ICS#35. 040
L 80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—2016

电子商务平台数据开放
第三方软件提供商评价准则

Data open for e-commerce platform - Third party software provider evaluation criteria

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前# # 言

本标准是依据 GB/T 1.1-2009 给出的规则起草。

本标准由全国电子业务标准化技术委员会（SAC/TC 83）提出并归口。

本标准的主要起草单位：阿里巴巴（中国）有限公司、中国标准化研究院。

本标准主要起草人：

引# # 言

本标准提出了电子商务第三方软件提供商的评价准则，对电子商务第三方软件提供商提供的第三方软件在技术要求和管理要求方面提供评价和认定提供标准依据，以规范我国快速发展的电子商务市场，提高第三方软件提供商的水平，保护消费者的利益，促进电子商务市场的长期健康发展。

本标准的读者对象主要是电子商务第三方软件的开发者、运营者、评价者、使用者和其他对第三方软件安全感兴趣的团体。

电子商务平台数据开放 第三方软件提供商评价准则

1 范围

本标准规定了对电子商务平台中的第三方软件提供商的评价总体框架和评价模块、评价方法和结果表示、评价规则与结论、评价报告以及扩展原则与方法。

本标准适用于对电子商务第三方软件提供商进行评价或认证，也适用于第三方软件提供商自我评价。

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。凡是标注日期的引用文件，仅注日期的版本适用于本文件。凡是未标注日期的引用文件，其最新版本（包括所有的修改版）适用于本文件。

GB/T ******　　电子商务平台数据开放 总体要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

电子商务 electronic commerce

以电子形式进行的商务活动。

注：经济活动主体之间利用现代信息技术和网络技术（含互联网、移动网络和其他信息网络）开展商务活动，实现网上接洽、签约、支付等关键商务活动环节的部分或全部电子化，包括货物交易、服务交易和知识产权交易等。

3.1.2

用户 user

使用第三方软件的机构或自然人，以注册的标识与用户信息为判断依据。

3.1.3

商家 merchant

租用电子商务平台进行经营活动的法人、法人委派的行为主体、其它组织机构或自然人。

3.1.4

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。[GB/T 25069-2010]

3.1.5

电子商务平台服务商 electronic commerce platform service provider

为电子商务活动提供平台服务的组织或机构。

3.1.6

第三方软件提供商 the third party software provider

以第三方身份提供软件或软件服务的企业。

注：在本标准中指专门开发、营销和支持电子商务卖家软件应用的服务商。

3.1.7

第三方软件 the third party software

由第三方软件提供商开发或提供的软件系统。

注：在本标准中，第三方软件特指用于辅助电子商务的开展的软件。

3.1.8

评价方法 evaluation method

为了获得对第三方软件提供商实施规定测量的结果而描述由评价方采取动作的规程。

3.1.9

评价模块 evaluation module

用于测量第三方软件提供商特性、子特性或属性的评价技术包。

注：该包包含评价方法和技术、评价的输入、待测量和待收集的数据以及支持规程和工具。

3.1.10

评价方 evaluator

实施评价的个体或组织。

3.2 缩略语

ARP	地址解释协议	(Address Resolution Protocol)
DDOS	分布式拒绝服务攻击	(Distributed Denial of Service)
IP	互联网协议	(Internet Protocol)
RDS	关系型数据库服务	(Relational Database Service)
SQL	结构化查询语言	(Structured Query Language)
URL	统一资源定位器	(Uniform Resource Locator)

4 评价总体框架和评价模块

4.1 评价总体框架

本标准是按照《电子商务平台数据开放 总体要求》中第 6 章的要求，对第三方软件提供商在技术要求和管理要求方面进行评价。

电子商务第三方软件提供商评价的总体框架图如图 1 所示。

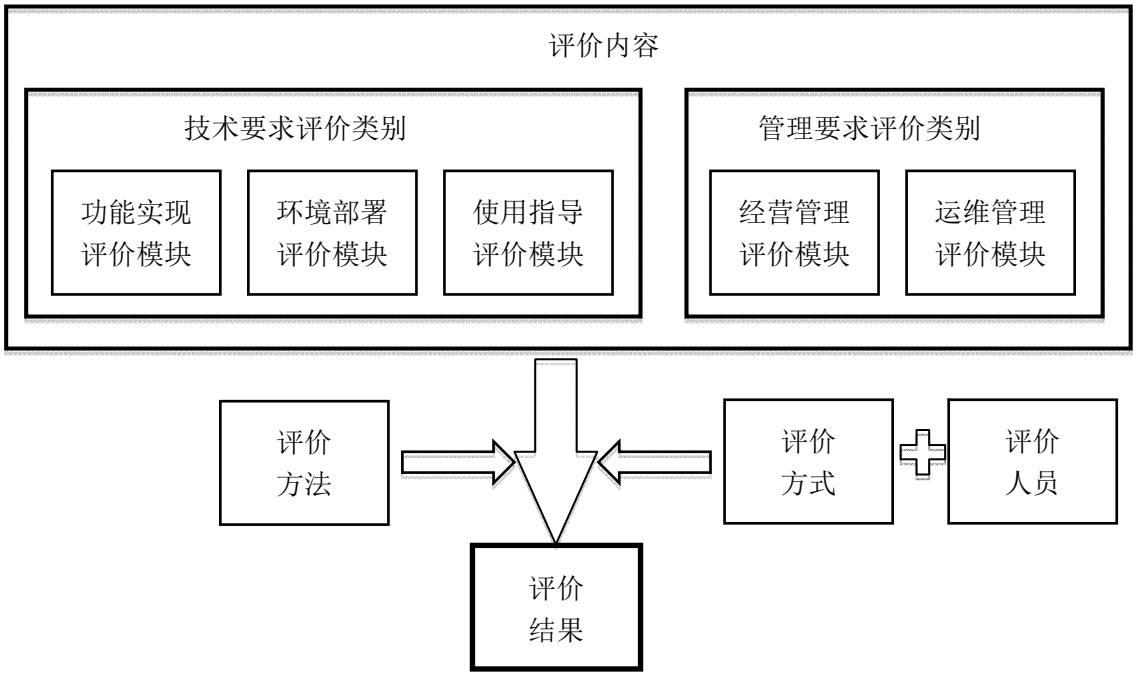

图1　第三方软件提供商评价总体框架图

第三方软件提供商评价应由技术要求和管理要求两大评价类别组成，技术要求的评价包括功能实现、环境部署、使用指导三个评价模块，管理要求的评价包括经营管理和和运维管理两个评价模块。这五个评价模块分别是：

——功能实现评价模块是对第三方软件提供商进行软件功能实现，所开发的第三方软件需具备的功能进行评价。

——环境部署评价模块是对第三方软件提供商需具备的第三方软件的部署环境进行评价。

——使用指导评价模块是对第三方软件提供商需提供的对第三方软件的使用指导进行评价。

——经营管理评价模块是对第三方软件提供商在资质、经营、服务等方面进行评价。

——运维管理评价模块是对第三方软件提供商需提供的对第三方软件的运维管理方面进行评价。

各个评价模块由若干个评价子模块以及评价内容构成，实际评价时不限于上述评价模块、评价子模块和评价内容。

4.2　评价模块和子模块表

评价模块和子模块及其评价选择项见表 1。

表1　第三方软件提供商评价模块、子模块和评价选择条件

评价类别	评价模块	评价子模块	评价条件
		账号体系	评价必备项
		账号口令	评价必备项

技术要求	功能实现	会话及权限管理	评价必备项
		审计管理	评价必备项
		数据安全	评价必备项
	环境部署	服务器环境	评价必备项
		数据库环境	评价必备项
		管理后台	评价必备项
		主机系统配置	评价必备项
		软件系统配置	评价可选项
		基础攻击防御	评价可选项
		入侵检测	评价可选项
		Web 应用防护	评价条件项
	使用指导	系统提示	评价必备项
		用户手册	评价可选项
管理要求	经营管理	资质要求	评价必备项
		经营要求	评价必备项
		服务管理	评价必备项
	运维管理	运维保障	评价必备项
		漏洞管理	评价必备项
		变更管理	评价必备项
		应急响应	评价必备项
		文档管理	评价可选项

5 评价方法和结果表示

5.1 评价方法

电子商务第三方软件提供商的评价是通过对评价内容、评价子模块和评价模块的评价来完成的，评价方法如下：

——确定各子模块的评价内容，评价内容是最小评价单元；

——采用多种审查方式（见 6.2）的组合使用，对评价内容进行评价，给出评价结果；

——依据评价内容的评价结果，给出子模块的评价结果；

——依据子模块的评价结果，按照评价规则给出模块的评价结果，具体见第 7~10 章；

——依据所有模块的评价结果，按照评价规则给出“合格提供商”的评价结论，并提供相应的评价报告。

5.2 评价方式

评价方式是对评价内容作出评价结论的主要手段，在评价过程中可使用一种审查方式，也可使用多种审查方式的结合形式。主要的审查方式有：

——文件审查：对所提供的审核文件的真实性和有效性进行审查，审核文件是指在第三方软件提供商评价过程中，被评价的提供商根据评价要求需提供的自我声明、相关文件、证件或证明等材料；

——人员访谈：对相关人员，针对评价内容进行访谈；

——现场巡查：赴现场了解有关内容，对事实相符性进行查验；

——功能检查：对软件进行使用、功能检查和测试，对软件功能进行查验。

5.3 评价人员

评价人员应取得相关的资格。

5.4 结果表示

符合评价规则要求的评价内容、评价子模块和评价模块，其结果表示为“通过”，不符合评价规则要求的评价内容、评价子模块和评价模块，其结果表示为“不通过”；可选的评价内容、子模块表示为“可选项”；某些情况下，不需要评价的内容结果表示为“不适用”。

对于第三方软件提供商，整体的评价结论为“合格”与“不合格”。

6 评价内容、评价细则与结果

6.1 功能实现评价模块

6.1.1 账号体系评价子模块

6.1.1.1 评价内容

账号体系为评价必备项，其评价内容包括但不限于：

a）软件系统应为不同的用户分配不同的账号，确保一个用户一个账号，应禁止多人使用同一个账号。

b）软件系统应及时冻结或禁用多余的、过期的用户帐号，避免共享帐号的存在。

c）软件系统应及时清理和回收软件系统相关的开发账号、测试账号和后台管理账号及权限，如：离职或转岗时。

d）软件系统应维护自有账号和电子商务平台账号的对应关系。

e）软件系统宜具备保护和管理平台账号的安全能力，能及时地识别帐号的异常风险（包括但不限于账号被盗、暴力破解等问题），并给与及时地管控。

f）软件系统宜在识别到用户账号存在登录异常风险时，对用户账号进行锁定一定时间，或者直到管理员启用该用户账号。

6.1.1.2 评价细则与结果

6.1.1.1 中 a）– d）的要求为评价必备要求，需同时满足 a）– d）的要求，则 6.1.1 的评价结果为通过；否则为不通过。

6.1.1.1 中 e) – f）的要求，为评价可选要求。

6.1.2 账号口令评价子模块

6.1.2.1 评价内容

账号口令为评价必备项，其评价内容包括但不限于：

a）软件系统管理员帐号的初始口令应为系统随机产生的满足口令强度要求的口令。

b）软件系统应定期提醒用户对口令进行修改。

c）口令强度应同时满足如下要求：

1） 软件系统应保存加密后的口令历史，并要求新口令与前四次使用的口令不同；

2） 口令不能为空；

3） 不得使用默认口令；

4） 口令长度至少 8 位以上；

5） 包含字母大写、字母小写、数字、特殊字符其中的三种或以上，不能使用连续字母或单纯数字，不能使用键盘上连续字符；

6） 不能使用与用户自身强关联（如生日、姓名）的单词。

d）软件系统应提供给用户口令重置功能，口令重置的功能需要经过第三方软件提供商客服人工确认或者经过“组合鉴别”通过才能生效，且重置后的口令必须通过短信、邮件等用户绑定的可信任的渠道告知用户。

6.1.2.2 评价细则与结果

6.1.2.1 中 a）– d）的要求为评价必备要求，需同时满足 a）– d）的要求，则 6.1.2 的评价结果为通过；否则为不通过。

6.1.3 会话及权限管理评价子模块

6.1.3.1 评价内容

会话及权限管理为评价必备项，其评价内容包括但不限于：

a）当会话空闲超过一定的时间，软件系统应要求用户重新验证或重新激活会话。

b）软件系统应对登录软件系统的用户进行身份标识和鉴别。

c）软件系统应支持对同一用户采用两种或两种以上组合的鉴别技术（口令验证、邮箱验证、短信验证等）实现用户身份鉴别；

d）在执行敏感操作（口令修改或重置）或账号行为异常的情况下，软件系统应采用两种或两种以上的组合鉴别方式。说明：短信、邮箱验证可以通过发送验证信息到用户绑定的可信手机号或邮箱中，并且需要对验证信息设置过期时间。

6.1.3.2 评价细则与结果

6.1.3.1 中 a）– d）的要求为评价必备要求，需同时满足 a）– d）的要求，则 6.1.3 的评价结果为通过；否则为不通过。

6.1.4 审计管理评价子模块

6.1.4.1 评价内容

审计管理为评价必备项，其评价内容包括但不限于：

a）软件系统应保护所存储的日志审计记录的完整性，避免其受到未预期的删除、修改或覆盖等。

b）软件系统应保存日志，并满足一定的时间期限。

c）软件系统应记录和上报来自用户端的日志；日志的内容应包括：用户在第三方软件提供商的自有账号、应用标识（AppKey）、源 IP、时间、访问的订单 URL 等。

d）软件系统应通过调用电子商务开放平台提供的日志 API，记录和上报软件系统所有的登录日志，包括且不限于：用户登录软件系统的日志；软件系统管理员登录管理后台的登录日志；主机端进行的系统登录。日志的内容应包括：时间、用户在第三方软件提供商的自有账号、用户的电子商务平台账号、应用标识（AppKey）、应用名称、源 IP、登录结果（成功或失败）、失败原因等。

e）软件系统应通过调用电子商务开放平台提供的日志 API，记录和上报用户通过软件系统查看、管理、导出订单的详细日志。日志的内容应包括：用户在第三方软件提供商的自有账号、源 IP、时间、应用标识（AppKey）、应用名称、订单 URL、订单编号列表、对订单的操作等。

f）软件系统应通过调用电子商务开放平台提供的日志 API，记录和上报软件系统服务器之间的涉及到订单的所有数据通信记录，包括且不限于：同软件系统内部的订单接口访问；不同软件系统之间的

数据传递。日志的内容应包括：源 IP、时间、用户在第三方软件提供商的自有账号、应用标识（AppKey）、应用名称、请求的 URL、订单编号列表、订单推送的目的接口 URL 等。

g）软件系统应通过调用电子商务开放平台提供的日志 API，记录和上报服务器端调用数据库服务的日志；日志的内容应包含：用户在第三方软件提供商的自有账号、源 IP、时间、应用标识（AppKey）、用户请求的 URL、数据库实例标识、SQL 语句等。

h）软件系统宜通过调用电子商务开放平台提供的日志 API，记录和上报服务器端调用电子商务开放平台的日志；日志的内容应包括：源 IP、时间、用户在第三方软件提供商的自有账号、应用标识（AppKey）、应用名称、用户调用电子商务开放平台 API 的 URL 等。

6.1.4.2 评价细则与结果

6.1.4.1 中 a）– g）的要求为评价必备要求，同时满足 a）– g）的要求，则 6.1.4 的评价结果为通过；否则为不通过。

6.1.4.1 中 h）的要求，为评价可选要求。

6.1.5 数据安全评价子模块

6.1.5.1 评价内容

数据安全为评价必备项，其评价内容包括但不限于：

a）软件系统中涉及敏感数据（比如订单数据）的传输必须进行加密传输和存储，实现系统管理数据、鉴别信息和重要业务数据传输保密性。

b）软件系统对用户口令应使用安全的不可逆的加密算法进行加密保存，防止特权用户获取用户口令。

c）软件系统应对涉及敏感数据（比如电话号码、邮箱、电子商务平台昵称等）的展示，进行脱敏处理（模糊化、匿名处理等）。

d）软件系统之间的数据传递应经过电子商务开放平台，软件系统不允许将数据直接传递给不同第三方软件提供商的软件系统，不能将数据再次传递给其他软件系统使用，包括同一第三方软件提供商的不同 APPKey 的软件系统。

e）软件系统中的数据宜部署在安全云主机内，涉及电子商务订单数据，应使用 RDS 进行数据存储，并且绑定内网 IP 白名单。

6.1.5.2 评价细则与结果

6.1.5.1 中 a）– d）的要求为评价必备要求，需同时满足 a）– d）的要求，则 6.1.5 的评价结果为通过；否则为不通过。

6.1.5.1 中 e）的要求，为评价可选要求。

6.1.6 模块评价结论

6.1.1～6.1.5 为评价必备项。需同时满足 6.1.1～6.1.5，则软件功能实现的模块评价结果为通过；否则为不通过。

6.2 环境部署评价模块

6.2.1 服务器环境评价子模块

6.2.1.1 评价内容

服务器环境为评价必备项，其评价内容包括但不限于：

a）软件系统所处运行环境应具备快照功能，和快照回滚功能，当需要进行数据恢复时，则需要根据快照进行恢复。

b）应具备端口控制的功能，对服务器上的特殊用途端口进行预留，不可被占用。

c）不同的服务器应被划分到不同的安全域里，安全域应进行网络隔离，避免因一台服务器被入侵，所有资源面临高风险的问题。

d）如果同一个第三方软件提供商有多个软件系统，第三方软件提供商应为不同的软件系统使用不同的 APPKey，不同的软件系统需要独立部署在不同的服务器中，确保软件系统之间是被安全隔离的。

6.2.1.2 评价细则和结果

6.2.1.1 中 a）– c）的要求为评价必备要求，需同时满足 a）– c）的要求，则 6.2.1 评价结果为通过；否则为不通过。

6.2.1.1 中 d）的要求，为评价可选项，仅适用于第三方软件提供商有多个软件系统的情况。

6.2.2 数据库环境评价子模块

6.2.2.1 评价内容

数据库环境为评价必备项，其评价内容包括但不限于：

a）数据库应提供数据备份的功能，保证数据库在出现问题后，数据不丢失。

b）数据库应只允许内网 IP 连接和访问，保证网络的安全。

c）数据库应禁止直接从数据库中进行数据转存。并且为了防止数据泄漏，针对大数据量的结果集获取，应限制条数。

d）数据库宜具备数据库防火墙的功能，防止 SQL 注入、漏洞入侵、窃取备份等数据库攻击。

6.2.2.2 评价细则和结果

6.2.2.1 中 a）– c）的要求为评价必备要求，需同时满足 a）– c）的要求，则 6.2.2 评价结果为通过；否则为不通过。

6.2.2.1 中 d）的要求，为评价可选要求。

6.2.3 管理后台评价子模块

6.2.3.1 评价内容

管理后台为评价必备项，其评价内容包括但不限于：

a）软件系统管理员应限制用户对软件系统和管理后台的登录，通过 VPN 拨入或者通过特定的 IP 登录。

b）软件系统管理员应通过安全接入 VPN 来登录安全域内的主机和管理后台。

c）软件系统的后台管理的终端应设置屏幕保护程序、锁屏保护及口令保护功能。

d）软件系统的后台管理终端应禁用访客帐户。

e）软件系统管理员应对软件系统管理员的默认帐号进行重命名，并修改帐号的默认口令，修改后的口令应达到一定的口令强度。

f）软件系统的后台管理终端应制定相应的操作系统和必要应用程序的补丁管理计划，定期或不定期的维护。

g）软件系统的后台管理终端应仅限于执行后台管理的业务功能，终端上不得安装与该业务功能无关的应用程序，和来源不明的应用程序。

h）软件系统的后台管理终端应安装防病毒软件，防护范围包括但不限于病毒、特洛伊木马、蠕虫

病毒、间谍软件、广告软件和内核型病毒等恶意代码。

i）软件系统管理员宜定期进行病毒库更新及全盘杀毒，防病毒软件应设置有系统全盘扫描计划，并开启病毒库的自动更新。

j）对于软件系统的后台管理员，第三方软件提供商宜提供详尽全面的操作指导文档（如电子文档或纸质文档），就管理员如何以安全方式使用终端进行详细而全面的说明，便于管理员查询，覆盖内容应包括：屏幕保护、禁用访客账号、重命名默认账号、系统补丁、禁用其他应用程序、病毒防护、病毒库更新等。

k）第三方软件提供商对于在文档中对于影响后台管理安全性的操作（如修改口令、更换密钥），宜明确提示相关的风险。对于会影响软件系统正常运行的关键配置项和操作，文档中也应用警告标志标示，并明示其可能的影响。

6.2.3.2 评价细则和结果

6.2.3.1 中 a）– h）的要求为评价必备要求，需同时满足 a）– h）的要求，则 6.2.3 的评价结果为通过；否则为不通过。

6.2.3.1 中 i）-k）的要求，为评价可选要求。

6.2.4 主机系统配置评价子模块

6.2.4.1 评价内容

主机系统配置为评价必备项，其评价内容包括但不限于：

a）主机系统管理员应在安装完成后，对默认帐号进行重命名，并修改帐号的默认口令，修改后的口令应达到一定的口令强度。

b）主机系统管理员应在安装完成后，删除临时账号和测试账号。

c）数据库管理员在完成 RDS 数据库的初始化后，对 RDS 管理员的默认帐号进行重命名，并修改帐号的默认口令，修改后的口令应达到一定的口令强度。

d）数据库管理员应在安装完成后，删除 RDS 管理员的临时账号和测试账号。

e）对于部署在主机系统上的 FTP 应用程序，应不得开启匿名登录的功能，其 FTP 目录不得为操作系统的根目录，并同时不能在 Web 的目录下。

f）主机系统管理员宜进行安全边界的设置，使主机系统限定来自外界对边界内的主机访问，只开放少数且必须的服务端口。

6.2.4.2 评价细则和结果

6.2.4.1 中 a）– e）的要求为评价必备要求，需同时满足 a）– e）的要求，则 6.2.4 的评价结果为通过；否则为不通过。

6.2.4.1 中 f）的要求，为评价可选要求。

6.2.5 软件系统配置评价子模块

6.2.5.1 评价内容

软件系统配置为评价可选项，其评价内容包括但不限于：

a）软件系统宜检查并绑定访问者的昵称白名单和访问来源的 IP 白名单，并提供绑定白名单的列表。

b）软件系统宜提供黑名单的保护机制，通过黑名单来拦截非法的访问，黑名单的纬度包括 IP、用户账号和终端标识。

6.2.5.2 评价细则和结果

6.2.5.1 中 a）– b）的要求，为评价可选要求。

6.2.6 基础攻击防御评价子模块

6.2.6.1 评价内容

基础攻击防御为评价可选项，其评价内容包括但不限于：

a）软件系统所处运行环境宜能阻止伪造 MAC、伪造 IP、ARP 欺骗等攻击。

b）软件系统所处运行环境宜具备内外双向网络流量监控的能力。

c）软件系统所处运行环境宜具备抵抗内外部网络发起的 DDoS 攻击的能力，当监控到某个 IP 入流量超过一定阈值时，能自动进行 DDOS 攻击流量清洗。

d）软件系统所处运行环境宜具备脆弱性检测的能力，具备检测 Web 漏洞、检测弱口令的能力。

6.2.6.2 评价细则和结果

6.2.6.1 中 a）– d）的要求，为评价可选要求。

6.2.7 入侵检测评价子模块

6.2.7.1 评价内容

入侵检测为评价可选项，其评价内容包括但不限于：

a）宜具备对网站后门 Webshell 的查杀能力；

b）宜具备异地登录告警的功能；

c）宜具备口令暴力破解拦截能力；

d）宜具备异常系统账号检测并告警的能力。

6.2.7.2 评价细则和结果

6.2.7.1 中 a）– d）的要求，为评价可选要求。

6.2.8 Web 应用防护评价子模块

6.2.8.1 评价内容

Web 应用防护为评价条件项，仅适用于 Web 应用系统的情况，其评价内容包括但不限于：

a）宜具备 SQL 注入攻击防御能力；

b）宜具备 Webshell 上传拦截的能力；

c）宜具备对扫描行为进行及时发现并告警和阻断的能力；

d）宜具备针对 Web 用户的 IP 设置为白名单的能力；

e）宜具备代码执行攻击防护能力。

6.2.8.2 评价细则和结果

6.2.8.1 为评价条件项，仅适用于 Web 应用的情况。其中 a）– e）的要求，为评价可选要求。

6.2.9 模块评价结论

6.2.1～6.2.4 为评价必备项。需同时满足 7.2.1～7.2.4 的要求，则本模块的评价结果为通过；否则为不通过。

6.3 使用指导评价模块

6.3.1 系统提示评价子模块

6.3.1.1 评价内容

系统提示为评价必备项，其评价内容包括但不限于：

a）软件系统应在合适的界面提示用户口令被盗的风险、使用默认口令的风险。

b）软件系统应在合适的界面提示用户使用访客账号的风险；

c）软件系统应在合适的界面提示用户使用默认账号的风险；

d）软件系统宜在合适的界面提示用户不及时安装补丁的风险；

e）软件系统宜在合适的界面提示用户病毒感染的风险。

6.3.1.2 评价细则和结果

6.3.1.1 中 a）– c）的要求为评价必备要求，需同时满足 a）– c）的要求，则 6.3.1 的评价结果为通过；否则为不通过。

6.3.1.1 中 d）– e）的要求，为评审可选要求。

6.3.2 用户手册评价子模块

6.3.2.1 评价内容

用户手册为评价可选项，其评价内容包括但不限于：

a）对于软件系统的商家用户，第三方软件提供商宜提供详尽全面的操作指导文档（如帮助文件和纸质文档），便于用户查询，用于指导用户使用或配置第三方软件提供商提供的软件系统的安全功能。

b）第三方软件提供商在文档中应写明软件系统中所提供的安全功能介绍，对于用户影响系统安全性的操作（如修改口令、配置权限等），在操作时应明确提示相关的风险；对于会影响软件系统正常运行的关键配置项和操作，文档中也应用警告标志标示，并明示其可能的影响。

c）第三方软件提供商宜告知用户对口令进行安全保护，包括：检验口令强度并提示用户设置强口令、设定口令修改默认时期，到期提示修改口令、口令不得存储在本地；

d）第三方软件提供商宜告知用户终端的安全使用需要注意的不安全的日常使用行为和基本安全建议：包括：屏保的安全设置、操作系统的及时升级、防病毒软件的有效安装、主机防火墙的正确配置、应用软件的下载与安装；

e）第三方软件提供商宜告知用户移动终端的安全使用，包括：设置屏幕解锁口令或图案、防病毒软件的有效安装等；

f）第三方软件提供商宜告知用户移动介质的安全管理，包括：U 盾、U 盘、移动硬盘的安全存放，设置用户口令等；

g）第三方软件提供商宜告知用户互联网的安全访问的注意事项，包括但不限于：无线上网、浏览上网、电子邮件、社交网络、即时通信、网上交易等方面；

h）第三方软件提供商宜告知用户防止基于社会工程的欺诈，包括但不限于：基于人：物理的非授权访问；基于电话：呼叫者电话的欺骗；基于电子邮件：钓鱼攻击、Email 地址欺骗；基于即时通信软件：通过 QQ、微信等的欺骗。

6.3.2.2 评价细则和结果

6.3.2.1 中 a）-h）的要求，为评价可选要求。

6.3.3 模块评价结论

6.3.1 为评价必备项。如果满足 6.3.1 的要求，则本模块的评价结果为通过；否则为不通过。

6.4 经营管理评价模块

6.4.1 资质要求评价子模块

6.4.1.1 评价内容

资质要求为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商应拥有真实、有效的《企业法人营业执照》、《组织机构代码证》和《税务登记证》；

b）第三方软件提供商应通过电子商务平台的实名认证；

c）第三方软件提供商应具有开发者身份，应拥有独立的运营和技术团队；

d）第三方软件提供商应登记其服务信息；

e）第三方软件提供商应与电子商务平台签署入驻协议，并应缴纳入驻保证金；

f）第三方软件提供商应拥有对接电子商务平台的能力；

g）第三方软件提供商应按需配合电子商务开放平台部署安全保障的工具和软件。

6.4.1.2 评价细则和结果

6.4.1.1中a）~g）为评价必备要求，需同时满足a）~g），则6.4.1的评价结果为通过，否则为不通过。

6.4.2 经营要求评价子模块

6.4.2.1 评价内容

经营要求为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商在电子商务开放平台所申请的APPKEY不得转让给他人使用；

b）第三方软件提供商不得在电子商务开放平台接入纯娱乐、游戏类的软件和应用；

c）第三方软件提供商不得未经用户授权，获取用户隐私数据（如地址、电话、购买记录等）；

d）第三方软件提供商发布的应用应具备完整的服务协议，应用详情的描述应详细清楚，无不良内容，无虚假广告；

e）第三方软件提供商发布的应用不允许获取店铺访客标识；

f）第三方软件提供商发布的应用功能未经用户授权和电子商务平台官方允许，不能主动骚扰买家；

g）第三方软件提供商发布的应用之间不得互相抄袭、恶意竞争，主流程基本一致等；

h）同一第三方软件提供商不允许重复提交相同功能应用上线。

6.4.2.2 评价细则和结果

6.4.2.1中a）~h）为评价必备要求，需同时满足a）~h），则6.4.2的评价结果为通过，否则为不通过。

6.4.3 服务管理评价子模块

6.4.3.1 评价内容

服务管理为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商应按照服务承诺的约定向商家提供服务；

b）第三方软件提供商与商家就其已发布的应用达成购买意向后，不得引导商家在后服务市场之外进行交易，不得以任何手段逃避后服务市场线上交易流程；

c）第三方软件提供商应当诚实守信，不得以恶意评价、恶意投诉、诋毁、虚假订购等方式进行不正当竞争。

6.4.3.2 评价细则和结果

6.4.3.1中a）~c）为评价必备要求，需同时满足a）~c），则6.4.3的评价结果为通过，否则为不通过。

6.5 运维管理评价模块

6.5.1 运维保障评价子模块

6.5.1.1 评价内容

运维保障为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商应将相关人员（开发、测试、运维、管理等）的安全职责到电子商务平台进行报备。

b）第三方软件提供商应指定专职的安全负责人作为与电子商务平台安全团队的安全接口人，定期保持安全联络和沟通。

c）第三方软件提供商的相关人员（开发、测试、运维、管理等）应签订数据安全责任书。

d）第三方软件提供商应至少每年执行一次安全自查，并在环境发生重大变更时（例如收购、合并、迁址等）不定期地对线上软件系统执行安全评估，根据安全评估执行相应操作（如补丁管理、软件升级、系统加固等），并将该安全评估结果和安全整改情况通报给评估方。

e）第三方软件提供商宜对相关人员（开发、测试、运维、管理等）每年进行至少一次的安全意识教育，并对对安全教育和培训的情况和结果进行记录并归档保存。

f）第三方软件提供商宜建立和文档化其必要的安全制度和操作流程，并要求相关人员（开发、测试、运维、管理等）每年至少一次确认自己已经阅读并了解公司的安全要求和制度流程。

g）软件系统（含前后台）宜附有详细的列表，列明软件系统所必须使用的系统服务和通信端口，且应仅开放软件系统运行所必须的系统服务和通信端口。

6.5.1.2 评价细则和结果

6.5.1.1中a)-d)为评价必备要求，需同时满足a）~d）的要求，则6.5.1的评价结果为通过，否则为不通过。

6.5.1.1中e)-g)为评价可选要求。

6.5.2 漏洞管理评价子模块

6.5.2.1 评价内容

漏洞管理为评价必备项，其评价内容包括但不限于：

a）在软件系统上线运行前，第三方软件提供商应对前后台系统执行漏洞扫描，保证上线软件系统不存在漏洞，并将扫描结果提交给电子商务平台。

b）第三方软件提供商应对漏洞进行跟踪管理，并及时进行修复。

c）第三方软件提供商发现自研软件系统、操作系统及所用到的相关第三方应用程序/代码组件中

存在安全漏洞时，应及时向电子商务平台通报。任何情况下，均不应在生产环境下尝试验证弱点。

d）第三方软件提供商宜提供给电子商务平台渗透测试报告，所评测应用应通过电子商务开放平台上线审核安全测试/渗透测试。上线应用不可存在如下漏洞：命令执行漏洞、用户信息泄露、代码执行漏洞、上传漏洞、SQL 注入、权限漏洞、跨站脚本漏洞、CSRF 漏洞、URL 跳转漏洞。该测试需由电子商务平台或电子商务平台授权的独立第三方独立进行。针对 BS 架构及有 WEB 服务的 CS 架构，电子商务平台安全工程师可以帮助进行针对系统的渗透测试。

6.5.2.2 评价细则和结果

6.5.2.1中a）-c）的要求为评价必备要求，需同时满足a）~c）的要求，则6.5.1的评价结果为通过，否则为不通过。

6.5.2.1中d）的要求为评价可选要求。

6.5.3 变更管理评价子模块

6.5.3.1 评价内容

变更管理为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商应识别软件系统开发和运维中的主要变更需求，并制定相关的变更方案。

b）第三方软件提供商宜建立相关的变更流程和审批机制。

c）当相关系统变更时，第三方软件提供商宜向所有相关人员（开发、测试、运维、管理等）通告；实施变更时，必须进行记录且应妥善保存这些记录。

6.5.3.2 评价细则和结果

6.5.3.1的a）为评价必备要求，需满足6.5.3.1中a）的要求，则6.5.3的评价结果为通过，否则为不通过。

6.5.3.1的b）-c）为评价可选要求。

6.5.4 应急响应评价子模块

6.5.4.1 评价内容

应急响应为评价必备项，其评价内容包括但不限于：

a）第三方软件提供商应制定安全事件报告和处置管理制度，明确安全事件的现场处理、事件报告和后期恢复的角色职能及处理流程。

b）第三方软件提供商应建立负责线上应急响应的团队，明确安全事件响应的角色和责任人员/组织。

c）第三方软件提供商宜制定有 7*24 应急响应计划（突发安全事件预案），并定期演练。

d）第三方软件提供商宜监控相关软件程序的安全漏洞和威胁情报，及时修复软件系统及相关支撑系统的安全漏洞。

e）第三方软件提供商宜记录和保存所有报告中的安全弱点和可疑事件，分析事件原因，监督事态发展，并采取措施避免安全事件发生。

6.5.4.2 评价细则和结果

6.5.4.1中a）－b）的要求为评价必备要求，需满足6.5.4.1中a）-b）的要求，则6.5.4的评价结果为通过，否则为不通过。

6.5.4.1的c）-e）为评价可选要求。

6.5.5 文档管理评价子模块

6.5.5.1 评价内容

文档管理要求为评价可选项，其评价内容包括但不限于：

a）第三方软件提供商宜针对软件系统的不同版本，宜交付规范的软件系统设计文档给电子商务平台，内容包含：范围、目标、设计约束、威胁分析、设计需求、设计原则、系统架构图、系统流程及功能模块。

b）第三方软件提供商宜提交给电子商务平台全面详尽的安全功能设计规格文档，阐明系统各安全功能的基本实现原理及相关设计规格，内容涵盖威胁分析、安全需求、设计原理、及支持的规格(如密钥的算法、密钥长度，通信加密协议及密码算法、口令强度等）；

c）第三方软件提供商的软件系统开发过程宜包含有安全活动的实施，如安全需求分析（威胁分析)、安全设计(安全架构及安全功能设计)、安全开发(安全编码、静态代码扫描、及人工代码检视)、安全测试（安全功能测试及渗透测试）；对于小型的版本修订（即功能改进），第三方软件提供商应提供详尽的版本修订说明（含修订的安全影响分析）；对于大规模的版本修订，软件系统应提前通报电子商务平台以启动重新的安全评测。

6.5.5.2 评价细则和结果

6.5.5.1中a）~e）的要求为评价可选要求。

6.5.6 模块评价结论

6.5.1 ~ 6.5.4 为评价必备项，如果 7.5.1 ~ 7.5.4 评价子模块评价结论全部为通过，则本模块的评价结果为通过。

6.6 评价结论

6.1 - 6.5 的五个评价模块为评价必备模块，如果 6.1 - 6.5 的评价结论全部为通过，则对第三方软件提供商的评价结果为合格。

7 评价报告

评价报告应由基本信息、第三方软件提供商概要、评价内容与结果、差距分析、证明材料和审核文件、评价结论六部分组成。

基本信息应包括第三方软件提供商名称、被评价第三方软件提供商地址、评价日期、评价人员、评价结果等信息。

提供商概要应包含被评价的第三方软件提供商类型等基础信息以及财务状况等能够说明其状况的信息。

评价内容和结果应包括功能实现、环境部署、使用指导、经营管理和运维管理五个评价模块的评价内容、证据描述和对应的结果。

差距分析应对第三方软件提供商评价过程中发现的，对审核要求而言存在的差距进行说明，并提出需改进的方面。

评价结论应给出“合格”或“不合格”的最终结论。

8 扩展原则与方法

本标准使用过程中，评价模块、评价子模块和评价内容可根据不同类别第三方软件提供商的业务特点和不同的评价需要进行扩展，扩展内容（评价模块、子模块和评价内容）不应与已有内容冲突。

扩展方法如下：

——增加评价模块，应相应增加本模块下的评价子模块和评价内容；

——增加现有模块下的子模块，应相应增加本子模块下的评价内容；

——增加子模块下评价内容；

——增加评价模块、子模块和评价内容后，评价规则应做适当调整，但不应与现有评价规则冲突。

参考文献

[1] GB/T 22239-2008 信息系统安全等级保护基本要求
[2] YD/T 2407-2013 移动智能终端安全能力技术要求
[3] GBT 20271-2006 信息系统通用安全技术要求
[4] GB/T 18811 电子商务基本术语
[5] GB/T 25069-2010　信息安全技术 术语