文 件 号	CEPREI-22-GM
版 本 号	2

C-STAR 云服务安全管理认证程序规则

赛宝认证中心

批　准　页

编制：胡友杰　　日期：2021.10.12

审核：刘小茵　　日期：2021.10.21

批准：赵国祥　　日期：2021.10.25

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 C-STAR 云服务安全管理认证的全过程，便于本中心有序、有效地开展 C-STAR 云服务安全管理认证工作，保证 C-STAR 云服务安全评估的工作质量，满足 CSA（Cloud Security Alliance）的授权要求，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 C-STAR 云服务安全管理认证工作，可为申请方/受审核方/获证组织进行 C-STAR 云服务安全管理认证/注册提供指导。

1.3. 主要依据文件

1) ISO/IEC 27006：2015 idt CNAS-CC170：2017《信息安全管理体系认证机构要求》;
2) Cloud Control Matrix V4.0《云安全控制矩阵》;
3) C-STAR 评估规则有关的规定；
4) ISO/IEC27001:2013idt GB/T22080-2016《信息技术 安全技术 信息安全管理体系要求》
5) GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》
6) GB/T 35273-2020 《信息安全技术 个人信息安全规范》

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：获得公 C-STAR 云服务安全管理认证证书后。

1.5. 职责

管理委员会、技术委员会、各业务部门的职责与 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 C-STAR 项目的评估工作时，应遵循本计划的要求。

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 C-STAR 云服务安全管理认证要求，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，但专业能力应考虑云计算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》。C-STAR 评估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

C-STAR 云服务安全管理认证涉及人员，如合同评审人员、评估方案管理人员、专业能力见证评价和专业培训指导人员、评估结论决定人员、专业评估师等的能力要求见《C-STAR 评估相关人员能力分析报告》和《C-STAR 审核员能力要求》。

4.2. 人员的选择与评价

C-STAR 云服务安全管理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

除依据 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外，中心

1) 每年对 C-STAR 云服务安全管理认证知识实施专题研讨培训，培训参与人员应覆盖 4.1 条所列人员；
2) 中心指定专人负责 C-STAR 云服务安全管理认证信息及知识的收集，该负责人应负责整理相关信息并传递到 4.1 条所涉及人员，并识别培训需求，实施必要培训。

5. 认证程序

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评估，为保持认证所需进行的监督评估，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评估和再认证决定等。

5.1. 认证决定人员管理

作为 C-STAR 云服务安全管理认证决定人员应特别强调如下条件：

1) C-STAR 云服务安全管理认证决定人员已经接受了 C-STAR 的培训，并评价合格；
2) 具有专业的认证决定人员对评估结论决定具有否决权。

5.2. 申请受理及合同评审

综合部依据 CEPREI-QP-06《合同管理程序》及 CEPREI-QP-11《认证申请受理程序》规定的步骤实施申请受理及合同评审，签订 C-STAR 云服务安全管理

认证合同时，还应由 C-STAR 的合同评审人员进行评审。对受评估方的要求如下：

1) C-STAR 云服务安全管理认证适用于所有采用云计算技术和/或提供云计算服务的组织；

2) 应提交《C-STAR 评估申请书》（含调查表）及其附件。

5.3. 评估人日

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 C-STAR 认证申请范围，则 C-STAR 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 C-STAR 认证申请范围，则 C-STAR 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 C-STAR 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 C-STAR 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）。

5.4. 评估策划和准备

5.4.1 评估组

如果 C-STAR 评估与 GB/T22080 认证审核共同开展，组成评估组的原则，除依照 CEPREI-QP-50《ISMS 第二阶段审核程序》中的相关要求进行外，还应满足《QP-48 ISMS 审核专业管理和审核员专业能力评定程序》。对于 C-STAR 评估组要求具备以下知识和能力：

1) 具有对 CCM（cloud control matrix）做出符合和不符合判断的能力；
2) 掌握云计算服务涉及的知识，并在评估的时候能对云计算服务安全措施做出合理的判断。

5.4.2 评估准备

评估组应根据提交的文件资料及受审核方云服务安全管理特点进行审核策划，包括：

1) 评估受评估方的管理文件，并依此确认受评估方对评估的准备程度；
2) 收集关于受评估方的体系范围相关的法律法规要求和遵守情况；
3) 审查现场评估所需资源的配置情况；
4) 结合可能的重要因素充明确现场评估关注点；
5) 拟制评估计划，并将经批准的评估计划提交申请方确认，评估计划应覆盖 C-STAR 的全部要求。

5.5. 现场评估

C-STAR 云服务安全管理评估的工作程序与 ISO27001 的审核相同。现场评估依照 CEPREI-QP-50《ISMS 第二阶段审核程序》执行，并重点关注虚拟化安全、可移植性与互操作性、数据安全等云计算核心领域的安全管理情况，最终形成《C-STAR 云安全评估报告》。

已经获得 ISMS 证书的企业，则评估工作可结合 ISMS 审核报告和 C-STAR 评估内容共同开展。

1) 首次会议

现场评估开始的时候，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评估审核计划、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

评估组根据评估计划，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，记录评估情况，对受审核方的云服务安全管理进行符合性、有效性和成熟度评价。

在评估审核期间，受审核方应予以协助、配合，并保证：

a. 评估组能够查阅和云服务安全管理有关的文件资料和相关记录，包括原始记录；

b. 评估组能够进入与云服务安全管理评估有关的场所(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. 评估组能够访问与云服务安全管理有关的人员；

d. 为评估组提供进行云服务安全管理评估审核所必需的设施和条件，并指定联络人员。

3) 末次会议

现场评估审核结束时，评估组长应主持召开受审核方领导参加的末次会议，对受审核方云服务安全管理的符合性、有效性和成熟度作出评价，宣布现场审核的结论；

a. 受审核方如对评估结论有不同看法，与评估组不能达成一致意见时，应记录在云安全评估报告中；

b. 审核组应就现场评估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。

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。

注：现场审核时应尽量避免 C-STAR 和 ISMS 条款的重复审核，审核条款的重复部分可参考 CCM。

5.5.1 评估记录

C-STAR 评估，具体评估的工作程序与 ISO27001 的审核相同，但是 C-STAR 云服务安全管理评估记录应使用 C-STAR 专用表格。

5.5.2 多场所（现场）和临时场所（现场）的评估

多场所（现场）和临时场所（现场）的评估依照 CEPREI-QP-26《多现场抽样审核控制程序》。评估计划中应明确对云计算服务多场所和临时场所的评估要求。

5.5.3 评估结果的判定

5.5.3.1 不符合项的判断准则

没有满足某个规定的要求称为不符合。判定不符合可遵照如下三条审核准则：

1) Cloud Control Matrix V4《云安全控制矩阵》；
2) C-STAR 评估规则有关的规定；
3) ISO/IEC27001:2013idt GB/T22080-2016《信息技术 安全技术 信息安全管理体系要求》
4) 安全管理手册、程序文件及其它相关管理文件；
5) 适用于组织的信息安全法律、法规及其他要求。

5.5.3.2 不符合类型

不符合项通常分为严重不符合项和一般不符合项。

1) 严重不符合项

a) 体系运行出现系统性失效。如某一要素或关键过程重复出现的失效现象，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。

b) 体系运行出现区域性失效。如某一部门要素的全面失效现象。

c) 造成严重的信息安全事件，或存在潜在严重后果的信息安全风险。

d) 组织信息安全行为违反法律法规或其它要求。

2) 一般不符合项

凡出现下列情况为一般不符合项:

a) 对满足信息安全管理体系要素或体系文件要求而言，是个别的、偶然的、孤立的性质轻微的不合格。

b) 对保证所审区域的体系而言，是个次要的问题。

严重不符合项和一般不符合项的判定对审核结论有决定性问题，对受审核方能否通过信息安全管理体系认证有关键作用，审核员应谨慎判定。

对不符合的判定依据 CEPREI-QP-50《ISMS 第二阶段审核程序》的 3.8 执行。

5.6. 评估的特殊要求

每次审核无论是初次评估、监督检查还是再评估，均应对以下方面给予特别关注：

1) 顾客对云服务安全管理的特殊要求；

2) 顾客对组织关于云服务安全管理过程的投诉及组织对投诉过程的处理；

3) 自我评估和管理评审提出的相关整改措施；

4) 顾客满意的情况。

6. 评估结论决定活动

6.1. 评估结论的批准

评估结论决定活动参照 CEPREI-QP-14《认证决定程序》中 ISMS 认证的相关要求执行。

6.2. 暂停、撤销和注销

本中心对获证组织做出的暂停、撤消和注销活动按照 CEPREI-QP-24《认证的暂停、撤销、注销管理程序》规定执行。

7. 评估证书和标志的管理

评估证书和标志的管理依照 CEPREI-QP-15《认证证书和标志管理程序》。

证书模板见附录一：C-STAR 证书模板

8. 监督和再评估

该过程参照 CEPREI-QP-16《监督审核、特殊审核和再认证程序》执行。

9. 评估要求变更管理

该过程参照 CEPREI-QP-23《认证变更的管理程序》执行。

10. 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。

11. 收费说明

体系认证费用严格按照本中心收费标准执行。

附录一：C-STAR 证书模板

C-STAR (Security, Trust & Assurance Registry) Certificate

(Cloud Control Matrix V4.0)

(Original)
This is to certify that

CSA C-STAR

XXXX CO., LTD.

Unified Social Credit Identifier: XXXXXXXXXXXX

Registration Address: XXXXXXXX, XXXX CITY, XXXX PROVINCE, CHINA

Has implemented and maintains a Cloud Security Management System in compliance with

C-STAR Assessment requirements

The Cloud Security Management System is applicable to:

Address	Zip Code	Main Activities
Site 1	XXXXXX	XXXXXXXXX
Site 2	XXXXXX	XXXXXXXXX

Registration Number：XXXXXX
Issue Date：MM DD, YYYY
Expiry Date：MM DD, YYYY
Re-Issue Date：MM DD, YYYY

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

No. 76 West of Zhucun Avenue, Zhucun,
Zengcheng District, Guangzhou, 511370 P.R.C

Zhao Guoxiang
General Manager
CEPREI CERTIFICATION BODY

云计算安全评估证书

（云控制矩阵 v4）

（正本）
兹证明

CSA C-STAR

XXXX 有限公司

社会统一信用代码： XXXXXXXXXXXXX

注册地址：XX 省 XX 市 XXXXXXXX

已建立并实施了符合 C-STAR 要求的云计算信息安全管理体系。
该管理体系适用于

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

注 册 号：XXXXXXX
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管管理委员会官方网站（www.cnca.gov.cn）上查询。

广州市增城区永和镇永和北路百 76 号
邮编：511370

总经理：