文 件 号	CEPREI-86-GM
版 本 号	2

基于 ISO/IEC 27701 的隐私信息管理体系认证程序规则

广州赛宝认证中心服务有限公司

批　准　页

编制：鲁　立　　日期：2021年3月26日

审核：刘小茵　　日期：2021年4月14日

批准：赵国祥　　日期：2021年4月21日

本文件自批准之日起实施

目　　录

1. 总则

1.1. 目的

为使申请方/受审核方/获证组织全面了解赛宝认证中心(以下简称本中心)受理并实施基于 ISO/IEC 27701 隐私信息管理体系（PIMS）认证的全过程，便于本中心有序、有效地开展 PIMS 认证工作，特制定本程序规则。

1.2. 适用范围

本程序规则适用于本中心开展的 PIMS 认证工作，可为申请方/受审核方/获证组织进行 PIMS 认证/注册提供指导。

1.3. 主要依据文件

1）CNAS-CC01《管理体系认证机构要求》;

2) 中心文件 CEPREI-QP-213-MR《PIMS 审核人日控制程序》。

1.4. 认证依据文件

1) ISO/IEC 27701：2019 Security Techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines 安全技术 扩展 ISO/IEC 27001 和 ISO/IEC 27002 的隐私信息管理 要求与指南。

2) GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》

3) GB/T 22081-2016《信息技术 安全技术 信息安全控制实用规则》

4) ISO/IEC TS 27006-2：2021《Requirements for bodies providing audit and certification of information security management systems – part 2: Privacy information management systems》

1.5. 术语说明

根据认证过程的变化,本规则对申请认证单位使用了不同的称呼:

申请方：认证审核之前

受审核方：审核过程中及获证前

获证组织：获得 ISO/IEC 27701 认证证书后。

1.6. 职责

管理委员会、技术委员会、各业务部门的职责与 ISO27001 信息安全管理体系认证相同，但在具体的运作要求上，在开展 PIMS 的认证工作时，应遵循本规则的要求。

2. 申请方应具备的基本条件

2.1. 申请方应具备的基本条件

1) 具备相关法定资质、资格，如独立法人地位证明文件等，如果申请方是大组织的一部分(无独立法人资格)，应持有大组织的授权证明等；
2) 已（或正在—指意向阶段）按 ISO/IEC27001 及 ISO/IEC 27701 认证标准要求，建立管理体系，并实施运行至少 3 个月。
3) 申请方已按规定实施了隐私信息管理体系内部审核和管理评审，且时间间隔不超过 12 个月，没有发现重大不足。
4) 未列入国家信用信息严重失信主体相关名录。
5) 认证申请组织应具备评价和保持法律法规符合性的机制，并按规定向有关部门及相关方通报所发现的不符合情况。

3. 申请方/受审核方的权利和义务

3.1. 申请方/受审核方的权利

1) 自主选择咨询单位（本中心不进行咨询）。
2) 与本中心协商确定认证采用的模式标准和认证时间。
3) 对参加评估审核的人员、审核日期安排有异议时，与本中心协商解决。
4) 有权对本中心的认证活动等提出申诉/投诉和异议。

3.2. 申请方/受审核方的义务

1) 按本中心要求提交申请文件（本中心提供申请书文本格式）及其附件；
2) 为本中心提供保证审核工作顺利进行必要的办公条件；
3) 为本中心审核组进入审核区域、调阅文件记录、安排被访问人员等提供必要的条件；适用时，为接纳到场的观察员（如认可机构评审员）提供条件。
4) 保留顾客和/或相关方就获证组织的活动、产品或服务所提出的所有投诉记录，信息沟通记录及相应纠正措施记录，并在本中心要求时提供。重要投诉应及时通报本中心。
5) 按规定及时交纳认证费用。
6) 管理体系认证申请组织有责任保持并评价法律法规要求的符合性。

4. 认证的公正性

4.1. 管理委员会的组成

管理委员会的组成原则应遵循 CEPREI-01《管理委员会章程》的要求，专业能力应考虑隐私信息管理的特殊性。

4.2. 评估结论决定人员的组成

相关要求参见 CEPREI-03《技术委员会工作细则》及 CEPREI-QP-14《认证决定程序》。隐私信息管理体系评估结论决定人员的能力要求，具体见 CEPREI-QP-218-MR-P《隐私信息管理体系人员能力评定程序》。

5. 能力管理

5.1. 人员能力要求

ISO/IEC 27701 认证涉及人员，如合同评审人员、审核方案管理人员、专业

能力见证评价和专业培训指导人员、审核结论决定人员、专业审核员等的能力要求见 CEPREI-QP-218-MR-P《隐私信息管理体系人员能力评定程序》。

5.2. 人员的选择与评价

ISO/IEC 27701 认证业务对口管理部门依本中心文件 CEPREI-QP-02《人员录用、培训及监督程序》对该业务人员进行选择和评价。

5.3. 能力保持、提高及行为监视

依据 CEPREI-QP-08《审核员管理程序》等程序实施能力保持提高及行为监视。

6. 认证程序

认证决定，ISO/IEC 27701 认证活动含申请的受理，初次认证的初次审核包含第一阶段和第二阶段审核，为保持认证所需进行的监督审核，在初次认证三年有效期满后获证组织希望保持认证资格而需进行的再认证审核和再认证决定等。

6.1. 申请

(1)确认申请意向后，申请方需向本中心市场拓展部提交认证申请书及其附件，综合部组织合同评审，评审通过后，市场拓展部与申请方签订《管理体系认证合同》；申请条件需符合以下任一项：

① 组织已获得基于 ISO/IEC 27001 的 ISMS 认证证书，且 ISMS 范围大于或等于 PIMS 范围

② 同时申请 ISMS 认证及 PIMS 认证

(2)申请方按合同约定金额及时间交纳认证费用。

若申请人有因法律特权或专利权关系，不能让审核组评审或获得与法律法规符合性有关的资料或信息，则不能获取/维持认证资格；除非审核组能够获得客观证据表明法律法规符合性和相关体系要求已得到有效实施。有此类情况时，双

方将在合同中说明要求。

综合部负责申请受理工作，对申请文件的齐套性进行检查，文件不齐套时，通知申请方重新提交或补充。市场拓展部负责《管理体系认证合同》商务条款的评审。审核部门负责《管理体系认证合同》技术条款的评审。综合部在确认中心可受理申请后，即把文件移交业务主管部门审核。

6.2. 审核人日

参考文件《PIMS 审核人日控制程序》。

6.3. 第一阶段审核

第一阶段审核活动包括文件审核，并通常包括现场审核。不需现场审核的特殊情况包括：

① 组织已获得 ISMS 证书，且 ISMS 范围覆盖 PIMS 范围的。

② 同时向我中心申请 ISMS 认证及 PIMS 认证，且已完成 ISMS 一阶段审核的。

③ 因特殊原因，已获证组织在证书有效期内采用初审流程重新认证。

(1) 审核部门指定审核组进行文件审核。

(2) 必要时审核组按审核计划进行第一阶段现场审核，以确定申请方是否做好第二阶段审核的准备收集必要的信息，识别第二阶段审核的重点并与受审核方交换信息及商定第二阶段审核的具体事宜。

(3) 第一阶段审核结束后，审核组将第一阶段审核报告提交申请人。

(4) 第一阶段审核结论为准备不够充分时，不能进入第二阶段现场审核。

6.4. 第二阶段现场审核前的准备工作

(1) 现场审核组的正式成员应为经过本中心评价合格的 PIMS 审核员，必要时可以聘请有关的技术专家协助审核工作。审核组至少有一名审核员具备 ISO17021 要求的组长能力。

审核部门应将审核组名单通知申请方，申请方如有异议且理由充足，由受审核部门和申请方协商调换。

(2) 审核组应根据提交的文件资料及受审核方隐私信息保护特点进行审核策划，包括拟制审核计划，并将经批准的审核计划提交申请方确认。

6.5. 第二阶段现场审核

(1) 首次会议

现场审核开始的时候，审核组长应主持召开受审核方领导参加的首次会议，向受审核方有关负责人说明审核计划、审核程序、方法、审核的可能结果、违反法律法规和其它要求的处理以及不符合类型及保密承诺等。

(2) 现场取证及评价

审核组根据审核计划，采取提问、交谈、查阅文件资料、现场观察、实际测定等方法，取得确切的证据，记录审核情况，对受审核方的隐私信息管理体系进行有效性评价。

在审核期间，受审核方应予以协助、配合，并保证：

a. 审核组能够查阅和隐私信息管理有关的文件资料和相关记录，包括原始记录；

b. 审核组能够进入与隐私信息管理审核有关的场所(若受审核方认为某些场所为本单位的机密场所，应在首次会议上说明，双方协商解决)；

c. 审核组能够访问与隐私信息管理有关的人员；

d. 为审核组提供进行隐私信息管理审核所必需的设施和条件，并指定联络人员。

(3) 末次会议

现场审核结束时，审核组长应主持召开受审核方领导参加的末次会议，对受审核方隐私信息管理体系的符合性和有效性作出评价，宣布现场审核的结论；

a. 受审核方如对审核结论有不同看法，与审核组不能达成一致意见时，应记录在审核报告中；

b. 审核组应就现场审核发现的不符合项（经确认的）与受审核方商定在一个适当的时间内采取纠正措施。对一般不符合项采取纠正措施的时间要求一般不超过一个月，严重不符合项一般不超过三个月。

不符合项通常分为严重不符合项和一般不符合项。

出现下列情况之一者，即为严重不符合：

① 体系运行出现系统性失效。如：某一或多个重要过程要求要素没有覆盖、没有得到实施，或多个一般不符合同时存在导致审核员认为认证要求的一个或多个要素未能被覆盖或实施即多次重复发生不符合现象，而又未能采取有效的纠正措施加以消除，形成系统性失效。

② 体系运行出现区域性失效。如：某一部门适用隐私信息保护要求的全面失效现象。

③ 组织的隐私信息管理行为严重违反法律法规或其它要求。

对存在严重不符合项的情况，将导致受审核方的 ISO/IEC 27701 认证不能给予注册或推迟给予注册。

凡出现下列情况为一般不符合项：

对满足认证要求而言，是个别的、偶然的、孤立的、性质轻微的不合格。或者说，对审核范围覆盖的体系而言，是个次要的问题。

在认证活动中，审核员所识别组织违反法律法规要求，且未予评价并采取措施的审核发现，将构成不符合。对有意不遵守法律法规（如决定交纳罚款后继续违规操作，而不寻找导致不符合的原因并制订措施）的组织，将不能通过认证或保持认证资格。对存在严重违反法律法规要求的组织，需经确认已采取措施恢复法律法规符合性后，方可获得或保持认证资格。

c. 现场审核全部结束后，审核组将现场审核报告及全套审核文件及记录的扫描件上传 OA 归档。

6.6. 颁发认证证书和证书注册

所采取的纠正措施经审核员书面验证（一般不符合项）或现场验证（严重不符合项）认为有效后，由业务主管部门报呈中心技术委员会审定。

如技术委员会的认证决定建议与审核组的审核结论有重大出入时，由审核部门向受审核方发出审核结果《更正通知书》。

技术委员会审定通过后，由申请受理部门办理证书注册和认证证书制作事宜。认证证书经中心主任签发，ISO/IEC 27701 认证的有效日期不得超过它所基于的 ISO/IEC 27001 认证的日期，最长有效期为三年。

7. 注册名录

获证组织名称、地址、认证依据的规范性文件和获准认证范围等列入本中心“获证组织名录”。本中心将定期更新该名录，社会公众可在本中心网站（www.ceprei.org）的“获证企业”，或 CNCA（中国国家认证认可监督管理委员会）网站（www.cnca.org.cn）左下侧“认证企业信息查询”，或直接向本中心综合部查询（查询电话：4008301909）相关注册名录。若获证组织因保密需要无意公开此信息，请通知我中心。

8. 获证组织的权利和义务

获证组织具有使用认证证书和标志、投诉/申诉等权利，以及按时接受监督审核等义务。

9. 认证证书和标志的使用

被批准管理体系注册后，获证组织可以向公众展示本中心的认证证书及标志，以证实获证组织管理体系通过了 ISO/IEC 27701 认证，但应遵守本中心和国家相关法规的规定。

10. 获准注册后的监督管理

(1) 本中心将定期进行监督审核，以确认获证组织的管理体系持续满足认证要求。作为最低要求，在初次认证决定日期起的 12 个月内应进行一次监督审核。此后，每个日历年内（应进行再认证的年份除外）进行一次监督审核。在达到监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，经本中心技术委员会同意，可以适当延长监督审核期限。

(2) 必要时，本中心将进行特殊审核。

11. 证书的更换

获证组织需更改获准认证/注册的 ISO/IEC 27701 认证信息时，应及时将更改情况报本中心综合部。在管理体系认证证书有效期内，当证书覆盖的范围、认证依据的标准、证书持有者、注册地址等发生变更时，应重新换证。

12. 认证资格的暂停或恢复，撤销，注销和扩大或缩小认证范围

当获证组织管理体系持续或严重不满足认证要求或认证合同规定的；被有关执法监管部门责令停业整顿的；被地方认证监管部门发现体系运行存在问题，需要暂停证书的；持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的等，均可能会导致认证资格的暂停，甚至撤销。如果认证范围的某些部分（如产品、区域）持续或严重地不满足认证要求，

会导致认证范围的缩小。获证组织不愿意保持认证资格，可提出认证的注销。获证组织范围内某些部分不愿维持纳入认证资格，也可提出缩小认证范围。

本中心关于注销、暂停、撤销体系认证证书持有者使用体系认证证书和标志资格的决定，以及解除暂停（恢复）的决定，扩大或缩小认证范围的决定，应书面通知体系认证证书持有者，并以适当方式予以公布，同时，还将上报国家认监委等机构。

13. 特殊审核

13.1. 扩大认证范围

获证组织需扩大认证范围时应提出申请，本中心将评审申请，确定必要的审核活动，以做出是否可予扩大的决定。

13.2. 提前较短时间通知的审核

赛宝认证中心为调查投诉，开展国家安排的检查任务，重大事故调查，对变更情况进行评价，或对被暂停的获证组织进行跟踪而进行的审核可能只能提前较短时间，甚至无法提前通知获证组织。请获证组织给予理解和配合。若获证组织届时对具体审核组成员有异议，仍可向本中心提出。

14. 再认证

当证书有效期到期后，证书将自动失效，获证组织如需继续保持注册资格，需在证书到期之前六个月与本中心市场拓展部重新签订合同，然后按上述程序在证书有效期之前进行再认证和换证。对再认证审核中发现的不符合，获证组织应在原认证周期终止前实施所要求的纠正与纠正措施。

15. 投诉和申诉

申请方/受审核方/获证组织在对本中心的结论、行为、决定等有异议时，可公平地提出，并具有投诉/申诉的权利。本中心申/投诉处理程序可向本中心综合部索取。

16. 附录一 ISO/IEC 27701 认证证书模板

隐私信息管理体系认证证书

（正本）
兹证明

XXXX 有限公司

统一社会信用代码：XXXXXX

注册地址：XXXXXX

已按照

ISO/IEC 27701:2019

标准要求建立并实施了隐私信息管理体系

该管理体系适用于

XXXXXX
（适用性声明版本：X）

涉及的场所及相关活动：

场所地址	场所邮编	场所主要活动
运营地址 1		填该场所涉及的活动
运营地址 2		填该场所涉及的活动

本认证基于以下 ISO/IEC 27001:2013 认证
注册号：XXXXX
ISMS 适用性声明版本：X

本证书的持续效力取决于定期接受监督审核并经审核合格，有关效力请扫描二维码

注 册 号：XXXXXX
颁证日期：YYYY.MM.DD
有效期至：YYYY.MM.DD
换证日期：YYYY.MM.DD

注：本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询。

广州市增城区朱村街朱村大道西 76 号
邮编：511370