CCAI–R–P30:2023

首席数据官 人员能力验证规则

Chief Data Officer: Rules for Personal Proficiency Testing

国家市场监督管理总局认证认可技术研究中心

2023年12月19日发布 2023年12月19日实施

目 录

前 言

首席数据官人员能力验证（Chief Data Officer Personal Proficiency Testing）是指对熟悉国内、国际数据安全合规政策，具备数据安全体系搭建能力，熟练掌握数据安全管理流程及数据安全技术保护措施的专业技术人员进行能力验证。

为提高数据安全领域从业人员的理论知识与实际工作水平，国家市场监督管理总局认证认可技术研究中心(以下简称“认研中心”、英文简称“CCAI”)决定开展首席数据官人员能力验证工作。为规范认研中心人员能力验证工作，依据《国家市场监督管理总局认证认可技术研究中心合格评定技术体系文件管理办法（试行）》《国家市场监督管理总局认证认可技术研究中心人员能力验证管理办法》等文件，组织制定《首席数据官 人员能力验证规则》。

1.本规则是认研中心开展首席数据官人员能力验证的基本依据，内容包括概况、基本要求、验证要求、验证规则、考核内容比重。

2.本规则以现阶段数据安全领域从业人员所需理论知识与实践水平为目标，在充分考虑经济发展、规范企业行为和提高企业竞争力的基础上，对数据安全领域从业人员的工作范围、岗位职责和知识水平做了明确规定。

3.本规则参考了《合格评定 能力验证的通用要求》(ISO/IEC 17043)、《利用实验室间比对进行能力验证的统计方法》（ISO 13528）中的全部或部分条款，既保证了规则体系的规范化，又对行业从业人员的水平及行业从业人员现状进行动态分析，促进行业良性发展，同时也使其具有根据行业发展进行调整的灵活性和实用性，符合人员能力验证的需求。

4.首席数据官人员能力验证考核不属于职业资格类考试，通过考试仅表明学员掌握了一定的数据安全专业理论知识和实际工作水平的能力。

首席数据官 人员能力验证规则

1 范围

本规则是认研中心首席数据官人员能力验证组织者和参加者双方都应当遵循的程序规则。

从事安全领域有相关经验的管理者和专业人士、相关研究人员；担任企业CIO、CSO等信息化相关的高层领导；担任政府机关单位的信息化主管领导，政府机关、企事业单位的法务人员、合规人员；担任信息技术总监、大数据部门研发总监、信息安全总监及经理；担任安全顾问、分析师、审计师、架构师、设计师；以及其它有志于从事数据安全领域咨询、管理和架构设计的人士及对数字安全和隐私保护有兴趣的相关人员，均可申请参加认研中心首席数据官人员能力验证。

2 引用文件

本规则参考并修改引用了下列文件中的全部或部分条款。所引用的文件不注明其发布日期，请各相关方注意使用这些文件的有效版本（包括其修订案）。

2.1 《合格评定能力验证的通用要求》(ISO/IEC 17043)

2.2 《利用实验室间比对进行能力验证的统计方法》（ISO 13528）

3 术语和定义

人员能力验证：是指按照相关规定或标准，根据考核验

证规则，采取专业知识学习、能力素质考核、结果分析比对及验证等方式，对人员的专业能力进行验证的合格评定过程。

原始分：参加考核人员答题得到的分数，最高为100分。

平均分：所有考核人员原始分的算术平均值，最高分为100分。

中等分：反映考核项目中等水平的分数，最高为100分。

标准差：反映原始分的分散性。

标准分：利用稳健统计方法，转化得到每位参加考核人员的分数，分值在-100至100之间。

百分比排名：比此原始分小的数据个数除以与此原始分进行比较的数据个数总数。

4 人员能力验证组织要求

4.1 学习时长

参加人员能力验证应满足相应的专业学习时长要求，不得少于60学时，并提供相关证明。

4.2 考核时间

首席数据官人员能力验证测验实行统一大纲、统一命题、统一组织的考试制度，原则上每年举行4次考试，分别安排在3月份、6月份、9月份、12月份的第四个周末，考试时间为120分钟。

4.3 考核方式

首席数据官人员能力验证采取线上考试，考生信息采用计算机考试系统进行统一管理，在线完成学员信息填报、考

试、电子试卷管理等工作。

考试系统应具有人脸识别等防作弊功能。

采取线上考试的形式，考生需在拥有摄像头的电脑前参加考试，监考人员与考生配比为 1:500，监考中心至少不少于 2 名监考人员。

4.4 考核结果

首席数据官人员能力验证结果划分为优秀、良好、合格、不合格。(注：人员能力验证结果详见第 6 部分人员能力验证结果评价规则)。

对于考生来说，纸质证书中赋予的原始分、标准分 Z 和百分比排名 PR 为当期(或者某一时间段)考核结果。同时要提醒考生，标准分 Z 和百分比排名 PR 会根据该项目全部参加考试人员的成绩“排大队”，考生可以随时登录账号，线上关注自己的标准分 Z 和百分比排名 PR 的变化。

4.5 考核内容

首席数据官能力考核的主要内容包括《GDPR 解读》《数据安全从业者》《信息安全，网络安全与隐私保护基础》《数据安全合规》《数据安全导论》《数据安全管理》《数据安全治理》《数据安全技术》《数据安全评估》《数据安全实践》《数据安全案例》十一部分内容，内容清单见附件。考核验证时，《GDPR 解读》《数据安全从业者》《信息安全，网络安全与隐私保护基础》《数据安全合规》《数据安全导论》《数据安全管理》《数据安全治理》《数据安全技术》

《数据安全评估》《数据安全实践》《数据安全案例》十一部分内容占比分别为10%、10%、5%、15%、15%、10%、5%、5%、5%、15%、5%。

5 考核申请条件

凡遵纪守法、参加专业学习时长满足要求，并符合下列条件中之一，可申请参加首席数据官能力考核:

5.1 全国各级政府主管数据安全的领导及负责人员;

5.2 企业分管数据安全的领导及负责人员;

5.3 企业首席数据官后备人才;

5.4 有志于加入数据安全事业的专业技术和管理人才。

6 验证结果评价

6.1 统计量计算

6.1.1 平均分 A

所有考核人员原始分的算术平均值，计算公式如下:

$$A = \sum^{p} x_i / p$$

x_i为第 i 名人员的原始分，p 为参加考试人员总数。

6.1.2 中等分 M

所有参加考核人员原始分的中位值。假设 p 名参加考核人员原始分按递增顺序表示为: x_1，x_2，…，x_p。当 p 为奇数时，中位值为第(p+1) /2 位的原始分值; 当 p 为偶数时，中位值为第 p/2 位和第（1+p/2）位原始分值的平均值。计算公式如下:

$$M = \begin{cases} X_{[(p+1)/2]}, & p\text{为奇数} \\ [X_{(p/2)} + X_{(1+p/2)}] / 2, & p\text{为偶数} \end{cases}$$

6.1.3 差值 D

参加考核人员原始分与中等分的差值。计算公式如下:

$$D_i = X_i - M$$

6.1.4 标准差 S

按照稳健统计方法，以标准化四分位距作为标准差。将参加考核人员的原始分按递增顺序排列，计算高四分位和低四分位原始分的差值，然后乘以系数 0.7413（因子 0.7413 是从“标准”正态分布中导出）即可得到标准化四分位距。计算公式如下:

$$S=0.7413\times(Q_3-Q_1)$$

式中，Q_1为低四分位数，该组原始分的四分之一低于 Q_1，四分之三高于 Q_1；Q_3为高四分位数，该组原始分的四分之一高于 Q_3。

6.1.5 标准分 Z

每位参加考核人员差值 D 与标准差之比。计算公式如下:

$$Z=D/S\times 50$$

标准分 Z 反映参加考核人员与中等水平间的差距。Z＞0 时，反映人员能力高于中等水平；Z＜0 时，反映人员能力低于中等水平。根据统计学原理，基于正态分布假设，D/S 在[-2，+2]的概率约为 95%。为了更加通俗易懂和直观显示，乘以系数 50 得到标准分 Z，而且，当计算 Z 值小于-100 或者大于

100 时，直接分别赋值为 Z=-100、Z=100。因此，标准分 Z 在-100 至 100 之间，Z 值越接近 100，说明参加考核人员的水平越高。

6.1.6 百分比排名 PR

某参加考核人员百分比排名为 90%，表明该人员成绩比 90%的人成绩高。

6.1.7 合格率

考核等级为合格以上的人数占参加考核总人数的比例。

6.2 人员能力评价

6.2.1 反馈给参加考核人员的指标

参加考核人员成绩单列出原始分、标准分 Z 和百分比排名 PR 三个指标值，并注明含义。其中，成绩是否合格以参加考核人员的原始分为评价基准。对于成绩合格的人员，再按标准分 Z 的大小，分级列出成绩。具体如下:

当原始分＜60 时，表明考生参加本次考核等级为“不合格”，建议考生进一步学习后，再次报名参加考核。

当 60≤原始分＜100，且标准分满足-100≤Z＜50 时，表明考生参加本次考核等级为“合格”。

当 60≤原始分＜100，且标准分满足 50≤Z＜100 时，表明考生参加本次考核等级为“良好”。

当原始分≥60，且标准分 Z=100 时，或当原始分=100 时，表明考生参加本次考核等级为“优秀”。

当标准差 S=0，则采取原始分判断规则：原始分<60 为

“不合格”；60≤原始分＜80为“合格”；80≤原始分＜90为“良好”；原始分≥90为“优秀”。

对于考生来说，纸质证书中赋予的原始分、标准分Z和百分比排名PR为当期（或者某一时间段）考核结果。标准分Z和百分比排名PR会根据该项目全部参加考试人员的成绩“排大队”，考生可以随时登录账号线上关注自己标准分Z和百分比排名PR的变化。

对每一名考核“不合格”的考生，在发送成绩单的同时，应有针对性地提出改进建议和再次参加考核的方法。

6.2.2 认研中心监测指标

及时发布并动态更新每个能力验证项目参加考核的总人数、平均分、中等分、标准差、合格率、最低分、最高分等指标。此外，可以使用顺序标准分Z直方图直观显示参加者能力。

附录（资料性附录）

首席数据官考核内容清单

分类	考核内容	
一、GDPR 解读	隐私与数据保护基础及法规	相关法规定义
		个人数据
		个人数据合法处理的原则与要求
		个人主体权力
		数据泄露及相关程序
	数据保护的组织工作	组织数据保护的重要性
		监管机构
		个人数据转移到第三国
		有约束力的公司规则与合同中的数据保护
	数据保护实践	与信息安全相关的基于设计与默认的数据保护
		数据保护影响评估
		使用中的个人数据
二、数据安全从业者	基于设计和认的数据保护	基于设计和默认的数据保护
		软件保证成熟度模型（SAMM）
		综合的轻量级应用安全过程 CLASP
		软件安全构建成熟度模型 BSIMM
		数据保护管理系统 DPMS 的五阶段
	控制者，处理者和数据保护官（DPO）的角色	控制者，处理者和 DPO 的角色
		DPO 的角色和责任
	数据保护影响评估	数据保护影响评估
		DPIA 的准则
		DPIA 的步骤
	数据泄露，通知和事件响应	数据泄露，通知和实践响应
		GDPR 关于个人数据泄露的要求
		数据泄露通知的要求
三、信息安全，	信息安全管理	信息和安全
		威胁和风险
		方法和组织

网络安全与隐私保护基础		措施
		监管和立法
	新版 ISO 27001 改版说明	ISO 27001 2022 改版说明
四、数据安全合规	国际数据安全合规政策情况	欧盟数据安全立法
		美国数据安全立法
		其他国家数据安全立法
	国内数据安全合规政策情况	我国数据安全法律体系
		数据安全法解读
		个人信息保护法解读
		其他政策法规解读
	数据安全标准规范	数据安全能力类标准
		数据安全管理类标准
		数据安全技术类标准
		个人信息安全标准
五、数据安全导论	数据安全发展背景	数据安全形势
		产业内涵与范畴及其研究方法
		产业指导意见解读
		数据安全日常管理
六、数据安全管理	DCMM 标准解读与实践	数据安全管理
七、数据安全治理	DSMM 标准解读与实践	数据安全成熟度模型介绍
		数据安全成熟度评估实施
	数据安全治理概述	数据安全治理背景、概念及框架
		数据安全
		数据安全治理
		咨询方法论
		咨询服务框架体系
八、数据安全技术	数据安全技术架构与规划	数据安全总体架构
		数据安全规划与信息架构
	数据安全应用技术	脱敏、水印、数据加密、日志管理
		身份鉴别与访问控制
		接口安全
		备份恢复

		安全审计
		交换管控
		大数据防护
		备份容灾
		数据销毁
	数据安全运营（审计）	数据安全运维的目标和内容
		数据安全运维方法
		数据安全运维技术措施和策略
九、数据安全评估	数据安全评估	网络数据安全风险评估
		个人信息保护评估
		数据出境安全评估
十、数据安全实践	数据安全咨询实践	数据安全治理咨询服务方案
		数据分类分级方法解构与应用实践
十一、数据安全案例	重点行业数据安全问题	数据安全在金融行业的应用
		数据安全在电信行业的应用
		数据安全在医疗行业的应用
		数据安全在汽车行业的应用
		数据安全在电力行业的应用
		数据安全在芯片半导体制造行业的应用