

DB4403

深圳市地方标准

DB4403/T XXX—XXXX

企业预防、识别和应对“帮助非法利用信息 网络行为”指南

Guidelines for enterprises to prevent, identify and respond to
“assisting behavior in illegal use of information networks”

（送审稿）

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发布

目 次

前 言 III

引 言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 2

5 合规管理职责 2

 5.1 最高管理者 2

 5.2 合规管理部门 3

 5.3 管理者 4

 5.4 全体员工 4

 5.5 合规管理协作 5

6 预防 5

 6.1 制度建设 5

 6.2 人员管理 5

 6.3 信息化建设 6

 6.4 合规培训 6

 6.5 应急预案 6

7 识别 7

 7.1 识别框架 7

 7.2 识别途径 7

 7.3 识别清单 8

 7.4 分析与评价 8

8 应对 8

 8.1 合规审查 8

 8.2 合规咨询 8

 8.3 合规举报 9

 8.4 内部调查 9

 8.5 沟通与报告 9

 8.6 处置措施 9

 8.7 合规奖惩 10

 8.8 配合执法 10

9 监督检查 10

附 录 A （资料性） 常见“帮信行为”的示例 11

附 录 B （资料性） 识别清单示例 14

附 录 C （资料性） 内部调查示例 15

参 考 文 献 18

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由深圳市司法局提出并归口。

本文件起草单位：深圳市腾讯计算机系统有限公司、深圳市标准技术研究院、深圳赛西信息技术有限公司、北京大成（上海）律师事务所

本文件主要起草人：邓国良、温利峰、潘瑶、温利群、周宏、陈立彤

引 言

近年来，随着互联网技术的飞速发展，信息网络已经渗透到人们生活的方方面面，极大地丰富和方便了人们的生活。与此同时，利用信息网络犯罪的手段和方法也呈现多样化的趋势，信息网络犯罪日益猖獗，其中，“帮助信息网络犯罪活动罪”（以下简称“帮信罪”）已成为一种常见的犯罪形式。

随着“帮信罪”案件整体呈增长趋势，涉案人数和企业的持续增加，犯罪手段越发隐蔽，给企业带来严重风险，对企业声誉和经济利益带来巨大威胁。

因此，为保障企业可持续发展，针对目前深圳市企业的合规现状、痛点和需求，深圳市司法局提出深圳市企业预防、识别和应对“帮助非法利用信息网络行为”指南的地方标准，用以指导企业在经营发展中开展“帮信罪”的防范工作，指导企业识别帮助非法利用信息网络行为，提升企业预防和应对“帮信罪”风险能力，推动企业合规建设，保护企业合法权益和业务正常运行，尽可能降低或避免因帮助非法利用信息网络行为给企业、个人和社会带来损失，促进企业合规治理和健康发展。

企业预防、识别和应对“帮助非法利用信息网络行为”指南

1 范围

本文件给出了企业预防、识别和应对“帮助非法利用信息网络行为”的合规实践指南，包括基本原则、合规管理职责、预防、识别、应对和监督检查。

本文件适用于指导深圳市辖内企业开展预防、识别和应对“帮助非法利用信息网络行为”的工作，也可供其他地区的企业参考

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 24353—2022 风险管理 指南

3 术语和定义

GB/T 35770界定的以及下列术语和定义适用于本文件。

3.1

信息网络服务 information network service

互联网接入服务、网络地址转换服务、域名注册服务、服务器托管服务、空间租用服务、云服务、内容分发服务、信息/软件发布服务、即时通讯服务、网络交易服务、网络游戏服务、网络直播服务、广告推广服务等网络服务或技术支持。

3.2

帮助非法利用信息网络行为 assisting behavior in illegal use of information networks

明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助服务的行为。

注：本文件中，帮助非法利用信息网络行为简称“帮信行为”。

3.3

相关方 interested party

能够影响决策或活动、受决策或活动影响或自认为受决策或活动影响的个人或组织。

注：相关方可以是企业内部利益相关方或企业外部利益相关方。

[来源：GB/T 35770—2022，3.2，有修改]

3.4

最高管理者 top management

在最高层指挥和控制企业的一个人或一组人。

注1：最高管理者有权在企业内部授权和提供资源。

注2：本文件中，“最高管理者”指最高级别的执行管理层。

[来源：GB/T 35770—2022，3.3，有修改]

3.5

合规义务 compliance obligations

企业强制性地必须遵守的相关法律、法规、规章及规范性文件等规定的要求，以及企业自愿选择遵守的要求。

[来源：GB/T 35770—2022，3.25，有修改]

4 基本原则合法正当

企业依照有关法律法规合规提供信息网络服务，防止因违规而可能造成的法律制裁、监管处罚、重大财产损失或声誉损失等。

4.2 全面覆盖

企业预防、识别和应对“帮信行为”活动覆盖企业经营管理的全过程和企业各级部门、各级子企业和分支机构及全体员工，贯穿决策、执行、监督、反馈全流程。

4.3 联动协作

企业预防、识别和应对“帮信行为”活动与法务、审计、内控、风险管理等工作相统筹，形成部门之间沟通协作制度化，监督和确保企业合规工作有效运行。

4.4 持续改进

企业预防、识别和应对“帮信行为”活动是适应企业内外部环境变化的动态过程，随着内外部环境的变化，企业面临的“帮信行为”风险也在不断发生变化，企业需要持续不断地对各种变化保持敏感并做出恰当反应。

5 合规管理职责

5.1 最高管理者

5.1.1 管理承诺

5.1.1.1 领导作用和承诺

最高管理者宜通过以下方面证实其对企业预防、识别和应对“帮信行为”活动的领导作用和承诺：

- a) 制定企业预防、识别和应对“帮信行为”的合规方针与合规目标，并确保与企业战略方向保持一致；
- b) 确保企业预防、识别和应对“帮信行为”的合规要求融入企业的业务流程；
- c) 明确企业预防、识别和应对“帮信行为”的合规管理职责和权限，确保合规管理部门的独立性，支持合规管理部门直接接触最高管理者，确保有效沟通；
- d) 确保为企业预防、识别和应对“帮信行为”合规管理工作提供必要的资源，包括但不限于人员、财务、技术和有关基础设施；
- e) 促进企业预防、识别和应对“帮信行为”合规管理工作持续改进。

5.1.1.2 合规文化

企业宜在其内部各个层级建立、维护并推进企业预防、识别和应对“帮信行为”的合规文化建设，包括但不限于：

- a) 企业宜将预防、识别和应对“帮信行为”作为合规文化建设的重要内容，通过制定合规手册、签订合规承诺书、开展合规宣誓和培训等方式将企业预防、识别和应对“帮信行为”有关合规理念传递至全体员工，确保其了解合规义务；
- b) 企业最高管理者与各级管理者以身作则，遵循和履行预防、识别和应对“帮信行为”的合规义务与合规行为准则，通过自身的行为和决策，倡导和推广合规文化；
- c) 通过合规建设情况公开披露、宣传等方式，将企业预防、识别和应对“帮信行为”有关合规文化传递至利益相关方，确保其了解企业预防、识别和应对“帮信行为”有关合规要求；
- d) 建立企业预防、识别和应对“帮信行为”合规绩效考核体系，宜将合规绩效考核结果作为薪酬待遇、职务任免等参考要素；
- e) 通过合规奖惩机制，奖励和支持合规行为，阻止和惩罚违规行为，营造良好合规氛围。

5.1.2 合规方针

最高管理者宜确立企业预防、识别和应对“帮信行为”合规方针，并确保方针：

- a) 在保持与企业战略方向一致的基础上，制定企业预防、识别和应对“帮信行为”合规方针与合规目标；
- b) 提及并描述企业预防、识别和应对“帮信行为”的合规职能，包括合规管理部门的职责；
- c) 明确要求遵守企业预防、识别和应对“帮信行为”有关合规义务；
- d) 明确不遵守企业预防、识别和应对“帮信行为”有关合规义务、方针、过程和程序的后果；
- e) 鼓励员工提出合规相关的疑虑，对其进行保密并且禁止任何形式的报复；
- f) 通过具体行动体现企业预防、识别和应对“帮信行为”合规方针的重要性，确保得到有效实施和执行；
- g) 将企业预防、识别和应对“帮信行为”合规方针形成文件化信息，易于所有人员理解其原则和意图，在企业内予以沟通，适当时，对相关方可用；
- h) 每年至少开展一次合规方针有效性评估，根据监管政策变化、司法案例及技术风险及时更新方针内容。

5.1.3 职责和权限

最高管理者宜明确相关岗位的职责和权限，最高管理者的主要职责包括：

- a) 为企业预防、识别和应对“帮信行为”合规管理工作配置适当的资源；
- b) 确保企业预防、识别和应对“帮信行为”合规管理工作有效实施；
- c) 建立、健全企业预防、识别和应对“帮信行为”合规管理部门；
- d) 作出企业预防、识别和应对“帮信行为”的合规承诺；
- e) 确保建立企业预防、识别和应对“帮信行为”相关合规管理制度及其绩效报告制度；
- f) 协调企业预防、识别和应对“帮信行为”合规管理工作与企业业务之间的关系，确保企业预防、识别和应对“帮信行为”合规管理要求与企业的业务流程相融合；
- g) 确保和维护合规奖惩机制，包括合规激励和违规处罚；
- h) 确保企业预防、识别和应对“帮信行为”合规绩效与人员绩效考核挂钩。

5.2 合规管理部门

最高管理者宜建立合规管理部门或任命合适人员、部门负责企业预防、识别和应对“帮信行为”合规管理工作的实施和运行，并确保其履职上具备足够的独立性和权威性，合规管理部门或相关人员、部门主要履行以下职责：

- a) 负责企业预防、识别和应对“帮信行为”相关合规管理制度的建立、实施和改进；
- b) 负责与 IT 部门协调制定信息网络技术防范策略和部署相关信息网络系统，利用数字化技术开展合规管理和“帮信行为”监测工作；
- c) 负责组织企业“帮信行为”风险评估，拟定风险应对方案，预防和应对“帮信行为”合规风险事件；
- d) 受理职责范围内的有关企业“帮信行为”的举报，执行对企业“帮信行为”的内部调查，并提出处理建议；
- e) 执行开展合规尽职调查，出具审查意见；
- f) 统筹推进企业预防、识别和应对“帮信行为”合规管理工作的执行，定期或适时向最高管理者报告实施成效；
- g) 发生较大或重大“帮信行为”合规风险事件，及时向最高管理者报告，并配合提供相应的解决方案；
- h) 向全体员工提供关于企业预防、识别和应对“帮信行为”合规培训、咨询、建议和指导；
- i) 组织或者配合业务、人事等部门开展企业预防、识别和应对“帮信行为”有关合规培训；
- j) 制定和实施企业预防、识别和应对“帮信行为”有关合规奖惩制度；
- k) 开展国内外有关非法利用信息网络、帮助非法利用信息网络的法律与政策的学习、研究，并组织内部宣贯协同。

5.3 管理者

最高管理者宜确保管理者对其职责范围内的企业预防、识别和应对“帮信行为”合规管理工作负责，管理者主要履行以下职责：

- a) 作出企业预防、识别和应对“帮信行为”有关合规承诺；
- b) 配合和支持合规管理部门或相关人员、部门，指导和监督其职责范围内的企业预防、识别和应对“帮信行为”相关合规管理工作；
- c) 确保企业预防、识别和应对“帮信行为”相关合规管理要求融入业务流程；
- d) 配合开展合规培训活动，培养员工的合规意识，提高员工的合规能力；
- e) 识别运行中的“帮信行为”风险并与合规管理部门或相关人员、部门及时沟通；
- f) 鼓励并支持员工对“帮信行为”进行内部举报，并防止任何形式的报复；
- g) 配合企业“帮信行为”风险评估，配合拟订风险应对方案，协助预防和应对“帮信行为”合规风险事件。

5.4 全体员工

最高管理者宜确保全体员工履行以下职责：

- a) 遵守企业预防、识别和应对“帮信行为”有关合规管理要求；
- b) 按照要求参加企业预防、识别和应对“帮信行为”有关合规培训，配合完成培训后安排的考核（如有）；
- c) 充分了解企业预防、识别和应对“帮信行为”合规管理工作的重要性；
- d) 充分了解自身岗位与企业预防、识别和应对“帮信行为”合规的关系；
- e) 充分了解不符合企业预防、识别和应对“帮信行为”合规管理要求的后果与责任；

- f) 充分了解企业预防、识别和应对“帮信行为”合规管理的内部举报流程;
- g) 依照流程及时报告有潜在合规风险的产品或业务。

5.5 合规管理协作

最高管理者宜确保企业预防、识别和应对“帮信行为”合规管理联动协作机制有效运行,明确以下职责:

- a) 各业务部门和各职能部门对其职责范围内的合规管理工作直接负责;
- b) 合规管理部门主要负责组织、实施、协调和监督合规管理工作等职责;
- c) 合规管理部门与其他部门在预防、识别和应对“帮信行为”中的协同职责,并建立内部信息共享与联合响应机制;
- d) 可设立监督职责部门,如审计部门、监察部门或人员,承担合规监督职责。

6 预防

6.1 制度建设

企业宜制定适宜企业发展目标、经营范围、治理结构、业务规模的企业预防、识别和应对“帮信行为”合规管理制度,包括但不限于:

- a) 建立企业预防、识别和应对“帮信行为”合规管理制度和员工普遍遵守的合规行为准则及其管理办法,并根据法律法规变化和监管动态,及时将外部有关合规要求转化为企业内部规章制度,保持制度更新,确保政策有效性和合规性;
- b) 制定企业员工预防、识别和应对“帮信行为”合规承诺书;
- c) 可结合企业实际和提供的信息网络服务范围,制定互联网接入、网络地址转换、域名注册、服务器托管、空间租用、云服务、内容分发、信息或软件发布、即时通讯、网络交易、网络游戏、网络直播、广告推广等具体领域的合规管理制度或专项指南。

6.2 人员管理

企业宜建立严格的人员筛选机制,确保员工具备诚信和职业道德素养,能够具备履行预防、识别和应对“帮信行为”有关合规管理要求的必要能力胜任其工作,包括但不限于:

- a) 入职前,企业按照相关法律法规、道德规范和对应的业务要求及岗位级别对候选人执行背景调查和信用记录查验;
- b) 将遵守企业预防、识别和应对“帮信行为”有关合规义务、方针、过程和程序作为人员聘用、调动或者晋升条件,将合规性作为重要考量因素;
- c) 入职前,企业与员工签署保密协议,根据需要,可与相关方签署保密协议;
- d) 在劳动合同中规定员工和企业对企业预防、识别和应对“帮信行为”合规责任,细化员工手册中关于员工权利与义务的约定;
- e) 要求新员工在入职时接受合规培训,签署合规承诺书,确保全面准确了解合规要求,定期或不定期对全体员工进行预防、识别和应对“帮信行为”合规培训;
- f) 作为任用过程的一部分,企业宜结合岗位和人员可能引发的“帮信行为”合规风险,在任何任用、调动和晋升之前按要求进行尽职调查;
- g) 规范离职管理过程,及时终止离职员工的所有访问权限和业务合作协议中的权限;

- h) 加强对管理人员、重要风险岗位人员、海外人员及其他需要重点关注的人员的合规管理，采取轮岗方式，有针对性加强培训和违规行为追责；
- i) 定期评审绩效目标和激励措施，确保与合规目标一致，防止不当激励导致不合规行为；
- j) 持续监督员工的合规表现，并将其作为绩效评估的一部分。

6.3 信息化建设

企业宜建立预防、识别和应对“帮信行为”合规管理工作的信息化建设，运用技术手段预防、识别和应对“帮信行为”，保障企业合规义务的实施、监测和管理，包括但不限于：

- a) 结合企业实际将企业预防、识别和应对“帮信行为”有关合规制度、典型案例、合规培训、违规行为记录等纳入信息网络系统；
- b) 定期梳理业务流程，查找合规风险点，运用信息化手段将合规要求和防控措施嵌入流程，针对关键节点加强合规审查，强化过程管控；
- c) 利用大数据、人工智能等技术手段，动态监测企业经营管理过程，重点监测互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等信息网络服务或技术支持领域，及时预防、识别和应对“帮信行为”；
- d) 建立高、中风险客户、供应商、合作伙伴等全流程业务管理，覆盖事前准入、事中监测、事后管控；
- e) 为企业开展合规培训、考核、审查、举报、调查等工作提供技术保障和支持。

6.4 合规培训

企业宜建立制度化、常态化、全员化且与合规风险相适应的预防、识别和应对“帮信行为”合规培训机制，包括但不限于：

- a) 将企业预防、识别和应对“帮信行为”合规培训纳入员工培训计划；
- b) 针对不同岗位和层级的员工，根据其特定合规风险和岗位职责，开展有针对性的合规培训。基于需要，可向客户、供应商、合作伙伴等相关方提供必要的合规培训；
- c) 培训内容可包括企业预防、识别和应对“帮信行为”合规方针、义务、程序；非法利用信息网络行为及其帮助行为的风险和危害性；如何预防、识别和避免非法利用信息网络行为及其帮助行为；举报非法利用信息网络行为及其帮助行为的渠道；有关非法利用信息网络行为及其帮助行为的典型案例等；
- d) 根据法律法规和监管环境变化，及时更新合规培训材料，确保培训内容的时效性；
- e) 考虑培训形式的丰富性，宜采用线上、线下或混合形式的培训方式，以适应不同员工的学习需求和习惯；
- f) 根据培训内容，对员工进行测试，以验证员工对培训内容的理解和掌握程度，对于测试不合格的员工，宜进行补充培训，测试结果可作为日常工作和绩效考核的参考依据；
- g) 培训记录和测试结果宜形成文件化信息予以保留，并定期对培训和测试的效果进行评估和改进；
- h) 鼓励邀请执法机关、法律专家、行业专家、第三方机构进行法律法规宣讲，提升员工的合规意识和“帮信行为”的识别能力，鼓励员工参加外部相关培训和研讨会。

6.5 应急预案

企业宜建立预防和应对“帮信行为”的应急预案，包括但不限于：

- a) 明确应急处理的相关组织机构、责任人、处理流程、沟通机制、应急措施和资源保障；

- b) 当发生较大或重大“帮信行为”合规风险事件时，及时启动应急预案，以降低企业和员工的损失，较大或重大“帮信行为”合规风险事件包括但不限于：
 - 1) 单日异常交易笔数超过日常均值300%；
 - 2) 用户个人信息泄露涉及5000人以上；
 - 3) 涉案资金流水累计达20万元人民币；
 - 4) 收到公安机关书面协查通知；
 - 5) 其他较大或重大“帮信行为”合规风险事件。
- c) 定期开展应急演练，评估演练效果，并持续改进预案，确保应急预案的适宜性、充分性和有效性。

7 识别

7.1 识别框架

企业宜根据容易发生“帮信罪”的业务领域，构建符合企业自身经营管理需求的“帮信行为”合规风险识别框架，主要包括：

- a) 根据企业主要的经营管理活动识别，重点梳理企业提供的互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等服务，识别可能存在的“帮信行为”，常见“帮信行为”的示例参见附录A；
- b) 根据企业组织机构设置识别，重点梳理与互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等服务相关的管理职能部门、岗位的业务管理范围和工作职责，识别可能存在的“帮信行为”；
- c) 根据利益相关方识别，梳理企业的利益相关方，如员工、客户、供应商、合作伙伴等，识别可能存在的“帮信行为”；
- d) 根据引发“帮信罪”风险的原因识别，对违规提供网络技术支持，或提供广告推广、支付结算等帮助引发“帮信罪”风险原因的识别，识别企业可能存在的“帮信行为”；
- e) 根据“帮信罪”风险事件发生后承担的责任识别，梳理“帮信罪”引发的刑事、行政、民事等法律责任，识别不同责任下企业可能存在的“帮信行为”；
- f) 根据以往发生的案例识别，梳理本行业、本企业发生的与“帮信罪”相关案例，发现企业可能存在的“帮信行为”。

7.2 识别途径

7.2.1 内部途径

企业宜通过以下内部途径识别“帮信行为”，包括但不限于：

- a) 投诉举报：企业员工、客户、供应商、合作伙伴、投资者等通过企业举报渠道揭露的企业或企业内部员工的“帮信行为”；
- b) 帮信风险预警监测：企业宜建立风险预警监测流程，开展异常行为监测和风险预警，通过对重要业务进行“帮信行为”风险预警监测，定位潜在的与“帮信行为”相关的异常行为。监测措施包括但不限于：
 - 1) 业务监控：监控企业业务交易，根据预设帮信风险因子，如异常价格波动，短期高频交易、服务资费异常、广告文本触发敏感词、命中高危客户名录等，识别可疑业务行为；

- 2) 财务监控：跟踪和管理日常的财务活动，包括收入、支出、现金流，跨境交易等执行情况，识别可疑财务记录；
- 3) 人员监控：对于核心岗位人员的日常系统访问，关键操作进行记录，定期复核。
- c) 审计检查：企业在内部审计和外部审计过程中识别“帮信行为”；
- d) 合规审查：企业在合规审查过程中识别“帮信行为”；
- e) 风险评估：企业通过开展风险评估工作，识别“帮信行为”，风险评估方法参见GB/T 24353—2022。

7.2.2 外部途径

企业宜通过以下外部途径识别“帮信行为”，包括但不限于：

- a) 监管通知：企业根据监管部门的举报平台信息、发布的相关通知、警示信息或行业动态，对涉及的业务活动和合作对象进行监测、评估和审查，识别“帮信行为”，并持续关注监管部门发布的风险提示或警告；
- b) 执法机关调查：执法机关调查诈骗、洗钱、舞弊等违法违规案件过程中，执法机构发现“帮信罪”的线索，识别“帮信行为”；
- c) 舆情报道：企业应及时关注线上、线下在本市、本省乃至全国范围内与企业相关的舆情报道，及时识别“帮信行为”。

7.3 识别清单

企业宜对不同途径识别出的“帮信行为”进行归类，形成“帮信行为”识别清单，并列示所适用的法律法规、可能产生的法律后果、法律分析意见及其涉及的业务部门、公司主体、经营管理流程等信息。

识别清单宜由企业合规管理部门进行管理和维护，识别清单示例参见附录B，企业可根据自身情况进行参考和制定。

7.4 分析与评价

企业宜对识别出的“帮信行为”合规风险进行分析和评价，以确定风险高低，包括但不限于以下措施：

- a) 针对“帮信行为”产生的原因、发生的可能性、影响范围、潜在后果等进行分析，可以是定性、定量的分析，也可以是这些分析的组合；
- b) 建立适宜的风险评价准则，确定风险等级。

8 应对

8.1 合规审查

企业宜建立合规审查机制，包括但不限于以下措施：

- a) 明确将企业预防、识别和应对“帮信行为”合规审查作为法律法规的遵守、规章制度制定、重大事项决策、重要合同签署、重大项目运营等经营管理工作的必经程序，及时对不合规的内容提出整改建议，未经合规审查不得实施；
- b) 基于风险分析和评价的结果，确定合规审查的重点领域和中高风险业务环节；
- c) 在企业提供的信息网络服务流程中嵌入审查点，确保合规审查成为常规操作的一部分。

8.2 合规咨询

企业宜建立合规咨询机制，包括但不限于以下措施：

- a) 明确企业预防、识别和应对“帮信行为”合规咨询渠道和流程，使业务部门能够就企业“帮信行为”风险或问题向合规管理部门咨询；
- b) 设定合理的响应时间，确保咨询问题能够及时得到解答；
- c) 保持咨询过程的记录，并对未解决的问题进行追踪；
- d) 适当时，可聘请外部专家或专业机构提供意见和支持。

8.3 合规举报

企业宜建立合规举报机制，包括但不限于以下措施：

- a) 明确企业“帮信行为”举报渠道，包括信箱、电话、电子邮件、APP、小程序、公众号和第三方平台；
- b) 畅通企业“帮信行为”举报渠道，明确企业员工、客户、供应商和第三方均可进行举报和投诉；
- c) 明确支持匿名举报，鼓励实名举报，对举报者的信息进行保密，保护举报者的合法权益和免于遭受打击报复。

8.4 内部调查

企业宜建立内部调查机制，由合规管理部门负责评估、受理、调查企业“帮信行为”的报告或举报，包括但不限于以下措施：

- a) 明确内部调查处置机制的启动条件、开展部门、调查流程和处置措施；
- b) 明确调查过程由具备相应能力的人员独立进行，不受其他部门或管理层干涉；
- c) 调查过程中保障被调查对象的合法权益；
- d) 确保调查过程遵循独立、客观、公正、保密原则；
- e) 调查结果后，依据问责处置截止对违规行为进行问责处理；
- f) 适当时，利用调查结果改进合规管理机制；
- g) 保留有关调查的文件化信息。

注：内部调查指南可参考ISO/TS 37008:2023 组织内部调查 指南，内部调查示例见附录C。

8.5 沟通与报告

企业宜建立沟通与报告机制，包括但不限于以下措施：

- a) 明确企业预防、识别和应对“帮信行为”的内外沟通与报告的准则、流程；
- b) 宜由合规管理部门定期与相关方沟通协调企业预防、识别和应对“帮信行为”合规管理情况，沟通内容可包括合规文化、合规义务、合规承诺；
- c) 宜由合规管理部门定期向最高管理者汇报企业预防、识别和应对“帮信行为”合规管理情况，报告内容可包括合规文化、合规义务、合规承诺、合规风险评估、合规审查、内部调查和与监管机构沟通和通报的事项等；
- d) 当发生性质严重或重大影响的“帮信行为”等违规行为时，及时向最高管理者汇报，由合规管理部门提出相应的应对措施。必要时，按有关要求向行政主管部门汇报或寻求帮助。

8.6 处置措施

企业宜根据合规审查（8.1）、合规咨询（8.2）、合规举报（8.3）、内部调查（8.4）、沟通与报告（8.5）等情况，采取适当的风险处置措施，应对“帮信行为”合规风险，包括但不限于以下措施：

- a) 对识别的“帮信行为”合规风险，采取适当、有效的应对处置措施，将“帮信行为”合规风险控制在企业可承受的范围；
- b) 对于重大“帮信行为”合规风险事件，宜制定应急预案（6.5），明确牵头部门和协同部门，最大程度化解风险、降低损失；
- c) 根据企业环境、法律法规的变化，对风险处置措施进行定期评审和修改。

8.7 合规奖惩

企业宜建立合规奖惩机制，包括但不限于以下措施：

- a) 根据合规方针，明确企业预防、识别和应对“帮信行为”奖励和惩罚标准；
- b) 对合规工作成效显著或合规考核优秀的相关团队或个人给予表彰和奖励；
- c) 对违规个人、团队、合作伙伴或相关方进行问责处置。问责处置措施包括警告、处分、处罚、降职、免职、解聘等；赔偿、终止合作、纳入黑名单等。对于涉事员工造成企业及关联公司、员工、客户、供应商、合作伙伴、投资者造成损失的，企业保留通过谈判、仲裁、诉讼等途径追偿的权利。

8.8 配合执法

企业宜考虑以下方式配合执法机关开展工作：

- a) 与属地公安机关建立稳定的沟通渠道，对已确认的“帮信行为”或线索，及时向执法机关报案；
- b) 涉事员工或相关企业触犯相关法律法规，企业宜按照内部规章制度进行处理，并向公安机关报案，以及配合司法机关调查；
- c) 依照相关规定配合执法部门调查取证，按照司法协助流程和有关调证文书，提供必要的信息和协助；
- d) 与司法机关开展案例研讨和合规培训工作。

9 监督检查

企业宜实时跟踪内外部帮信罪领域环境的变化，及时监督和检查预防、识别和应对“帮信行为”合规管理工作的运行情况，以确保防范措施的有效执行和防范工作的持续改进，包括但不限于：

- a) 定期审计：企业定期开展防范“帮信行为”专项审计，以确保各项防范措施得到有效执行；
- b) 定期自查：企业定期进行防范“帮信行为”自查，查找漏洞、排除隐患，及时整改问题和经验总结；
- c) 不定期检查：企业不定期对企业经营管理开展“帮信行为”合规检查，调阅所需的记录和文件，访谈和检查相关部门及员工；
- d) 风险提示：根据内外部“帮信行为”风险环境的变化，如法律法规、相关政策、标准的出台和变化，司法、执法及社会守法环境的变化，企业自身战略的调整改变、重大交易、投资等，及时发布帮信预警信息和风险提示；
- e) 第三方评估：必要时，邀请第三方机构进行防范“帮信行为”合规专项评估，查找潜在的“帮信行为”风险和漏洞；
- f) 外部合作：与相关执法机构、安全机构、行业协会等建立合作关系，共同防范“帮信行为”的发生。

附录 A
(资料性)
常见“帮信行为”的示例

A.1 常见“帮信行为”示例

- a) 违规提供支付结算服务：明知他人使用支付结算工具用于结算犯罪收益或支付合作方存在刑事风险或不当交易，仍继续提供支付结算服务；
- b) 违规提供第三方支付接口：未按规定落实商户实名制管理要求，为假名、匿名商户提供第三方支付接口，使第三方支付接口被用于转移犯罪收益；或明知第三方支付接口可能被用于转移犯罪收益，仍继续提供第三方支付接口等支付结算的帮助；
- c) 违规提供网络存储服务：明知存储的内容涉及犯罪活动，仍提供存储服务或提供安装、调试及配置系统等技术支持服务；
- d) 违规提供互联网接入服务：明知互联网接入服务可能被用于电信网络诈骗等信息网络犯罪，仍继续为其办理或提供安装、调试及配置系统等技术支持服务；
- e) 违规提供服务器托管：明知其所托管服务器被用于实施犯罪活动，如非法网站、恶意软件传播等，仍继续提供托管服务；
- f) 违规提供通讯传输等技术知识：明知他人将利用通讯传输技术实施犯罪，仍继续提供相应的技术知识帮助；
- g) 违规提供广告推广：明知其广告内容或目标链接与犯罪活动相关，仍继续提供广告推广服务；
- h) 违规提供 APP、小程序、网站的开发、技术支持等服务：明知 APP、小程序、网站涉及赌博、诈骗、传销、虚假股票、虚假期货证券交易，仍继续提供开发、技术支持等服务；
- i) 提供信息网络服务的资费明显不符合行业一般标准：明知提供信息网络服务所收取的业务费用金额明显不符合行业一般标准，仍继续提供信息网络服务；
- j) 平台商户出现交易价格或方式明显异常：明知平台中的商户的交易价格或者方式明显异常，可能涉及违法行为，仍继续提供技术支持服务，不履行平台义务和监管职责；
- k) 平台商户出现虚假身份或逃避监管的行为：明知平台中的商户使用虚假身份，逃避监管或者规避调查的行为，仍继续提供技术支持等服务；
- l) 平台商户违规收集、泄漏个人信息：明知平台中的商户非法收集、泄漏公民个人信息，仍继续提供技术支持等服务；
- m) 平台商户存在中高风险账户资金流水明显异常情况：明知平台中的中高风险账户存在资金流水明显异常，仍继续提供技术支持等服务；
- n) 帮助他人违规开办银行卡、信用卡：明知他人开办银行卡、信用卡可能用于实施典型网络诈骗等犯罪行为，仍帮助其开办银行卡、信用卡的；
- o) 收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书的；
- p) 收购、出售、出租他人手机卡、流量卡、物联网卡的；
- q) 明知收寄的物品存在性质、数量、重量及其他可能涉及诈骗或洗钱犯罪等的异常情况，仍继续提供寄递服务的。

A.2 认定为“明知”的行为

帮助非法利用信息网络行为中，具有下列情形之一的，可认定为“明知”，但是有相反证据的除外：

- a) 经监管部门告知后，仍然实施有关行为的；
- b) 接到举报后不履行法定管理职责的；
- c) 交易价格或者方式明显异常的；
- d) 提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的；
- e) 频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的；
- f) 为他人逃避监管或者规避调查提供技术支持、帮助的；
- g) 其他足以认定行为人明知的情形。

注：上述认定为“明知”的行为，参考《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（2019年6月3日最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院第十三届检察委员会第二十三次会议通过，自2019年11月1日起施行）第十一条规定的“明知”。

A.3 认定为“情节严重”的行为

帮助非法利用信息网络行为中，具有下列情形之一的，可认定为“情节严重”：

- a) 为三个以上对象提供帮助的；

注：“为三个以上对象提供帮助”，指的是分别为三个以上行为人或团伙组织提供帮助，且被帮助的行为人或团伙组织实施的行为均达到犯罪程度。为同一对象提供三次以上帮助的，不是“为三个以上对象提供帮助”。

参考《最高人民法院、最高人民检察院、公安部关于“断卡”行动中有关法律适用问题的会议纪要》（2022年3月22日）第二点中的规定。

- b) 支付结算金额二十万元以上的；
- c) 以投放广告等方式提供资金五万元以上的；
- d) 违法所得一万元以上的；

注：“违法所得一万元”中的“违法所得”，指的是行为人为他人实施信息网络犯罪提供帮助，由此所获得的所有违法款项或非法收入；行为人收卡等“成本”费用无须专门扣除。参考《最高人民法院、最高人民检察院、公安部关于“断卡”行动中有关法律适用问题的会议纪要》（2022年3月22日）第三点中的规定。

- e) 出租、出售的信用卡被用于实施电信网络诈骗，达到犯罪程度，该信用卡内流水金额超过三十万元的；

注：“流水金额超过三十万元”，指的是单向流入涉案信用卡中的资金超过三十万元，且其中至少三千元经查证系涉诈骗资金。行为人能够说明资金合法来源和性质的，应当予以扣除。参考《最高人民法院、最高人民检察院、公安部关于“断卡”行动中有关法律适用问题的会议纪要》（2022年3月22日）第四点的规定。

- f) 被帮助对象实施的犯罪造成被害人及其近亲属死亡、重伤、精神失常等严重后果的；

注：参考《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（2019年6月3日最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院第十三届检察委员会第二十三次会议通过，自2019年11月1日起施行）第十二条（六）的规定和《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》第二点（二）第1项的规定。

- g) 二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；
- h) 收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书五张（个）以上的；
- i) 收购、出售、出租他人手机卡、流量卡、物联网卡二十张以上的；

- j) 确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第 b 项至第 d 项规定标准五倍以上，或者造成特别严重后果的；
- k) 其他情节严重的情形。

注1：上述认定为“情节严重”的行为，参考《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》(2019年6月3日最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院第十三届检察委员会第二十三次会议通过，自2019年11月1日起施行)第十二条规定的“情节严重”。

注2：h) i) 参考《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》第九点的规定。

附 录 B
(资料性)
识别清单示例

企业“帮信行为”合规风险识别清单可以划分三个信息区，第一部分为基础信息区，主要为识别代码、风险/行为名称、风险/行为描述、识别途径；第二部分为管理信息区，主要为涉及的部门和公司主体以及相关业务活动，第三部分为法律信息区，主要为涉及的法律法规、法条、责任与后果和法律建议。见表B.1所示。

表B.1 企业“帮信行为”合规风险识别清单示例

基础信息区				管理信息区			法律信息区			
识别代码	风险/行为名称	风 险 / 行为描述	识别途径	涉 及 的 部 门	涉 及 的 主 体 公 司	涉 及 的 业 务 活 动	涉 及 的 法 律 法 规	涉 及 的 法 条	引发的责任与后果	法 律 建议

附录 C

（资料性）

内部调查示例

C.1 组建调查团队

合规管理部门负责企业的内部调查工作，由合规管理部门组建调查团队，对内、外部途径识别出的“帮信行为”展开调查。

如有必要，调查团队可申请其他团队支持，如技术部门、相关业务部门、审计部门和法律部门等，企业最高管理者宜给予支持并配置必要资源。

调查团队可包括独立的外部顾问。

C.2 预评估

在开展内部调查之前，由调查团队对“帮信行为”线索进行初步研究和评估，包括但不限于：

- a) 确认举报内容是否真实可靠；
- b) 举报内容是否符合“帮信行为”范畴；
- c) 确定主要参与者、涉及的业务结构、技术问题、适用的法律法规和公司内部制度；
- d) 确认举报内容是否需要提交给执法或监管机构；
- e) 确认是否需要立即停止或暂停业务活动；
- f) 确认在企业外被举报的可能性；
- g) 评估是否需要进行全面调查，并利用评估结果制定调查计划；
- h) 评估聘请外部顾问的必要性；
- i) 预评估的结果为企业最高管理者提供审查和决策依据；
- j) 预评估的结果以书面形式记录，并妥善保存和保密，预评估报告可能包括下列一项或多项内容：
 - 1) 如有需要，可与其他职能部门合作，并在不影响调查的信任、公正性和保护的情况下支持调查；
 - 2) 收集更多的信息；
 - 3) 采取初步措施（如暂停业务、获取证据等）；
 - 4) 调查“帮信行为”的报告；
 - 5) 参考或协调其他程序；
 - 6) 通知有关部门（如执法部门或监管机构）；
 - 7) 总结案件。

C.3 内部调查

C.3.1 调查原则

调查团队宜按照企业内部调查制度对予以受理的“帮信行为”的案件开展内部调查，企业宜确保调查过程遵循独立、客观、公正、保密的原则，调查结果以书面形式记录，保存调查的全部记录和最终调查报告，保证记录和报告的可追溯性、真实性和完整性。

C.3.2 确定调查范围

调查团队宜根据初步评估的结果和以下因素，确定调查对象和范围，以便充分、有效地开展调查工作，包括但不限于：

- a) 调查的预期目标；
- b) “帮信行为”的具体特征和行为过程；
- c) 调查的时间周期；
- d) “帮信行为”具体发生的地点；
- e) 调查范围覆盖哪些地区或国家；
- f) 涉及“帮信行为”的违规企业、部门、人员等信息；
- g) 在调查过程中，如发现有其他违法违规的情况，调查团队需要相应调整调查范围，并将调查范围的变更记录在案。

C.3.3 制定调查计划

调查团队制定调查计划时，宜考虑以下因素：

- a) 调查的背景资料、范围、任务分工、计划表、方法、目的和目标；
- b) 需要访谈或提供信息协助调查的人员；
- c) 实现目标所需和可用的内、外部资源，以及可能需要的专家资源，如会计师、审计师、法律顾问、外部调查员、行业专家等；
- d) 评估是否必须在调查期间暂停涉事人员对办公室或信息系统的访问权限及工作职权；
- e) 潜在的证据来源以及如何处理证据的收集、保存和评估；
- f) 如何进行访谈及访谈时间表；
- g) 是否存在重大法律问题；
- h) 调查对象可能给调查和企业带来的风险或挑战，以及如何应对这些风险或挑战；
- i) 如何记录调查情况，需要向哪些相关方报告，何时报告，报告的详略程度；
- j) 是否需要向监管机关报告；
- k) 调查团队可以随情况的变化调整调查计划，以确保调查符合调查范围、目标和原则，调查计划的变更宜记录在案。

C.3.4 访谈

访谈通常包括与可能知情或涉及案件的员工、供应商、客户、合作伙伴等相关方的交流，帮助企业了解和核实涉及“帮信行为”的情况，获取重要信息和证据。访谈工作包括但不限于：

- a) 准备工作：在进行访谈之前，调查团队需要准备以下工作：
 - 1) 确定访谈对象名单，一般包括投诉举报人、涉事员工及周围人员、企业内部相关部门人员、相关企业人员，还可以访谈相关政府机构工作人员；
 - 2) 确定调查访谈人员，调查访谈人员的配置和素质至关重要，确保至少有两名调查人员，调查访谈人员需要具备高度的职业操守、道德规范和专业素养；
 - 3) 确定访谈计划，包括主题大纲、必要的问题和访谈中使用的文件资料或其他材料，并确认访谈的时间安排和顺序；
 - 4) 采用适当的访谈技巧，以便获取准确信息并促使访谈对象配合；
 - 5) 采用适当的访谈方式、形式和技术工具，以有效获取关键信息和证据。
- b) 执行访谈：在访谈中，一名访谈人员负责访谈，另一名负责记录或录音，或帮助出示一些材料。访谈人员宜准确记录访谈过程，访谈结束后，访谈人员需要访谈对象确认所记录的陈述是否

真实和准确，并询问是否有任何进一步的补充或澄清。在适当和允许的情况下，访谈对象可以在访谈记录上签字；

- c) 保存访谈记录：访谈记录宜充分、适当地记录在案，访谈结果宜妥善保管并保密。

C.3.5 证据收集和存储

调查团队在法定框架和企业有关制度下，及时并尽可能收集与“帮信行为”相关的证据和信息，所有收集到的证据和信息宜进行备份和安全存储，确保数据不被丢失或篡改。

有关书面、音频、视频证据材料，确保没有修改或剪辑，并存储原始文件。

C.3.6 技术隔离

企业宜采取技术手段隔离或证据固定涉及“帮信行为”的信息系统、设备，并冻结相关系统权限，防止事态扩大。

C.3.7 调查完成

调查团队完成所有必要的调查步骤，收集足够的证据来支持调查结果，并且达到内部调查的目的，调查结果满足启动补救和实施整改的充分条件，表明调查工作完成。

C.4 调查报告

调查报告根据书面、音频、视频和口头证据编写，宜充分说明相关事实、局限性和遇到的制约因素，并仅限于调查范围，调查报告内容包括但不限于：

- a) 报告摘要：通常包括主要调查结果、结论和补救措施建议；
- b) 背景说明：通常包括所涉部门或单位、所涉单位的相关活动、所涉员工和员工关系、事件的背景事实以及有待解决的事实问题；
- c) 证据分析：通常包括各方立场、支持各方立场的证据、评估事实、确定相关事实、驳回无关事实以及评估争议事实的可信度；
- d) 调查结论：通常包括参考的法律法规和标准、用于实现所调查事实的目标的结论、用于确定举报或识别的“帮信行为”是否成立或确定的调查结果等关键要素；
- e) 整改和建议：如企业需要，还可包括整改和建议等内容。

参 考 文 献

- [1] 中华人民共和国刑法修正案（九）
 - [2] 中华人民共和国网络安全法
 - [3] 最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释
 - [4] 最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见
 - [5] 最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）
 - [6] 最高人民法院、最高人民检察院、公安部关于“断卡”行动中有关法律适用问题的会议纪要
 - [7] 非银行支付机构网络支付业务管理办法
 - [8] 中华人民共和国反电信网络诈骗法
 - [9] 中华人民共和国反洗钱法
 - [10] 中华人民共和国广告法
 - [11] GB/T 26317—2010 企业治理风险管理指南
 - [12] GB/T 27914—2023 风险管理 法律风险管理指南
 - [13] GB/T 35770—2022/ISO 37301:2021 合规管理体系 要求及使用指南
 - [14] SZDB/Z 245—2017 反贿赂管理体系
 - [15] DB4403/T 350—2023 企业合规管理体系
 - [16] ISO 22361:2022 安全与韧性 危机管理 指南
 - [17] ISO 37000:2021 组织治理 指南
 - [18] ISO 37001:2016 反贿赂管理体系 要求及使用指南
 - [19] ISO 37002:2021 举报管理系统 指南
 - [20] ISO/DIS 37003 舞弊控制管理体系 组织应对舞弊风险的指南
 - [21] ISO/TS 37008:2023 组织内部调查 指南
 - [22] ISO/AWI 37009 利益冲突指南
-