瑞岳认证（江西）有限公司

网络数据安全管理认证实施规则

编号:GZ-DSMC-2025

版本:A/1

编制：技术研发部

审核：王敏捷

批准：王敏捷

发布日期：2025年9月4日实施日期：2025年9月4日

修改日期：2025年11月25日

序号	修订章节	修订内容摘要	修订版本	修订日期	修订人	批准

目录

网络数据安全管理认证实施规则

1适用范围

本规则依据认证认可相关法律法规，结合相关技术标准，规定了瑞岳认证（江西）有限公司（以下简称瑞岳）开展网络数据安全管理认证的程序与管理的基本要求，是瑞岳认证从事网络数据安全管理认证活动的基本依据，保证网络数据安全管理认证活动的规范有效。

2认证依据

与本认证实施规则所规定认证审核活动相关的网络数据安全管理技术规范为瑞岳自有企业标准《网络数据安全管理技术规范》（RY-GF-001-2025，现行有效版本）。

3对认证人员的基本要求

3.1遵守认证认可相关法律法规、部门规章及规范性文件的要求，具有从事认证工作的基本职业操守，对认证活动及其结果的真实性和有效性承担相应责任。

3.2审核员应取得QMS审核员注册资格。

3.3审核员不得接受超出其注册资格的认证审核任务。

3.4不得发生影响认证公正性的行为，应主动告知瑞岳认证其所了解的任何可能使本人或瑞岳认证陷入利益冲突的情况。因认证人员未履行告知义务而导致非公正性认证结果的，认证人员应当负有连带责任（如承担因此造成的经济损失）。

3.5按要求接受人员注册/保持注册所要求的继续教育培训，以及瑞岳认证要求的能力（包括知识和技能）提升活动，以持续具备从事QMS认证工作相适宜的能力。

4初次认证

4.1认证申请

4.1.1申请人应具备以下条件：

a)申请组织应具有明确的法律地位，取得国家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），即法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）；若覆盖多场所活动，应附每个场所的法律地位证明文件（适用时）；

b)在国家、地方或行业有要求时，申请组织取得相关法规规定的行政许可文件和备案证明（适用时），其申请认证范围应在法律地位文件和资质规定的范围内；

c)申请组织近一年内，未发生违反相关法律法规的情况，且未列入国家信用信息严重失信主体相关名录；

d)已按认证依据要求，建立和实施了文件化的网络数据安全管理制度文件，申请人的体系运行时间必须满足至少运行3个月以上的要求。

e)三年内，获证组织未因出现数据安全事故；或对相关方重大投诉未能采取有效处理措施的；获证组织虚报、瞒报获证所需信息的；而被瑞岳认证撤销认证证书。

f)申请组织承诺遵守国家的法律、法规其他要求，承诺始终遵守认证的有关规定，承诺按合同约定和法律规定承担与认证有关的相关法律责任；

g)申请组织承诺获得认证证书后，持续有效运行，按认证合同约定支付有关费用，按规定接受瑞岳认证和认证监管部门的监督/检查,按瑞岳认证规定使用认证证书、标志和审核报告，并将组织发生的可能影响数据安全管理活动持续满足认证标准要求的能力的事宜向瑞岳认证报告。

4.1.2申请人应提交的文件和资料:

a)认证申请书；

b)法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。若覆盖多场所活动，应附每个场所的法律地位证明文件（适用时）；

c)申请认证范围所涉及的法律法规要求的资质，覆盖的活动所涉及法律法规要求的行政许可文件和备案证明文件（适用时）；

d)按照适用的认证依据标准要求，建立和实施了文件化的网络数据安全管理制度文件（包括管理手册、程序文件、适用的法律法规和强制性标准清单等）；

e)组织机构与职责说明；

f)多场所清单及外包情况说明（适用时）；

g)承诺遵守相关法律、法规、瑞岳认证要求及提供材料真实性的自我声明；

h)其他需要的文件。

4.2认证受理

4.2.1瑞岳认证应向申请人至少公开以下信息：

a)依法从事认证活动的自我声明；

b)可开展认证领域、认证业务的范围，以及获得相应认可的情况；

c)开展认证活动所依据的认证标准及认证流程；

d)本认证规则的完整内容、认证程序；

e)批准、保持、变更、暂停、恢复和注销或者撤销认证证书的规定与程序；认证证书有效性查询方式；

f)拟向组织获取的信息，以及对相关信息的保密规定；

g)认证证书样式、认证标志及相关的使用规定；

h)证书有效期；

i)对认证过程的申诉、投诉规定；

j)认证要求变更的规定；

k)认证业务收费标准；

l)设立的承担其认证活动的分公司名称、地址和认证活动内容。

4.2.2申请评审

4.2.2.1瑞岳认证应实施认证申请评审，根据瑞岳认证能力确定是否受理认证申请。瑞岳认证应根据认证依据、程序等要求，对申请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：

a)认证要求规定明确、形成文件，并得到理解；

b)瑞岳认证和申请人之间在理解上的差异得到解决；

c)对于申请的认证范围、申请人的工作场所和任何特殊要求，瑞岳认证均有能力开展认证服务；

d)瑞岳认证不应将能够影响认证范围内终产品数据安全管理的活动、过程、产品或服务排除在认证范围之外。

4.2.2.2申请评审

应对申请组织提交的申请资料进行审查，并确认：

a)申请资料齐全。

b)申请组织从事的活动符合相关法律法规的规定。

c)申请组织为达到网络数据安全管理的目标而建立了文件化的过程和程序。

4.2.2.3根据申请组织申请的认证范围、场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

4.2.2.4对符合4.2.2.2、4.2.2.3要求的，瑞岳认证可决定受理认证申请；对不符合上述要求的，瑞岳认证应通知申请组织在规定时间内补充和完善，或者不受理认证申请。

4.2.2.5存在以下情况的组织，瑞岳认证不得受理其认证申请：

a)组织存在不符合4.1.1情形的；

b)被执法监管部门责令停业整顿期间的；

c)被行政主管部门认定或被媒体曝光有不符合、违规违法行为，且尚在处理期间的。

4.2.3评审结果处理

受理认证申请：申请获得受理后，将与客户签订具有法律效力的书面认证合同，明确认证服务的费用、付费方式和违约条款，及机构和获证组织的责任。认证费用应由申请人向认证机构直接支付。

不受理认证申请：当申请方不满足申请条件的将不予受理，待条件具备时再申请，并将拒绝的原因告知申请组织。

4.3签订认证合同

在实施认证审核前，瑞岳认证应与每个申请组织订立具有法律效力的认证合同或等效文件，以明确双方的责任、权利和义务，合同应至少包含以下内容：

a)申请组织获得认证后持续有效运行网络数据安全管理的承诺；

b)申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺；

c)申请组织承诺获得认证后发生以下情况时，应及时向瑞岳认证通报：

1）获证组织出现数据安全事故；

2）出现有关数据安全相关的重大负面新闻；

3）相关情况发生变更，包括：法律地位、环保设施运行状况、组织状态或所有权变更的信息；取得的行政许可资格或其他资质证书变更；法定代表人、最高管理者等变更；联系地址和场所变更；网络数据安全管理覆盖的活动范围变更；网络数据安全管理和过程重大变更；有关产品、工艺、数据安全变化的信息等；

4）相关方重大投诉未能采取有效处理措施；

5）行政主管部门监督检查发现有数据安全问题的信息，或不合规被行政主管部门通报、处罚的；

6）出现影响网络数据安全管理运行的其他重要情况。

d)申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不擅自利用认证证书和相关文字、符号误导公众认为其产品或服务通过认证；

e)拟认证的网络数据安全管理覆盖的产品和或服务的活动范围；

f)在认证审核实施过程及认证证书有效期内，瑞岳认证和申请组织各自应当承担的责任、权利和义务；

g)认证服务的费用、付费方式及违约条款。

4.4审核方案策划

4.4.1审核方案

4.4.1.1瑞岳认证应针对每一认证委托人建立认证周期内的审核方案，以清晰地识别所需的审核活动。

4.4.1.2初次认证的审核方案应包括两阶段初次认证审核、获证后的监督审核和认证到期前的再认证审核。再认证的审核方案应包括再认证审核、获证后的监督审核和认证到期前的再认证审核。

4.4.1.3初次认证审核和再认证审核是对认证委托人完整体系的审核，应覆盖《数据安全管理体系技术规范》（RY-GF-001）所有要求，以及认证范围内的典型产品和服务。认证证书有效期内的监督审核累计应覆盖《网络数据安全管理技术规范》（RY-GF-001）所有要求。

4.4.1.5瑞岳认证应考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的控制水平来策划对不同班次实施的审核程度，以确保审核的有效性

4.4.1.4初次认证及再认证后的第一次监督审核应在认证证书签发之日起12个月内进行。此后，监督审核间隔不应超过12个月。

4.4.1.5瑞岳认证考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的控制水平来策划对不同班次实施的审核程度，以确保审核的有效性：

（1）每次审核应至少对其中的一个班次的生产或服务的活动现场进行审核；

（2）未审核其他班次生产或服务活动现场的，应记录未审核的理由。

4.4.2审核时间

4.4.2.1审核时间包括在认证委托人现场的审核时间以及在现场审核以外实施策划、文件审核和编写审核报告等活动的时间。审核时间以人日计，1人日为8小时，不应通过增加工作日的工作小时数以减少审核人日数。

如果认证委托人工作日的实际工作时间不足8小时，则应延长现场审核天数以满足审核时间要求。

4.4.2.2瑞岳认证应以附录1《网络数据安全管理认证审核人日表》所规定的审核时间为基础，考虑认证委托人有效人数、风险类型等因素，建立文件化的不同审核类型审核时间（包括现场审核时间）的确定方法。

4.4.2.3每次审核的审核时间确定过程应形成记录，尤其是减少审核时间的理由，减少的审核时间不得超过附录1《网络数据安全管理认证审核人日表》所规定的审核时间的30%，现场审核时间不得少于所确定的审核时间的80%。如果审核人日计算后结果包括小数，宜将其调整为最接近的半人日数。

4.4.2.4瑞岳认证应建立文件化的结合审核时间确定方法，网络数据安全管理认证审核和其他管理体系实施结合审核的，结合审核的总审核时间不得少于多个单独体系所需审核时间之和的80%。

4.4.3多场所抽样

4.4.3.1条件

当客户管理体系的每个场所均实施非常相似的过程、活动时，在审核中可使用多场所抽样。并非所有满足“多场所组织”定义的组织都具备抽样的资格。对抽样计划的合理性在审核方案策划中进行明确。

并非所有的管理体系标准都适合适于多场所认证。例如，当标准要求对差异性的当地因素审核时，对多场所的抽样是不适宜的。

抽样宜具有显著的统计学特性，并覆盖组织的服务认证范围。样本的选取宜考虑随机抽样与有目的选择相结合的方式，以使得抽取的样本更具典型性、代表性和合理性。抽样方法可以是（但不限于）配额抽样、分层抽样、判断抽样、随机抽样或是几种抽样方法的组合。

4.4.3.2抽样方案

瑞岳认证宜基于风险评估的结果，并在风险可控的基础上设计抽样方案。

设计和确定抽样方案时，宜基于以下方面的考虑：

a)组织的中心职能不参与抽样；

b)样本中宜有一部分样本根据下列因素（但不限于）选取，一部分随机抽取；选取结果宜尽可能选到具有代表性的不同场所：

对场所内部审核、管理评审和/或以前认证审核的结果；

投诉记录以及纠正和预防措施的其他相关方面；

各场所在规模上的显著差异；

在倒班安排和工作程序上的差异；

管理体系以及在场所实施过程的复杂程度；

上次认证审核后的变化；

管理体系的成熟度和组织的理解程度；

文化、语言和法律法规方面的差异；

地理位置的分散程度；

场所是常设的、临时的或虚拟的。

c)至少25%的场所样本随机抽取。

4.4.3.3样本（25%随机抽取的场所除外）的选择，宜使得证书有效期内所选场所尽可能不同，且场所间差异尽可能大。

4.4.3.4并不是必须在审核过程一开始就完成抽样。也可能在完成对中心职能的审核时完成抽样。不论哪种情况，应将样本中所包括的场所通知中心职能。这可能是在相对较短时间内通知，但应给出充分的时间用于审核准备。

4.4.3.5瑞岳认证进行多场所抽样应使用抽样方案，同时满足以下条件，以确保管理体系认证进行有效的审核：

a)每次审核最少审核的场所数量是：

初次认证审核：样本的数量应为场所数量的平方根（$y=\sqrt{x}$），计算结果向上取整为最接近的整数，其中y为将抽取场所的数量、x为场所总数。

监督审核：每年的抽样数量应为场所数量的平方根乘以0.6即（$y=0.6\sqrt{x}$），计算结果向上取整为最接近的整数。

再认证审核：样本的数量应与初次审核相同。然而，如果证明管理体系在认证周期中是有效的，样本的数量可以减少至乘以系数0.8即（$y=0.8\sqrt{x}$），计算结果向上取整为最接近的整数。

b)在初次认证审核、每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能审核。

c)增加抽样的情况：当瑞岳认证对拟认证或获证管理体系涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率。

场所的规模和员工的数量；

过程、活动以及管理体系复杂程度和风险水平；

工作方式的差异（如：倒班）；

所从事过程、活动的差异；

发生重大投诉或社会负面影响的事件，以及纠正措施和预防措施的其他相关方面；

与跨国经营有关的任何方面；

内部审核和管理评审的结果。

d)增加场所

如果对已认证的多场所组织增加新场所或增加一组新的场所，公司应考虑新增场所的规模、风险及复杂程度、管理体系绩效等因素，采取资料审核、与原场所一同抽样、新增的多场所按照初次审核抽样等方式进行审核，纳入认证范围。

在新场所纳入证书后，需要确定后续监督或再认证审核的抽样数量。

e)多场所组织的抽样量

如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。

示例：

1个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都审核；

4个全国性办公室：样本数量＝2，至少1个为随机抽样；

27个地区办公室：样本数量＝6，至少2个为随机抽样；

1700个地方分支：样本数量＝42，至少11个为随机抽样。

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。这样可能导致每个等级的场所抽样数量超过按照第a）条计算的最小抽样数量。

f）公司每个日历年至少对管理体系的中心办公室（职能）进行一次审核；

g）公司每年至少应对规定数量的抽样场所进行监督审核；

h）应将抽样场所的审核发现视为整个体系的情况，并应实施相应的纠正。

4.4.3.6对一些大型集团型组织，例如大型食品企业，虽然不属于多场所，但由于其生产线多，流程长，多为连续生产，过程复杂，计算人日时可参照多场所的模式。例如化工企业若有几套相同生产装置，则可以按多场所抽样原则进行抽样，增加的人日数则可按装置加工能力及装置数量适当增加人日；

4.4.3.7多场所组织的临时性场所抽样时应考虑一、二阶段的一致性，审核时机应确定在主要过程的实施阶段。一阶段对多场所抽样的原则：

a）选择高风险专业场所，数量不做限定；

b）同等级风险水平，选择规模较大的；

c）选择经审核组长现场评估，受控程度较低的场所。

4.4.3.8通用的临时场所审核时间策划原则

a）如果客户在临时场所提供其产品或服务，则该临时场所应被纳入审核方案。临时场所可以是较大的项目管理现场，也可以是较小的服务/安装现场。应评估对与客户运行相关的管理体系风险的控制失效所产生的风险，根据该风险评估的结果来确定是否需要审核这些临时

场所以及抽样的范围与程度。所选取的临时场所样本宜代表客户的认证范围、活动和过程的规模和类型、所涉及的污染物和相关的风险类型、以及项目进行的不同阶段及相关的数据安全及影响。

b）通常情况下，应将对纳入审核方案的临时场所进行现场审核。但是，可以考虑用下列方法来代替一部分现场审核。在每种情况下，宜完整地记录审核方法，并充分证明审核方法的有效性：

1）通过面对面或电视电话会议的方式，与客户及（或）其顾客进行访谈，或者参与他们的进度会议；

2）对临时场所的活动实施文件审查；

3）远程审核包含同管理体系与临时场所的评审有关的记录或其他信息的电子化场所；

4）使用电视电话会议及其他技术实施有效的远程审核。

4.4.3.9抽样过程应作为审核方案管理的一部分。在任何时候（即：在策划监督审核之前、或组织的任何场所变更其结构时、或将在认证边界之内增加新的场所时），瑞岳认证应预先评审审核方案中的抽样安排，以便在为保持认证对样本审核之前能确定抽样数量调整的需求。

4.5组建审核组

4.5.1瑞岳认证应根据实现审核目的所需的能力和公正性要求组建审核组，至少1名实施第一阶段审核的审核员应参加第二阶段审核，每个审核组应包括：

（1）审核组长：瑞岳认证应建立并实施审核组长的选择、培训以及任用的管理制度；审核组长应当具有管理和领导审核组达成审核目标的知识和技能，其能力应至少满足GB/T 19011《管理体系审核指南》中对审核组长的通用要求；

（2）至少1名与认证委托人所属认证业务范围相匹配的专业人员（专业领域审核员或技术专家）。网络数据安全管理审核和其他管理体系实施结合审核的，审核组还应包括其他管理体系的专业人员，确保专业人员的能力覆盖实施结合审核的全部管理体系；

4.5.2技术专家主要负责为审核组提供技术支持，不作为审核员实施审核，不计入审核时间。

4.5.3实习审核员应在正式审核员的指导下参加审核，不计入审核时间，其在审核过程中的活动由负责指导的正式审核员承担责任。审核组中实习审核员的数量不得超过正式审核员的数量。

4.5.4审核组成员不得与认证委托人存在利益关系。

4.6编制审核计划

4.6.1瑞岳认证应当为每次现场审核制定书面的审核计划。审核计划应明确认证范围内的所有过程。审核计划至少包括以下内容：审核目的、审核准则、审核范围、现场审核的日期、审核过程、时间安排和场所、审核组成员等。

4.6.2现场审核应安排在审核范围覆盖产品种类的生产期进行，审核组应在现场观察该产品种类的生产活动。

4.6.3申请组织体系覆盖了多个场所时，瑞岳认证应对包含中心职能部门在内场所及多场所抽样要求实施现场认证审核，以确保审核的有效性。当受审核方将影响数据安全的重要生产过程采用委托加工等方式进行时，除非被委托加工组织的被委托加工活动已获得相应的认证，否则应对委托加工过程实施现场审核。

4.6.4现场审核开始之前，审核组应将书面的审核计划交申请组织确认，遇特殊情况如需临时调整审核计划，应经双方协商一致后实施。

4.7审核实施

4.7.1现场审核实施程序

a)审核准备会

审核组长应按照审核基本规范、基于过程的结合审核等相关要求召开审核准备会并做好记录。审核准备会不应走形式和走过场，为有效实施审核奠定基础。

b)首次会议

现场审核开始前，审核组长应主持召开首次会议，其表现应自信、大方、语言流利并营造融洽的气氛，首次会议的程序和内容应符合4.7.1的相关规定。无论何种原因均不能不召开首次会议。

应与客户的管理层举行一次正式的首次会议，如有必要应包括负责拟审核部门或过程的人员，并应记录与会人员。首次会议应由审核组长主持，其目的是简单说明审核活动将如何开展，并应包括下列信息。说明的详细的程度视客户熟知的审核过程的程度而定。

1)介绍参与人员，包括简介其角色；

2)确认认证的范围、边界；

3)与客户确认审核计划（包括审核的类型和范围、目标和依据）、任何变化以及其他相关安排，如末次会议的日期和时间、审核小组和客户管理层之间的临时会议；

4)确认审核小组和客户之间的正式沟通渠道；

5)确认具备审核小组所需的资源和设施；

6)确认保密相关问题；

7)确认审核小组的相关工作安全、紧急及安全事项；

8)确认陪同人员和观察员，其角色和职责；

9)报告方式，包括对审核发现的分级；

10)审核可能提前终止的情况；

11)审核组长及审核小组对审核负责，且应控制审核计划的执行，包括审核活动和审核线索；

12)如适用，确认前次审查或审核发现的状态；

13)根据抽样进行审查所需使用的方法和过程；

14)确认审核中使用的语言；

15)确认在审核中，将会向客户及时通报审核进度及任何关注的问题；

16)客户提问的机会等。

c)现场审核过程中，审核组长应协调审核组的审核活动，营造和谐的审核组内部氛围，及时和有效处理突发事件，当需要调整审核计划时，应合理进行调整。

d)审核组长应按照审核基本规范、基于过程的结合审核的要求每日召开审核组沟通会，沟通会应有效传递审核信息，为过程的连续性审核及审核的有效性、充分性以及客观、充分地确定审核发现和提出审核结论创造条件。

e)现场审核方法和程序是基于抽样审核的原则，审核范围内的产品和过程不能抽样，但其相同或相似活动可抽样。

f)审核员应记录和收集审核证据，并确定审核发现。

g)审核组长应持续关注认证风险，对于发现的严重问题不回避、不迁就、不扩大、不推断，与受审核方坦诚交流并按照瑞岳认证的相关要求进行处理，规避瑞岳认证的风险。

h)审核组长应及时与审核组成员交流，负责掌握审核进程，必要时调整审核计划，确保完成审核任务。

i)现场审核过程中，审核组长应与受审核方保持沟通，包括必要的资源支持、听取受审核方的意见、审核计划的调整、审核组成员的表现、通报和澄清发现的问题等，对于受审核方的合理要求应予以满足。

j)审核组长负责与受审核方沟通，告知审核进程；对发现可能影响通过认证的结论的重大问题，应及时与瑞岳认证审核部和受审核方沟通并确定审核活动变更事宜（如：修改审核计划、改变审核目的或审核范围、终止审核等）。

k)现场审核中需变更审核范围时，审核组长（必要时和专业审核员）现场确认可行性，同时报告瑞岳认证项目管理部和审核部进行可行性评估。

l)现场审核活动应在向导陪同下实施。

m)审核取证方法

1)查阅

审核的查阅方式包括但不限于：

（1）非在线方式，如文件传送给审核员查阅；

（2）在线方式，如共享屏幕、视频查看等，未经受审核方许可，审核员不得拷贝、拍照。

2)访谈

审核员宜在访谈开始时确认被访谈者的身份，向其说明访谈主要事项并告知访谈是获取审核证据的方法之一。

3)观察

观察适用于受审核方的运行现场，观察时宜考虑：

①证明实况画面的真实性（适宜于远程）；

②通过时间特征、人员特征等必要信息，确保现场的实时性；

③现场工作环境，如光线、噪声等，宜满足审核证据收集的要求。

n)审核发现

审核组长应协调审核组的审核发现，综合考虑不符合报告的数量和分布，对于关键和（或）涉及合规问题应开具不符合报告，并根据问题严重程度确定不符合的性质。不符合报告和提出“受审核方重点关注的问题”应以事实为依据，描述清晰、具体且可追溯、客观不推断，避免与受审核方争议。不符合报告应有认证标准和（或）受审核方规定的判据。

1)于审核中发现的不符合，应出具书面不符合报告，审核组应当根据审核发现形成严重或轻微不符合；

2)不符合事实应基于审核证据和审核准则，其描述应客观、公正、准确、具体、清晰，并可追溯，易于被客户理解，应与检查表保持一致，切忌使用推断、猜测、笼统的语言；

3)不符合报告开在发现部门并应得到客户对不符合事实的确认。不符合报告的表述和判定应有利于客户准确理解管理体系存在的问题，有利于纠正和纠正措施的制定。不符合报告应准确判定其事实不符合与有关审核准则的具体要求；

4)提出改进机会时，审核组长应确保这些确实是改进机会而非下述定义中的不符合项；

①主要/严重不符合：

客户体系中没有提及解决标准的某一要求；

频繁的或无故不遵循公司体系中的具体书面要求；

未能达到系统要求的基本目的；

受审核方管理体系未能达到法律或法规的要求；

标准或公司体系的同一要求出现多个次要不符合项；

受审核方无故不纠正不符合项；

如受审核方已通过其内部审核及纠正措施过程识别出了该问题，且具有纠正措施计划，并正在实施中，则瑞岳认证审核员无需提出不符合项。

②轻微不符合:所审核的体系未能满足书面要求，但不属于主要不符合项。

③改进机会:当前符合过程/活动/文件，但可以通过改进为客户带来利益。

④问题项/观察项:需要关注的方面，过程、文件或活动目前符合要求，但如果不改进的话可能造成体系、产品或服务要求的不符合。

5)要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施

(轻微不符合可以是纠正措施计划),将在下一次审核时验证纠正措施的有效性。瑞岳认证应审查受审核方提交的纠正和纠正措施，以确定其是否可被接受。初审时，对于严重不符合，受审核方应在30天内采取纠正措施并经验证合格；对于轻微不符合，受审核方应在45天内采取纠正措施并经验证合格；监督、再认证、扩项、非例行审核时，对于轻微不符合，受审核方应在30天内完成纠正措施或纠正措施计划并经验证合格；

6)受审核方对不符合采取纠正和纠正措施的时间不得超过3个月；

对于需要换发新证书的情况，应限制纠正和纠正措施的时间，以便在证书过期前实施措施；

o)如果跟踪访问和不合格关闭未在上述期限内结束，审核被认为是无效的；

对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、保持认证或再认证；

p)确定推荐的认证范围

审核组推荐的认证范围应基于客户的法律法规许可及现场实际运作的边界界定。审核组长应汇总审核发现，审核组按照瑞岳认证的相关要求客观、合理界定拟推荐的认证范围（含多场所）。

q)沟通会

审核结束前，审核组应召开与受审核方管理层的沟通会，通报审核情况：

审核组长进行主要发言，应将审核发现汇总、分类并提升高度，从正、反两方面按类别进行通报，审核组其他成员做适当补充。沟通会不宜宣读不符合报告，应将不符合报告和所提问题的内容融入问题分类通报中；

审核组应将界定的拟推荐的认证范围与受审核方沟通，征询意见，受审核方合理的要求应予以满足。

r)末次会议

现场审核结束前，审核组长应主持召开末次会议，其表现同首次会议，末次会议的程序和内容应符合瑞岳认证的相关规定。若出现与受审核方争议的情况，审核组长应妥善处理。沟通会与末次会也可合并为一个会议。

应与客户的管理层举行一次正式的末次会议，如有必要应包括被审核部门或过程的负责人员，并应记录与会人员。末次会议应由审核组长主持，其目的是陈述审核结论，包括发证相关建议。任何不符合项应以客户可以理解的方式进行陈述，并应就相应的回应时间安排达成一致。

末次会议还应包括下列信息。具体详细程度应与客户熟知的审核过程一致：

告知客户，审核证据的收集是采用抽样方法，因此可能存在不确定性；

报告的方法和时间安排，包括对审核发现的分级；

瑞岳认证处理不符合项的过程，包括任何与客户证书相关的结果；

客户对审核中识别的任何不符合项提出纠正和纠正措施的时间安排；

瑞岳认证审核后的活动；

投诉处理和上诉过程信息。

应给客户提问和澄清的机会。任何审核小组和客户对于审核发现或结论的不同意见均应得到讨论，并尽可能解决。无法解决的意见分歧应予记录，并尽快报告审核部经理。末次会议的与会者一般应为首次会议的与会者。

审核组应会同认证委托人召开首、末次会议，认证委托人的最高管理者、相关职能部门负责人应参加首、末次会议，应保留首、末次会议签到记录、图片/音像证明材料。认证委托人的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会，审核组应记录最高管理者缺席理由。

审核组应通过面对面访谈等形式，对认证委托人的最高管理者在管理体系中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的方针、目标，未亲自参与并推动管理体系实施的，认证审核应不予通过。

4.7.2初次认证审核

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。两个阶段审核时间间隔最短不应少于5日，最长不应超过6个月。如需要更长的时间间隔，应重新实施第一阶段审核。

审核组中应至少有1名专职审核员参与全程审核。技术专家主要负责为审核组提供技术支持，不作为审核员实施审核，不计入审核时间。实习审核员应在正式审核员的指导下参加审核，不计入审核时间，其在审核过程中的活动由负责指导的正式审核员承担责任。审核组中实习审核员的数量不得超过正式审核员的数量。

认证审核应在认证委托人现场且认证委托人的生产或服务处于正常运行时进行。

4.7.2.1第一阶段审核

4.7.2.1.1第一阶段审核要求

第一阶段的目标是通过了解组织的网络数据安全管理是否已具备实施认证审核的条件，策划第二阶段的关注点，并通过审查组织的以下方面，了解组织对第二阶段的准备情况，第一阶段审核应关注但不限于以下方面内容：

a）法律地位证明文件、资质、标准备案或自我公开声明、相关法律法规识别及遵守情况、相关方的特定要求等合规性、有效性进行现场核实、确认。

b）收集客户的管理体系的信息；

1）范围、边界(包括生产装置、活动)、场所(工作场所、现场及多场所的分布、距离和所处区域)、过程和使用的设备及其控制水平(特别为多场所时)；

2）受审核方管理体系的有效人数，包括认证范围内涉及的固定和非固定人员(如承包商人员、兼职人员)的所有人员；

3）受审核方管理体系是否已有效运行并且超过3个月(认证规则中规定有特殊要求的按规定执行)。

c）审查客户理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素及其过程和目标以及运作的识别情况。评价客户实施标准要求的情况。

d）了解客户进行生产/服务的状况、流程及倒班情况。了解客户管理体系及其过程策划情况（管理体系范围内的各类活动及过程）：控制过程识别的充分性、适宜性。各部门职责与过程管理的对应关系等。

e）关注认证范围内产品和或服务实现过程中数据安全控制等过程运行的策划及运行控制情况。

f）关注体系文件结构性以及与企业实际情况的符合性、适宜性、一致性、充分性、有效性及可操作性。

g）审查第二阶段审核所需资源的配置情况，以确保审核组专业人员及审核人日配置的充分性。与客户商定第二阶段审核的时间、路线安排等细节，对于有临时活动或临时场所的客户在确定第二阶段审核时间时，应充分考虑客户关键活动的实施阶段(如建筑施工企业应选择其主体施工阶段，而不宜选择在地基基础或装修装饰阶段)，同时应考虑合理的时间间隔，使客户有充分的时间解决第一阶段审核中发现的问题，具体的时间间隔应根据一阶段审核提出问题的严重程度和整改难度来确定。

h）结合重要数据安全的运行控制，充分了解客户的管理体系和现场运作情况，识别对目标的实现具有重要影响的关键点，并结合其他因素，为第二阶段审核确定重要审核点。

i）评价客户是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段审核做好准备。

j）基于上述审核结果，评价客户管理体系能否进行第二阶段审核。对管理体系文件不符合客户实际、管理体系运行尚未超过3个月或者无法证明超过以上规定时间的(管理方针发布时间可以作为体系运行时间的证据)，以及其他不具备二阶段审核条件的，不能实施二阶段审核。

k）第一阶段审核，客户存在不符合法规要求，如质检不合格等情况尚未进行有效纠正时，不应进行第二阶段审核。

l）确认审核方案策划的合理性，结合管理体系标准或其他规范性文件充分了解组织的管理体系和现场运作，以便为策划第二阶段提供关注点。

4.7.2.1.2第一阶段审核应在客户现场进行（尤其是数据安全复杂或者标为高风险的企业）审核，以达到第一阶段的目标；特殊情况下，瑞岳认证经过风险评估后，第一阶段可不在现场实施：

a）受审核组织已获瑞岳认证颁发的其他有效认证证书，瑞岳认证已对受审核组织数据安全管理体系有充分了解。

b）瑞岳认证有充足的理由证明受审核组织的生产经营或服务的技术特征明显、过程简单，通过对其提交文件化信息的审查可以达到第一阶段审核的目的和要求。

c）受审核组织获得了其他经CNAS认可的瑞岳认证颁发的有效的织网络数据安全管理认证证书，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，第一阶段审核应在受审核组织的生产经营或服务现场实施。

第一阶段可不在现场实施，但应提供证据证明第一阶段的目标全部实现，且合理的理由也应记录在第二阶段的报告中。特殊情况可包括客户地处偏远地区；或产品为短暂季节性生产；或服务周期极短等。

4.7.2.1.3审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注第一阶段的结果可能导致推迟或取消第二阶段审核。

4.7.2.1.4第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题,并在第二阶段审核前完成对审核发现采取措施的跟进。

4.7.2.1.5第一阶段审核所产生的问题应在二阶段审核前关闭。在审核组推荐的情况下，可以进入二阶段审核。

4.7.2.1.6对于第一阶段审核过的织网络数据安全管理的相应部分，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，瑞岳认证应确保织网络数据安全管理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。

4.7.2.1.7第一阶段和第二阶段的时间间隔不应超过6个月。如果需要更长的时间间隔，应重新实施第一阶段。

4.7.2.2第二阶段审核

4.7.2.2.1第二阶段审核应当在申请组织现场进行。第二阶段审核是完整条款、完整体系的审核。审核组长必须确保标准所有条款要求在审核过程中被验证。目的是评价受审核方织数据安全管理体系实施的符合性和有效性。

第二阶段审核的要求如下：

（1）认证委托人网络数据安全管理与《网络数据安全管理技术规范》（RY-GF-001）标准的符合情况及证据；

（2）依据网络数据安全管理QMS关键绩效、目标和指标，对绩效进行的监视、测量、报告和评审；

（3）认证委托人实施网络数据安全管理以及在符合适用法律法规要求方面的绩效；

（4）认证委托人数据安全管理过程的运作控制；

（5）认证委托人的内部审核和管理评审；

（6）针对认证委托人数据安全管理方针的管理职责。

4.7.2.2.2在审核中应通过适当的抽样来获取与审核目的、范围和准则相关的信息并进行验证，使之成为审核证据。信息获取方法可包括面谈、观察、文件和记录的审查等。

4.7.2.2.3审核组应确定审核发现（概述符合性并详细描述不符合），并予以分级和报告，为认证决定或保持认证提供充分的信息。

4.7.2.2.4对于审核中发现的不符合，审核组应出具书面不符合报告，要求受审核方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。审核组应评审受审核方提交的纠正和纠正措施，以确定其是否可接受。受审核方对不符合采取纠正和纠正措施的时间不得超过3个月。

4.7.2.2.5审核组应对在第一阶段和第二阶段审核中收集的所有信息和证据进行分析，以评审审核发现并就审核结论达成一致。

4.7.2.2.6发生以下情况时，审核组应向瑞岳认证审核部报告，经审核部负责人同意后终止审核。

a）受审核方对审核活动不予配合，审核活动无法进行；

b）在重大问题发现时，申请组织要求不再继续审核的情况；

c）受审核方合规、数据安全风险很大，如现场发现因不满足法规要求造成的较严重的事故等；

d）其他导致审核程序无法完成的情况。

4.8不符合纠正的验证

4.8.1要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施(轻微不符合可以是纠正措施计划),将在下一次审核时验证纠正措施的有效性。瑞岳认证应审查受审核方提交的纠正和纠正措施，以确定其是否可被接受。初审时，对于严重不符合，受审核方应在30天内采取纠正措施并经验证合格；对于轻微不符合，受审核方应在45天内采取纠正措施并经验证合格；监督、再认证、扩项、非例行审核时，对于轻微不符合，受审核方应在30天内完成纠正措施或纠正措施计划并经验证合格；受审核方对不符合采取纠正和纠正措施的时间不得超过3个月。

对于需要换发新证书的情况，应限制纠正和纠正措施的时间，以便在证书过期前实施措施。

审核组应对措施的完成情况及有效性进行验证，验证可以是后续审核活动的一部分。结果应报告给审核方案管理人员，并报告给受审核方进行管理评审。

4.8.2如果跟踪访问和不合格关闭未在上述期限内结束，审核被认为是无效的。

4.8.3对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、保持认证或再认证。

4.8.4通常由审核组长对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证后，再连同审核报告一起交给技委会评审。

4.9编制审核报告

4.9.1瑞岳认证应当就每次审核向受审核方提供完整详实的审核报告。审核组长应对审核报告的内容负责。

4.9.2审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告的内容应当反映受审核方管理体系的真实状况，描述对照标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

a）申请组织的名称和地址。

b）申请组织活动范围和场所。

c）审核的类型、准则（含客户管理体系手册的修改状态）和目的。

d）审核组组成员的信息。

e）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

f）审核细节；叙述审核报告列明的各项要求的审核工作情况，其中：对各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；重点反映受审核方所取得的绩效，受审核方实际情况与其预期管理体系目标之间存在的差距和改进机会。

g）识别出的不符合和其他未解决的问题。不符合的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、含糊的语言表述不符合项。适用时，包括任何与客户以前审核结果的比较。

h）与审核类型的要求一致的审核发现、对审核证据的引用及审核结论，特别是对数据安全控制过程运行的策划及运行控制情况实施有效性的评价；

i）管理体系在达成其方针和目标，以及体系持续改进方面的有效性；

j）对组织的内部审核过程及管理评审过程（见下述注解）信赖程度的陈述。

注：关于内部审核过程及管理评审过程：标准要求至少每年进行一次，因此每年至少需要进行一次内部审核，之后必须进行一次管理评审。若组织将进入认证过程，进行第一阶段审核前必完成一次（最好两次）内部审核和一次管理评审。

k）审核组对是否通过认证的推荐意见。

4.9.3瑞岳认证应保留用于证实审核报告中相关信息的证据（审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料）。

4.9.4瑞岳认证应在作出认证决定后将审核报告提交申请组织，并保留签收或提交的证据。

4.9.5对终止审核的项目，审核组应将已开展的工作情况形成报告，瑞岳认证应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

4.10认证决定

4.10.1综合评价

瑞岳认证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，特别是对认证范围内数据安全运行控制情况进行综合评价。必要时，瑞岳认证应对申请人满足所有认证依据的情况进行风险评估，以做出申请人所建立的数据安全管理能否获得认证的决定。

瑞岳认证在做出认证决定时，应获得初次认证的所有信息，且所有不符合已关闭。

4.10.2瑞岳认证应在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。认证决定人员应为瑞岳认证管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

4.10.3瑞岳认证在作出认证决定前应确认如下情形：

a）审核报告符合本认证规则第4.7条要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

b）反映以下问题的不符合项，瑞岳认证已评审、接受并验证了纠正和纠正措施的有效性。

1)在持续改进的有效性方面存在缺陷，实现目标有重大疑问。

2)制定的目标不可测量、或测量方法不明确。

3)对实现目标具有重要影响的风险点（如适用法规的动态识别、应用和合规性评价等）的监视和测量未有效运行，或者对这些风险点的报告或评审记录不完整或无效。

4)其他严重不符合项。

c）瑞岳认证对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.10.4在满足4.10.3条要求的基础上，瑞岳认证有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

a）申请组织的数据安全管理符合标准要求且运行有效。

b）认证范围覆盖的产品、活动和服务符合相关法律法规要求。

c）申请组织按照认证合同规定履行了相关义务。

4.10.5认证决定

对于符合认证要求的申请人，瑞岳认证应颁发认证证书。

对于不符合认证要求的申请人，瑞岳认证应以书面的形式明示其不能通过认证的原因。

4.10.6对认证决定的申诉

申请人如对认证决定结果有异议，可在10个工作日内向瑞岳认证申诉，瑞岳认证自收到申诉之日起，应在一个月内进行处理，并将处理结果书面通知申请人。

申请人如认为瑞岳认证行为严重侵害了自身合法权益的，可以直接向认证监管部门投诉。

4.11认证证书

4.11.1瑞岳认证应当向认证决定符合要求的组织出具认证证书，认证证书的生效日期不应早于认证决定的日期。

4.11.2初次认证认证证书有效期最长为3年。

a）认证周期：自认证决定之日起三年减一天。再认证的决定应该在三年周期内完成，应在现有证书的有效期之内做出。

b）如果再认证在原有证书到期前三个月内完成，则新的认证周期自原有证书失效日算起后延三年（原周期保持不变）。

c）如果现有证书有效期短于三年，则不需要重发证书将有效期延长到三年。如果认证决定在现有的认证证书失效之后完成，则证书的连续性将被打破，新证书应自再认证的批准日期开始计算。

d）延期:证书期满后不允许延期。

4.11.3认证证书载明的信息应清晰、明确、容易理解、设计上不会以任何方式产生误导。

4.11.4瑞岳认证应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

4.11.5认证证书式样应符合相关法律、法规要求，认证证书应涵盖以下基本信息（但不限于）：

a）证书编号；

b）获证组织名称、注册地址、生产/服务场所的地址，如经营地址与注册地址不同，还应注明经营地址。若认证的管理体系覆盖多场所（多现场的认证应明确总部和所有其它场所，每个现场可以在附件中列出，总部应列在证书的主页上；地址必须精确到可以区分其场所而不导致混淆），应表述认证所覆盖的所有场所的名称和地址信息；

c）认证覆盖范围（含产品生产场所、具体产品和/或服务种类、过程等信息），当不同的现场涉及不同的过程和类别时，应在证书上予以明确，每个场所范围的不同应在证书附件中体现，且没有误导或歧义；

d）认证依据；

e）适当的产品、过程或服务；

f）颁证日期：生效日期/批准日期，对于初次认证为认证决定日期，对于再认证如再认证工作在原证书失效前3个月内完成，则从前原证书到期日算起。证书有效期限；

g）认证机构名称、地址；

h）相关的认可标识及认可注册号（适用时）；

i）签字（非强制）；

j）证书应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息；

k）证书状态的查询方式。

4.12认证标志

客户通过认证并获得认证证书后，可以在认证范围内使用认证标志。并应当遵守以下规定：

a)建立认证标志的使用和管理制度，对认证标志的使用情况如实记录和存档；

b)保证使用认证标志符合认证等级要求；

c)在广告、介绍等宣传材料中正确地使用认证标志、不得利用认证标志误导消费者；

d)当认证证书被暂停、注销或撤消认证时，应停止使用认证标志和发放带有认证标志的所有文件和宣传资料；

e)除了认证证书，客户还可以使用认证铜牌以示组织通过相应等级的管理体系认证。

认证标志如图：

4.13证书信息上报

瑞岳认证在颁发认证证书后，应当在当月按照规定的要求将相关信息报送全国认证认可信息公共服务平台。

5监督审核

5.1瑞岳认证对获证组织进行有效跟踪，依据审核方案对获证组织开展监督审核，并要求获证组织的最高管理者参与审核访谈，以确认获证组织网络数据安全管理与《网络数据安全管理技术规范》（RY-GF-001-2026）标准的持续符合性和运行的有效性。

5.2每次监督审核应尽可能覆盖认证范围内的典型产品/服务及有代表性的生产/服务过程，并确保在认证证书有效期内的监督审核覆盖认证范围内的所有典型产品/服务、有代表性的生产/服务过程。

5.3监督审核的时间应根据获证组织当前有效人数和风险类型确定，不少于依据附录1所确定的初次认证审核时间的1/3。

5.4监督审核应重点关注获证组织的变更以及数据安全管理绩效的持续改进，监督审核的内容至少包括：

（1）内部审核和管理评审；

（2）对上次审核确定的不符合采取的纠正措施及效果；

（3）数据安全管理在实现获证组织目标和数据安全管理预期结果方面的有效性；

（4）为持续改进而策划的活动的进展；

（5）持续的运作控制；

（6）任何变更；

（7）认证证书、认证标志的使用和（或）任何其他对认证信息的引用；

（8）相关投诉的处理；

（9）上次审核后发生的数据安全事故的调查与处理。

5.5不符合项的纠正和纠正措施及其结果的验证

5.5.1在监督审核中发现的不符合项，瑞岳认证应要求获证组织分析原因，规定时限要求获证组织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。

5.5.2瑞岳认证应采用适宜的方式及时验证获证组织对不符合项进行处置的效果。

5.5.2.1如发现了严重不符合项，要求在30天内采取措施并进行现场验证；

5.5.2.2通常由审核组长对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证后，再连同审核报告一起交给技委会评审。

5.5.3监督审核的审核报告，应按4.9、5.4条列明的审核要求逐项描述列明的审核要求的审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

5.5.4监督审核结果评价

瑞岳认证按照本规则4.10的要求对监督审核报告及其他相关信息，作出持续保持或暂停、撤销认证证书的决定。

6再认证审核

6.1认证证书期满前，获证组织申请继续持有认证证书的，瑞岳认证应依据审核方案实施再认证审核，以判断获证组织的数据安全管理作为一个整体与《网络数据安全管理技术规范》（RY-GF-001-2025）持续符合性和运行的有效性。

6.2再认证审核策划时应考虑获证组织最近一个认证周期内的绩效，包括调阅以往的监督审核报告。

6.3再认证审核的审核时间应按4.4.2的要求，根据获证组织当前有效人数和风险类型情况来确定，不少于依据附录1所确定的初次认证审核时间的2/3内的数据安全管理绩效，包括调阅以往的监督审核报告。

6.4再认证审核应在获证组织现场进行，并应在认证证书到期前完成。再认证审核的内容至少应包括：

（1）结合其内部环境和外部环境的变化情况，确认获证组织数据安全管理有效性及认证范围的持续相关性和适宜性；

（2）数据安全管理绩效持续改进的证实；

（3）数据安全管理在实现获证组织目标和数据安全管理预期结果方面的有效性。

6.5不符合项的纠正和纠正措施及其结果的验证

6.5.1在再认证审核中发现的不符合项，瑞岳认证应要求获证组织分析原因，规定时限要求获证组织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。

6.5.2瑞岳认证应采用适宜的方式及时验证获证组织对不符合项进行处置的效果。

6.5.2.1对再认证审核中发现的不符合，瑞岳认证应规定时限要求获证组织实施纠正与纠正措施，并在原认证证书到期前（最长不超过30天，距离原认证证书到期不足30天的，按照实际日期）完成对纠正与纠正措施的验证。

6.5.2.2通常由审核组长对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证后，再连同审核报告一起交给技委会评审。

6.6再认证审核的审核报告，应按3.9条、6.4列明的审核要求逐项描述列明的审核要求的审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

6.7瑞岳认证按照本规则4.10的要求，以及认证周期内的体系评价结果和获证组织相关方的投诉，作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发新认证证书。

6.8如果在当前认证证书到期前完成了再认证活动并决定换发认证证书，新证书的终止日期可基于当前认证证书的终止日期确定。新证书上的颁证日期不应早于再认证决定日期。

6.9如果在当前认证证书终止日期前，瑞岳认证未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

6.10在当前认证证书到期后，如果瑞岳认证能够在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不应早于再认证决定的日期，终止日期应基于原证书的终止日期。

7特殊审核

7.1扩大认证范围

对于已授予的认证，认证机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。这类审核活动可以结合监督审核同时进行。

7.2缩小认证范围

7.2.1在认证证书有效期内，需要缩小认证范围的获证组织应向瑞岳认证正式提交缩小认证范围的申请，或瑞岳认证审核组在现场审核中发现客户的管理体系部分不符合标准要求时，其过程/数据安全影响/风险独立，可以缩小认证范围。若发现认证范围中某些产品在一个认证周期内未能提供时，也应缩小相应的认证范围，并提供理由和证据。瑞岳认证的审定意见和日常监督结果也可作为认证范围缩小的信息来源和理由。经认证双方沟通后达成一致意见。需要时，获证组织与瑞岳认证补充签订认证合同/协议。

7.2.2经瑞岳认证审定，决定获证组织缩小认证范围后不会对仍保持的认证范围产生影响，满足缩小认证范围批准认证资格的条件，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的证书号和有效期截止日期保持不变。

7.3提前较短时间通知的审核

为调查投诉、数据安全事故，对变更做出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核，此时：

（1）认证机构应说明并使获证组织提前了解将在何种条件下进行此类审核；

（2）由于获证组织缺乏对审核组成员的任命表示反对的机会，认证机构应在指派审核组时给予更多的关注。

获证组织认证范围内的产品在产品质量国家监督抽查中被查出不合格时，自市场监管部门发出通报起30日内，认证机构应对该组织实施提前较短时间通知的审核。

8认证证书的暂停、恢复、撤销和注销

8.1认证证书的暂停

8.1.1获证组织有以下情形之一的，认证机构应在调查核实后5日内暂停其认证证书，并保留相应证据：

（1）持续或严重不满足认证要求的，包括文件与实际业务运作严重脱离；

（2）不满足适用的法律法规要求，且未采取有效纠正措施的；

（3）受到与数据安全相关的行政处罚，且尚未完成整改的；

（4）发生重大事故，反映获证组织数据安全管理运行存在重大缺陷的；

（5）拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息的；

（6）持有的与数据安全管理范围有关的行政许可文件、资质证书、强制性认证证书等过期失效的；

（7）不能按照规定的时间间隔接受监督审核的；

（8）未按相关规定正确引用和宣传获得的认证证书和有关信息，包括认证证书和认证标志的使用；

（9）不承担、履行认证合同约定的责任和义务的；

（10）被有关行政监管部门责令停业整顿的；

（11）发生与数据安全相关重大舆情的；

（12）主动请求暂停的；

（13）其他应暂停认证证书的。

8.1.2认证机构可根据暂停的原因和性质确定暂停期限，暂停期限最长不得超过6个月。

8.1.3暂停期间，认证证书暂时无效。如获证组织采取有效的纠正措施，造成暂停的原因已消除的，认证机构应恢复其认证证书，并保留相应证据。

8.2认证证书的恢复

8.2.1当暂停的原因已消除，整改措施有效，确认其具备恢复的条件，经技委会做出认证决定，批准后恢复认证证书使用。

8.2.2恢复认证资格的获证组织要按照瑞岳认证的要求，从恢复决定之日起恢复使用认证证书和认证标志，以及任何其他对认证资格的引用。

8.2.3当认证证书状态发生变化时，如暂停恢复，瑞岳认证应于生效日期起两个工作日内通过全国认证认可信息公共服务平台报送证书暂停恢复的相关信息。

8.3认证证书的撤销

获证组织有以下情形之一的，认证机构应在获得相关信息并调查核实后5日内撤销其认证证书，并保留相应证据：

（1）被注销或撤销法律地位证明文件的；

（2）被“国家企业信用信息公示系统”和“信用中国”列入严重违法失信名单的；

（3）认证证书的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

（4）经行政监管部门确认因获证组织违规而造成产品和服务等重大数据安全事故的；

（5）没有运行或者已不具备运行条件的；

（6）其他应撤销认证证书的。

8.4认证证书的注销

获证组织主动申请不再保持认证证书时，认证机构应确认在不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

9申诉、投诉处理

9.1瑞岳认证应当建立必要的申诉、投诉处理程序。组织对认证决定有异议时，可以向瑞岳认证提出申诉。瑞岳认证应接受获证组织申诉并且及时进行处理，在30日内将处理结果形成书面通知送交组织。

9.2书面通知应当告知组织，若认为瑞岳认证未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉。

9.3瑞岳认证应当及时、公正、有效地处理申诉和投诉，必要时采取纠正措施。

10认证记录的管理

10.1认证记录按瑞岳认证现有制度实施，记录认证活动全过程并妥善保存。

10.2记录应当真实、准确，以证实认证活动得到有效实施。认证记录应当使用中文，存档留存时间及相关要求按瑞岳认证程序文件规定执行。

10.3记录可以用纸质或电子文档的方式加以保存。

10.4瑞岳认证至少保存两个周期的认证记录,认证活动参与各方盖章或者签字的认证记录、资料等，应当保持具有法律效力的原件。

11认证收费

瑞岳认证为树立品牌形象，避免市场低价竞争，坚持优质优价原则，坚持按照认证方案策划的审核人日进行报价，并公开认证项目收费标准。

12其他

本认证规则内容提及《网络数据安全管理技术规范》（RY-GF-001-2025）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，均应采用当时有效版本的完整标准号。

13附则

本认证规则由瑞岳认证负责解释。

附录1：

网络数据安全管理认证审核人日表（仅适用于初次审核)

有效人数	审核时间 第1阶段＋第2阶段（天）	有效人数	审核时间 第1阶段＋第2阶段（天）
1-10	5	176-195	13.2
11	5.2	196-215	13.4
12	5.4	216-235	13.6
13	5.6	236-255	13.8
14	5.8	256-275	14
15	6	276-305	14.2
16-17	6.2	306-335	14.4
18-19	6.4	336-365	14.6
20-21	6.6	366-395	14.8
22-23	6.8	396-425	15
24-25	7	426-465	15.3
26-29	7.3	466-505	15.6
30-33	7.6	506-545	15.9
34-37	7.9	546-585	16.2
38-41	8.2	586-625	16.5
42-45	8.5	626-675	16.7
46-49	8.8	676-725	16.9
50-53	9.1	726-775	17.1
54-57	9.4	776-825	17.3
58-62	9.7	826-875	17.5
63-65	10	876-935	17.7
66-69	10.2	936-995	17.9
70-73	10.4	996-1055	18.1
74-77	10.6	1056-1115	18.3
78-81	10.8	1116-1175	18.5
81-85	11	1176-1250	18.7
86-93	11.2	1251-1325	18.9
94-101	11.4	1326-1400	19.1
102-109	11.6	1401-1475	19.3
110-117	11.8	1476-1550	19.5
118-125	12	1551-1645	19.8
126-135	12.2	1646-1740	20.1
136-145	12.4	1741-1835	20.4
146-155	12.6	1836-1930	20.7
156-165	12.8	1931-2025	21
166-175	13	>2025	遵循上述递进规律