楚地表述第一阶段审核已经确立的符合性。

4.5.1.4 第一阶段审核提出的影响实施第二阶段审核的问题应在第二阶段审核前得到解决。第一阶段审核和第二阶段审核的时间间隔不应超过 3 个月。如果需要更长的时间间隔，应重新实施第一阶段。

4.5.1.5 在下列情况，第一阶段审核可以不在申请组织现场进行：

（1）申请组织已获本认证机构颁发的其他有效认证证书，认证机构已对申请组织信息安全管理体系有充分了解。

（2)申请组织获得了其他经认可机构认可的认证机构颁发的有效的管理体系认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在申请组织的现场进行。

4.5.2 第二阶段审核

4.5.2.1 审核组按照审核计划的安排对受审核方进行二阶段审核，二阶段审核应考虑一阶段审核结果，对受审核方的管理过程和控制措施的运行情况进行评价，对一阶段审核提出的问题改进情况进行验证。

4.5.2.2 二阶段审核的内容包括但不限于：

1）组织环境(应对风险和机会的措施，管理目标和达标计划)；

2）领导（管理承诺，方针，组织的角色、责任和权限）；

3）策划(应对风险和机会的措施，管理目标和实现计划)；

4）支持(资源，能力，意识，沟通，文件化信息)；

5）运行(运行的策划和控制，风险评估，风险处置)；

6）绩效评估(监视、测量、分析和评价，内部审核，管理评审)；

7）改进(不符合和纠正措施，持续改进)。

4.5.2.3 对于审核中发现的不符合，ZICC 应出具书面不符合报告，要求认证委托人在规定的期限内分析原因、说明为消除不符合已采取或拟采取的具体纠正和纠正措施，并提出明确的验证要求。ZICC 应评审认证委托人提交的纠正和纠正措施，以确定其是否可被接受。

4.5.2.4 如果 ZICC 不能在第二阶段审核结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则应在推荐认证前再实施一次第二阶段审核。

4.6 认证决定

ZICC 应制定批准、拒绝、保持、扩大或缩小认证范围、暂停、恢复或撤销认证的认证决定的规定与程序。

ZICC 在做出认证决定时，应获得与认证决定相关的所有信息，且所有不符合整改完成并得到验证。

ZICC 应制定认证决定人员的能力准则，被指定进行认证决定的人员应具有相应能力。审核组成员不应参与认证决定。

（1）综合评价

ZICC 应根据审核过程中收集的信息和其他有关信息，对审核结果进行综合评价，以及对产品的实际安全状况进行评价。必要时，ZICC 应对认证委托人满足所有认证依据的情况进行风险评估，以做出认证委托人所建立的信息安全管理体系能否获得认证的决定。

（2）认证决定

对于符合认证要求的认证委托人，ZICC 应颁发认证证书。

对于不符合认证要求的认证委托人，ZICC 应以书面的形式告知其不能通过认证的原因。

4.7 监督

4.7.1 监督审核

每次监督审核应尽可能覆盖认证范围内的有代表性的行业类别与子行业类别的典型产品/服务，如因产品/服务的季节性或客户需求等原因，监督审核难以覆盖认证范围内所有代表性的行业类别与子行业类别的典型产品/服务的，应保证在认证证书有效期内的监督审核覆盖认证范围内的所有代表性的行业类别与子行业类别的典型产品/服务。每次监督审核应至少包括对以下方面的审查：

（1）内部审核和管理评审；

（2）对上次审核中确定的不符合采取的措施；

（3）投诉的处理；

（4)信息安全管理体系在实现获证组织目标和信息安全管理体系的预期结果方

面的有效性；

（5）为持续改进而策划的活动的进展；

（6）持续的运作控制；

（7）任何变更；

（8）认证证书和标识和（或）任何其他对认证资格的使用。

4.7.2 监督审核结果评价

ZICC 应依据监督审核结果，对获证组织做出保持、暂停或撤销其认证资格的决定。

4.8 再认证

4.8.1 获证组织宜在认证证书有效期结束前 3 个月向 ZICC 提出再认证申请。

4.8.2 ZICC 应及时策划并实施再认证审核，再认证审核应在认证证书到期前完成。再认证审核应确保对认证范围内有代表性的行业类别与子行业类别的典型产品/服务进行审核。

4.8.3 当获证组织的信息安全管理体系、组织结构或信息安全管理体系运作环境（如区域、法律法规、信息安全标准等）有重大变更，并经评价需要时，再认证需实施第一阶段审核。

4.8.4 再认证审核应包括针对下列方面的现场审核：

（1）根据内部和外部变化，信息安全管理体系在保持认证范围相关性和适宜性方面的整体有效性；

（2）经证实的对保持信息安全管理体系有效性并改进信息安全管理管理体系，以提高整体绩效的承诺；

（3）信息安全管理体系在实现获证组织目标和管理体系预期结果方面的有效性。

4.8.5 再认证审核中发现的严重不符合项，ZICC 应规定实施纠正和纠正措施的时限要求，并在原认证证书到期前完成对纠正和纠正措施的验证。

4.8.6 如果在当前认证证书的终止日期前完成了再认证活动，新认证证书的终止日期可以基于当前认证证书的终止日期确定。新认证证书上的颁证日期应不早于再认证决定日期。

4.8.7 如果在当前认证证书到期前，ZICC 未能完成再认证审核或未能对严重不符合

项的纠正和纠正措施进行验证，则不应推荐再认证，也不应延长认证证书的有效期。ZICC 应告知获证组织并解释后果。

4.8.8 在原认证证书到期后，如果 ZICC 能够在 6 个月内完成未尽的再认证活动，则可以维持再认证，否则应按照初次认证要求重新认证。再认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期确定。

4.9 认证范围的变更

4.9.1 获证组织拟变更认证范围时，应向 ZICC 提出申请，并按 ZICC 的要求提交相关材料。

4.9.2 ZICC 根据获证组织的申请进行评审，策划并实施适宜的审核活动，这些审核活动可单独进行，也可与获证组织的监督或再认证审核一起进行。

4.9.3 对于申请扩大认证范围的，应对获证组织实施现场审核。

4.9.4 如果获证组织申请缩小认证范围，或获证组织在认证范围的某些部分持续地或严重地不满足认证要求，ZICC 应缩小其认证范围，以排除不满足要求的部分。认证范围的缩小不应将能够影响认证范围内终产品信息安全的活动、过程、产品或服务排除在认证范围之外。

4.10 认证要求变更

4.10.1 认证要求变更时，ZICC 应制定相应的认证要求转换计划，至少应考虑：

（1）认证要求变更对 ZICC 管理体系的影响；

（2）认证要求变更对认证人员能力的影响；

（3）ZICC 依据新认证要求开展认证活动的安排；

（4）ZICC 依据新认证要求实施转换的安排。

4.10.2 ZICC 应采取适当方式对获证组织实施变更后认证要求的有效性进行验证，确认认证要求变更后获证组织信息安全管理体系的有效性，符合要求可继续使用认证证书。

5 认证证书及认证标志

5.1 认证证书有效期

信息安全管理体系认证证书的生效日期不得早于认证决定的日期。初次认证证书有效期为三年。再认证证书的终止日期不得超过上一认证周期认证证书的终止日期再加三年。认证证书应至少包括（但不限于）以下基本信息：

（1）获证组织名称、生产/服务场所的地址；

（2）与活动、产品/服务类型等相关的认证范围，适用时，包括每个场所相应的认证范围，且没有误导或歧义；

（3）认证依据；

（4）证书编号。

（5）认证机构名称、地址；

（6）颁证日期、证书有效期；

（7）相关的认可标识及认可注册号（适用时）；

（8）证书状态的查询方式。

5.2 认证证书的管理

ZICC 应当对获证组织认证证书使用的情况进行有效管理。

5.2.1 认证证书的暂停

获证组织有下列情形之一的，ZICC 应暂停其使用认证证书：

（1）获证组织未按规定使用认证证书的；

（2）获证组织未履行认证合同义务的；

（3）获证组织的信息安全管理体系或相关产品不符合认证依据，不需要立即撤销认证证书的；

（4）获证组织未能按规定间隔期接受监督审核的；

（5）获证组织未按要求对信息进行通报的；

（6）获证组织与 ZICC 双方同意暂停认证资格的；

（7）其他应暂停认证证书的。

暂停期限不超过 6 个月。在暂停期间，获证组织的信息安全管理体系认证暂时无效。ZICC 应在获证组织完成对造成暂停的不符合的纠正和纠正措施进行确认后，恢复被暂停的认证。如果获证组织未能在 ZICC 规定的时限内完成对不符合的纠正和纠正措施，ZICC 应撤销或缩小其认证范围。

5.2.2 认证证书的撤销

有下列情形之一的，ZICC 应撤销其认证证书：

（1）获证组织信息安全管理体系不符合认证依据或相关产品不符合标准要求，需要立即撤销认证证书的；

（2）认证证书暂停期限已满，获证组织未针对导致暂停的问题采取有效纠正和纠正措施的；

（3）获证组织出现安全事故、市场监督管理部门监督抽查产品和信息安全管理体系检查不合格等情况，需要立即撤销认证证书的；

（4）获证组织对相关方重大投诉未能采取有效处理措施的；

（5）获证组织虚报、瞒报获证所需信息的；

（6）获证组织故意或持续的不满足国家信息安全管理相关法律法规要求的；

（7）获证组织拒不接受相关监管部门或 ZICC 对其实施监督的；

（8）被执法监管部门认定存在严重违法失信行为的；

（9）其他应撤销认证证书的。

5.3 认证标志的管理

5.3.1 ZICC 和获证组织可在认证证书、印刷品、网站和其他宣传资料中使用信息安全管理体系认证标志。使用信息安全管理体系认证标志可以等比例放大或缩小，但不应变形、变色。如其他文字或图像均为黑白，允许使用黑白标识。

5.3.2 获证组织不得在产品、产品标签及产品内、外包装上使用信息安全管理体系认证标志。

6 信息通报

6.1 信息通报

6.1.1 为确保获证组织的信息安全管理体系持续有效，ZICC 应做出在法律上具有强制实施力的安排，以确保获证组织及时将可能影响信息安全管理体系持续满足认证要求的事宜通报给 ZICC，包括但不限于与以下内容有关的变更：

（1）有关法律地位、经营状况、组织状态或所有权变更的信息；

（2）联系地址和场所变更的信息；

（3）信息安全管理体系和过程重大变更的信息，包括但不限于：组织管理层重要人员变化；

（4）有关信息安全事故及信息安全投诉的信息；

（5）政府部门组织的市场抽查中被发现有信息安全问题或信息安全生产规范体系检查中被发现有不符合的信息；

（6）其他重要信息。

6.1.2 信息分析

ZICC 应对上述信息进行分析，视情况采取相应措施，如增加监督审核频次、暂停或撤销认证资格等。

7 认证记录的管理

7.1 ZICC 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。

7.2 记录应当真实准确以证实认证活动得到有效实施。保存时间为当前认证周期加上一个完整的认证周期。

7.3 记录可以用纸质或电子文档的方式加以保存。

8 受理转换认证证书

8.1 ZICC 严禁及牟利为目的受理不符合信息安全管理体系标准、不能有效执行信息安全管理体系标准的组织申请认证证书的转换。

8.2 ZICC 受理组织申请转换 ZICC 的认证证书，应该详细了解申请转换的原因，不符合《认证证书转换实施指南》的通知要求的，不得接受转换申请。

9 申诉

ZICC 应建立申诉的处理程序，能够及时、有效、公正地对申诉进行处理，并将处理结果书面通知申诉人。

认证委托人如对认证决定结果有异议，可在 10 个工作日内向 ZICC 申诉，ZICC 自收到申诉之日起，应在 30 日内进行处理，并将处理结果书面通知认证委托人。申诉人如认为 ZICC 行为违反了相关法规，处理结果严重侵害了自身合法权益的，可以直接向各级认证监管部门投诉。

10 其他

本规则内容提及信息安全管理体系标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，均采用当时有效版本的完整标准号。

附录 A：审核时间

下表为 ISMS 初次认证的审核人日基数，具体审核时间需要考虑受审核方的规模、特性、业务复杂程度、ISMS 涵盖的范围、认证要求和其承担的风险等因素。根

据受审核方的特点在项目方案制定过程中可以在人日基数上进行增减。

当 ISMS 与其他管理体系结合审核时,ISMS 的审核时间可根据结合审核的一体化程度进行打折。

监督审核的人日数不少于初次认证人日数的三分之一，再认证的人日数不少于初次认证人日数的三分之二。

基本人日数计算表：

雇员数量	初次审核审核时间（审核人日）	雇员数量	初次审核审核时间（审核人日）
1 ～ 10	5	876 ～ 1175	18.5
11 ～ 15	6	1176 ～ 1550	19.5
16 ～ 25	7	1551 ～ 2025	21
26 ～ 45	8.5	2026 ～ 2675	22
46 ～ 65	10	2676 ～ 3450	23
66 ～ 85	11	3451 ～ 4350	24
86 ～ 125	12	4351 ～ 5450	25
126 ～ 175	13	5451 ～ 6800	26
176 ～ 275	14	6801 ～ 8500	27
276 ～ 425	15	8501 ～ 10700	28
426 ～ 625	16.5	＞ 10700	沿用以上规律
626 ～ 875	17.5		

附录 B

ISMS认证机构认证业务范围分类与分级

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	二	医疗服务	
	02.06	三	教育	
	02.07	三	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	三	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	