北京中鼎乾元认证有限公司

信息安全管理体系认证实施规则

文件编号：ZDQY-GL/GZ-03-ISMS

版 本 号：A/0

编　　制：李超

审　　核：金海亮

批　　准：牛宇

生效日期：2023 年 8 月 1 日

1. 适用范围

本规则用于规范北京中鼎乾元认证有限公司（简称“中鼎乾元”或“ZDQY”）开展信息安全管理体系（ISMS）认证活动。

2. 认证依据

以标准 ISO/IEC27001:2022《信息技术 安全技术 信息安全管理体系 要求》为认证依据。

3. 术语和定义

3.1. 现场审核

中鼎乾元指派审核组到受审核方或获证组织所在办公地点进行管理体系运行的符合性进行审核。

4. 认证类别

认证类型分为初次认证，监督审核和再认证。为满足认证的需要，中鼎乾元可以实施特殊审核，特殊审核采取现场审核方式进行。

5. 审核人员及审核组要求

认证审核人员必须取得其管理体系认证注册资格，并得到中鼎乾元的专业能力评价，以确定其能够胜任所安排的审核任务。

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。审核组应：

a） 对拟认证 ISMS 范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识（技术专家可以履行此项职责）；

b） 理解客户，足以基于客户 ISMS 范围和组织环境对 ISMS（该体系管理着客户活动、产品和服务的信息安全）进行可靠的认证审核；

c） 适当地理解适用于客户 ISMS 的法律法规要求。

注：适当地理解法规要求不意味着要有深厚的法律背景。

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监督下进行工作，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。

6. 认证信息公开

中鼎乾元应向申请认证的社会组织(以下称申请组织)至少公开以下信息：

1) 认证服务项目；

2) 认证依据；

3) 证书有效期；

4) 认证收费标准。

7. 认证程序

7.1. 初次认证

7.1.1 认证申请

中鼎乾元应要求申请组织的授权代表至少提供以下必要的信息：

1) 认证申请书，包括但不限于以下内容：

a. 企业基本信息，包括业务活动、组织架构、联系人信息、物理位置和体系范围等基本内容

b. 法律地位资格证明(工商营业执照、事业单位法人证书或社会团体法人

登记证书，组织代码证和税务登记证（如果有））；

c． 体系运行的时间；

d． 取得相关法规规定的行政许可文件(适用时)。

2）信息收集表，包括但不限于：

a． 组织的资源管理

b． 组织的过程管理

c． 组织的风险管理

3）客户应说明适用的关于认证机构的资质、诚信守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并即时更新该说明，以便中鼎乾元判断是否具备对该客户实施认证活动的资格或条件。

7.1.2. 申请评审

中鼎乾元应根据认证依据、程序等要求，在要求时间内对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录，做出评审结论，以确定：

1）所需要的基本信息都得到提供；

2）申请组织的行业类别和与之相对应的管理体系所管理的过程特性和管理要求；

3）国家对相应行业的管理要求，满足工信部联协[2010]394号文《关于加强信息安全管理体系认证安全管理的通知》要求；

4）中鼎乾元与申请组织之间任何已知的理解差异得到消除；

5）中鼎乾元有能力并能够实施认证活动；

6）申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

7）中鼎乾元应建立关于审核人日的确定准则，根据受审核方的规模、特性、业务复杂程度、管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。将确定后的人日数记录在审核方案中，审核人日的确定规则参考附录A。

7.1.3. 建立审核方案

在申请评审后，中鼎乾元应针对申请组织建立审核方案（申请组织变更为受审核方），并由专职人员负责管理审核方案。审核方案范围与程度的确定应基于受审核组织的规模和性质，以及受审核管理体系的性质、功能、复杂程度以及成熟度水平。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应包括以下内容：

1）审核目的：应包括确定管理体系的有效性，以确保客户已根据风险评估实施了适用的控制并实现了所设立的信息安全目标；

2）审核的范围与程度、数量、类型、持续时间、地点、日程安排；

3）审核准则；

4）审核方法；

5）审核组的选择；

6）所需的资源，包括交通和食宿；

7）处理保密性、信息安全、健康和安全，以及其它类似事宜。

8）应考虑所确定的信息安全控制。

9）宜与拟审核的组织就选择一个能最有效地证实其整个ISMS范围的审核时

间达成一致意见。适当时，可考虑季度、月份、日期和班次。

7.1.4. 确定审核组

中鼎乾元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5章。

7.1.5. 一阶段审核

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）

为了确保获得上述信息，一阶段的部分审核需到客户现场进行。

7.1.6. 现场审核计划

审核组应结合受审核方的申请材料、审核方案对现场审核的策划以及一阶段审核的结果对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对受审核方按岗位和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排，如适宜，审核计划应识别在审核中使用的网络支持的审核技术。审核组长应至少在实施现场审核3个工作日之前，与受审核方就审核计划进行充分沟通，确保双方在理解上没有歧义。

7.1.7. 现场审核

审核组按照审核计划的安排对受审核方进行现场审核，现场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。

现场审核的内容包括但不限于：

a. 组织环境(应对风险和机会的措施，管理目标和达标计划)；

b. 领导（管理承诺，方针，组织的角色、责任和权限）；

c. 策划(应对风险和机会的措施，管理目标和实现计划)；

d. 支持(资源，能力，意识，沟通，文件化信息)；

e. 运行(运行的策划和控制，风险评估，风险处置)；

f. 绩效评估(监视、测量、分析和评价，内部审核，管理评审)；

g. 改进(不符合和纠正措施，持续改进)。

应重点关注客户：

最高管理者的领导力和对信息安全方针与信息安全目标的承诺；

ISO/IEC 27001中所列的文件要求；

评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

基于风险评估和风险处置过程，确定控制目标和控制；

信息安全绩效和ISMS有效性，以及根据信息安全目标对其进行评审；

所确定的控制、适用性声明、风险评估与风险处置过程的结果、信息安全方针与目标，它们相互之间的一致性；

控制的实施，考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

方案、过程、规程、记录、内部审核和对ISMS有效性的评审，以确保其可被追溯至管理决定和信息安全方针与目标。

7.1.8. 初次认证的审核结论

审核组应该对一阶段审核和现场审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果现场审核发现不符合项和观察项应开具不符合项报告，且获得受审核方认同。

现场审核结束后，审核组长完成审核报告编制工作，并与受审核方进行沟通，确保双方对报告的理解上没有歧义。

现场审核结束，审核组应形成是否推荐认证注册的结论；审核组可以根据一阶段审核结果和现场审核的结果对受审核方的管理体系是否满足所有适用的认证依据的要求进行评价，并判断是否推荐认证注册。

审核报告应提供以下信息或对这些信息的引用：

审核的说明，其中包括了文件评审摘要；

对客户信息安全风险分析进行认证审核的说明；

与审核计划的偏离（例如：在某一预定的活动上花费更多或更少的时间）；

ISMS的范围。

7.1.9. 认证决定

中鼎乾元应指派认证决定人员，对受审核方的认证申请实施认证决定，以决定：

a. 同意认证注册，颁发认证证书；

b. 补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

c. 不同意认证注册。

认证决定应基于审核报告中审核组对客户ISMS是否通过认证的建议。

通常情况下，对授予认证做出决定的人员或委员会不宜推翻审核组的负面建议。如果发生这种情况，应记录其作出推翻建议的决定的依据，并说明其合理性。

只有具备充分的证据证实管理评审和ISMS内部审核的安排已经实施，且是有效的并将得到保持，才可向客户授予认证。认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实受审核方建立管理体系得到了建立、实施、运行、监视、评审、保持和改进。

注1：参加审核的人员不能再作为认证决定人员实施认证决定。

注2：受审核方获得认证注册资格后变更为获证组织。

7.1.10. 审核方案记录与变更

审核方案管理人员应收集一阶段审核、现场审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中。 并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.2. 监督审核

7.2.1. 监督频次

中鼎乾元应在满足认可要求的基础上，根据获证组织管理体系覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织管理体系发生重大变更，或发生重大问题、业务中断事故、客户投诉等情况时，中鼎乾元可视情况增加监督的频次。

监督审核的最长时间间隔不超过12个月。由于获证组织业务运作的时间(季节)特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的两次监督审核涉及的条款之和必须覆盖管理体系认证范围内的所有条款。

7.2.2. 信息收集

在进行监督审核之前，中鼎乾元需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

1) 信息确认文件，包括但不限于：

a. 基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b. 组织信息，包括范围、组织架构、人员数量等信息的变化情况；

c. 管理体系相关信息，关键文件化信息的变化情况。

7.2.3. 确定审核组

中鼎乾元应根据获证组织的行业、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5章。

7.2.4. 信息评审

审核组应对获证组织的信息确认文件进行评审，以确定：

1) 获证组织的管理体系变化情况，尤其是管理体系范围的变化；

2) 是否需要修订审核方案，应针对与信息安全问题相关的风险及其对客户的影响来调整监督方案，并说明监督方案的合理性。

监督审核可以与其他管理体系的审核相结合。报告应清晰地指出与每个管理体系相关的方面。

7.2.5. 制定现场审核计划

审核组应结合获证组织的信息确认文件、审核方案对监督审核中现场审核的策划和一阶段审核的结果对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按岗位和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。审核组长应至少在实施现场审核3个工作日之前，与获证组织就审核计划进行充分沟通，确保双方在理解上没有歧义。

ISMS的监督审核并不覆盖标准所有条款，监督审核的抽样采取部门抽样的方式进行， 抽样准则为：

1) 两次监督审核必须覆盖标准所有条款和所有部门；

2) 标准中对信息安全管理过程有决定作用的条款和部门每次监督审核都需要抽到；

3) 获证组织前一次审核问题较多的部门在本次监督审核中需要抽到；

4) 审核组认为重要的条款应考虑进行抽样。

每次监督审核的内容应包括以下方面：

1) 管理体系的保持要素，如信息安全风险评估与控制的维护、ISMS内部审核、管理评审和纠正措施；

2) 对上次审核中确定的不符合项采取的措施；

3) 投诉的处理；

4）管理体系在实现获证客户目标和各管理体系的预期结果方面的有效性——SMS在实现客户信息安全方针的目标方面的有效性；

5）为持续改进而策划的活动的进展；

6）持续的运作控制——控制的实施和有效性（根据审核方案来审查）；

7）任何变更：文件化管理体系的变更；发生变更的区域；所确定的控制的变更，及其引起的SoA的变更；

8）标志的使用和（或）任何其他对认证资格的引用 ；

9）如适宜，审核计划应识别在审核中使用的网络支持的审核技术；

10）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

11）根据ISMS标准ISO/IEC 27001和认证所需的其他文件的要求，与来自外部各方沟通。

7.2.6. 现场审核

审核组按照审核计划的安排对获证组织进行现场审核，由于监督审核并不要求覆盖体系的所有方面，因此在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

在监督审核过程中，应检查客户提交给认证机构的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应检查客户是否对其自身的ISMS和规程进行了调查并采取了适当的纠正措施

7.2.7. 监督审核结论

审核组应该对现场审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果现场审核发现不符合项和观察项应开具不符合项报告，且获得获证组织认同。

现场审核结束后，审核组长完成审核报告编制工作，并与获证组织进行沟通，确保双方对报告的理解没有歧义。监督报告应包括有关消除以往出现的不符合、SoA版本和从上次审核之后发生的重大变更的信息。监督审核报告应至少完全覆盖本文件的7.2.5的要求

现场审核结束，审核组应形成是否推荐保持认证注册的结论；审核组可以根据一阶段审核结果和现场审核的结果对获证组织的管理体系是否满足所有适用的认证依据的要求进行评价，并判断是否推荐保持认证注册。

7.2.8. 认证决定

中鼎乾元应指派认证决定人员，对获证组织的认证申请实施认证决定，以决定：

a． 同意保持认证注册，颁发认证标志；

b． 补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

c． 不同意保持认证注册，做出暂定或撤销的决定。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织建立管理体系得到了建立、实施、运行、监视、评审、保持和改进。

7.2.9. 审核方案记录与变更

审核方案管理人员应收集一阶段审核、现场审核和认证决定的信息，特别是形成的结论和变化的信息，同时记录到审核方案中。 并确定审核方案是否需要

进行变更，如需要则更新相应项目内容。

7.3. 再认证

认证证书有效期满前，中鼎乾元根据获证组织的申请对获证组织实施再认证，以保证管理体系认证证书持续有效。

再认证审核的形式和过程与初次认证保持一致，但再认证的一阶段审核可以与二阶段审核一起进行，但当获证组织或其管理体系的运作环境（如法律的变更）有重大变更时，再认证审核活动可能需要有单独的第一阶段审核。

再认证审核将包括针对下列方面的现场审核

1）结合内部和外部变更来看的整个管理体系的有效性，以及认证范围的持续相关性和适宜性；

2）经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；

3）管理体系在实现获证客户的目标和管理体系预期结果方面的有效性。

7.4. 管理体系结合审核

当申请组织在运行信息安全管理体系的同时还运行了其他管理体系，若其他管理体系在中鼎乾元的认证业务范围内，中鼎乾元可以根据申请组织的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但中鼎乾元需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。

对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要要素的描述并易于识别。

7.5. 特殊审核

7.5.1. 变更或扩大认证范围

获证组织申请变更或扩大认证范围时，中鼎乾元应按再认证的过程对获证组织变更或扩大认证范围进行特殊审核，最终形成是否同意变更或扩大认证注册范围的决定。变更或扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证同时进行。

7.5.2. 中鼎乾元在调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪时，应指派审核组提前较短时间通知获证组织后对其进行特殊审核。特殊审核以现场审核方式进行，此时：

1）应向获证组织说明并使其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，中鼎乾元应在指派审核组时给予更多的关注；

3）审核组应制订审核计划，形成审核结论；

4）中鼎乾元应根据审核结论作出认证决定。

7.5.3. 审核方案记录与变更

审核方案管理人员应收集特殊审核的信息，特别是形成的结论和变化的信息，并记录到审核方案中。同时确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.6. 暂停、撤消认证或缩小认证范围

7.6.1. 中鼎乾元应有暂停、撤消认证或缩小管理体系认证范围的政策和形成文件的程序，并规定中鼎乾元的后续措施。

7.6.2. 发生以下情况(但不限于)时，中鼎乾元应在暂停情况确认后的五个

工作日内暂停获证组织的管理体系认证资格：

1）获证组织的管理体系持续地或严重地不满足认证要求，包括对管理体系有效性的要求；

2）获证组织不允许按要求的频次实施监督或再认证审核；

3）获证组织不接受或不配合认证认可监督管理部门的监督管理；

4）获证组织主动请求暂停。

7.6.3. 认证资格暂停期最长不超过6个月。

7.6.4. 在暂停认证期间，获证组织的管理体系认证证书暂时无效。中鼎乾元应做出具有强制实施力的安排，避免暂停认证期间获证组织继续宣传管理体系认证资格。中鼎乾元应使认证证书的暂停信息可公开获取。

7.6.5. 如果获证组织未能在中鼎乾元规定的时限内解决造成暂停认证的问题，中鼎乾元应在情况确认后的五个工作日内撤销其管理体系认证或缩小其相应的认证范围。

7.6.6. 如果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，中鼎乾元应缩小其管理体系认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

7.6.7. 中鼎乾元应与获证组织就撤消管理体系认证时的要求做出具有强制实施力的安排，以确保获证组织接到撤消认证的通知时，立即停止使用任何引用管理体系认证资格的广告材料。

7.6.8. 在任何组织提出请求时，中鼎乾元应正确说明获证组织的管理体系认证被暂停、撤消或缩小的情况。

8. 认证证书

8.1. 证书有效期

信息安全管理体系认证证书有效期为三年

8.2. 证书内容

8.2.1. 认证证书内容应以中文书写，至少包括以下方面：

1）认证证书名称，例如：信息安全管理体系认证证书；

2）符合本规则8.3项规定的证书编号；

3）获证组织名称、注册地址、获证地址和邮政编码；

4）符合本规则2项的认证依据；

5）通过认证的业务类别；

6）颁证日期、换证日期以及证书有效期的起止年月日。如颁证日期：2002 年5月1日，有效期：2002年5月1日至2005年4月30日；

7）中鼎乾元的名称及其标志；

8）中鼎乾元的印章和法定代表人代表或其授权人的签字；

9）认可标识及认可注册号(应为国家认监委确定的认可机构的标识，以申请认可为目的发出的证书可没有此内容)；

8.2.2. 如果认证所覆盖业务(或服务)的类别涉及到多个过程和覆盖的场所的，视情况需要颁发证书附件。

8.3. 证书编号

8.3.1. 对同一个受审核方实施的同一个管理体系认证，赋予一个认证证书编号。

8.3.2. 证书编号规则由中鼎乾元进行明确规定。

8.3.3. 有效期内因名称、地址、范围等变更换发证书，认证证书编号和有效期保持不变，应注明换证日期。

8.3.4. 撤销证书后，原认证证书编号废止，不再它用。
8.3.5. 认证证书上的中鼎乾元名称应与相应的中鼎乾元批准书上的名称一致。
8.4. 对获证组织正确宣传认证结果的控制
中鼎乾元应采取授权使用标识的方式来要求获证组织在认证结果的宣传和使用中采用本规则确定的认证依据，同时注明通过认证的业务类别和认证证书编号。在认证证书被暂停期间或撤销后，应收回相应的授权。
不应授权获证组织在产品上使用上述标识，或以表示产品合格的方式使用上述标识。

9. 对获证组织的信息通报要求及响应

为确保获证组织的管理体系持续有效，中鼎乾元应要求获证组织建立信息通报制度，及时向中鼎乾元通报以下信息：
1) 业务、地点、组织机构变化等情况的信息(及时通报)；
2) 顾客投诉的相关信息；
3) 组织的体系文件和业务重大变化时进行通报；
4) 有严重与管理体系相关事故的信息(及时通报)
5) 其他重要信息。(视情况)

中鼎乾元应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次以及暂停或撤销认证资格的措施等。在发生重大客户投诉等严重情况时，中鼎乾元需立即采取相应处理措施。

10. 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。
审核人日包括一阶段审核、现场审核以及报告编写的时间。

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其他管理体系的特点进行减少。

监督审核的人日数为初次认证人日数的三分之一，再认证的人日数为初次认证人日数的三分之二，上述原则仅限于获证组织的认证范围和组织规模未发生变化的情况。
附录A

基本人日数计算表

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