ICS 03.120.10
A 00

团　　体　　标　　准

T/ZEA 001—2020

电子商务交易产品第三方检测机构服务通用要求

Basic requirement for service of third-party testing organization with e-commerce transacting commodity

2020－1－7 发布　　2020－2－1 实施

浙江省电子商务促进会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准的某些内容可能涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准由浙江省电子商务促进会提出并归口。

本标准起草单位：浙江方圆检测集团股份有限公司、杭州市标准化研究院、国家电子商务产品质量监测处置中心、宁波市食品检验检测研究院、杭州市标准化协会。

本标准主要起草人：陈洪波、周玲、朱萍、吴晓雯、黄时炜、王娜、童艳、陆品、李秀娣、蒋宏、朗铖、钟唯奇、徐梦、李南阳、励丹。

电子商务交易产品第三方检测机构服务通用要求

1 范围

本标准规定了电子商务交易产品第三方检测机构（以下简称“检测机构”）服务的术语和定义、基本要求、服务类别、服务保障要求，以及服务评价与改进。

本标准适用于第三方检测机构对电子商务交易产品质量的检测活动。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 22081 信息技术 安全技术 信息安全控制实践指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 35408 电子商务质量管理 术语

RB/T 214 检验检测机构资质认定能力评价 检验检测机构通用要求

SB/T 10409 商业服务业顾客满意度测评规范

3 术语和定义

GB/T 29246、GB/T 35408、RB/T 214 界定的以及下列术语和定义适用于本文件。

3.1

电子商务交易产品 e-commerce transacting commodity

通过电子商务平台进行交易的有形产品。

3.2

第三方检测机构 third-party testing organization

依法成立，既独立于提供检测对象的人员或组织、又独立于在对象中具有使用方利益的人员或组织的机构，依据相关标准或者技术规范，利用仪器设备、环境设施等技术条件和专业技能，对产品或者法律法规规定的特定对象进行检测的专业技术组织。

3.3

实验室信息管理系统 laboratory information management system

实验室用于收集、处理、记录、报告、存储或检索信息的软件系统。

3.4

信息安全 information security

保护网上信息免受未经授权的访问、使用、披露、破坏、修改、检视、记录及销毁，即确保信息的保密性、完整性和可用性。

3.5

信息安全管理 information security management

通过在组织环境下建立、实现、维护和持续改进信息安全的一系列活动和过程来管理和保护信息的保密性、完整性和可用性。

3.6

外部接口 external interface

为应对不同的外部系统的访问而设计的统一且与内部系统相对隔离的数据交换接口。

4 基本要求

4.1 公正性

4.1.1 检测机构应公正实施检测活动，从组织结构和管理上保证公正性，并作出公正性承诺。

4.1.2 应持续识别影响公正性的风险。这些风险应包括其活动、检测机构的各种关系，或者检测人员的关系而引发的风险。

注：危及检测公正性的关系可能基于所有权、控制权、管理、人员、共享资源、财务、合同、市场营销（包括品牌）、支付销售佣金或其他引荐新客户的奖酬等。

4.1.3 如果识别出公正性风险，检测机构应能够证明如何消除或最大程度降低这种风险。

4.2 保密性

4.2.1 检测机构应通过作出具有法律效力的承诺，对在检测活动中获得或产生的所有信息承担管理责任。应将其准备公开的信息事先通知客户。除客户公开的信息或检测机构与客户有约定（例如：为回应投诉的目的）外，其他所有信息都被视为专有信息，应予保密。

4.2.2 检测机构依据法律要求或合同授权透露保密信息时，应将所提供的信息通知到相关客户或个人，除非法律禁止。

4.2.3 检测机构从客户以外渠道（如投诉人、监管机构）获取有关客户的信息时，应在客户和检测机构间保密。除非信息的提供方同意，检测机构应为信息提供方保密，且不应告知客户。

4.2.4 检测机构从事检测活动相关的技术人员和管理人员，应对在实施检测活动过程中获得或产生的所有信息保密，法律要求除外。

5 服务类别

5.1 监管部门委托

商品质量监管部门依法对在电子商务平台销售的产品进行抽样并委托检验，对抽查结果进行处理等的活动。

5.2 电子商务平台经营者委托

电子商务平台经营者在线采样后委托的产品质量检测，并依据平台管理规则按相关条款进行处理等的活动。

5.3 电子商务平台内经营者委托

电子商务平台内经营者为控制商品质量，自主委托的产品质量检测活动。

5.4 其他社会组织委托

行业组织、研究机构等社会组织，对在电子商务平台销售的产品进行抽样并委托检验，结合抽查结果开展内部处置或研究的活动。

6 服务保障要求

6.1 检测机构资质

检测机构应按照RB/T 214建立实验室质量管理体系，取得相应的资质，确保在资质有效期和批准的能力范围内开展电子商务交易的产品质量检测工作，并持续符合条件和要求。

6.2 信息化管理

6.2.1 总则

检测机构应具备确保网络安全的资源和能力、实验室信息管理系统和电商平台的接口、支付管理以及安全应急处置能力。

6.2.2 网络配备

应包括对涉及开展电子商务产品第三方检测的物理环境、基础信息网络、平台/系统及其他信息终端或设备等的要求。

检测机构根据GB 17859划分的安全保护等级，应满足GB/T 22239中相应安全等级的通用要求；租用云服务平台的检测机构，应满足GB/T 22239中对云服务商选择的扩展要求；采用移动互联技术的检测机构应满足GB/T 22239中对移动互联安全的扩展要求；采用物联网技术的检测机构应满足GB/T 22239中对物联网安全的扩展要求。

6.2.3 实验室信息管理系统

检测机构应采用实验室信息管理系统进行检验数据和信息的采集、记录、处理、分析、报告、存储、传输或检索，并具备利用互联网为客户提供服务的能力，检测机构应对实验室信息管理系统的安全性、有效性和适用性进行验证，并满足如下要求：

a) 实验室信息管理系统的安全保护技术能力应符合 GB 17859 中规定的二级以上的要求，并按照 GB/T 22239 规定进行等级测评；
b) 系统建设应符合 GB/T 22239 中相应等级的产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付等要求；具有移动端的系统应符合 GB/T 22239 中相应等级的移动互联安全建设管理要求；
c) 应满足 6.2.4 中与各电商平台的接口要求；
d) 员工应参加培训以便正确操作软件，防止造成软件误操作；
e) 与信息系统相关的说明书（包括数据结构、系统安装、功能配置）、使用指南及参考数据应易于被员工获得；

f） 信息系统由外部供应商建立、管理、维护的，该供应商应签署保密协议，防止敏感信息泄露，供应商应符合本标准所有适用要求；
g） 信息系统所有过程文件应被保留，包括建设、管理、维护过程的配置信息；
h） 信息系统应满足检测机构的安全指导需求；
i） 应根据 GB/T 22239 中相应等级的恶意代码防范管理要求定期对软件源代码进行审查，防止存在后门和隐蔽信道等安全隐患；
j） 信息系统应有权限控制，防止信息被未经授权的访问、篡改、删除和窃取等；
k） 系统在投入使用前或更改后都应进行测试，确认安全后经授权方可使用，所有过程应形成文件；
l） 应有相应的有效措施保障系统运行过程中的数据在发生意外时正确回滚，及时恢复运行，并可追溯、验证，确保信息的有效性；
m） 信息系统应有安全风险管理流程，应具备 GB/T 22239 中相应等级的漏洞和风险管理要求，不断改进系统，预防安全事故。

6.2.4 接口管理

接口包括检测机构组织内各信息系统使用的内部接口及供电商平台使用的外部接口。检测机构应确保：

a) 编制自己的基于风险的接口控制及实施规范并可应用；
b) 接口的开发环境应符合 GB/T 22081 中安全开发环境的控制要求，外包开发时应符合 GB/T 22081 中外包开发的控制要求；
c) 根据接口连接方式及业务特点，应制定相应的接入策略，保证接口的数据传输和数据处理的安全性，确保信息系统数据的保密性、完整性及可用性；
d) 外部接口应在接入点的网络边界实施接口安全控制，包括但不限于安全评估、访问控制、入侵检测、口令认证、安全审计、防恶意代码、加密等控制策略；
e) 接口在移植入正式环境前应得到测试，包括安全测试、验收测试；
f) 接口应实现平滑的移植和扩展，保证被接入信息系统的稳定性；
g） 接口的接入应保障被接入信息系统的正常运行，应防止大量访问，以及大量占用资源的情况发生，保证被接入系统的可用性；
h） 应实现接口的容错性，防止意外情况下信息系统数据的完整性及可用性；
i） 接口提供日志等有效的可监控机制，使得接口的运行情况可监控，便于及时发现错误及排除故障；
j） 接口应设置访问控制，防止未经授权的访问；
k） 每个接口应有配置信息，并有专人维护；
l) 应定期对接口进行漏洞等脆弱性检查，做好风险防范，发现问题及时整改完善。

6.2.5 支付管理

支付管理要求如下：

a） 检测机构应提供可选的支付、收取、结算等服务，其中支付服务包括但不限于：网上银行转账、汇款，第三方支付平台支付，移动支付，线下支付；其中移动支付应满足GB/T 22239中相应安全等级的移动互联安全的扩展要求；
b） 检测机构应根据国家有关支付安全管理要求，建立相应支付管理制度，明确各个支付方式的支付、退款规则，并保障资金的可追溯性；
c） 检测机构应对各个支付账户（平台）建立档案信息，并指定专人对其维护，设立专人对各支付账户（平台）的资金收支情况进行监控；

d） 应确保整个资金交易过程的保密性、真实性、完整性和不可否认性；
e） 检测机构在提供支付服务时，应告知用户服务的具体功能、操作方法、注意事项、相关风险和收费标准等事项，不得在未经用户授权的情况下，附加进行不合理交易；
f） 检测机构在提供支付服务后，应及时向用户提供符合约定方式的确认支付的信息，并要求用户签字；
g） 检测机构不得在未经用户授权的情况下获取用户账户等敏感信息进行商业化操作，应做好敏感数据保密工作；
h） 检测机构对用户的支付疑问应制定相应的处理流程，并及时查找原因，必要时应立即采取措施防止损失扩大，事后应采取相关措施予以纠正。造成用户损失的，应承担赔偿责任。

6.2.6 信息安全应急管理

检测机构对信息安全的应急管理应符合GB/T 22239中相应安全等级的应急预案管理、备份与恢复管理、安全事件处置的要求。外包运维处理应急事务的应满足GB/T 22239中相应安全等级的外包运维管理要求。

6.3 人力资源

从事电子商务交易产品质量服务的第三方检测机构应配备RB/T 214要求的人员，以及以下人员：
a） 采样人员。根据委托方的要求配置并遵循相关行为准则的样品采样人。
b） 在线合同评审人员。负责网上受理检测业务的人员，评审确定实验室检测能力、合同执行时限、检测依据、样品一致性等。
c） 客服人员。负责提供网上检测服务展示并与客户在线沟通的服务人员。
d） 网管人员。负责检测机构电子商务运营需要配置的保障网络安全、稳定运行、防范网络违法、并有效应对网络安全事件、保障电子商务交易安全的信息技术人员。

6.4 合同管理

6.4.1 合同评审

合同评审应考虑法律法规、财务和时间等方面的影响，并充分评审检测的可行性和有效性。应保证：
a） 与 5.1、5.2、5.3 类客户签订框架性合同时，应确定所采用的检测合同形式，对双方权力、职责、义务等要素进行约定；
b） 客户委托的单次任务合同评审，应对检测所用方法、检测时限、检测收费、检测依据、检测结果的判定要求等要素在合同书上予以约定；
c） 通过网络平台、客户端实施任务委托的，网上填写信息视同确认合同内容；
d） 通过客服提出要求、填写在线委托的，双方确认的沟通记录视同确认合同内容；
e） 通过任务文件、邮件形式实施任务委托的，相关委托要求经邮件书面确认后视同确认合同内容。

6.4.2 合同签订

签订合同前，应对对方当事人的主体资格、资信能力、履约能力进行调查，不得与不能独立承担民事责任的组织或个人签订合同，也不得与法人单位签订与该单位履约能力明显不相符的合同。

6.4.3 合同履行

检测机构应严格按照与客户签订的委托合同书内容开展检测活动，在合同规定时限内按照约定的检测项目完成检测工作，并确保其数据真实、准确、可靠。

6.4.4 合同变更

合同变更包括检测合同内容变更和合同解除，需采用书面形式。合同变更应与委托方协商一致，在未达成或未批准之前，原合同仍应履行。

6.4.5 合同备案

所有合同应由统一的部门登记管理。宜建立以下管理要求：

a） 合同档案管理。

b） 合同台帐管理。

c） 合同执行情况跟踪。

6.5 检测过程管理

6.5.1 流程管理

检测机构应根据机构内部资源现状，设计电子商务交易产品检测控制流程。流程设计应考虑监管部门委托、电子商务平台经营者委托、电子商务平台内经营者委托、其他社会组织委托等委托方不同，设计不同的进入模式，明确关键控制点。

6.5.2 关键控制点管理

检测机构在流程控制过程中，应对采样、存证、异议等关键控制点制定适宜的关键控制程序，明确操作要求，规范工作流程，确保检测工作的公正性和有效性。

6.5.3 流程优化

检测机构应定期对控制流程的适宜性进行评估。可通过内部审核、管理评审、客户满意度调查、质量监控等方式，定期对控制流程进行优化。

6.5.4 质量监控

质量监控要求如下：

a) 检测机构应建立质量控制程序识别电子商务交易产品检测活动的有效性，确保检测结果准确可靠。

b) 检测机构应建立和保持应用评定测量不确定度的程序，当检测出现临界值、内部质量控制或客户有要求时，应报告测量不确定度。

c) 检测机构应根据项目特征选择关键的产品/参数开展日常周期性的质量监控活动，优先选择新开展的、有新人员上岗的、技术难度较大的、设备变更或性能不稳定的、存在客户对检测结果投诉的、发生过重大质量问题的和能够选择确定的方法的项目或参数。当发现质量监控数据将要超出预先确定的判定依据时，应采取相应措施纠正问题，以防止出现报告不正确的结果。

d) 检测机构在确定质量监控对象时，应考虑但不限于以下因素：

   1) 承担电子商务交易产品检测的业务量；

   2) 首次承担电子商务交易产品检测的产品/参数；

   3) 检测结果的用途；

   4) 检测方法的稳定性与复杂性；

5） 对技术人员经验的依赖程度；
6） 参加外部比对（包含能力验证）的频次和结果；
7） 人员能力和经验、人员数量及变动情况；
8） 新采用或变更的方法；
9） 质控样品的检测结果。

7 服务评价与改进

7.1 服务评价

7.1.1 检测机构自我评价

检测机构应按照策划的时间间隔对电子商务交易产品检测活动的各项保障资源（网络环境、实验室信息管理系统、人力资源、资质能力）、服务流程、客户投诉、客户满意度等进行自我评价，识别存在的不符合、潜在风险和可改进的服务内容。

a） 评价活动应根据检测机构自身存在的可能影响检测服务的变化、外部评审活动（包括电子商务交易平台经营者、政府抽检部门等对检测机构实施的抽查）的结果、客户反馈以及质量控制要求策划、制定评价方案，实施评价活动，并形成评价报告；
b） 评价活动的记录应完整、有效并妥善管理，能满足存储、保护、检索、调用的相关要求。

7.1.2 投诉管理

检测机构应建立投诉管理的程序，明确接收、确认、调查和处理投诉的职责与方式。

a） 接收投诉时，应对投诉人的投诉内容进行记录，投诉内容经确认受理后，应及时告知投诉人；
b） 投诉调查和处理过程应得到有效跟踪和记录，与投诉内容相关的人员应进行回避。投诉处理完毕后应形成相应的投诉处理报告，报告中应至少包括以下内容：投诉人，投诉内容，投诉接收、确认、调查过程的说明，以及解决投诉所采取的处理措施；
c） 投诉处理后，应由与投诉内容不相关的人员通知投诉人并告知相关的处理意见。

7.1.3 客户满意度调查

检测机构应提供客户评价的渠道，建立客户满意度调查的程序，持续保持与客户的良好沟通，跟踪客户的需求，提升客户满意度。满意度调查可参照SB/T 10409实施。

a） 满意度调查的内容应包括（不限于）：网上客服人员服务态度、沟通及时性与有效性、检测服务时效性、服务质量、投诉处理及时性与满意度、价格、客户的建议及需求等方面；
b） 满意度调查方式可采用（不限于）：网上调查、电话调查、邮件调查、面访等；
c） 满意度调查结果统计分析可按时间、分要素进行，以便检测机构建立持续改进服务的目标。

7.2 服务改进

7.2.1 纠正

检测机构针对客户投诉、评价活动中识别出的不符合，应采取纠正措施，及时进行纠正。

实施纠正应分析不符合产生的原因，评估是否存在或可能发生的类似不符合，纠正措施应充分具体、可操作性强，能有效控制和避免不符合。

7.2.2 改进

检测机构应根据评价活动识别出的潜在风险与需改进的内容，制定改进措施。改进措施可包括（不限于）资源配置增加、系统升级、流程优化、人员培训等。

改进应在保证公正性与保密性的基础上，重视客户需求，持续完善服务内容，提升客户满意度。