文 件 号	CEPREI-94-GM
版 本 号	1

数据安全能力成熟度评估程序规则

广州赛宝认证中心服务有限公司

批　准　页

编制：鲁　立　　日期：2020-12-23

审核：刘小茵　　日期：2020-12-23

批准：赵国祥　　日期：2020-12-24

本文件自批准之日起实施

目　录

1、目的

为规范广州赛宝认证中心服务有限公司（以下简称本中心）数据安全能力成熟度评估(以下简称能力评估)工作，符合国家认证认可监督管理委员会规定的要求，保障能力评估工作的质量及符合性，特制定本规则。

2、适用范围

本制度适用于本中心数据安全能力成熟度评估活动。

3、职责

3.1 市场拓展部负责能力评估市场开发、合同签订、并进行《评估合同》商务条款的评审；

3.2 综合部负责能力评估申请受理工作，组织合同评审，对申请文件的齐套性进行检查，文件不齐套时，通知受评估方重新提交或补充。评估结束后依据评估组的评估结论制作和发放证书、管理纸质档案归档；

3.3 业务部门进行《评估合同》技术条款的评审，协调能力评估任务安排工作；

3.4 技术委员会负责评估材料评审、做出评估决定。

3.5 合规审计部负责对能力评估过程的合规性进行质量抽查。

3.6 评估师职责：

a) 遵守相应的评估要求；

b) 传达和阐明评估要求；

c) 独立完成分工范围内的评估任务、收集证据，进行评估组内部交流，对分工范围内受评估方数据安全能力的真实性、符合性和有效性等方面做出评价；

d) 将评估情况形成文件；

e) 向评估组长报告评估结果；

f) 收存和保护与评估有关的文件，按要求提交这些文件；确保这些文件的机密性；谨慎处理特殊的信息；

g) 配合并支持评估组长的工作；

h) 必要时，负责文件审核；

i） 对于超出评估范围之外的引起关注的问题，应当指出并向评估组长报告，适宜时，向业务部门和受评估方通报。

3.7 评估组长除具有评估师的职责外，还应有以下职责：

a） 全权负责各阶段的工作；

b） 编制评估计划；

c） 代表评估组同受评估方的评估发起人沟通；

d） 有权对评估工作的开展作最后决定；

e） 提交评估报告。

4、能力管理

4.1 数据安全能力成熟度评估师能力要求

应具备以下知识：

a) 熟悉适用的法律、法规和评估程序；

b) 透彻了解《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》以及评估方法；

c) 具备有效的书面和口头交流和表达能力；

d) 网络安全相关工作年限≥2 年；

e) 计算机、信息技术或网络安全相关专业毕业；

f) 从事过数据开发、数据库管理员、数据产品、数据安全、技术安全中任一工作等至少 1 年，或安全相关的开发、测试、运维、项目管理、质量管理、风险控制、审计中任一工作至少 2 年；

g) 了解 CMM/CMMI 或 ISO27001 或 ITSS 标准，熟悉相关安全评估方法和过程；

h) 具有较丰富的项目管理经验, 熟悉测评项目的工作流程和质量管理的方法,具有较强的组织协调和沟通能力，能提供证明材料者优先。

合同评审人员、方案管理人员、技术委员会人员的能力要求见《数据安全能力成熟度评估师能力评定程序》。

4.2 技术委员会人员能力要求

复核评估报告和做出认证决定的人员应：

a)理解评估原则、程序和技术的应用；

b）理解受审核方数据安全能力与评估准则的关系；

c）理解如何确定组织的数据能力成熟度范围；

d）理解评估中运用抽样技术的适宜性和后果；

e）具备数据安全能力成熟度评估师所需知识和技能，见 4.1

4.3 合同评审人员、方案管理人员

该类职能属于实施申请评审以确定所需的审核组能力、选择审核组成并确定审核时间的职能人员。该职能人员需具备以下常规知识和技能：

a) 数据安全能力成熟度标准和（或）规范性文件的知识：应具有认证过程中使用的 DSMM 标准和其他规范性文件的相关知识，包括 DSMM 相关术语和定义、受审核方所处的环境知识和隐私信息管理过程中的关系。

b) 中心 DSMM 业务过程的知识：需足以指派有能力的评估组成员以及准确地确定评估时间。

c) 数据安全领域的知识：数据安全领域的通用术语、实践和过程的知识。

4.4 人员的选择与评价

业务部门依本中心文件 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。

4.5 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。

发

5、工作流程

评估准则：《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》

5.1 受理申请

本中心受理的能力评估申请，应确定受评估方符合下列条件：

a)中华人民共和国境内注册的独立法人单位；

b)生产经营活动中没有重大违法、违规及不良信用记录；

c)能够提供数据安全能力的真实性、适宜性和有效性证据；

d)承诺并遵守行业公约。

受评估方应提供以下材料：

《申请表》和申请表附件材料；

5.2 受理确认与合同评审

检查申请企业提供相关材料的完整性，按合同评审要求，在业务系统中进行合同评审，合同评审流程结束后，业务系统向申请企业发送受理通知，与通过申请评估的申请企业签订正式能力评估合同书。

市场拓展部各业务经理负责与顾客的信息交流。综合部负责组织合同评审。针对能力评估合同，合同评审内容包括：

a）合同书中阐述各项要求是否明确与合理；

b）申请企业要求评估的级别是否在可评估范围内；

c）申请企业申请表、申请表附表填写信息是否完整；

d）申请企业是否为中华人民共和国境内注册的独立法人单位；

e）申请企业近三年内是否存在不良信用记录（需在国家企业信用信息公示系统核实（http://gsxt.saic.gov.cn/）等。

评审通过的合同由市场拓展部负责签订。

5.3 评估策划

5.3.1 分析需求

评估组与评估发起人（或评估发起人的委托人）进行沟通，双方确定本次评估的目标、评估的限制条件、评估范围和评估输出，并获得对评估输出的承诺。

评估组与评估发起人（或评估发起人的委托人）共同填写《评估输入》，双方相互沟通，对《评估输入》中所有内容达成一致。

评估组长和评估发起人在达成一致的《评估输入》签字确认。确认后《评估输入》置于变更控制之下，对评估输入的变更要得到评估发起人的批准。

5.3.2 拟定评估计划

评估组和评估发起人就有关评估的需求、协定、估计值、风险、评估方法剪裁、进度和后勤保障等达成一致意见，并填写《评估计划》。

评估组应事先应告知被评估组织评估活动的安排，并向参与评估活动的人员介绍评估过程、目的和计划等。

评估计划可以是包括所有评估活动的计划，或是针对某项特定活动的系列计划（例如:现场评估计划、风险管理计划、客观证据收集计划等）。

5.3.3 选择和准备评估组

5.3.3.1 选择评估组

业务部门应指派具有适当资格的人员去执行评估任务。在“顾客选择评估”模式下，如果某些人或其所在机构已经以某种方式在一定时期内参与了被评估组织的活动，可能与公正性有冲突时，则不应委派这些人员参与此项评估活动。

业务部门应任命符合要求的评估组及评估组长，代表中心对从申请人收集到的资料进行评价和实施评估。

业务部门在选定评估组成员后，应提前将评估组成员的信息通知被评估方，使其有足够的时间提出对所指派评估师是否有异议。

业务部门通过《评估任务书》正式任命评估组，评估组各成员在《评估师公正性声明》中签字，承诺在评估活动中遵守评估机构制定的包括保密要求在内的各项规则。给评估组的指令应清楚明确并通知申请人，同时应要求评估组核实申请人的结构、方针和程序并确认能满足有关评估范围的所有要求。

5.3.3.2 准备评估组

评估组长负责确保评估成员在按计划执行评估活动之前得到充分的准备。包括熟悉《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》、评估方法，评估计划、被评估组织的有关情况以及评估期间使用的评估工具和技术。中心应向有关人员提供适用的工作文件，包括标准、评估指南、评估检查表等，

为确保评估工作顺利开展，评估组长应负责评估前的准备工作。包括对评估角色的指定、评估任务的分配等。评估组的成员必须接受过《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》的培训。

5.4 评估人日计算

参考文件《DSMM 评估人日控制程序》。

5.5 详细评估流程

a）确定模型适用范围：分析需要保护的数据资产及业务范围，确定模型使用和评估范围；

b）确定能力成熟度级别目标：分析组织机构数据安全风险，确定能力成熟度等级建设目标；

c）选取安全 PA：针对组织机构的数据相关的业务现况，选取适当的数据安全 PA。例如，对于有的组织机构而言，不存在数据对外共享的处理，则无需选择共享安全的 PA。

d）评估 BP 执行情况：依据标准对各等级数据安全 BP 要求，确定 4 个关键能力落地情况。

e）PA 安全评估：基于选择的安全 PA 范畴，针对各项安全 PA 对组织机构的数据安全实践情况进行现状的调研和分析。按《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》附录 A 各级别的 GP 描述确定该 PA 的等级。

f）确定组织机构整体等级：结合所有 PA 的等级，确定组织机构整体的数据安全能力成熟度等级，适用时对数据安全能力持续建设和改进提出建议。

5.6 具体评估工作

5.6.1 文件评审

评估组收到评估任务后，文件评审由组长或由经组长授权的评估组成员负责实施，评审的内容至少包括：

a) 申请表是否完整；

b) 申请表能否表明申请企业达到所申请的能力等级。

文件评审时，必须填写《文件评审报告》，报告中必须明确文件评审结论。

由文件评审人员将《文件评审报告》发送企业,并将文件评审结论及时通知申请企业，文件评审结论：

a) 符合要求，可进入现场评估。

b) 基本符合要求，请申请企业在规定日期之前完成申请材料修订并反馈，经再次确认后，可进入现场评估。

c) 文件发现资料存在较多问题，无法给出文审结论时，需及时反馈给申请企业，待其进行修改后，重新提交相关资料进行文件评审。

d） 不符合所申请能力评估级别要求。通知申请企业，退回其能力评估申请，并结束本次评估任务。

每一次文件评审都应形成《文件评审报告》。

5.6.2 评估准备

编制现场评估计划

评估组长负责编制现场评估计划，评估组长应根据申请企业提供的材料，及时与申请企业联系，充分了解申请企业的组织结构、职能分配、主要经营和技术研发场所等信息，保证计划的适宜性和可操作性。

评估计划至少应包括以下信息：

a) 申请企业名称；

b) 评估地点；

c) 评估目的；

d) 评估准则；

e) 评估组成员及职务；

f) 评估日期及日程安排；

g) 申请企业需提供的支持；

h) 保密及公正性承诺；

评估计划的要求：

a)评估计划应由项目管理人员批准（项目管理人员包括中心总经理/技术负责人、业务部门主任，须在业务系统中进行审批），确保评估计划安排合理，并应提前得到申请企业确认。

b)评估计划应覆盖本次评估所涉及的该能力级别，评估计划应注意其协调性，并考虑评估人员的专业能力问题。实习评估师不能单独进行评估，需与评估师一组评估，不计算评估人日。

c)评估工作人日根据相关要求另行规定。具体现场评估人日数，评估组长按照评估任务书要求执行。

d)原则上，评估计划应至少提前 24 小时发送给申请企业确认。如被评估方对评估人员和日程安排等有异议，应立即反馈给评估组长，并确保在现场评估开始前，双方协商解决。

e)如果评估计划的某些细节过早公开将影响客观证据的收集，这些细节可在评估过程中陆续通知给申请企业。

5.6.3 现场评估

现场评估必须在申请企业的主要经营和技术研发所在地进行。

5.6.3.1 首次会议

评估组按计划召开首次会议，与会人员签到，首次会议至少要包括以下内容：

a) 介绍评估组成员（包括评估师、实习评估师）及其职责；

b) 了解申报单位参加会议的人员；

c) 阐明评估的目的、类型和准则；

d) 确认评估日程安排；

e) 介绍评估方法和程序；

f) 说明评估结果的提交方法；

g) 列举可能存在的评估结论；

h) 确认评估组陪同人员、所需的资源和设施，以及评估组工作时的限制区域等情况；

i) 陈述公正性声明和保密承诺；

j) 申报企业负责人发言。

5.6.3.2 现场评估实施

a)对 4 个关键能力的评估方法如下

组织建设：评估是否具有开展工作的专职/兼职岗位，团队或技术人员，其工作职责是否通过规范要求或其它手段得到确认和保障。

制度流程：检查是否有关键数据安全领域的制度规范和流程及其在组织机构内的落地执行情况；

技术工具：检查组织机构内的各项安全技术手段，通过产品工具固化安全要求或自动化的安全作业的实施运作情况；

人员能力：执行数据安全工作的人员是否经过专业的技能和安全意识教育。

b)现场评估如遇情况变化，由评估组长视具体情况按评估机构的要求进行协调处理、改变计划，并将变化情况给予记录。对于涉及重大变更，评估组长需通知机构负责人后作出决定。

c)在现场评估期间，可以包括但不限于以下几种手段：

1) 人员访谈：通过访谈的方式与被评估方进行交流、讨论等活动，获取相关证据，了解有关信息；

2) 文档审核：由被评估方输入与数据安全相关的文档材料（如数据安全的方针政策、制度规范流程、培训教育材料、以及与产品技术相关的设计实施方案、配置说明、运行记录和其他配套表单）、评估小组审核相关的文档材料是否已涵盖完整数据生存周期的 PA 和控制项；

3) 配置检查：根据被评估方提供的技术材料，登陆相关的系统工具平台，检查配置是否与材料保持一致，对文档审核内容进行核实；

4) 工具测试：利用技术工具对系统工具进行测试，验证是否符合数据安全成熟度模型特定等级的技术能力要求，也可采信第三方的测试报告。

5）旁站式验证：评估人员在现场通过实地观察人员行为、技术设施和环境状况判断人员的安全意识、业务操作、管理程序等方面的安全情况。

d)评估组根据日程安排，对申请企业进行评估时，要求陪同人员始终在现场，以利于评估工作的顺利实施。

e)对于评估组不能确认的证据可采取再检查核对的方式给予确认。

f)现场评估要对文件评审中提出的问题进行验证，并做出相关记录。

g)由于申请企业的原因，使评估的目的不可能实现时，或发现有重大要素不符合申请要求时，评估组长应先向业务部门主任报告评估发现的问题，再与申请企业管理层沟通,做出终止评估的决定，并向申请企业讲明终止的理由。

5.6.3.3 末次会议

由评估组长按日程安排主持有申请企业管理层参加的末次会议，与会人员签到，末次会议应至少包括以下内容：

a） 提出问题报告，阐述问题要点与风险点；

b） 如有抽样，须说明抽样的局限性；

c） 提出最终材料经技术委员会评审后，做出评估结论的可能性包括：

1）评估机构同意对申请企业所申请的能力级别；

2）补充提供充分证据，并经评估组再次验证符合要求后，再次提交技术委员会评审；

3）评估机构不同意对申请企业所申请的能力级别，或授予较低的能力级别。

d） 告知申报后续事项和发证的流程；

e） 告知如获得证书后，到期换证、变更及年度自查/监督评估的要求；

f） 告知投诉、申诉程序；

g） 申请企业负责人发言。

5.6.4 后续活动

5.6.4.1 评估报告

评估组组长向中心提交书面评估报告；必要时评估机构向委托方提交经过审查和批准的最终评估报告；

现场评估完成后，评估组组长向业务部门提交评估资料，包括：

a） 被评估组织文件（可包含程序文件目录、组织概况、程序文件及其相关背景材料）；

b）申请书；

c）评估输入及评估计划；

d）评估报告；

e）过程方面检查表；

由业务部门组织技术委员会对所有资料进行评审，确定最终评估结论。

必要时，评估机构向委托方提交经审查和批准的最终评估报告。

5.6.4.2 保密处置

在现场评估中，涉及到保密要求的项目或活动，为了获得必要的证据，也应对保密要求的项目或活动进行评估。但在评估过程中，应：

a）由有保密资格的人员实施；

b）必要时，可与申请企业签订相应的保密承诺书；

c）在申请企业规定的场所内查看涉及到保密要求工作内容的原件；

d）记录应进行脱密处理。

申请企业提交的申报材料不能涉及国家秘密，涉密单位应签署《申报材料不涉及国家秘密的承诺函》。

5.7 维持评估

评估证书的有效期为三年，企业希望持续维持能力证书的有效性可申请开展维持评估，维持评估的间隔不能超过 36 个月，评估时间为初次评估的 80%，连续三次维持评估后，必须进行全面评估才可维持能力证书。

5.8 归档管理

能力评估工作结束后，由评估组整理并提交如下申请企业相关材料：

a）数据安全能力成熟度评估申请表及附件；

b）能力评估文件评审报告；

c）能力评估计划；

d）能力评估首（末）次会议签到表；

e）组织确认表；

f）评估报告；

g）评估师公正性声明；

h）申报材料不涉及国家秘密的承诺函；

i）其他。

业务部门对评估组提交的申请企业电子版和纸质材料齐套性进行检查，留存的申请企业纸质材料提交综合部进行归档管理，保存期限为3年。申请企业上报的材料中有涉及国家秘密的，脱密后的归档材料单独管理。

6、相关文件

《记录的管理程序》

7、相关记录

a）数据安全能力成熟度评估申请表及附件；

b）能力评估文件评审报告；

c）能力评估计划；

d）能力评估首（末）次会议签到表；

e）组织确认表；

f）评估报告；

g）评估师公正性声明；

h）申报材料不涉及国家秘密的承诺函；

i）其他。