文 件 号	CEPREI-64-GM
版 本 号	2

基于 ISO/IEC 29151 的个人信息安全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：2020.03.02

审核：汪修慈　　日期：2020.04.22

批准：赵国祥　　日期：2020.04.22

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 ISO/IEC 29151 个人信息安全安全管理体系认证（以下简称为“ISO 29151 认证”）的全过程，便于本中心有序、有效地开展 ISO 29151 认证工作，保证 ISO 29151 认证的工作质量，满足本中心的要求，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 ISO 29151 认证工作，可为申请方/受审核方/获证组织进行 ISO 29151 认证/注册提供指导。

1.3. 依据文件

下列文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的文件，其最新版本（包括所有的修改单）适用于本文件。

1) GB/T22080《信息技术 安全技术 信息安全管理体系要求》;
2) ISO/IEC 29151 《Information Technology-Security Techniques-Code of Practice for Personally Identifiable Information Protection》;
3) CNAS-CC01《管理体系认证机构认可要求》;
4) CNAS-CC170《信息安全管理体系认证机构要求》;
5) CEPREI-WI-348-DM《基于 ISO 29151 的个人信息安全管理体系认证特殊要求》。
6) CEPREI-WI-352-DM《基于 ISO 29151 的个人信息安全管理体系认证审核人日数要求》。

1.4. 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 29151 认证证书后。

1.5. 职责

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

2. 申请方条件、责任和义务

2.1. 申请方应具备的基本条件

1) 持有法定登记注册证明，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）按相应的 ISO 29151 认证要求，建立文件化的管理体系，并实施运行至少 3 个月。
3) 申请方已按规定实施了信息安全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) 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。

2.2. 申请方/受审核方的权利和义务

2.2.1 申请方/受审核方的权利

1) 自主选择咨询单位。
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。

2.2.2 申请方/受审核方的义务

1) 按本中心要求提交申请文件及其附件；

2) 为本中心提供保证审核工作顺利进行必要的食、宿、行及办公条件；

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赛宝认证中心。

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。

3. 认证的公正性

3.1. 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，无进一步要求，但专业能力应考虑信息安全管理行业的特殊性。

3.2. 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》。ISO 29151 认证结论决定人员的能力要求与 ISMS 体系一致，具体见《QP-48 ISMS 审核专业管理和审核员专业能力评定程序》。

4. 能力管理

4.1. 人员能力要求

ISO 29151 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《ISMS 相关人员能力分析报告》和《ISMS 审核员能力要求》。

相关人员应了解 PII 相关法规及标准。

额外的，审核人员应掌握 ISO 29151 标准。审核方案管理人员应理解 ISO 29151 标准。合同评审人员、专业能力见证评价和专业培训指导人员、审核结论决定人员应了解 ISO 29151 标准。

4.2. 人员的选择与评价

ISO 29151 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。

4.3. 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。

5. 认证程序

认证决定，ISO 29151 认证活动含申请的受理，初次认证的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。

5.1. 申请

(1) 确认申请意向后，申请方需向本中心申请受理部门提交认证申请书，申请受理部门进行合同评审，并与申请方签定《管理体系认证合同》（CEPREI M-02-O）；申请条件需符合以下三种之一：

① 组织已获得本中心发出的信息安全管理体系（ISMS）证书，且 ISMS 范围覆盖 ISO 29151 的范围

② 同时申请 ISMS 认证及 ISO 29151 认证

③ 组织已获得非本中心发出的带认可标识（包括但不限于 CNAS、ANAB）

的 ISMS 证书，并满足：ISMS 范围覆盖 ISO 29151 范围，在 CNCA 网站确认有效。

(2) 在希望正式审核前一个月，申请方按合同金额交纳认证费用。

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。综合部对申请资料进行评审，在确认中心可受理申请且申请方已交纳认证费用后，即把文件移交业务主管部门审核。

5.2. 审核人日

参考文件 CEPREI-WI-352-DM《基于 ISO 29151 的个人信息安全管理体系认证审核人日数要求》。

5.3. 第一阶段审核

第一阶段审核活动包括文件审核，在适用时，可增加现场审核。文件审核要求如下：

(1) 业务主管部门指定审核组进行文件审核。

(2) 审核组进行文件审核，为确定申请方是否作好现场审核的准备收集必要的信息，识别现场审核的重点并与受审核方交换信息及商定现场审核的具体事宜。

(3)文件审核结束后，审核组将文件审核报告提交申请人。

(4) 文件审核结论为准备不够充分时，不能进入二阶段现场审核。

5.4. 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赛宝认证中心评价合格的审核员，必要时可以聘请有关的技术专家协助审核工作。审核组至少有一名具备 ISO17021 要求的具备组长能力的审核员。

业务主管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，由业务主管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个人信息安全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。

5.5. 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，对受审核方的个人信息安全保护进行有效性评价。

在审核期间，受审核方应予以协助、配合，并保证：

a. 审核组能够查阅和个人信息安全保护有关的文件资料和相关记录，包括原始记录；

b. 审核组能够进入与个人信息安全保护审核有关的场所(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. 审核组能够访问与个人信息安全保护有关的人员；

d. 为审核组提供进行个人信息安全保护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，对受审核方个人信息安全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。如某一部门适用个人信息安全保护要求的全面失效现象。

③.所发现不符合事项严重影响个人信息安全保护业绩。

④. 组织业务连续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 29151 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交部门行政人员。

5.6. 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，由业务主管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，由综合部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，有效期为三年。

6. 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”，或直接向本中心客户服务部门查询（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，请通知我中心客户服务部门（电话号码：4008301909）。

7. 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。

8. 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 29151 认证，但应遵守本中心和国家相关法规的相关规定。

9. 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 ISO 29151 认证持续满足认证要求。作为最低要求，在初次认证决定日期起的至少 12 个月内应进行一次监督审核。此后，每个日历年内应进行一次监督审核。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。

10. 证书的更换

获证组织需更改获准认证/注册的 ISO 29151 认证时，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。

11. 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。

赛宝中心关于注销、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、认可委等机构。

12. 特殊审核

12.1. 扩大认证范围

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

12.2. 提前较短时间通知的审核

赛宝认证中心为调查投诉，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，仍可向赛宝认证中心提出。

13. 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综合部重新签订合同，然后按上述程序在证书

有效期之前进行再认证和换证。

14. 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。

15. 收费说明

本中心严格执行国家有关主管部门的收费规定。

附录一 ISO29151 认证证书模板

个人信息安全管理体系

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

按照 ISO/IEC27001:2013 标准和基于 ISO/IEC 29151:2017 标准的个人信息安全管理体系认证特殊要求在以下范围实施了个人信息保护：

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
经营地址 1		该场所涉及的活动
经营地址 2		该场所涉及的活动

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