

TC260-PG-2023XA

---

# 网络安全标准实践指南

## —大型互联网平台网络安全评估指南

---

(征求意见稿 v1.0-202312)

全国信息安全标准化技术委员会秘书处

2023年12月

本文档可从以下网址获得：

[www.tc260.org.cn/](http://www.tc260.org.cn/)



**全国信息安全标准化技术委员会**

NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

## 前言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。



## 声明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

## 技术支持单位

本《实践指南》得到国家计算机网络应急技术处理协调中心、蚂蚁科技集团股份有限公司、淘天有限公司、北京百度网讯科技有限公司、北京小桔科技有限公司、北京三快科技有限公司、北京今日头条科技有限公司等单位的技术支持。

## 摘要

大型互联网平台既是企业的重要商业平台，也是网民生活、工作的公共空间，掌握了关系国计民生的大量资源。平台网络安全风险很容易传导影响社会稳定、公共利益。

为帮助大型互联网平台在网络安全合规基础上，进一步评估发现和防范可能影响社会稳定、公共利益的网络安全风险，指导平台提升安全水平，本文件指出了平台应该关注的影响或可能影响社会稳定、公共利益的风险以及网络安全评估方法，供有关单位参考。



全国信息安全标准化技术委员会  
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

# 目录

1 范围 .....	1
2 术语和定义 .....	1
3 评估工作组织 .....	2
4 评估内容 .....	4
5 评估方法 .....	9
附录 A（资料性）大型互联网平台网络安全评估总结报告 .....	12

## 1 范围

本实践指南从影响或者可能影响社会稳定和公共利益的角度，给出了开展大型互联网平台网络安全评估的评估内容和评估方法。

本实践指南为大型互联网平台开展网络安全评估提供参考。

## 2 术语和定义

### 2.1 大型互联网平台 **large internet platform**

通过网络技术将个人与个人、商品、信息、服务、线下资源、数据、资金、软件等进行连接，并以此为基础提供业务的较大规模的网络平台。

注1：较大规模是指在过去的一年期间，在我国累计活跃用户总数不低于5000万。

注2：提供业务包括但不限于即时通信、社交网络、电子商务、直播、短视频、资讯、应用商店、网络预约汽车、网络支付等。

### 2.2 关键业务 **critical service**

占平台营业收入、用户规模、资源投入较大比例的业务。

### 2.3 重要设施 **Important facilities**

支撑关键业务的网络、系统、服务和其他资产。

### 2.4 关键软硬件 **critical software or hardware**

构成重要设施、处理重要数据的核心网络设备、重要通信产品、高性能计算机和服务、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务等网络产品和服务，以及其中包含的核心芯片、固件、操作系统、关键组件等。

## **2.5 重要岗位和人员 important position and personnel**

有条件操作、查询、导出、下载、复制、删除、修改大量重要数据、个人信息的工作人员；可以获取推荐算法运行结果并对其进行调整的人员；负责重要系统平稳运行，如操作系统、数据库、网络环境的关停、配置工作的人员。

注：工作人员包括本单位人员以及承担相关工作任务的外单位人员。

## **2.6 弹性 resilience**

业务在受网络攻击、自然灾害、供应链中断、设备故障、不当操作等情况下，保持业务连续性的能力，以及在业务中断的情况下，恢复业务的能力。

# **3 评估工作组织**

## **3.1 工作组的设立**

大型互联网平台开展网络安全评估需要首先设立网络安全评估工作组：

- a) 工作组由平台主要负责人直接领导，工作组在其领导下制定管理制度和工作程序；

注1：平台主要负责人指平台经营主体的主要负责人或实际控制人。

- b) 工作组各项具体工作由平台主要负责人指定的牵头人组织推动，牵头人应是平台高级管理人员。

注2：高级管理人员包括平台运营者的经理、副经理、首席执行官、首席运营官、财务负责人、人力资源负责人、法务负责人、董事会秘书等，以及公司章程规定的其他人员。

### 3.2 工作组的职责

工作组的职责是全面落实大型互联网平台网络安全评估工作，包括：

- a) 根据各项关键业务发生网络安全问题时对社会稳定、公共利益或公民合法权益的影响程度明确网络安全评估范围；
- b) 组织开展年度网络安全评估；
- c) 研究制定重要事项网络安全评估工作方案并组织开展相关评估工作；
- d) 根据网络安全评估中发现的安全问题组织开展整改。

### 3.3 工作组的能力保障

工作组牵头人需要识别与平台网络安全评估工作相关的主要部门，并由各部门选派代表加入工作组，以确保工作组具备开展以下工作的条件：

- a) 识别适用的法律法规及标准要求，统筹协调各部门开展评估工作；
- b) 掌握平台运营者控股主体、实际控制人、高级管理人员、重要岗位人员、核心外包商情况；



- c) 识别分析网络安全、数据安全、个人信息相关风险，包括基础计算环境、物理环境相关安全风险，以及业务模式相关安全风险；
- d) 识别、汇总并分析平台涉及本实践指南评估内容的安全事件，如关键服务中断、大规模网络攻击等，特别是其中涉及刑事案件、行政执法、有关部门约谈通报等情况的安全事件；
- e) 对平台的用户投诉、商业纠纷、公益诉讼等，具备进行汇总、分析能力，能够及时发现并处置其中潜在的安全问题；
- f) 识别跨境提供服务、跨境传输数据等场景因不同国家、地区网络安全政策、法治环境、保护水平差异可能导致的网络安全问题；
- g) 识别供应链风险，汇总供应链风险与事件相关情况。

## 4 评估内容

### 4.1 关键业务弹性

评估内容包括：

- a) 评估可能导致平台长时间业务瘫痪的情形；
- b) 评估过去一年中，平台的关键业务发生过长时间业务瘫痪的安全事件，是否举一反三，找到问题根源，予以安全防范；

- c) 评估过去五年中，本平台以及国内外同等级平台发生的导致业务长时间中断、大面积瘫痪事件及情形，分析在本平台发生类似事件的可能性；
- d) 评估是否存在关键硬件、软件、组件等，一旦发生故障或功能瘫痪会对全平台造成影响；

## 4.2 容灾备份能力

评估内容包括：

- a) 评估平台弹性冗余、容灾备份及抗毁顽存能力；
- b) 评估平台容灾备份系统能否独立运行；
- c) 评估灾难发生后，关键业务从停顿到恢复的时间，以及系统和数据必须恢复到的时间点要求；
- d) 评估过去一年中是否实际启动过容灾备份系统；以桌面演练、模拟演练、实际切换演练或其他形式开展演练的，评估灾难恢复的实际效果。

## 4.3 关键软硬件产品供应链安全性

评估内容包括：

- a) 评估关键软硬件产品安全性、开放性、透明性、来源多样性，以及供应渠道的可靠性；
- b) 评估关键软硬件产品是否可能因为政治、外交、贸易等因素导致供应中断；

- c) 评估关键软硬件产品是否可能发生被恶意植入后门、不明功能、超级权限；
- d) 评估其他可能影响关键软硬件产品供应的可能性因素；
- e) 评估过去一年中，关键业务是否发生过供应链安全事件；并评估事件发生后，针对关键业务是否采取整改、缓解、预防措施，以及措施的有效性；还需评估如果导致安全事件的威胁再次产生，可能造成的安全影响以及当前平台的应对抵御效果。

注：供应链安全事件主要是指，因政治、外交、贸易、专利授权等非技术因素导致产品和服务供应中断、不及时、不足量的供应，以及被恶意植入代码或后门所引起安全事件。

#### 4.4 对外提供数据的可控性

围绕对外提供重要数据、个人信息开展网络安全评估，特别是评估相关安全管理制度，以及评估已对外提供数据的失控、泄露、滥用风险。该评估需要平台业务、法务、合规、安全等相关部门共同参与，并重点考虑对社会稳定、公共利益可能造成的安全影响。评估内容包括：

- a) 评估是否具有健全的对外提供重要数据、个人信息的管理制度：
  - 1) 评估管理制度中对外提供重要数据、个人信息的审批制度是否集中统一，审批层级在高管层面；审批的适用场景、数据范围，以及审批部门、审批要素、审批流程等内容是否明确；查看审批事项是否包括提供数据的必要性、正当

性、合法性；审批人员是否具备充分的安全经验和管理权限；

- 2) 评估管理制度中对数据接收方数据保护义务和责任做出的规定是否充分：是否包含接收方对重要数据和个人信息的使用目的、使用期限、使用方式的限制；是否包含接收方将重要数据和个人信息再转移、再扩散、转委托的处理条件；是否明确要求接收方将重要数据和个人信息再转移、再扩散、转委托，或变更使用目的、使用方式，延长使用期限前，需要取得平台的同意；是否明确要求接收方达成使用目的或约定使用期限到期后，需要及时删除重要数据和个人信息；
- 3) 评估是否具有对不同国家、地区网络安全、数据安全、个人信息保护等最新政策和案例进行分析、响应的机制。

b) 评估已对外提供的个人信息和重要数据是否存在失控、泄露、滥用的风险：

- 1) 评估是否存在接收方未经同意，向其他第三方提供数据的情况；
- 2) 评估是否具备对已对外提供数据失控、泄露、滥用风险的跟踪、监督、防范措施；
- 3) 评估过去3年内以及正在提供的重要数据、累计100万以上的个人信息、或累计10万以上的敏感个人信息，接收方是否能够有效保障数据安全以及按照约定合理使用。

#### 4.5 数据泄露事件发生后应急处置

评估一旦发生严重数据泄露，能否采取有效措施减缓对社会稳定、公共利益造成危害：

- a) 评估数据加密情况、被破解难度，以及所采用密码算法是否符合我国相关政策法规要求；
- b) 评估发生严重数据泄露事件后，平台及时感知处理事件、阻断泄露、追溯事件来源、定位数据去向的能力。
  - 1) 评估平台对数据泄露、数据窃取行为的感知、阻断能力；
  - 2) 评估平台是否具备对事件溯源、泄露数据定位的能力。
- c) 评估过去一年中，平台发生的大规模数据泄露事件以及事件过程中平台所体现的感知处理事件、阻断泄露、追溯事件来源、定位数据去向的能力情况。

#### 4.6 平台控制权

评估当前平台对重要设施和数据的控制权情况，评估内容包括：

- a) 评估平台运营实体的控股主体、实际控制人、高级管理人员、重要岗位人员的国籍、背景、历史信用记录、遵守中国法律的情况；
- b) 核验重要岗位人员清单台账，核验是否账实相符，是否完整包括具有接触重要设施和数据的正式工作人员和外包人员；
- c) 评估平台重要岗位设置及相应权限设置情况；评估是否具备完整记录、感知、回溯重要岗位人员的行为操作的能力；

- d) 评估是否对重要岗位人员开展安全背景审查；
- e) 评估承担重要岗位人员的外包供应商背景情况，了解其控股主体、实际控制人、高级管理人员的国籍、背景、历史信用记录。

#### 4.7 用户权益保护

评估用户个人信息权益保障情况，以及平台面向用户提供算法应用服务的合理性。评估内容包括：

- a) 过去一年中，制定或修订隐私政策或使用协议的：
  - 1) 是否从用户反馈、用户投诉、消费者权益保护组织、主管监管部门等渠道充分听取社会意见；
  - 2) 是否采用社会公示、向内设个人信息保护监管机构通告或其他有效方式充分征求公众意见；
  - 3) 是否将公众的反馈意见、采纳情况及其理由在平台界面的显著位置发布公示；
- b) 保障用户便利行使其个人信息查询权、复制权、删除权、更正权、转移权等权益的情况：
  - 1) 是否在平台界面便利位置提供行使以上权利的访问或操作渠道；
  - 2) 说明平台实际响应用户行权请求的落实情况，包括行权请求的总次数、请求内容、响应完成度、办理时限，拒绝行权请求的，应说明原因；

- 3) 用户选择转移个人信息后，平台是否仍保留、存储、处理其个人信息；
- c) 平台利用算法向用户定向推送信息的真实性、准确性、安全性以及来源的合法性：
  - 1) 是否在显著位置做出标识，是否允许用户拒绝接收定向推送信息，是否向用户提供重置、修改推送参数的选项；
  - 2) 是否向用户明示推送算法决策所依赖的用户网络历史行为或个人信息。

## 5 评估方法

### 5.1 年度网络安全评估

工作组每年组织开展一次覆盖第4章内容的、完整的网络安全评估：

- a) 年度网络安全评估工作由工作组牵头，可组织平台各部门自行开展，也可委托第三方帮助开展；
- b) 开展年度网络安全评估时，按本文件第4章要求逐条开展评估，并逐条记录评估结果：
  - 1) 未发现安全问题与安全风险时，需要记录评估情况，保留相关材料；
  - 2) 发现安全问题或安全风险时，需要记录评估情况，并及时组织分析研判，并根据研判结果对发现的问题和风险进

行整改，记录整改情况或未整改原因，对突出问题、风险按照有关部门要求上报；

- c) 工作组组织撰写年度网络安全评估报告，模板见附录A；
- d) 年度网络安全评估报告完成后，由牵头人及工作组组成部门会签，并由平台负责人审批签字确认留档。

## 5.2 重要事项网络安全评估

当平台拟开展下述调整变更前，工作组需要先就该调整变更对社会稳定、公共利益可能造成的影响补充进行重要事项网络安全评估；重要事项网络安全评估的工作过程、报告模板由工作组自行研究制定：

- a) 平台的实际控制人变更；
- b) 启动新关键业务、关停现有关键业务，或关键业务的重要岗位人员变更；
- c) 在关键业务中增设或调整具有舆论属性或者社会动员能力的功能；
- d) 在关键业务中增设或调整与人身安全、人身健康密切相关的自动化决策功能；
- e) 扩大收集用户敏感个人信息的范围、数量或频率；
- f) 变更支撑关键业务的重要设施，或调整重要设施供应商；
- g) 增加重要数据、累计100万以上的个人信息，或10万以上的敏感个人信息的接收方，或向已有接收方提供数据的技术方式发生变更；



- h) 对外提供重要数据、累计100万以上个人信息，或10万以上敏感个人信息的，接收方对信息的使用目的、使用方式发生变更。

### **5.3 报告使用**

大型互联网平台网络安全评估报告以及重要事项网络安全安全评估报告应真实、完整、详实，并基于自愿原则向社会公开。选择向社会公开时，如涉及商业秘密且不易分割的，平台可基于完整的网络安全评估报告另外裁剪公开发布版本。

## 附录 A

(资料性)

### 大型互联网平台年度网络安全评估报告模板

#### A.1、企业情况简介

- 1、平台规模；
- 2、业务范围；
- 3、股权结构/主要股东；
- 4、经营情况；
- 5、涉海外分支结构情况；
- 6、其他情况。

#### A.2、网络安全评估落实情况

- 1、网络安全评估工作组设立、运行情况；
- 2、平台日常运行相关安全情况；
- 3、年度网络安全评估工作开展基本情况；
- 4、重要事项网络安全评估情况。

#### A.3、年度网络安全评估结果

(按照本文件第 5 章评估方法,对照本文件第 4 章评估内容逐条填写本章各节内容)

##### 1. 关键业务弹性

(按照本文件 4.1 内容逐条进行 4 项网络安全评估,其中 4.1b 相关信息的填写使用表 A.1,其中 4.1c 相关信息的填写使用表 A.2)

表 A.1 业务瘫痪安全事件列表

序号	事件名称	事件起始时间	主要内容与经过	事件原因	事后缓解措施与效果

填表说明:

1) 过去一年中, 平台的关键业务发生过长时间业务瘫痪安全事件的, 逐一列明安全事件的时间、主要内容与经过, 分析事件原因, 列明缓解措施;

2) 事后缓解措施: 事件发生后, 针对关键业务采取的整改、缓解、预防措施, 及其有效性; 若导致安全事件的威胁因素再次发生, 分析判断平台的应对抵御效果和风险后果;

表 A.2 极端情况下长时间业务瘫痪风险列表

序号	过去发生的风险事件(本平台、其他平台)	风险原因	本平台发生类似事件的可能性	如可能性较小, 请说明理由(已采取措施)

填表说明:

1) 过去五年中, 本平台以及国内外同等级平台发生的导致业务长时间中断、大面积瘫痪事件及情形的, 逐一列明安全事件的时间、原因, 分析本平台发生类似事件的可能性;

## 2. 关键业务灾难恢复情况

(按照本文件 4.2 内容逐条进行 4 项网络安全评估, 其中 4.2 d 相关信息的填写使用表 A.3)

表 A.3 灾难恢复演练记录列表

序号	灾难恢复演练时间	演练形式	演练内容与过程	演练结果与效果

填表说明:

1) 逐一列举过去一年中, 开展关键业务灾难恢复演练的记录;

2) 演练形式: 桌面演练、模拟演练、实际切换演练或其他形式;

3) 演练结果与效果: 开展实际切换演练的, 容灾冗余系统是否具备独立承载关键业务的能力; 关键业务的 RTO 与 RPO; 其他经演练证实的灾难恢复结果;

### 3. 关键软硬件产品供应链安全性

(按照本文件 4.3 内容逐条进行 5 项网络安全评估,其中 4.3 b、c、d 相关信息的填写使用表 A.4,其中 4.3 e 相关信息的填写使用表 A.5)

表 A.4 产品和服务供应链风险列表

序号	关键软硬件名称	存在供应链中断的风险大小及理由	被恶意植入后门的风险大小及理由	如前两项存在风险较大情况,请说明对关键业务的影响

填表说明:

- 1) 逐一列举关键软硬件,评估其供应链风险对平台关键业务影响的程度;
- 2) 如前两项存在风险较大情况,请说明对关键业务的影响:分析认为关键业务是否仍可持续、安全运行的,说明支撑该结论的分析依据;分析认为关键业务连续性受影响的,评估关键业务能力的影响范围和程度,以及恢复业务的时间;

表 A.5 供应链安全事件列表

序号	事件名称	事件起始时间	主要内容与经过	事件原因	事后缓解措施

填表说明:

- 1) 过去一年中,关键业务是否发生过供应链安全事件的,填写表A.4,逐一列明供应链安全事件的时间、主要内容与经过、事件原因,以及事后缓解措施;
- 2) 事后缓解措施:如果导致安全事件的威胁再次产生,可能造成的安全影响以及当前平台的应对抵御效果;

### 4. 对外提供数据的可控性

(按照本文件 4.4 内容逐条进行 2 项网络安全评估,信息的填写使用表 A.6)

表 A.6 向第三方提供重要数据和个人信息的情况

序号	时间	第三方单位主	字 段	数据 量	审批 人	接收方是否能够有效保障数据安全,是否按照约定合理使用,	评估结果 及理由

		体				是否存在未经本公司同意，又向其他方提供的情况。	

填表说明：

1) 填写过去一年中，向第三方提供重要数据和个人信息的事例情况；

## 5. 数据泄露事件发生后应急处置

(按照本文件 4.5 内容逐条进行 3 项网络安全评估，其中 4.5 a 相关信息的填写使用表 A.7，其中 4.5 c 相关信息的填写使用表 A.8)

表 A.7 重要数据保护情况

重要数据	数据内容	存储载体和网络位置	是否加密及采取的加密算法	被破解难度

填表说明：

1) 存储载体和网络位置：包括但不限于，数据库、通信线路、云存储、PC 终端、网络缓存等；

2) 数据是否加密及采取的加密算法：数据是否加密，是否采用国密算法；

表 A.8 大规模数据泄露事件表

序号	事件名称	事件时间	主要内容与经过	数据保护机制有效性情况	数据泄露的感知、阻断、溯源情况

填表说明：

1) 过去一年中，平台发生大规模数据泄露的安全事件的，填写表 A.7；

2) 数据保护机制有效性：按照 3.4 的方法和内容分析数据保护机制的有效性；

3) 数据泄露的感知、阻断、溯源情况：按照 3.4 的方法和内容分析平台对大规模数据泄露安全事件的感知、阻断、溯源能力；

## 6. 平台控制权

(按照本文件 4.6 内容逐条进行 5 项网络安全评估，相关信息的填写使用表 A.9)

表 A.9 控制权变更事件表

序号	变更时间	变更过程	对社会稳定、公共利益的影响	缓解措施


填表说明:

1) 过去一年中, 平台发生股权和控制协议变更, 实际控制人、高级管理人员、重要岗位人员和核心外包人员变更的, 逐一系列明事件的时间、经过, 填写表格A.8。

## 7. 用户权益保护

(按照本文件 4.7 内容逐条进行网络安全评估)