文件号	CEPREI-23-GM
版本号	2.0

CSA

云计算产品信息安全认证实施规则

广州赛宝认证中心服务有限公司

目　　录

1 适用范围

本规则适用于所有云计算产品，包括 IaaS/PaaS/SaaS 产品及解决方案，包括以软件版本方式交付的产品和以互联网方式交付的产品。以软件版本方式交付的产品是指云计算开发商向其客户交付一个具体的软件版本，传统的软件产品交付模式大多是这种方式。以互联网方式交付的产品是指在互联网上部署，快速迭代的方式开发和发布，没有明确的版本号，或既使有版本号，版本号也是更新频繁。

2 认证模式

CSA 云计算产品信息安全认证(以下简称 CSTC 认证)的认证模式为：资料审核+产品检测+现场检查（如适用）+获证后监督。

认证的基本环节包括：

a) 认证的申请及受理

b) 产品检测

c) 现场检查（如适用）

d) 认证结果评价与批准

e) 获证后的监督。

3 认证申请

3.1 认证单元划分

按云主机、云存储、云分发、云数据库、负载均衡、在线应用等云计算产品的云能力进行划分，每个云能力为一个认证单元。当申请方云计算产品对应多个云能力时可按一个认证单元进行申请。

3.2 申请认证提交资料

3.2.1 申请资料

应提交《CSA 云计算产品信息安全认证申请书》及其附件。

3.2.2 证明资料

a) 申请人、厂商的注册证明如营业执照、组织机构代码（首次申请时）；

b) 申请人为销售者、进口商时，还须提交销售者和生产者、进口商和生产者订立的相关合同副本；

c) 代理人的授权委托书（如有）；

d) 有效的监督检查报告或现场检查报告（如有）。

3.2.3 提供与产品有关的资料

a) 产品说明书和或使用手册；

b) 产品研制主要技术人员情况表（如适用）；

c) 产品测试技术人员情况表（如适用）；

d) 其他需要的文件（如适用）。

3.2.4 安全保障要求方面的文档（如适用）

4 产品检测

4.1 依据标准

GB/T 18336《信息技术 安全技术 信息技术安全评估准则》；

ISO/IEC 17025《检测与校准实验室能力的通用要求》；

CSA 0001-2016《CSA 云计算安全技术要求》。

4.2 检测项目、检测方法及要求

试验项目为 GB/T 18336 和 CSA 0001-2016 中规定的全部适用项目。

检测可由检测机构利用自身的检测设备和检测人员完成，也可由检测机构充分评估考量受审核方既有资源后，全部或部分利用受审核方检测设备/资源的方式完成。

4.3 检测时限

原则上，产品送检后 20 个工作日内完成产品检测并出具检测报告。

4.4 检测报告

由赛宝指定的检测机构对样品进行试验，并按规定格式出具检测报告。认证批准后，检测机构负责给申请人寄送一份检测报告。

5 现场检查

申请方在申请认证时如已取得 ISO27001、C-STAR、等级保护等信息安全认证（其证书范围涵盖 CSTC 认证范围）则可申请并经乙方同意后豁免现场检查。

5.1 检查内容

检查内容为信息安全保证能力、质量保证能力和产品一致性检查。

5.1.1 信息安全保障能力检查

对受审核方参考附件 1《信息安全保证能力评估项目》进行信息安全保证能力检查。

5.1.2 质量保证能力检查

对受审核方参考附件 2《质量保证能力基本要求》进行质量保证能力检查。

5.1.3 产品一致性检查

对产品进行一致性检查，重点核实以下内容：

1）认证产品的包装上所标明的及运行时所显示的产品名称、型号/版本与产品检测报告上所标明的内容是否一致；

2）认证产品所用的软件（含开源软件）与产品检测报告所列明的是否一致；

3）非认证的产品是否违规使用了认证标识。

5.2 检查时间

一般情况下，产品检测合格后，再进行现场检查。特殊情况时，产品检测和现场检查也可以同时进行。原则上，现场检查应在一年内完成，否则应重新进行产品检测。

现场检查时间主要根据所申请认证产品的单元数量确定，至少为 2 个人日。

5.3 检查结论

检查组负责报告检查结论。检查结论为不通过的，检查组直接向赛宝报告。检查存在不符合项时，受审核方应在 3 个月内完成整改，赛宝采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过的，按现场检查不通过处理。

6 认证结果评价与批准

6.1 认证结果评价与批准

赛宝对产品检测结论、现场检查结论进行综合评价。评价合格后，按认证单元向申请人颁发认证证书。

6.2 认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的工作日，一般在 90 个工作日内，最长不超过 150 个工作日。整改时间不计算在内。

6.3 认证终止

当产品检测不合格、现场检查不通过或整改不通过，赛宝做出不合格决定，终止认证。终止认证后如需继续申请认证，则重新申请认证。

7 获证后的监督

7.1 获证后的监督的时间及内容

7.1.1 监督检测频次

获证后由赛宝对云产品进行周期性持续监督。其中以互联网方式交付的产品的监督周期为 3 个月；以软件版本方式交付的产品监督周期为 12 个月。以互联网方式交付的认证产品的证书持有者可根据认证产品的实际情况（如产品没有变更或只有细微变更）申请并经乙方同意后豁免监督，连续豁免监督的次数最多不能超过 2 次。

如果发生下述情况之一可增加监督频次：

1）获证产品出现严重质量问题时,或者用户提出投诉并经查实为证书持有者责任时；

2）认证机构有足够理由对获证产品与规定的标准要求的符合性提出质疑时；

3）有足够信息表明受审核方因组织机构、信息安全管理体系等发生变更，从而可能影响产品信息安全时；

4）以互联网方式交付的获证产品发生重大变更时。

7.1.2 监督检测的内容

获证后监督主要采用产品检测的方式进行。初次认证申请时的检测项目都可以作为监督时的检测项目，检测机构可根据具体情况进行部分或全部项目的检测，一般在 10 个工作日内完成。

必要时可以对获证组织针对信息安全保证能力、认证产品一致性和质量保证能力进行现场监督检查。

7.1.3 监督检测结论

检测机构负责报告监督检测结论。监督检测结论为不通过的，检测机构直接向赛宝报告。监督检测存在不符合项时，受审核方应在 3 个月内完成整

改，检测机构采取适当方式对整改结果进行验证。未能按期完成整改的或整改不通过，按监督检测不通过处理。

7.2 监督结果评价

赛宝组织对监督检测结论、现场监督检查结果进行综合评价，评价合格的，认证证书持续有效。当监督检测不通过或监督检查不合格时，则判定年度监督不合格，按照 8.3 规定处理相关认证证书。

8 认证证书

8.1 认证证书的保持

8.1.1 证书的有效性

本规则覆盖产品的认证证书有效性通过定期的监督维持。

8.1.2 认证产品的变更

8.1.2.1 变更的申请

获证后的产品，如果其获证组织、证书持有者等发生变化时，应向认证机构提出变更申请。

8.1.2.1 变更评价和批准

赛宝根据变更的内容和申请人提供的资料进行评价，必要时送样进行检测。检测合格或经资料验证后，对符合要求的，批准变更。证书内容发生变化的，换发证书，证书的编号、批准有效日期不变。

8.2 获证单元覆盖产品的扩展

证书持有者需要增加与已获证产品为同一认证单元的安全认证时，应提交扩展申请。赛宝核查扩展产品与获证产品的一致性，确认认证结果对扩展产品的有效性，针对扩展产品的差异进行补充检验，必要时安排产品检测。评价合格后，根据需要颁发新证书或换发证书。

8.3 认证证书的暂停、恢复、注销和撤销

证书的使用应符合赛宝有关证书管理规定的要求。当证书持有者违反认证有关规定或认证产品达不到认证要求时，赛宝按有关规定对认证证书做出相应的暂停、注销和撤消的处理，并将处理结果进行公告。证书持有者可以向赛宝申请暂停、注销其持有的认证证书。

证书暂停期间，证书持有者如果需要恢复认证证书，应在规定的暂停期限内向赛宝提出恢复申请，赛宝按有关规定进行恢复处理。否则，赛宝将注销或撤销被暂停的认证证书。

9 认证标志的使用

持证人可以按赛宝 QP-15《证书和标志管理程序》申请备案或购买认证标志。使用标志应符合赛宝 QP-15《证书和标志管理程序》。

9.1 准许使用的标志样式

获证产品允许使用如下认证标志：

不允许使用变形标志、不允许加以文字说明。

9.2 认证标志的加施

证书持有者可以向赛宝购买标准规格的标志，或者申请并按赛宝规定加施认证标志。

10 收费

认证费用按赛宝有关规定收取。

附件 1 信息安全保证能力评估项目（参考）

1. 配置管理能力

- 受审核方应为产品提供一个参照号。
- 受审核方应使用一个配置管理系统。
- 受审核方应提供配置管理文档。
- 产品参照号对产品的每一个版本应是唯一的。
- 应该给产品标记上参照号。
- 配置管理文档应包括一个配置清单。
- 配置清单应唯一标识组成产品的所有配置项。
- 配置清单应描述组成产品的配置项。
- 配置管理文档应描述用于唯一标识产品所包含配置项的方法。
- 配置管理系统应唯一标识产品所包含的所有配置项。

2. 交付与运行

2.1 交付

- 受审核方应将把产品或其部分交付给用户的程序文档化。
- 受审核方应使用交付程序。
- 交付文档应描述，在向用户方分发产品版本时，用以维护其安全性所必需的所有程序。

2.2 安装、生成和启动

- 受审核方应将产品安全地安装、生成和启动必需的程序文档化。
- 安装、生成和启动文档应描述产品安全地安装、生成和启动必需的所有步骤。

3. 开发

3.1 功能规范

- 受审核方应提供一个功能规范。

- 功能规范应使用非形式化风格来描述产品安全功能及其外部接口。
- 功能规范应是内在一致的。
- 功能规范应描述所有外部安全功能接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节。
- 功能规范应完备地表示产品安全功能。

3.2 高层设计

- 受审核方应提供产品安全功能的高层设计。
- 高层设计的表示应是非形式化的。
- 高层设计应是内在一致的。
- 高层设计应按子系统描述安全功能的结构。
- 高层设计应描述每个安全功能子系统所提供的安全功能性。
- 高层设计应标识安全功能所要求的任何基础性硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。
- 高层设计应标识安全功能子系统的所有接口。
- 高层设计应标识安全功能子系统的哪些接口是外部可见的。

3.3 表示对应性

- 受审核方应提供一个所提供安全功能表示的所有相邻对之间对应性的分析。
- 对于所提供安全功能表示的每个相邻对，分析应证实，较为抽象的安全功能表示的所有相关安全功能都在较不抽象的安全功能表示中得到正确且完备地细化。

4. 指导性文档

4.1 管理员指南

- 受审核方应提供针对系统管理员的管理员指南。
- 管理员指南应描述产品管理员可使用的管理功能和接口。
- 管理员指南应描述如何以安全的方式管理产品。
- 管理员指南应包含一些关于安全处理环境中应被控制的功能和特权的警示信息。
- 管理员指南应描述所有关于与产品安全运行有关用户行为的假设。
- 管理员指南应描述所有受管理员控制的安全参数，适当时应指明安全值。
- 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性。

- 管理员指南应与供评估的所有其他文档保持一致。
- 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

4.2 用户指南

- 受审核方应提供用户指南。
- 用户指南应描述产品的非管理员用户可使用的功能和接口。
- 用户指南应描述产品所提供的用户可访问安全功能的使用。
- 用户指南应包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息。
- 用户指南应清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责。
- 用户指南应与供评估的所有其它文档保持一致。
- 用户指南应描述所有与用户有关的 IT 环境安全要求。

5. 测试

5.1 覆盖范围

- 受审核方应提供测试覆盖的证据。
- 测试覆盖的证据应说明测试文档中所标识的测试与功能规范中所描述的安全功能之间的对应性。

5.2 功能测试

- 受审核方应测试安全功能，并文档化检测报告。
- 受审核方应提供测试文档。
- 测试文档应包括测试计划、测试程序描述、预期的检测报告和实际的检测报告。
- 测试计划应标识要测试的安全功能和描述要执行的测试的目标。
- 测试程序描述应标识要执行的测试和描述每个安全功能的测试脚本。这些脚本应包括对于其它检测报告的任何顺序依赖性。
- 预期的检测报告应指出测试成功执行后的预期输出。
- 受审核方执行测试所得到的检测报告应证实每个被测试的安全性功能都按照规定运转。

5.3 独立性测试

- 受审核方应提供用于测试的产品。

- 产品应适合测试。

6. 脆弱性评定

6.1 安全功能强度

- 受审核方应对安全目标中所标识的每个具有产品安全功能强度声明的安全机制进行产品安全功能强度分析。
- 对于每个具有产品安全功能强度声明的安全机制，产品安全功能强度分析应说明该机制达到或超过安全目标中定义的最低强度级别。
- 对于每个具有特定产品安全功能强度声明的安全机制，产品安全功能强度分析应说明该机制达到或超过安全目标中定义的特定功能强度度量。

6.2 脆弱性分析

- 受审核方应执行脆弱性分析。
- 受审核方应提供脆弱性分析文档。
- 脆弱性分析文档应描述为搜索用户能违反安全策略的明显方法而执行的产品可交付材料分析。
- 脆弱性分析文档应描述对明显的脆弱性的处置。
- 脆弱性分析文档应针对所有已标识的脆弱性，说明脆弱性不能在产品的预期使用环境中被利用。

附件 2 质量保证能力基本要求（参考）

为保证批量交付的认证产品与测试样品的一致性，受审核方应满足本文件规定的质量保证能力基本要求。

1. 职责和资源

1.1 职责

受审核方应规定与质量活动有关的各类人员职责及相互关系，且受审核方应在组织内指定一名质量负责人，无论该成员在其他方面的职责如何，应具有以下方面的职责和权限：

a）负责建立满足本文件要求的质量体系，并确保其实施和保持；

b）确保加贴认证标志的产品符合认证标准的要求；

c）建立文件化的程序，确保认证标志的妥善保管和使用；

d）建立文件化的程序，确保获证产品变更后未经认证机构确认，不加贴认证标志。

质量负责人应具有充分的能力胜任本职工作。

1.2 资源

受审核方应配备必须的检测设备以满足稳定生产符合本规则中规定的标准要求的产品；应配备相应的人力资源，确保从事对产品质量有影响工作的人员具备必要的能力；建立并保持适宜产品检测的必备的环境。

2. 认证产品一致性

a）受审核方应对现场的产品与测试样品的一致性进行控制，以使认证产品持续符合规定的要求；

b）受审核方应建立产品变更控制程序，认证产品的变更在实施前应向认证机构申报并获得批准后方可执行。

3. 认证产品外包软件模块管理

3.1　软件模块的外包商的控制

a）受审核方应制定软件模块外包商的选择、评定和日常管理的程序，以确保软件外包商提供的软件模块满足要求；

b）受审核方应保存对软件外包商的选择评价和日常管理记录。

3.2 外包软件模块的验证

a）受审核方应建立并保持对软件外包商提供的软件模块的验证程序及定期确认程序，以确保软件模块满足认证所规定的要求；

b）受审核方应保存外包软件模块的验证记录、确认记录及软件外包商提供的合格证明及有关数据等。