ICS 33.040
M 10

YD

中华人民共和国通信行业标准

YD/T 3169－2016

互联网新技术新业务信息安全评估指南

The guidance of information security evaluation ofnew technology and services on internet

2016－07－11 发布　　2016－10－01 实施

中华人民共和国工业和信息化部　发 布

目　　次

前　　言

本标准是“互联网新技术新业务安全评估”系列标准之一。该系列标准预计结构及名称如下：

1. 《互联网新技术新业务安全评估指南》（本标准）
2. 《互联网新技术新业务安全评估实施要求》
3. 《互联网新技术新业务安全评估要求即时通信业务》

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国移动通信集团公司、中国电信集团公司。

本标准主要起草人：陈　湉、张媛媛、翟羽佳、覃庆玲、陈慧慧、任　彦、魏　亮、杜翠兰、周丽丽、易　立、刘利军、周文君、杜　伟。

互联网新技术新业务信息安全评估指南

1 范围

本标准对互联网新技术新业务安全评估的工作要求、组织流程、评估内容和方法进行了描述和规范。本标准涉及的互联网不包括专用网，仅指公众互联网（含移动互联网）。

本标准适用于在通信行业中组织开展的互联网新技术新业务安全评估工作。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

信息安全 security

信息安全是指互联网技术、业务、应用制作、复制、发布、传播的公共信息内容应该满足《互联网信息服务管理办法》等相关法律法规要求。

2.1.2

信息安全事件 security incident

由于互联网技术、业务、应用自身的特性和功能，或被恶意使用，导致互联网技术、业务、应用被利用制作、复制、发布、传播违法信息，组织非法串联等，对信息安全危害情况。

2.1.3

信息安全风险 security risk

互联网技术、业务、应用被利用导致安全事件的发生及其对经济正常运行、社会稳定、国家安全造成的影响。

2.2 缩略语

下列缩略语适用于本文件。

IP	Internet Protocol	互联网协议

3 概述

互联网新技术新业务安全评估（以下简称“安全评估”）是指运用科学的方法和手段，系统地识别和分析互联网技术、业务、应用可能引发的信息安全风险，评估信息安全事件一旦发生可能造成的危害程度，评估企业配套的信息安全保障能力是否能够将风险控制在可接受的水平，提出有针对性的预防信息安全事件发生的管理对策和安全措施，为最大限度地保障互联网技术、业务、应用的信息安全提供科学依据。

互联网新技术新业务安全评估的目标是为了进一步加强对互联网技术、业务、应用的管理，帮助企业提早防范潜在安全风险，提早部署安全保障措施，促进互联网创新健康发展。

4 安全评估工作要求

4.1 安全评估对象

安全评估的对象是基础电信企业及增值电信企业（含三网融合涉及的广电企业）运营的互联网技术、业务或应用。

4.2 安全评估启动条件

互联网技术、业务或应用满足下列情形之一的，应及时启动安全评估：

a）互联网技术、业务或应用上线前（含合作推广、试点、试商用）。

b）互联网技术、业务或应用运营阶段定期开展评估，或在基础资源配置、技术实现方式、业务功能或用户规模等方面发生较大变化时开展评估。

其中，基础资源配置发生较大变化，是指IP地址、域名等网络资源的分配方式发生较大变化；技术实现方式发生较大变化，是指采用新技术，或技术升级改造，或网络拓扑结构发生较大变化，或网络设备升级改造等情况；业务功能发生较大变化，导致互联网技术、业务、应用的信息传播渠道、传播能力发生较大变化；用户规模发生较大变化，包括互联网技术、业务、或应用的用户数量发生较大变化，或接入网站的数量发生较大变化。

c）应行业主管部门要求，或行业主管部门规定的其他情况。

4.3 安全评估实施流程

安全评估的实施流程包括如下三个阶段。

a）评估准备阶段

评估准备阶段包括成立评估组，确定小组成员；准备评估材料，包括相关技术文档、管理文档等，以及业务、技术或应用的市场发展情况、企业已有安全管理措施和技术保障措施情况等。

b）组织实施阶段

组织实施阶段包括评估组根据评估准备阶段收集的评估材料，采用文档分析、人员访谈、会议质询、检查测试等方式，实施业务安全风险评估流程和企业安全保障能力评估流程，并记录结果。

c）评估总结阶段

评估总结阶段包括对评估结果进行判定，评估组召开评估总结会对评估结果进行评审和确认，完成评估报告。

4.4 安全评估报告的规范要求

安全评估报告应当包括以下组成部分（见附录A）：

a) 业务基本情况，包括业务名称、业务功能、技术实现方式、（潜在）用户规模及市场发展情况等；

b) 安全评估情况，包括评估工作情况概述、评估人员组成、评估实施流程、评估结果（包括业务安全风险评估结果和企业安全保障能力评估结果）以及整改落实情况；

c) 配套安全管理措施，包括企业配套的日常管理措施、应急管理措施、对同类业务的监管建议等；

d) 评估结论确认签字表。

4.5 安全评估报告的报备要求

企业应在安全评估完成后30个工作日之内，将书面评估报告向对本企业颁发电信业务经营许可证或者进行电信业务备案的行业主管部门备案。

5 安全评估总体思路

互联网新技术新业务安全评估应与安全管理工作紧密结合，始终围绕违法信息监测发现、定位处置、追踪溯源等关键监管环节开展安全评估工作，主要涉及业务安全风险评估和企业安全保障能力评估两个流程。安全评估实施过程中，应首先完成业务安全风险评估，识别业务潜在信息安全风险，再基于风险识别的结果完成企业安全保障能力评估。

业务安全风险评估是评估互联网技术、业务、应用（以下简称“业务”）的功能、属性、特点、技术实现方式、市场发展情况、（潜在）用户规模等关键要素对安全管理工作的威胁和挑战，分析、识别信息安全风险。

企业安全保障能力评估是评估企业信息安全管理措施和技术保障手段能否将信息安全风险控制在可接受范围内，可从安全管理机构、安全管理制度、技术保障手段建设情况等多个方面，评估企业的信息安全保障工作水平。

为了能够科学、统一地规范安全评估的实施，本标准提出了业务安全风险评估模型（见第7章），用以规范业务安全风险评估的实施；提出了企业安全保障基线要求（见第8章），用以规范企业安全保障能力评估的实施。

6 业务安全风险评估

业务安全风险评估的实施需要使用业务安全风险评估模型，见图1所示。业务安全风险评估模型从业务应用安全、业务平台安全两个层面提出了11个评估模块。每个评估模块归纳列举了业务关键因素可能产生的对安全管理工作的威胁和挑战，以此指导评估人员识别业务的信息安全风险。

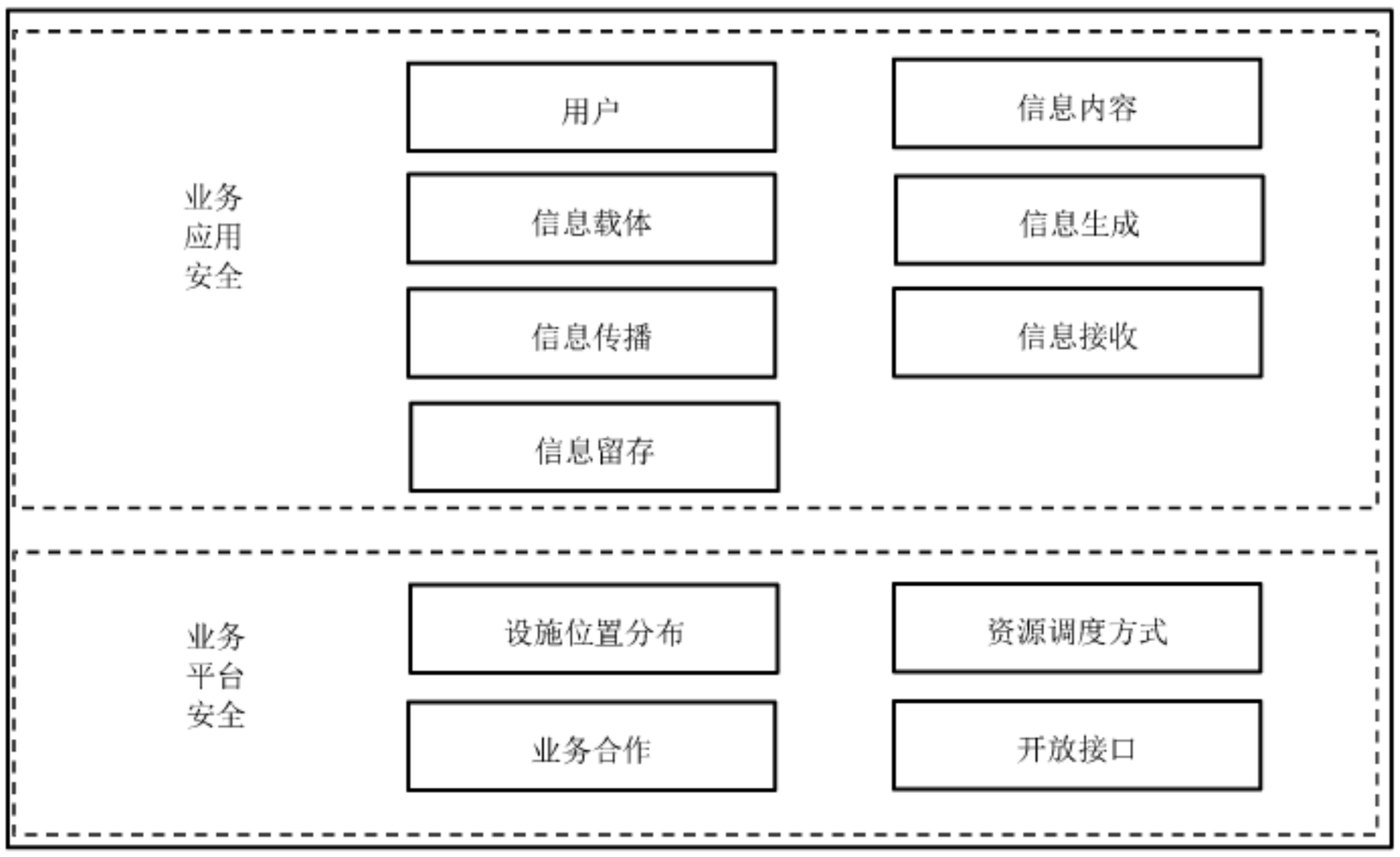

图1 业务安全风险评估模型

评估人员使用业务安全风险评估模型时，可以根据被评估业务的具体情况，识别业务对应于每个评估模块是否存在相应的信息安全风险。此外，还应视具体情况，识别业务是否存在特殊的信息安全风险。评估人员也可以根据业务安全风险评估模型，设计不同业务类型（业务分类参考《电信业务分类目录》）的风险评价指标体系，对业务安全风险进行量化处理。

本标准将依据互联网技术、业务、应用的发展情况、安全评估工作范围的延展，适时修订、增加评估模块。

6.1 业务应用安全

业务应用安全层以业务实现功能、使用情况为基本出发点，以业务系统中传输的公共信息内容为核心评估点，评估模块包括用户、信息内容、信息载体、信息生成、信息传播、信息接收、信息留存。

a）用户

用户主要关注用户规模、用户类型、用户相关性、用户身份信息真实性等。①用户规模主要关注使用业务的用户数量，数量越庞大，发生信息安全事件造成的影响范围越大，信息安全风险越高；②用户类型主要关注使用业务的用户属性特点，包括年龄分布、地域分布等。③用户相关性反映了用户之间联系的紧密程度，若用户间紧密关系被用于传播违法信息，则信息的流通性、可信赖性、关注程度将提高，信息安全风险将有所增加。④用户身份信息真实性关注的是用户使用业务时是否提供了真实身份信息或有助于识别真实身份的相关信息，如果未提供上述信息，将影响企业配合完成事后溯源工作的开展。

b）信息内容

信息内容主要关注公共信息内容的可审核性、多样性和相关性。①信息内容可审核性是指违法信息的识别处置能力，综合考虑审核范围是否覆盖全部业务功能模块和信息载体，识别粒度、处置范围、时效性是否满足相关法律法规要求；若无法有效进行对公共信息内容的监测处置，则存在生产及传播违法信息的信息安全风险。②信息内容多样性主要指信息内容围绕的主题类别数量，微博客类业务的信息内容多元化，主题类别繁杂，数量庞大，从多元信息中识别处置违法信息的难度更大。③信息内容相关性反映信息之间联系是否紧密。若内容大多围绕一个或几个相近主题，那么如果主流主题中包含违法信息，则违法信息可能在相关主题中大范围和快速传播。

c）信息载体

信息载体包括信息呈现方式、语言类型。①信息呈现的方式包括简单文本、文本、图片、音视频、二维码等文件、流媒体等。考虑到对图片、音频、视频等文件及流媒体的内容识别技术尚不能完全满足相关法律法规要求，此类信息载体存在含有、传播违法信息的信息安全风险。②语言类型主要包括中文、英文及其他小语种等。考虑到小语种语言的内容识别技术不成熟，此类信息载体存在含有、传播违法信息的信息安全风险。

d）信息生成

信息生成主要关注信息产生方式。如果业务系统中生成的信息不由业务运营企业控制，例如用户生成信息（UGC）、第三方合作者提供信息等，则信息来源不唯一，对违法信息进行处置的工作难度将大幅增长。

e）信息传播

信息传播主要关注信息流动方向、信息传播方式、通信媒介、信息传递实时性等。①信息传播方式包括了点对点、点对多点（如公众平台）、多点对多点（如群组聊天）、以及病毒裂变式传播（如微博客）等，点对多点、多点对多点、病毒裂变式等传播方式扩大了单位时间内信息的传播范围，存在传播违法信息的信息安全风险。②通信媒介主要考虑网络类型、支持平台类型等，若业务具备跨平台、跨网络（例如IPTV业务中涉及有线电视网和电信网之间的传输切换）的信息流动能力，将导致信息传播链条复杂、多维，提高信息传播速度，增加违法信息快速识别和处置的工作难度。③信息传递实时性关注信息接收

端用户能否实时读取信息，实时通信提高了信息读取概率，提高了信息传播速度，存在传播违法信息的信息安全风险。

f） 信息接收

信息接收环节主要关注信息收取方式等。信息收取方式主要包括信息主动推送、用户主动获取等方式，信息的主动推送提高了信息读取概率，间接提高了信息传播速度，扩大了信息传播范围，存在传播违法信息的信息安全风险。

g）信息留存

信息留存关注的是业务系统中传输的公共信息内容和用户使用业务行为的日志记录，如果企业未按相关法律法规要求保留日志信息，都会直接影响企业配合完成事后溯源、取证工作的开展。

6.2 业务平台安全

业务平台安全层以承载业务的系统平台为核心评估点，评估模块包括设备地理位置、资源调度方式、业务合作、开放接口。

a） 设备位置分布

设备位置分布是指承载业务的服务器、机房或节点的地理位置分布。如果业务的服务器、机房或节点在境内外均有分布，且境内外有数据传输，则可能存在因数据跨境流动引发的国家、个人敏感信息泄露的信息安全风险。

b）资源调度方式

资源调度方式是指业务系统的计算资源、存储资源、带宽资源、IP地址及域名资源的调度方式。如果计算、存储、带宽资源采用了云化或虚拟化，或者IP地址及域名采取动态分配方式，则可能增加企业违法信息处置工作的难度。

c） 业务合作

业务合作是指业务运营企业与其他企业开展任意形式的合作。企业首先需要对任何一种合作方式进行合规性评估（是否符合现行行业管理相关规定），同时还需要评估合作企业的信息安全管理工作及保障措施能否满足相关法律法规要求，能否保障业务的信息安全。例如IPTV业务，如果未按照相关规定选择具备资质的电信企业经营其传输业务，将会影响IPTV集成播控平台与用户端之间提供信号传输的安全。

d）开放接口

开放接口是指业务系统为第三方提供的标准API接口。第三方调用开放API接口的过程中，如果与业务系统之间产生了信息内容交互，可能增加业务系统发布、传输、存储违法信息的信息安全风险；如果业务系统开放的API接口未做好权限管理及安全审计，可直接影响业务系统自身安全。

7 企业安全保障能力评估

企业安全保障能力评估是对照业务安全风险评估的结果，结合企业安全保障基线要求，综合评价企业在业务运营过程中信息安全保障能力水平，其评价结果能够成为企业健全信息安全保障体系，提升信息安全保障能力的重要参考。

7.1 企业安全保障基线要求

企业应按照通信行业安全管理要求明确本企业的安全责任人，成立专职安全部门，建立落实相应安全管理制度，配备与业务规模相匹配的专职安全工作人员及7×24h应急联系人，建立企业互联网新技术新业务安全评估工作制度，积极开展企业自评估工作，及时将自评估报告向行业主管部门进行报备。

具体分为业务应用安全保障基线要求和业务平台安全保障基线要求。

7.1.1 业务应用安全保障基线要求

7.1.1.1 用户管理

用户管理要求主要包括账号注册、日常管理、用户投诉等方面的要求。

a）普通账号身份验证

企业在普通账号注册环节应对注册申请人提交的个人信息进行真实性验证，包括但不限于邮箱验证、手机短信验证、身份证真实性查询（通过联网比对、配备和使用二代身份证识别设备等技术措施）等。

对于用户以虚假身份信息骗取账号名称注册的，企业按照相关法律法规，应采取通知限期改正、暂停使用、注销等管理措施。

对于用户冒用、关联机构或社会名人注册账号名称的，企业应按照相关法律法规，注销其账号，留存相关信息以备主管部门查询。

b）公众账号身份验证

企业应要求公众账号在注册环节提供真实身份信息或组织机构信息，并配套必要管理机制、手段对公众账号提交信息的真实性进行审核。

c）注册信息审核

企业应在注册环节明确告知用户，账号名称、头像和简介等注册信息不得含有违法信息。

企业应配备与服务规模相适应的专业人员和必要技术手段，对用户提交的账号名称、头像和简介等注册信息进行审核，按照相关法律法规，对含有违法信息的，不予注册。

d）用户账号分级管理

企业可以根据累计发送违法信息次数等参数对个人账号、公众账号、聊天群组进行安全等级划分，配套差异化的违法信息处置机制。

e）用户投诉管理

企业应向社会公示违法信息用户举报途径，设立处理用户举报的岗位，依法公开透明的接受和处理违法信息用户举报。

企业应向行业主管部门及时上报用户举报的重大违法事件情况并配合相关处置工作。

7.1.1.2 信息内容管理

企业应建立针对公共违法信息内容监测处置的管理机制和技术手段，能够有效识别、即时停止发布、传输法律法规禁止发布或者传播的信息内容，并依照国家相关法律法规要求留存日志信息。

企业应建立违法信息样本库并进行定期更新。

企业应配套建设与业务经营相适应的技术支撑体系，确保上述信息内容管理要求有效落实；针对不同信息内容载体配套差异化的违法信息处置技术手段，并能够设置相应内容识别、处置策略。

7.1.1.3 信息搜索功能管理

企业应按照国家相关管理要求，确保检索出的链接和指向网站内容不包含违法信息；对用户输入的含有违法信息的检索内容，不予提供服务。

7.1.1.4 信息发布递送功能管理

企业应配套专门人员和必要技术手段对于公众账号发布的公开信息内容作违法信息日常监测巡查。

企业发现公众账号推送的信息有违反国家相关法律法规，或协议约定，应当视情节采取警示、限制发布、暂停更新直至关闭账号等措施，并保存有关记录。

7.1.1.5 信息社区平台功能管理

企业应针对信息发布环节的链接转发、添加评论转发、跨平台分享等功能，配套必要的违法信息监测和处置的管理机制和技术手段。

7.1.1.6 应用分发平台功能管理

应用分发平台功能管理要求包括对应用开发者和应用程序的相关管理要求。

a）应用开发者管理

企业应按照国家相关法律法规，要求应用开发者提交能够证明其已经取得新闻、出版、教育、医疗等前置审批许可和业务经营资质的文件，并留存必要信息。

企业应要求应用开发者提交相关身份和经营资质信息，并进行留存备案；对于备案信息应配套必要的管理措施进行定期核查更新。

企业应和应用开发者签订协议，明示要求应用开发者对上线销售的应用负有安全责任。

企业应建立应用开发者违规记录档案，对上传违法应用的应用开发者，应采取警告教育、应用重点审查、禁止新上传应用等处置措施。

b）应用安全审查

企业应按照国家相关法律法规，对应用进行上线前的安全审查。企业对应用的安全审核至少应包括软件漏洞检测、安全加固措施验证、恶意代码检测（病毒、木马、广告吸费、后门遥控、隐私窃取等）、违法信息内容检测。

c）日常监测

企业应对上架应用，以及开发者论坛、用户论坛等业务平台开展应用恶意行为及应用传播违法信息的日常监测，并留存相关记录。

d）违法应用处置

企业应建立违法违规应用下架处理机制，及时对判定存在违法违规行为的应用进行下架处理。

7.1.1.7 信息即时交互功能管理

信息即时交互功能管理要求主要从即时通信服务常见的功能，如群组聊天、匿名发布消息、转发消息、信息销毁等功能的相关管理要求。

a） 群组功能管理

企业应明确设置群组人数上限。

企业应向群组功能申请人明确告知：

1）不得复制、发布、传播违法信息；

2）群创建者和群管理者对群组负有管理责任，应承诺本群组不发布、传播违法信息。

企业对于违反上述告知行为的群组，应采取限制新成员加入、中止或终止本群组聊天服务等措施。

b） 匿名发布功能管理

针对匿名发布功能，企业应配套必要管理机制和技术体系，确保实现“前台匿名、后台实名”。

c） 转发功能管理

企业应将用户生成信息、内容复制转发、本地存储上传转发、链接转发、跨平台分享等功能，与相

同信息转发次数、用户安全等级等参数相关联，实施发送内容长短，显名或匿名，信息载体类别，复制、存储、转发、分享次数等权限管理。

d）信息销毁功能管理

企业针对信息接收环节的短暂留存呈现、但无法本地存储的信息销毁功能，应配套必要的日志留存等工作机制及技术手段，以依法配合相关部门完成违法信息的调查取证。

7.1.1.8 安全规则张贴与主动提示

企业在用户注册、新功能上线、业务使用过程中的关键环节，应明确告知用户禁止发布、复制、传播违法信息。

企业应与用户在注册账号环节签订协议，要求用户承诺按照国家有关法律法规，遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等7条底线。

7.1.1.9 溯源管理

溯源管理要求主要包括对用户身份信息的变更留存要求及业务相关各类日志的留存要求。

a）用户身份信息变更留存

对于已经进行真实身份信息验证的用户账号，企业应定期核查并更新与用户账号捆绑关联的身份信息，确保其真实有效，对用户身份信息变更做好记录。

b）日志留存管理

企业应按照相关法律法规，记录并留存访问日志；用户访问日志留存系统应支持全部字段内容的精确查询、检索与统计；访问日志的保存时间应满足国家相关法律法规要求。

7.1.1.10 信息联动管理

针对企业内具有信息联动发布、分享功能的不同业务平台，企业应能够在紧急、必要情况下，迅速切断同步或关联关系，并联动删除各关联平台上的违法信息，同时留存相应删除日志信息。

7.1.1.11 应急处置

企业应制定应急预案，明确应急工作机制和实施流程，明确应急领导责任人和沟通联络人，设置7×24h应急联系电话，并将配合应急工作情况反馈行业主管部门。

企业应按照相关法律法规，及时启动应急处置流程机制，采取有效的管理措施和技术手段，配合行业主管部门追究相关责任人安全责任，并保存相关记录。

企业应配套建设安全应急处置技术手段，具备对特定区域、特定服务、特定功能的限制或关闭能力。

7.1.2 业务平台安全保障基线要求

7.1.2.1 业务平台部署

业务平台部署要求主要包括信息备案、设施分布等相关管理要求。

a）平台设施信息备案

企业应将业务机房/节点列表、占用机房位置、使用的通信链路和IP地址等业务开办信息向行业主管部门报备。上述信息发生变化时，企业应及时向行业主管部门上报相关更新信息。

b）设施境内外分布

如果业务的服务器、机房或节点在境内外均有分布，且境内外有数据传输，企业应按照相关法律法规，确保境外违法信息不在境内业务系统中传输、存储，确保公民隐私安全，对于与国家经济、社会、政治相关的敏感数据不能向境外传输。

7.1.2.2 资源调度

资源调度要求是对业务平台相关关键资源如何使用调度的具体要求。

a）资源实时监控

企业应建立相关管理制度及技术手段实现对计算、存储、带宽、IP地址及域名等资源分配使用情况的实时监控和日志记录，并根据相关标准要求提供标准接口，有能力实现向行业主管部门上报实时监控数据和日志数据。

b）违法信息监测处置

企业应建立相关管理制度及技术手段实现违法信息的监测和处置，并根据相关标准要求提供标准接口，有能力接收行业主管部门下发的监测和处置指令。

c）系统日志留存

企业应按照相关管理要求建立相关管理制度及技术手段做好日志留存，日志应全面记录业务系统中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息。日志记录保存时间应满足相关法律法规要求。

7.1.2.3 用户接入要求

用户接入要求主要包括用户资质审核、信息备案、第三方开放接口等方面的相关管理要求。

a）资质审核

企业应认真核查服务对象（如网站）的资质，不得为未经许可或未备案的服务对象提供服务。

b）用户信息备案

企业应在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。企业应记录所有用户真实身份信息、网站或系统名称、域名、IP地址等信息。服务协议中应明确要求用户不得制作、发布、传播违法信息。

c）开放接口

对于提供开放接口的企业，应做好开放数据的审核，确保第三方获取的数据不会导致用户隐私信息，与国家经济、社会、政治相关的敏感数据的泄露；第三方提供的数据不得含有违法信息。

附　录 A
（规范性附录）
评估报告模板

（封面）

（企业简称）互联网新技术新业务
安全评估报告

业务名称：XXXX

（企业名称）
年　　月

1　业务基本情况介绍

……

1.1　业务名称

……

1.2　业务功能介绍

……

1.3　技术实现方式介绍

……

1.4　（预期）用户规模

……

1.5　市场发展情况

……

2　安全评估情况

2.1　安全评估情况概述

……

2.2　评估人员组成

……

2.3　评估实施流程

……

2.4　评估结果及整改落实情况

……

3　配套安全管理措施

……

3.1　日常安全管理介绍

……

3.2　应急管理措施介绍

……

3.3　同类业务的监管建议

……

4　评估结果签字确认表

……