ICS 35.240.60
L 67

DB33

浙　江　省　地　方　标　准

DB33/T 978—2015

电子商务平台安全管理规范

Security management specifications for electronic commerce platform

2015－07－16 发布　　2015－08－16 实施

浙江省质量技术监督局　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由浙江省商务厅提出并归口。

本标准主要起草单位：淘宝(中国)软件有限公司、阿里巴巴（中国）有限公司、浙江省标准化研究院、中国计量学院。

本标准主要起草人：谢俊军、颜鹰、沈锡镛、李宁、孙艳、刘洛丹、方强、杨军。

引　言

电子商务平台是电子商务发展的载体，其信息的安全性是电子商务健康发展的基础。电子商务发展越来越快，今后一段时期，其发展趋势，仍将以超越传统产业的速度发展，而作为电子商务的重要支撑平台，其安全保障水平已日益成为妨碍电子商务发展的最大障碍。

鉴于目前国家还没有这方面的标准，根据《商务部“十二五”电子商务发展指导意见》的精神，参考SB/T 10519-2009《网络交易服务规范》、GB/T 18769-2003《大宗商品电子交易规范》，结合浙江省电子商务平台建设实际，浙江省商务厅组织制定了本标准。

电子商务平台安全管理规范

1 范围

本标准规定了电子商务平台在安全运营管理中应满足的基本要求、人员和机构管理、应急预案和应急响应、安全运营管理的工作流程方面的要求。

本标准适用于全省各地提供互联网电子商务平台服务的安全运营管理。

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，仅所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/T 18811 电子商务基本术语

GB/Z 20986 信息安全事件分类分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子商务

以电子形式进行的商务活动。它在供应商、消费者、政府机构和其他业务伙伴之间通过任一电子方式实现标准化的非结构化或结构化的业务信息的共享，以管理和执行商业、行政和消费活动中的交易。

3.2

电子商务平台

即是一个为企业或个人提供网上交易洽谈的平台。是建立在Internet进行网上商务活动的虚拟网络空间和保障商务运营的管理环境；是协调、整合信息流、物质流、资金流的重要场所。企业、商家可利用电子商务平台提供的网络基础设施、支付平台、安全平台、管理平台等共享资源开展自己的商业活动。

3.3

信息安全

数据处理系统而采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、泄露。

3.4

安全策略

主要指为信息系统安全运营管理制定的行动方针、路线、工作方式、指导原则或程序。

3.5

用户

用注册的ID与用户信息来判断的使用电子商务交易平台的机构或自然人。

3.6

商户

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。

3.7

网络交易

发生在企业（或其他组织机构）之间、企业（或其他组织机构）与消费者之间、消费者之间通过网络手段缔结的商品或服务交易。

3.8

二次验证

在用户注册或登录后进行一些重要或敏感业务操作时，通过除密码之外的如验证码、手机短信、安全问题、数字证书等对用户进行第二次校验的方式。

3.9

数字证书

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.10

加密

通过密码系统把明文变换为不可懂的形式。

3.11

电子商务安全事件

电子商务平台因故意、过失或非人为原因引起的信息和服务遭到破坏，所造成的事件，也包括电子商务业务应用中出现的欺诈、盗号、违禁等恶意行为。

3.12

电子商务安全运营管理部门

在组织机构中根据业务的规模、结构建立的独立负责电子商务安全运营管理的小组或部门，以下简称安全运营管理机构。

3.13

开源情报

从公开可用的资源中，如极端分子的网站，收集信息，对这些信息加以分析生成情报。

3.14

计算机网络嗅探

秘密潜入一套网络或信息系统，并获取私人信息。

4 基本要求

4.1 应遵守国家有关法律、行政法规及规章等相关规定。
4.2 应遵守国家制定的相关的网络技术规范和安全规范。
4.3 应遵循诚信自律的原则。
4.4 应遵循国家有关知识产权的法律法规，不应侵害他人的专利权、商标权、著作权等，并有权利和义务保护有关知识产权。
4.5 应禁止通过网络从事法律法规和国家其他相关规定禁止的违法犯罪行为，如赌博、洗钱、传销以及贩卖枪支、毒品、禁药、盗版软件、淫秽商品和服务等。
4.6 网络交易不应提供和买卖未经审批的需要相应资质的商品或服务，应遵循国家规定开展经营活动。

5 机构和人员管理

5.1 安全运营管理机构

5.1.1 基本要求

5.1.1.1 在组织机构中应根据实际的规模、结构建立一个独立的负责电子商务平台安全运营管理机构。
5.1.1.2 最高管理层中应有一人分管安全运营管理机构的工作。

5.1.2 安全运营管理机构的职责

安全运营管理机构的职责包括但不限于：

a) 应根据国家和行业有关电子商务平台安全的政策、法律和法规，批准平台业务的安全策略和规则规划；
b) 应协调单位内部其它机构在平台安全工作中的职责，领导安全工作的实施；
c) 应监督安全措施的执行，并对重要安全事件的处理进行决策；
d) 指导和检查应急处理小组等下设机构的各项工作；
e) 建设和完善平台安全的集中控管的组织体系和管理机制；
f) 收集、分析、预警最新的电子商务平台安全事件和应对方案。

5.1.3 与组织内其他部门的关系

5.1.3.1 安全运营管理机构的管理者及成员应具有某种等级授权。
5.1.3.2 根据业务的安全风险，在安全事件管理策略和方案中，应详细说明安全运营管理机构在相应风险点部署的安全措施。

5.1.4 与外部机构的关系

安全运营管理机构应与公司外部机构建立沟通渠道，完善沟通机制，公司外部机构可能包括但不限于以下：

a) 签订合同的外部支持人员；
b) 外部组织的相关安全运营管理机构或小组；
c) 执法机关；
d) 其他应急处理机构；
e) 相关的政府部门；
f) 公共关系官员和/或媒体记者；
g) 安全业务伙伴；
h) 用户。

5.2 人员管理

5.2.1 应配备专职安全运营管理人员。

5.2.2 应登记安全运营管理机构成员及其备用人员的姓名和联系方式，一些必要的细节应清晰记入相关文件中，包括规程文件和报告单。

5.2.3 应统一管理关键岗位的安全操作人员。关键岗位的安全操作人员要求如下：

a) 允许一人多岗，但安全操作人员不宜由其他关键岗位人员兼任；
b) 关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识。

5.2.4 人员录用的基本要求如下：

a) 对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握安全运营管理基本知识；
b) 除劳动合同外，应签订安全保密协议。

5.2.5 定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，可作为人员是否适合当前岗位的参考。

5.2.6 对咨询人员、临时性的短期职位人员，以及辅助人员和外部服务人员等第三方人员的管理要求如下：

a) 签署包括不同安全责任的合同书或保密协议；
b) 规定各类人员的业务操作权限，离岗前必须及时转移或关闭相关权限；
c) 第三方人员必须进行逻辑访问时，应划定范围并经过负责人批准。

5.2.7 安全运营管理人员的退出与离职规定如下：

a) 人员离职之后仍对其在任职期间接触、知悉的属于本单位或者虽属于第三方但本单位承诺或负有保密义务的秘密信息，承担如同任职期间一样的保密义务和不擅自使用的义务，直到该秘密信息成为公开信息，而无论离职人员因何种原因离职；
b) 离职人员因职务上的需要持有或保管的一切记录着本单位秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器以及其他任何形式的载体，均归本单位所有，而无论这些秘密信息有无商业上的价值；
c) 离职人员应当于离职时，或者于本单位提出请求时，返还全都属于本单位的财物，包括记载着本单位秘密信息的一切载体。若记录着秘密信息载体是由离职人员自备的，则视为离职人员已同意将这些载体物的所有权转让给本单位，本单位应当在离职人员返还这些载体时，给予离职人员相当于载体本身价值的经验补偿；但秘密信息可以从载体上消除或复制出来时，可以由本单位将秘密信息复制到本单位享有所有权的其他载体上，并把原载体上的秘密信息消除；

d) 离职人员离职时，应将工作时使用的电脑、U 盘及其他一切存储设备中关于工作相关或与本单位有利益关系的信息、文件等内容交接给本单位相关人员，不得在离职后以任何形式带走相关信息。

5.3 教育和培训

5.3.1 应让电子商务平台相关员工了解电子商务平台安全的重要性，应掌握的平台安全基本知识和技能等。

5.3.2 应制定并实施安全教育和培训计划，培养电子商务平台各类人员安全意识，并提供对安全政策和操作规程的认知教育和训练等。

5.3.3 安全意识培训，包括但不限于：

a) 积极宣传安全运营管理的作用，作为总体信息安全意识和培训计划的一部分；
b) 安全意识计划及相关材料应该对所有人员可用，包括新员工，以及相关第三方用户和合作伙伴；
c) 根据安全事件类型、频率及其与安全运营管理方案交互的重要程度的不同，直接参与事件管理的各组成员需要不同类型不同级别的培训；
d) 在有些情况下，可将有关安全事件管理的安全意识教育细节包括在其他培训计划，如面向员工的培训计划或一般性的总体安全意识计划。

6 应急预案和应急响应

6.1 概述

当发生安全事件时，需要根据安全事件的严重程度，按照相应的处理规程及时响应，并随时跟踪新的安全事件的发生。

6.2 电子商务平台安全事件

根据GB/Z 20986的相关规定，在电子商务平台运营安全上出现的常见安全事件主要是网络攻击事件、信息破坏事件、信息内容安全事件，包括但不限于：

——钓鱼木马；
——账户被盗；
——欺诈；
——垃圾账户注册与垃圾信息传播；
——违反知识产权商品发布；
——用户隐私信息的窃取和篡改；
——恶意信息传播。

6.3 安全事件评估价值判断与衡量尺度

6.3.1 根据 GB/Z 20986 相关的规定，信息安全事件的分级主要考虑三个要素：信息系统的重要程度、系统损失和社会影响。

6.3.2 电子商务平台信息系统的重要程度划分标准：

a) 特别重要系统:影响平台交易与支付的信息系统；
b) 重要信息系统：用户信息记录与操作相关系统；
c) 一般信息系统：其它辅助管理系统。

6.3.3 系统损失划分要求如下：

a) 特别严重系统损失：信息或系统涉及资金损失，信息未授权泄露和修改、抵赖以及不可用或遭受破坏且持续造成用户资金损失或因行动迟缓或没有行动造成网络欺诈导致大量用户网上资金损失；特别重要系统不可用或遭受破坏造成大面积长时间中断平台的服务运行；
b) 严重系统损失：信息或系统涉及资金损失，信息未授权泄露和修改、抵赖以及不可用或遭受破坏且造成用户资金损失，因行动迟缓或没有行动造成网络欺诈导致用户网上资金损失；重要系统不可用或遭受破坏造成局部中断平台的服务运行；
c) 较大系统损失：信息或系统故障，明显影响系统效率，使重要信息系统或一般信息系统业务处 理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，但系统是可恢复的；
d) 较小系统损失：信息或系统故障，影响系统效率，使一般信息系统受到影响，但系统是可恢复的。

6.3.4 社会影响划分要求如下：

a) 主要根据个人信息保护、法律法规义务、平台商业规则等三方面影响到的用户群体数，划分为重大社会影响、较大社会影响、一般社会影响，用户群体的数值范围可根据平台规模制定，一般如影响到平台 10%的用户，则为重大社会影响；影响到平台 5%的用户则为较大社会影响；影响到平台 1%以内用户为一般社会影响；
b) 个人信息保护。根据我国个人信息保护相关法律法规以及国家标准的规定，平台应按相关要求，被授权采集和使用个人信息，明确个人信息使用范围，并对信息施以保护，以防泄露。
c) 法律法规义务。平台持有和处理的信息应遵从国家相关法律法规规定的义务，可能涉及违禁、违反知识产权等信息的发布，无论有意还是无意，都有可能导致对相关组织或个人采取法律诉讼或行政处罚的行动；
d) 平台商业规则。信息如果泄露的话，可能会引起公众反应，造成该规则无法实施或恶劣影响；此外，对承诺的否认也可能会对组织带来负面后果。

6.4 事件分级

6.4.1 概述

参见GB/Z 20986，结合电子商务安全事件及价值判断尺度，电子商务安全事件分级见6.4.2、6.4.3、6.4.4和6.4.5。

6.4.2 特别重大事件

特别重大事件是指能够导致特别严重影响或破坏的安全事件，包括但不限于：

a) 会使特别重要信息系统遭受特别严重的系统损失；
b) 产生重大的社会影响。

6.4.3 重大事件

重大事件是指能够导致严重影响或破坏的安全事件，包括但不限于：

a) 会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失；
b) 产生较大的社会影响。

6.4.4 较大事件

较大事件是指能够导致较严重影响或破坏的安全事件，包括以下情况：

a) 会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信 息信息系统遭受特别严重的系统损失；
b) 产生一般社会影响。

6.4.5 一般事件

一般事件是指不满足以上条件的信息安全事件，包括会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信 息系统遭受严重或严重以下级别的系统损失。

6.5 应急响应预案

根据以下事件等级，应启动应急响应机制：

a) 一般事件：应急响应行动首先是对业务系统的监控加强。应在适当的地方增加监视防护措施，并进行专项数据分析，以帮助发现具有安全事件症状的异常和可疑事态。这样的监视还可更深刻地揭露安全事件，同时确定还有哪些系统受到危及。
b) 较大事件：应启动相关业务连续性计划中特定的响应。这样的应急响应涉及系统的所有方面，不仅包括那些与 IT 直接相关的方面，还应包括关键业务功能的维护和以后的恢复。另外在产生社会影响情况下，当突发事件被确定属实时，需要同时通知部门人员(不在安全运营管理机构的正常联系范围内)和外部人员(包括新闻界)。这种情况可能会发生在事件处理的各个阶段。
c) 重大事件：在启动相关业务连续性计划的同时，需要准备一些材料，并根据安全事件的具体情况迅速通报给新闻界和/或其他媒体。任何有关安全事件的消息在发布给新闻界时，应遵照组织相关公关发布策略。需要发布的消息应由相关方审查，其中包括组织高级管理层、公共关系协调员和信息安全人员。
d) 特别重大事件：除以上措施外，必须将事情上报给高级管理层，以对处理安全事件的建议行动做出决定，并为了对事件做出进一步评估以确定需要采取什么行动。

7 安全运营管理工作流程

7.1 工作流程四个阶段

电子商务平台安全运营管理建设流程可被划分为四个阶段：规划；运行；检查；改进。

7.2 规划

根据风险评估结果、法律法规要求、组织业务运作自身需要来规划安全运营管理方案：

——安全运营管理机构下设分支团队，承担安全规划与建设职能；
——收集有关风险及安全信息，制订相对应标准、流程；
——使用组织内认可的评估体系，获得其它部门与管理层承诺；
——取得安全技术方合作，规划相关安全系统，并开发建设；
——把安全相关标准、规定以及安全产品使用等安全知识对相关人员进行培训；
——建立安全宣传平台和渠道，对用户进行安全宣传，提升用户安全意识。

7.3 运行

运行阶段应满足如下要求：

——安全运营管理机构下设分支团队，执行安全运营管理方案规定的内容，并承担安全系统运行与策略配置的职能；

——确定安全事件是否处于可控制状态；
——重视情报的收集，为策略制订提供足够依据；
——如果安全事件不在控制下，启动应急响应机制；
——对安全事件根据事件等级的应急响应流程，组建虚拟小组解决问题。

7.4 检查

检查阶段应满足如下要求：
——安全运营管理机构下设分支团队，承担安全检查评估职能；
——与其它部门协同，对系统安全事件进行评估，以确定安全策略的有效性；
——按要求上报便于进一步评估和/或决策；
——确保所有活动被恰当记录，以便于日后分析；记录内容包含且不限于：用户登录和退出时间、主叫号码、账号、互联网地址或域名、系统维护日志等；
——对安全风险进行分析，以确保安全系统覆盖所有的风险点。

7.5 改进

改进阶段应满足如下要求：
——总结安全事件的经验教训并形成文件；
——根据所得的经验教训，审核和确定信息安全的改进；
——审核相关过程和规程在响应、评估和恢复每个安全事件时的效率，根据所总结的经验教训，确定电子商务安全运营管理方案在总体上需要改进的地方；
——监控安全数据的异常情况，并审核其原因，形成报表，传递到相关人员，形成改进建议；
——循环改进整体的安全，实施新的和 / 或经过改进的防护措施。

8 规划

8.1 总则

根据风险评估结果、法律法规要求、组织业务运作自身需要来规划电子商务安全运营管理方案，此阶段应着重于：

a) 建立安全运营管理机构；
b) 建立电子商务安全运营管理方案；
c) 建立安全审计规范；
d) 安全技术支持：规划和开发安全信息系统；
e) 安全培训。

8.2 安全运营管理机构

安全运营管理机构的建立要求与职能，按 5.1 给出的要求。

8.3 安全运营管理方案

8.3.1 方案内容

方案包含且不限于以下内容：

a) 安全评估依据；
b) 安全事件分类；

c） 信息系统操作访问权限的管理规范。

以上相关内容及其它规定应形成正式文件，并获得相关部门及管理层的承诺。

8.3.2 方案适用人群与覆盖范围

方案适用于组织全体员工且不限于全体员工的其它相关人员，方案应覆盖平台所有可能有安全风险的系统以及外部引发平台安全风险的相关因素。包括但不限于：

——发现和报告安全事件，可以是组织内任何员工，包括正式员工和外包人员；

——评估、响应以及安全事件解决后必要的经验教训以及总结、改进、修订安全运营管理方案的工作中包括的成员、管理层、公关部人员和法律代表等；

——应该考虑任何平台用户，以及第三方组织、政府和合作伙伴。

8.3.3 安全评估依据

采用对组织、信息造成的负面后果来评估安全事件，包括但不限于：

——未授权泄露信息；

——未授权修改信息；

——抵赖的信息；

——信息和/或服务不可用；

——信息和/或服务遭受破坏；

——信息被窃取；

通过上列分类，定义事态 / 事件严重性衡量尺度的细节，为安全事件分级，并规定相应操作规程，符合6.5给出的要求。

8.3.4 权限管理要求

应建立对访问用户信息与信息系统操作的权限管理制度，统一全平台的权限管理；

——不得非法获得权限，不得越权使用、滥用、妨碍、窃取组织及其他用户的信息；

——在安全事件管理策略和方案中，需临时授权时，必须详细说明并审批。

8.4 安全管理审计要求

8.4.1 安全运营管理人员审计

安全运营人员需经过安全培训方能上岗。审核人员分工与权限授权是否一致。

8.4.2 信息保存规范

重要信息系统与特别重要信息系统，需保留供审计日志，包含且不限于：

a） 保留用户注册信息以及修改历史记录；

b） 保留用户登录（登录时间、登录 IP）、信息发布等日志信息；

c） 保留交易列表、交互信息及交互对象用户列表；

d） 用户注册信息、登录长期保存，其他所有日志信息（包括已删除的信息）应保留一年以上。

8.4.3 信息发布管理

对平台上所发布信息落实7×24小时信息巡查制度，不得制作、复制、发布、传播法律法规禁止的任何内容。

8.4.4 信息加密、传输、存储安全运营管理

信息加密、传输、存储安全运营管理包括：

——明确定义使用信息的安全级别；

——根据安全级别对信息进行不同强度的加密；

——对相应安全级别数据进行加密传输；

——对相应安全级别数据进行加密存储；

——保障密钥的安全性。

8.4.5 规程有关要求

8.4.5.1 在电子商务安全运营管理方案执行过程中，必须形成正式文件并经过检查的规程可供使用。

8.4.5.2 每个规程文件应指明其使用和管理的负责人员。

8.4.5.3 操作规程的内容取决于许多准则，可能与某一特定事件类型或实际上与某一类型安全产品相关联。

8.4.5.4 每个操作规程都应清楚注明需要采取哪些步骤以及由谁执行。

8.5 安全技术支持

8.5.1 使用电子安全事件数据库和技术手段快速建立和更新数据库，分析其中的信息，以便于对事件做出响应(并不排除有要求或使用手工记录的情况)。

8.5.2 快速获得安全事件和事件报告。

8.5.3 对已评估的风险采取适当的预防措施，以确保系统、服务和网络遭受攻击时仍然可用。

8.5.4 根据已得到评估的风险采取措施，利用加密来确保数据的完整性和防泄漏。

8.5.5 便于对已收集信息的归档和安全保存。

8.5.6 所有技术手段都应认真挑选、正确实施和定期测试。

8.6 安全培训

按5.3给出的要求。

9 实施

9.1 总则

实施是对安全事件的立即响应和长期响应，所有的安全事件都需要提早分析其潜在负面影响，包括短期和长期影响。此外，对完全不可预见的安全事件作出某些响应是必要的。

策略与运行，包括：

——策略制订；

——情报收集；

——应急响应。

9.2 策略制订原则

策略制定原则包括：

——确保各项策略的一致性；

——做好安全事件紧急处理预案，确保对突发安全事件作出及时、全面、系统和有效的处理；

——明确指定负责授权和/或执行某些关键行动的人员；

——策略应要求建立适当的审批机制，特别是会造成较大影响的处罚策略。

9.3 安全事件管理策略制订内容

9.3.1 按照制订的安全运营管理方案，监控平台上重点安全事件，如平台上账户安全、商品与信息发布安全的问题。

9.3.2 安全事件管理策略是根据电子商务平台实际出现的问题有针对性的制订；并随时跟踪新的安全事件的发生，而及时响应。

例如：账户安全、商品与信息发布安全的策略规范；可参见附录 A 和附录 B。

9.4 安全情报收集

9.4.1 在网络空间内收集情报包括开源情报、传统的信号情报和计算机网络嗅探等类型。

9.4.2 情报系统的建设包含人工智能及识别技术，通过一个基于知识库的主动式专题搜索引擎完成专题情报的收集，并过滤与分类收集信息。

9.5 应急响应

如果确定安全事件不在策略规定范围内，应启动应急响应机制。具体规程见6.5。

10 检查

10.1 概述

检查评估环节要求安全运营管理机构与其它部门协同合作，检查安全策略执行情况，是确保对内部、外部风险策略进行有效覆盖的重要环节。在检查评估阶段，应与组织各部门达成共识，并建立沟通机制。通过对风险的评估，来决定如何优化系统或策略。

10.2 关键过程

发现和报告电子商务平台系统开发、上线、运行的安全状况；开发、上线应建立系统提交机制，安全运营管理机构根据安全运行管理方案，启动下列检查评估流程：

——任何平台上运行的系统都应该设置安全监控点，在系统开发阶段，收集有关数据访问风险的信息，在系统上线测试阶段，收集业务逻辑风险信息；根据所需访问的安全级别、业务逻辑风险程度，由安全运营管理机构与相应部门进行风险评估，来确定部署的安全措施、策略是否有效；

——确保对流程中所有相关信息进行收集和安全保存，同时确保系统安全状态得到持续监控，以供审核所用。

10.3 发现和报告

系统的开发与上线，触发安全事件，发现的安全人员要负责启动下列检查评估流程：

——对已经运行的系统安全状态，可通过监控数据发现，如安全监控系统在预设参数被激发的情况下发出的警报，发现的人员可根据规程启动安全评估流程；

——在大部分情况下，电子商务安全事件来自于偶然发现（包括系统漏洞），发现的人员可以是组织内任何一名员工。该员工应遵照相关规程，并使用电子商务安全运营管理方案规定的安全事件响应流程在第一时间把安全事件报告给评估团队；

——安全事件的响应，要保证准确性和及时性。如报告人对事件等级确定没有信心，在提交时应加上适当的标记，以便后来沟通时修改。

10.4 首次检查评估和安全运营策略优化决策

平台系统在首次触发安全事件，安全检查评估人员应从开发得到详细说明，并从其他使用业务部门进一步收集可用的任何必要和已知信息。随后，与相应系统开发和使用部门共同进行如下评估，以确定这个系统安全策略的有效性：

a) 如果确定该系统暂时不需要优化安全措施，或者优化安全措施理由不充分，可暂时只监控系统的运行；

b) 如果确定系统存在安全隐患，标准来源于安全事件分级划分以及以前类似系统已经出现的安全事件；则需要优化相适应的安全策略。而且安全评估成员可以进行进一步评估，如果 当一个系统确定为有重大安全隐患(安全事件等级为重大事件及以上)时，应上报高层管理。如果出现危机情况，应该及时宣布，但最可能的情况是，必须对系统的安全事件进行进一步检查评估和采取措施，直至有改进方案或者替代方案；

c) 无论决定下一步要采取什么行动，安全评估组成员都应尽可能地将信息收集完整。

10.5 再度评估和安全策略优化调整

引发安全事件，且安全事件等级为重大事件及以上时，需进行再度安全评估：

a) 进行再度评估以及对是否调整安全策略是安全运营管理机构的职责，接收报告的人员应：
——签收由填写完成的安全事件报告单；
——向系统使用部门寻求任何必要的澄清说明；
——评审报告内容；
——从其他地方进一步收集可能用的任何必要和已知信息；
——组织系统开发和使用方启动再度评估。

b) 如果安全事件的真实性或报告信息的完整性仍然存在某种程度不确定，安全运营管理机构成员应借助数据分析进行一次安全运营管理机构内部评估，以确定该安全事件是否属实还是仅为一次误报。如果安全事件被确定为误报，应完成填写安全事件报告并记录保存；

c) 如果安全事件被确定是真实的，评估小组成员(包括系统开发和使用方代表)应进行进一步的评估，以尽快确认：
——该安全事件是什么样的情形；
——是如何被引起的
——由什么或由谁引起；
——带来或可能带来什么危害，对组织业务造成的影响或潜在影响；
——事件等级；
——评估完成，根据事件等级做出响应，并调整相应安全策略。

10.6 安全日志和变更控制

10.6.1 所有参与安全评估、安全事件报告和管理的人员应完整地记录下所有的活动以供日后分析之用。这些内容应包含在安全事件数据库中，要在从第一次报告单到事件后评审完成的整个过程中不断更新。

10.6.2 记录下来的信息应妥善保存并留有完整备份。在追踪安全事件以及更新安全事件报告单和安全事件数据库的过程中所做的任何变更，应遵照已得到正式批准的变更控制方案进行。

11 改进

11.1 概述

根据检查评审结果，确定有哪些经验教训需要汲取，并采取措施，优化策略。

11.2 进一步的数据分析

在改进环节，安全系统的监控数据与安全事件库数据将得到进一步的数据分析，并为改进提供依据，改进阶段的工作包括前面各阶段提出的建议，即改进安全风险分析和管理结果、改善安全状况和改进电子商务安全运营管理方案。

11.3 事件分析

安全事件的检查评估工作结束，应该迅速从安全事件中总结经验教训并采取措施，反映在以下方面：

——新的或优化的安全策略：可能是技术或非技术的防护措施，根据总结出来的经验教训，可能需要迅速更新和发布安全培训简报(给用户和其他人员)，以及迅速修订和发布安全标准和方案；

——电子商务安全运营管理方案及其过程、报告单和安全事件/事件数据库的变更；

——此外，这项工作应不仅限于某一次安全事件的范畴，还应分析事件的发展趋势和发生模式，以确定防护措施或方法需要有哪些改变。根据安全事件的情况进行信息安全测试，尤其是脆弱性评估；

——在安全事件发生过程中所获得的相关信息应该用来进行事件发展趋势／发生模式的分析，以预警可能的安全事件发生；

——对安全事件做出分析总结，并呈递到组织管理层的信息安全运营管理协调小组会议上。

11.4 确定改进计划

在改进环节，根据需要，可能确定新的或改变的防护措施。改进建议和相关防护措施需求可能因运作上的原因不能立即付诸实施，在这种情况下应作为组织的长期目标逐步实行。

11.5 确定方案改进

在改进环节，安全运营管理机构下设的数据智能部门或其代表应该审核所发生的一切以进行分析，从而量化对安全事件整体响应的效果。

响应后分析的一个重要方面是将信息和知识反馈到电子商务安全运营管理方案中。如果事件相当严重，应在事件解决后尽快安排所有相关方召开会议。这样的会议应该考虑以下因素：

——电子商务安全运营管理方案规定的规程是否发挥了预期作用；

——是否有对发现事件有帮助的规程或方法；

——是否确定过对响应过程有帮助的规程或工具；

——在事件发现、报告和响应的整个过程中向所有相关方的事件通报是否有效。

11.6 安全风险分析和管理改进

根据安全事件的严重程度和影响，在评估安全风险分析和管理评审的结果时，必须考虑新的威胁和脆弱性。作为完成安全风险分析和管理评审更新的后续工作，引入更新的或全新的安全策略可能是必要的。

附 录 A
（资料性附录）
用户账户安全管理规定

A.1 用户实名制

用户实名制应满足以下规定：
——要求注册用户提供真实身份信息，并进行核验；
——电子商务交易平台服务单位应对用户注册的昵称进行审核，禁止使用违反法律法规和社会道德的昵称。

A.2 个人用户注册

电子商务交易平台服务单位对个人用户注册需满足以下规定之一：
——要求用户提供真实的身份信息及联系方式；
——通过“二次验证”等方式将账号与手机号码建立关联；
——用户提供有效身份证件的扫描件等真实身份信息，并通过人工或技术方式对其身份信息进行有效核验。

A.3 平台商户注册要求

开店的个人商户，应满足以下规定：
——满足 A.2 规定，并提交身份证信息和与身份证原件比对大头照及本人上半身照；
——以单位名义开店的商户，需提供国家规定的相关证照及联系方式。

A.4 用户登录/注册安全运营管理

电子商务交易平台服务单位可提供以下措施，如：
——注册页面需要有验证码，有异常登录，应出现验证码；
——登录页面需要使用安全控件；
——登录过程需要使用 https 安全通道；
——对登录成功后需要跳转的 URL 进行验证；
——密码强度校验，不能使用弱密码；
——完整的登录日志管理；
——建立重置密码或找回密码的验证体系；
——涉及资金支付功能的需要增加与登录密码不同的支付密码；
——不在常用地区登录等类似异常登录情况的风险预警提示。

A.5 用户的账户保护

电子商务交易平台服务单位应对账户信息进行加密存贮，并对账户提供除密码之外的如手机短信、动态令牌、数字证书等二次验证保护。

A.6 用户发布有害信息的处理措施

电子商务交易平台服务单位应根据相关法律法规，对制作、复制、发布、传播违法有害信息的用户，以及公安机关通报的涉嫌违法犯罪的用户制订相应处罚措施，如：

——限制为其提供服务；

——控制其信息发布与平台内的活动；

——对其信息发布内容实施先审后发措施；

——屏蔽其发布信息，不进入搜索引擎；

——限制其参加相应活动；

——关闭账户。

A.7 用户信息使用要求

电子商务交易平台服务单位根据相关法律法规，对用户信息的使用应制订相应规范，应严格保护用户隐私，其保护规定包括但不限于：

——保护注册用户的个人隐私与通讯信息；

——需要明确告之用户获取用户数据的方式和内容；

——需要明确告之用户获取数据的用途；

——用户对自己的隐私数据有可操作权限。

附 录 B
（资料性附录）
商品与信息发布安全管理规定

B.1 商品与信息屏蔽

应满足以下规定：

——具备对发布法律禁止发布的商品与信息的屏蔽过滤措施；

——支持基于关键词的违法信息的屏蔽过滤，支持基于样本数据特征值的违法音视频、图片的屏蔽过滤，支持基于违法外域链接的屏蔽过滤。

B.2 商品与信息删除

应满足以下规定：

——具备对违法信息的快速处置功能；

——对特定文本、图片、视频、链接等信息能够在合理时间内进行删除，并支持批量处理。

B.3 商品与信息控制

应满足以下规定：

——具备特定用户商品与信息发布控制功能。可对特定用户发布的商品与信息（包括文本、图片、视频、链接等信息）进行屏蔽、审核控制；具备特定发布来源控制功能，可识别手机客户端、web 客户端等发布源，并进行审核控制或切断一项甚至多项发布来源；

——具备指定用户或指定商品与信息控制功能 。对特定用户发布的单条或全部商品与信息内容采取屏蔽、禁止访问、交易等措施。

B.4 商品与信息检索

应满足以下规定：

——具备完备的后台商品与信息检索功能；

——支持关键字的逻辑组合查询，支持对本网站所有商品与信息进行全文搜索。

B.5 第三方软件商品与信息发布管理

应满足以下规定：

——具备对第三方软件发布商品与信息的管控功能，能够限制或切断信息与其他互联网应用的互联互通；

——根据法律法规，对第三方数据接口（API）发布的信息进行审核，发现违法信息需采取必要措施。

B.6 商品与信息发布管理

应满足以下规定：

——具备停止全部或单项发布服务功能；

——可停止全部或单项服务（包括停止发布、交易、评论、上传图片、上传视频、上传音频、第三方应用、搜索等）等。