隐私信息管理体系认证实施规则（PIMS）

文　件　编　号：ZDQY-GL-03-058

版　　本　　号：A/0

编制人及编制日期：杨延飞 2022.7.29

审核人及审核日期：金海亮 2022.7.29

审批人及审批日期：张学群 2022.7.29

北京中鼎乾元认证有限公司

目 录

1 适用范围

本规则适用于北京中鼎乾元认证有限公司（简称 ZDQY）开展隐私信息管理体系（简称 PIMS）认证活动。

2 认证依据

ZDQY 对申请 PIMS 认证的组织按照 ISO/IEC 27701:2019《安全技术-ISO/IEC27001 和 ISO/IEC27002 关于隐私信息管理的延伸-要求和指南》开展认证活动~~活动~~。

3 认证程序

3.1 认证申请

3.1.1 ZDQY 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)认证范围；

(2)认证实施规则；

(3)认证依据；

(4)证书有效期；

(5)认证收费标准。

3.1.2 申请组织的授权代表签署《管理体系认证申请》，并至少提供以下必要的申请信息：

(1)申请认证的组织名称、注册地址、经营地址、通讯地址及邮编、联系人、职务、联系方式；（注册地址与经营地址不同址时，提供经营场所的房本或租赁合同等法律文书证明）

(2)认证类型；

(3)认证依据;

(4)体系覆盖的人数;

(5)根据业务、组织、位置、资产和技术等方面的特性所确定的PIMS的范围和边界，包括对任何范围、删减的详细说明和正当性理由;

(6)经营场所、分场所、临时场所以及各场所从事的活动等;

(7)服务器数量、终端数量、用户的数量;

(8)适用性声明、资产列表;

(9)保密协议、信息安全敏感区域的声明;

(10) 申请组织对ZDQY的资质、诚信守法记录或认证人员身份背影的要求以及适用的、最新的与保守国家秘密或维护国家安全有的法律法规要求，以便ZDQY判断是否具备为申请组织实施认证活动的资格或条件;

(11) 关于认证活动的限制条件(如出于安全和/或保密等原因，存在时)。

(12) 在认证审核之前，ZDQY应要求客户组织报告是否存在因包含保密性或敏感性信息而导致不能提供给审核组核查的PIMS相关信息。ZDQY应确定PIMS是否能在缺少这些信息的情况下得到充分审核。如果ZDQY的结论是若不核查已识别的保密性或敏感性信息就不能对PIMS进行充分的审核，那么ZDQY将会告知客户只有在适当的访问安排获得许可后才能进行认证审核。

(13) 认证协议应就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确认证机构和客户及其有关人员的责任与义务。

3.1.3 申请组织还提供以下资料:

(1)法人资格证明(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)；

(2)取得相关法规规定的行政许可文件(适用时)；

(3)满足工信部联（2010）394号文《关于加强信息安全管理体系安全管理的通知》以及有关主管部门/监管部门对信息安全管理体系认证的管理要求的证据；

(4)手册及相关体系文件；

(5)支持PIMS的规程和控制措施、风险评估方法的描述、风险评估报告、风险处置计划、组织为确保其信息安全过程的有效规范/运行和控制以及描述如何测量控制措施的有效性的文件。

3.1.4 上述必要信息应使 ZDQY 确定：

(1)申请组织的行业类别和管理要求；

(2)申请认证的范围；

(3)申请组织的一般特征，包括其名称、物理场所的地址、隐私信息安全管理体系对组织风险管理的控制说明及任何相关的法律义务；

(4)认证领域的一般信息，包括其活动、人力与技术资源、以及适用时其在一个较大实体中的职能和关系；

(5)所有影响符合性的外包过程的信息；

(6)PIMS 有关的咨询的情况。

3.2 申请评审

ZDQY 应根据认证依据、程序等要求，及时对申请组织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)识别申请组织的行业类别和与之相应的 PIMS 特性和要求；

(2)掌握国家对相应行业的隐私信息安全管理体系认证的管理要求；

(3)申请组织及其 PIMS 的信息充分，可以进行审核；

(4)认证要求已有明确说明并形成文件，且已提供给申请组织；

(5)解决了与申请组织之间任何已知的理解差异；

(6)有能力并能够实施认证活动；

(7)考虑了申请的认证范围、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；

(8)保持了决定实施审核的理由的记录。

3.3 审核的准备

3.3.1 确定审核组

3.3.1.1 审核员必须满足本实施规则 4.1 和 4.2 的要求。

3.3.1.2 审核组应由具有 PIMS 审核员资格的成员组成，其中至少有一名专职审核员。必要时可以补充技术专家以增强审核组的技术能力。

3.3.1.3 具有 PIMS 及相关法规等方面的特定知识的技术专家可以成为审核组成员。不具备专业的审核员在审核专业过程或部门时应在技术专家的技术指导下实施审核工作，技术专家可就受审核方 PIMS 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。

3.3.2 ZDQY 应根据申请组织的产品、服务和活动的数量及种类，组织规模，复杂程度（园区、隐私信息安全复杂程度等）、审核范围等因素核算并确定审核人日，以确保审核的适宜性、充分性和有效性。

3.4 初次认证审核

3.4.1 第一阶段审核应在申请组织的现场进行，审核内容包括：

(1)审核申请组织的 PIMS 管理体系文件，了解体系建立情况；

(2)评价申请组织的运作场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况；

(3)审查申请组织理解和实施 PIMS 标准要求的情况，特别是对关键绩效、风险等级、关键隐私信息安全、过程、目标和管理体系的运行方面。收集和确定必要的信息资料，包括管理体系的范围（含边界），过程，场所（含虚拟场所），以及相关的法律和法规合规性；

(4)审查申请组织是否系统而充分地识别与 PIMS 相关的法律法规和其他要求及其遵守情况；

(5)审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

（6）结合申请组织 PIMS 方针和目标，了解其审核准备状态，为策划第二阶段的审核提供重点；

（7）评价申请组织是否策划和实施了内部审核与管理评审，以及 PIMS 实施程度能否证明其已为第二阶段审核做好准备。

（8）确定认证活动引发的客户信息安全风险（包含保密性或敏感性信息），以及控制措施。

3.4.2 ZDQY 应将第一阶段审核发现及一阶段审核结论形成文件并告知申请组织，包括任何应引起关注的、在第二阶段审核中可能被判定为不符合的问题。

3.4.3 第二阶段审核

第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，通过与受审核方的沟通/访谈/现场观察/调阅相关的文件或记录/选择认证范围内典型样本进行抽样，证实并评价申请组织的 PIMS 是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。

ZDQY 应要求申请组织证实其已依据 ISO/IEC 27701:2019《安全技术-ISO/IEC27001 和 ISO/IEC27002 关于隐私信息管理的延伸-要求和指南》及相关法律法规和需求对隐私信息安全管理体系进行了相应的策划、实施、监视和改进，应至少包括：

(1) 关于符合 PIMS 所有要求的信息和证据；

(2) 制定 PIMS 方针、目标，实现和测量目标的方法，分配了角色、职责和权利；

(3) 风险评估、绩效监控、测量、报告对关键绩效目标指标的评审；

(4) PIMS 与法律合规性；

(5) 建立并实施隐私信息安全策略和程序；

(6) 内部审核和管理评审/不合格处置及持续改进活动。

3.4.4 PIMS 文件与其他管理体系文件的整合

只要 PIMS 以及与其他管理体系的适当接口（共同的过程）能够清楚地被识别，可以允许申请组织将 PIMS 文件与其他管理体系文件(如：质量管理体

系、信息技术服务管理体系、信息安全管理体系等)相结合。但一体化后的管理体系应满足认证范围内适用的 PIMS 的所有要求。

3.4.5 管理体系结合审核

3.4.5.1 ZDQY 可以仅提供 PIMS 认证服务，或结合其他管理体系提供认证服务。但是这种结合必须以审核活动满足 PIMS 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。

3.4.5.2 ZDQY 应有程序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。在结合审核报告中，应清晰体现所有与 PIMS 有关的重要要素的综合评价描述并易于识别。

3.4.6 初次认证的审核结论

审核组应该对第一阶段和第二阶段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。

3.5 认证决定

3.5.1 原则

3.5.1.1 参加审核的人员不能再作为认证决定人员实施认证决定。

3.5.1.2 应该以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立隐私信息安全管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。

3.5.2 决定

3.5.2.1 对于通过认证的申请组织，向其颁发 PIMS 认证证书。

3.5.2.2 对于未通过认证的申请组织，应以书面的形式明示其不能通过认证的原因。

3.6 监督审核

3.6.1 监督频次

依据相关管理体系审核要求和获证组织的 PIMS 特点及风险，合理设计监督审核的时间和频次。当获证组织 PIMS 发生重大变更，或发生重大问题、信息安全事件、客户投诉等情况时，ZDQY 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监督审核必须覆盖 PIMS 认证范围内的所有业务活动。

3.6.2 监督审核应包括，但不限于以下内容：

(1)体系保持和变化情况；

(2)顾客投诉情况；

(3)涉及变更的范围；

(4)内部审核与管理评审；

(5)PIMS 的事件及处理结果是否达到了目标；

(6)对上次审核时提出的不符合所采取纠正措施的审查；

(7)标志的使用和（或）任何其他对认证资格的引用；

(8)适当时，其它选定的范围。

3.6.3 对于监督审核合格的获证组织，应作出保持其隐私信息安全管理体系认证资格的决定；否则，应暂停、撤销或注销相应的认证资格。

3.7 再认证审核

3.7.1 再认证证书有效期满前，根据获证组织的申请对获证组织实施再认证，以保证 PIMS 认证证书持续有效。

3.7.2 再认证审核的策划

3.7.2.1 应策划和实施再认证审核，以评价获证组织是否持续满足 PIMS 标准和相关的认证规范性文件的所有要求。

3.7.2.2 再认证审核应考虑 PIMS 在认证周期内的绩效，包括调阅以前的监督审核报告/不符合报告。

3.7.2.3 当获证组织、获证组织的 PIMS 或其运作环境有重大变更时，ZDQY 应有程序确保对再认证审核活动可能需要进行的第一阶段审核实施管理。

3.7.2.4 对于多场所认证或依据多个管理体系标准进行的认证，再认证审核的策划应确保现场审核具有足够的覆盖范围，以提供对 PIMS 认证的信任。

3.7.3 再认证程序应与管理体系认证审核的要求和指南保持一致。

3.7.4 ZDQY 应根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，作出是否更新认证的决定。

3.8 特殊审核

3.8.1 扩大认证范围

对于已授予的认证，应对获证组织扩大认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的 PIMS 的适宜性和有效性，以作出是否可予扩大的决定。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一起进行。

3.8.2 为调查投诉、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，可能需要在提前较短时间通知获证组织后对其进行审核。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，ZDQY 应在指派审核组时给予更多的关注。

3.9 暂停、撤消认证或缩小认证范围

3.9.1 ZDQY 应有暂停、撤消认证或缩小 PIMS 认证范围的政策和形成文件的程序，并规定后续措施。

3.9.2 发生以下情况(但不限于)时，ZDQY 应暂停获证组织的 PIMS 认证资格：

(1)获证组织持续地或严重地不满足认证要求；

(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。

3.9.3 认证资格暂停期最长不超过 6 个月。

3.9.4 在暂停认证期间，获证组织的 PIMS 认证证书暂时无效。ZDQY 应做出具有强制实施力的安排，以确保暂停认证期间避免获证组织继续宣传 PIMS 认证资格。ZDQY 应使认证证书的暂停信息可公开获取，并采取其认为适当的任何其他措施。

3.9.5 如果获证组织未能在规定的时限内解决造成暂停认证的问题，ZDQY 应撤消其 PIMS 认证或缩小其相应的认证范围。

3.9.6 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，ZDQY 应缩小其 PIMS 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。

3.9.7 ZDQY 应与获证组织就撤消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 PIMS 认证资格的广告材料。

3.9.8 在任何组织提出请求时,ZDQY 应正确说明获证组织的 PIMS 认证被暂停、撤消或缩小的情况。

4 对认证人员的要求

为了确保审核能力，ZDQY 基于 ISO19011 的要求，对隐私信息安全管理体系审核员、认证过程管理人员进行资格审批和管理，应满足以下条件：

4.1 基本要求

4.1.1 个人素质：有道德，思想开明，善于交往，善于观察， 有感知力，适应能力强，坚韧不跋，明断，自立。

4.2 审核员能力要求

隐私信息安全管理体系审核员应具备 ISMS 信息安全注册审核员资格，熟悉隐私相关专业知识。

4.3 认证过程管理人员能力要求

对于 PIMS 申请评审人员、审核方案管理人员、认证决定管理人员、认证决定人员、认证规则制定人员、人员能力评价人员，应至少具备信息安全相关人员岗位能力授权，并了解隐私相关知识，在审核运营部评价后给与 PIMS

相应岗位授权。

5 认证证书

5.1 证书内容

认证证书内容应以中英文书写，至少包括以下方面：

(1)认证证书名称，即“隐私信息安全管理体系认证证书”；

(2)符合本规则 5.2 项规定的证书编号；

(3)获证组织名称、注册地址、受审核地 址和邮政编码；

(4)符合本规则要求的认证依据；

(5)认证覆盖的范围；

(6)颁证日期、换证日期以及证书有效期的起止年月日，有效期 3 年。

(7)ZDQY 的名称及其标志；

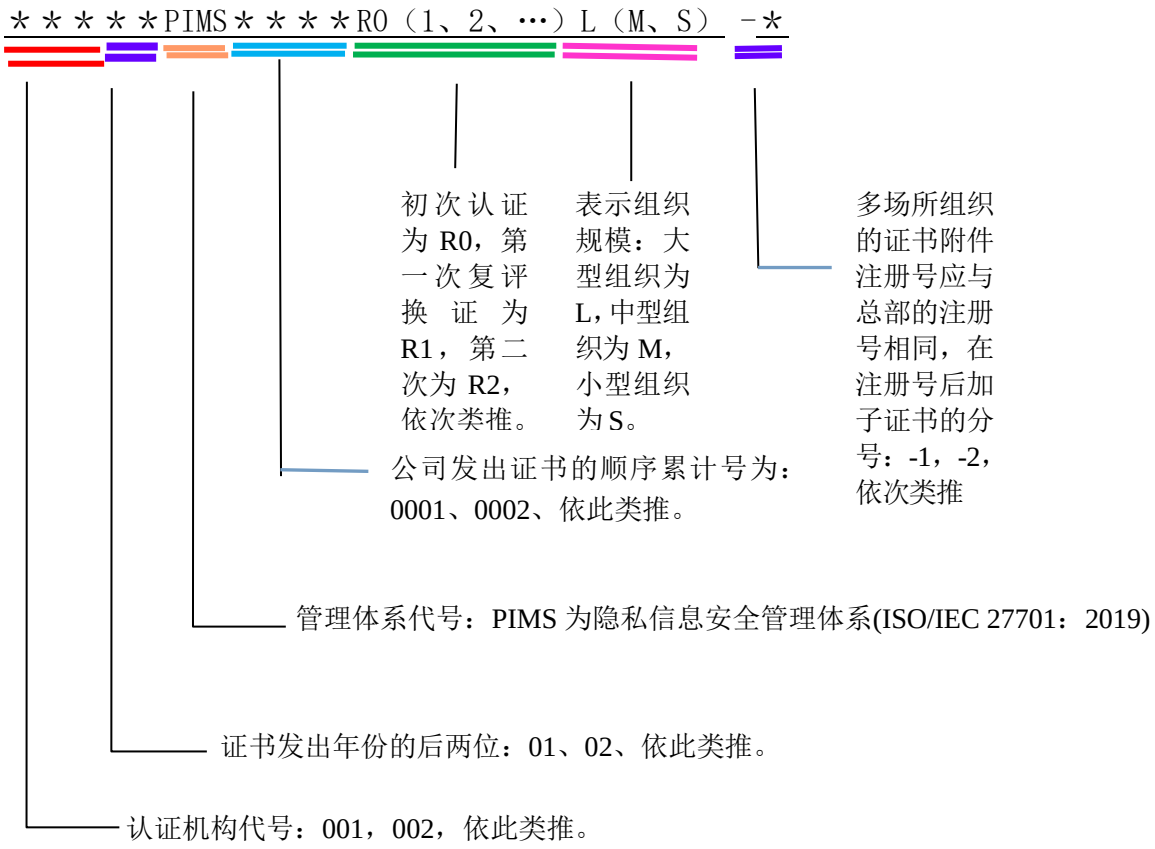
(8)ZDQY 的印章和法定代表人代表或其授权人的签字；

如果认证所覆盖产品(或服务)的类别及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

5.2 证书编号

5.2.1 对同一个组织实施的同一个 PIMS 认证，应使用同一个证书编号；

5.2.2 证书编号由 ZDQY 认证机构代号，证书发出年份，管理体代号，发出证书顺序号，初次及复评次数，组织规模，多场所序号构成，格式如下：



5.2.3 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

5.2.4 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

5.2.5 再认证完成后换发证书，按 5.2.2 规定重新赋予认证证书编号，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

5.2.6 撤销证书后，原认证证书编号废止，不再使用。

5.2.7 认证证书上的认证机构名称应与 ZDQY 的认证机构批准书上的名称一致。

5.3 对获证组织正确宣传认证结果的控制

ZDQY 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服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。

6 对获证组织的信息沟通和要求

6.1 信息沟通

为确保获证组织的 PIMS 认证持续有效,ZDQY 应要求获证组织建立信息通报制度，及时向 ZDQY 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(每三个月通报一次)；

(3)组织的体系文件、资产识别、信息安全策略和控制措施；适用性声明等信息的变化；

(4)有严重隐私信息安全事件的信息(及时通报)；

(5)其他重要信息(视情况)。

6.2 响应要求

ZDQY 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在内的措施和暂停或撤销认证资格的措施。在发生重大客户投诉等严重情况时，需立即采取措施。

7.涉及的相关文件

ZDQY-CX-02-01 认证申请、评审及受理控制程序

ZDQY-CX-02-03 认证证书、标志制作发放及暂停、撤销控制程序

ZDQY-CX-02-09 人力资源控制程序

ZDQY-CX-02-10 认证人员岗位任职要求及能力评定控制程序

ZDQY-CX-02-11 审核员监视和再评价控制程序

ZDQY-GL-03-010 审核方案管理规则

ZDQY-GL-03-021 特殊审核管理规则

ZDQY-GL-03-023 认证评定实施规则

ZDQY-GL-03-028 见证评价人员的管理规则

ZDQY-GL-03-029 审核员能力现场评价规则

ZDQY-GL-03-033 认证审核人员管理规则

ZDQY-GL-03-042 一阶段审核要求

ZDQY-GL-03-043 现场审核通用要求

ZDQY-GL-03-021 特殊审核管理规则

信息安全管理体系（ISMS）认证要求补充程序
隐私信息管理体系（PIMS）认证要求补充程序