文 件 号	CEPREI-44-GM
版 本 号	4

基于 ISO 27018 的公有云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：胡友杰 日期：2021-2-19

审核：刘小茵 日期：2021-3-12

批准：赵国祥 日期：2021-3-17

本文件自批准之日起实施

更 改 页

序号	更 改 前	更 改 后	更改日期
1	版本号 3	版本号 4 1） 修改依据文件标准版本号为 ISO/IEC 27018:2019 2）修改了 14 收费说明 3）修改了附录 1 证书模板的内容，增加了英文版本的证书模板	2021-2-19

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 27018 公有云个人可识别信息（PII）安全管理体系认证（以下简称 ISO27018 标准认证）的全过程，便于本中心有序、有效地开展 ISO27018 标准认证工作，保证 ISO27018 标准认证的工作质量，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 ISO27018 标准认证工作，可为申请方/受审核方/获证组织进行 ISO27018 标准认证提供指导。

1.3. 主要依据文件

1) ISO/IEC27001:2013idt GB/T22080-2016《信息技术 安全技术 信息安全管理体系要求》;
2) ISO/IEC 27018:2019 Information technology--Security techniques--Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors；
3) 中心文件《基于 ISO27018 的公有云个人信息安全管理体系认证特殊要求》。

1.4. 认证其它依据文件

1) ISO/IEC 27006：2015 idt CNAS-CC170：2015《信息安全管理体系认证机构要求》。

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 ISO27018 标准认证证书后。

1.6. 职责

技术委员会、各业务部门的职责与 ISO/IEC 27001 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 ISO27018 标准认证项目的审核工作时，应遵循本规则的要求。

2. 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 ISO27018 标准认证要求，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的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。

3. 申请方条件、责任和义务

3.1. 申请方/受审核方的权利

(1) 自主选择咨询单位（本中心不开展咨询服务）。

(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。

4. 认证程序与要求

认证活动含申请的受理，初次认证的初次审核所包含的文件审核和现场审核，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。

4.1. 申请

(1) 确认申请意向后，申请方需向本中心综合部提交认证申请书及其附件，综合部组织评审；

(2) 在希望正式审核前一个月，申请方交纳认证费用。

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。

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。

4.2. 审核人日

若申请方已获得由广州赛宝认证中心服务有限公司颁发的GB/T22080(ISO/IEC27001,IDT)有效认证证书，并且范围覆盖了ISO27018认证申请范围，则ISO27018标准认证部分的审核人日数按照CEPREI-QP-51-IS《信息安全管理体系审核人日数控制程序》中规定的审核时间的0.5倍进行计算（向上取整至0.5人天）。

若申请方已获得由其他认证机构颁发的 GB/T22080(ISO/IEC27001,IDT) 有效认证证书，并且范围覆盖了 ISO27018 认证申请范围，则 ISO27018 标准认证部分的审核人日数按照 CEPREI-QP-51-IS《信息安全管理体系审核人日数控制程序》中规定的审核时间的 0.5 倍+1 人天进行计算（向上取整至 0.5 人天）。

若申请方未获得GB/T22080(ISO/IEC27001,IDT) 有效认证证书，则ISO27018标准认证部分的审核结束时间不得早于GB/T22080(ISO/IEC27001,IDT)审核结束时间。单独开展ISO27018标准认证审核时，人日数按照CEPREI-QP-51-IS《信息安全管理体系审核人日数控制程序》中规定的审核时间的0.5倍进行计算；ISO27018标准认证审核与ISO27001审核共同开展时，人日数按照CEPREI-QP-51-IS《信息安全管理体系审核人日数控制程序》中规定的审核时间的0.4倍进行计算（向上取整至0.5人天）。

4.3. 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。

4.4. 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注册审核员/高级审核员，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 认证要求并经本中心评价满足个人可识别信息（PII）信息安全管理体系组长能力的审核员。

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管理体系特点进行审核策划，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。

4.5. 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. 审核组能够查阅和管理体系有关的文件资料和相关记录，包括原始记录；

b. 审核组能够进入与管理体系审核有关的场所(若受审核方认为某些场所为

本单位的保密场所，应在首次会议上说明，双方协商解决)；

c. 审核组能够访问与管理体系有关的人员；

d. 为审核组提供进行管理体系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（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。对一般不符合采取纠正措施的时间要求一般不超过一个月，严重不符合一般不超过三个月。

不符合通常分为严重不符合和一般不符合。严重不符合指影响管理体系实现预期结果的能力的不符合。严重不符合可能是下列情况：

-对过程控制是否有效或者产品或服务能否满足规定要求存在严重的怀疑；

-多项轻微不符合都与同一要求或问题有关，可能表明存在系统性失效，从而构成一项严重不符合。

对存在严重不符合的情况，将导致受审核方的管理体系不能给予注册或推迟给予注册。

一般不符合指不影响管理体系实现预期结果的能力的不符合。通常来讲，一般不符合对满足管理体系要求或体系文件的要求而言，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。

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。

4.6. 颁发 ISO27018 标准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）或现场验证（严重不符合）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，证书有效期为三年。

证书模板见附录一：ISO27018 标准认证证书模板。

5. 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（认监委）网站（cx.cnca.cn）左侧“认证结果”查询，或直接向本中心综合部查询（查询电话：020-87236606）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。

6. 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。

7. ISO27018 标准认证证书的使用

被批准 ISO27018 标准认证注册后，获证组织可以向公众展示本中心的认证证书，以证实获证组织管理体系通过了管理体系认证，但应遵守本中心和国家相关法规的相关规定。

8. 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。

9. 证书的更换

获证组织需更改获准认证/注册的管理体系时，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。

10. 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，要暂停证书；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，还将上报上级主管部门。

11. 特殊审核

11.1. 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。

11.2. 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。

12. 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向本中心提出申请，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。

13. 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。

14. 收费说明

体系认证费用严格按照本中心收费标准执行。

15. 附录一 ISO27018 标准认证证书模板

中文版：

公有云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：XXXXXXXXX

注册地址：XXXXXXXXX

按照 ISO/IEC27001:2013 标准和基于 ISO/IEC 27018:2019 标准的公有云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：

XXXXXXXX
（适用性声明版本：XX）

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	XXXXXX	运营场所涉及的活动
运营地址 2	XXXXXX	运营场所涉及的活动

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：XXXXXXXXX
颁证日期：YYYY.MM.DD
有效期至：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。

广州市天河区东莞庄路 110 号
广州市 1501-33 信箱（邮编：510610）

英文版：

Public Clouds Personal Information Security Management System Certificate

(Original)
This is to certify that

XXXX CO., LTD.

Unified Social Credit Identifier:XXXXXXXX

Registration Address: XXXXXXXX

Implements PII protection by following **ISO/IEC 27001:2013** and certification special requirements of personal information security in public clouds based on **ISO/IEC 27018:2019** for the following scope:

XXXXXXXX

This is in accordance with the Statement of Applicability, XX

Involved site (s) and relevant activities

Address	Zip Code	Main Activities
Address 1	XXXXXX	XXXXXXXX
Address 2	XXXXXX	XXXXXXXX

Continuing validity of this certificate depends on reception regular surveillance audit and qualified, please scan the QR code to get the related validity.

Registration Number: XXXXXXXX
Issue Date: MM DD, YYYY
Expiry Date: MM DD, YYYY

Note: The information of this certificate may be verified by visiting Official CNCA Website (www.cnca.gov.cn).

P.O. 1501-33 GZ 510610 P.R.C