国际标准

ISO
37002

第一版

2021-07-27

举报管理体系　指南

文件号
ISO 37002:2021(E)

ISO 版权办公室

地址：Ch.de Blandonnet 8· CP 401

CH-1214 Vernier, Geneva, Switzerland

电话：+ 41 22 749 01 11

传真：+ 41 22 749 09 47

邮箱：copyright@iso. org

网址：www.iso.org

目录

意识

前言

举报是指举报可疑的不法行为或不法行为风险的行为。研究和经验表明，很大一部分不法行为是通过组织内部或接近组织 的人员的报告引起受影响组织的注意的。

各组织越来越多地考虑引入或改进内部举报政策和流程， 以响应监管或自愿。

本文件为组织建立、实施、维护和改进举报管理体系提供了指导，其结果如下：

a） 鼓励和便利举报不当行为；

b） 支

c） 确

d） 改

e） 减

对组织

-允许组

-帮助防

-确保遵

-吸引和

- 向社会、市场、监管机构、所有者和管理者展示管理、道德的治理实践

其他相关方。

有效的举报管理系统将通过以下方式建立组织信任：

-展示领导层对预防和解决不当行为的承诺；

-鼓励人们尽早举报不当行为；

-减少和防止对举报人和其他相关人员的有害待遇；

-鼓励一种文化公开、透明、正直和问责。

本文件为组织基于信任、公正和保护原则创建举报管理系统提供指导。它是适应性强的，其使用将随组织活动的规模、性质、复杂性和管辖权而变化。它可以帮助一个组织改进其现有的举报政策和程序，或遵守适用的举报立法。

本文件采用了 ISO 制定的“协调结构”（即条款顺序、通用文本和通用术语），以提高管理体系国际标准之间的一致性。各组织可采用本文件作为其组织的独立指南，或与其他管理体系标准一起采用，包括解决其他 ISO管理体系中与举报相关的要求。

图 1 是推荐的举报管理系统的概念性概述，显示了信任、公正和保护原则如何覆盖此类系统的所有要素。

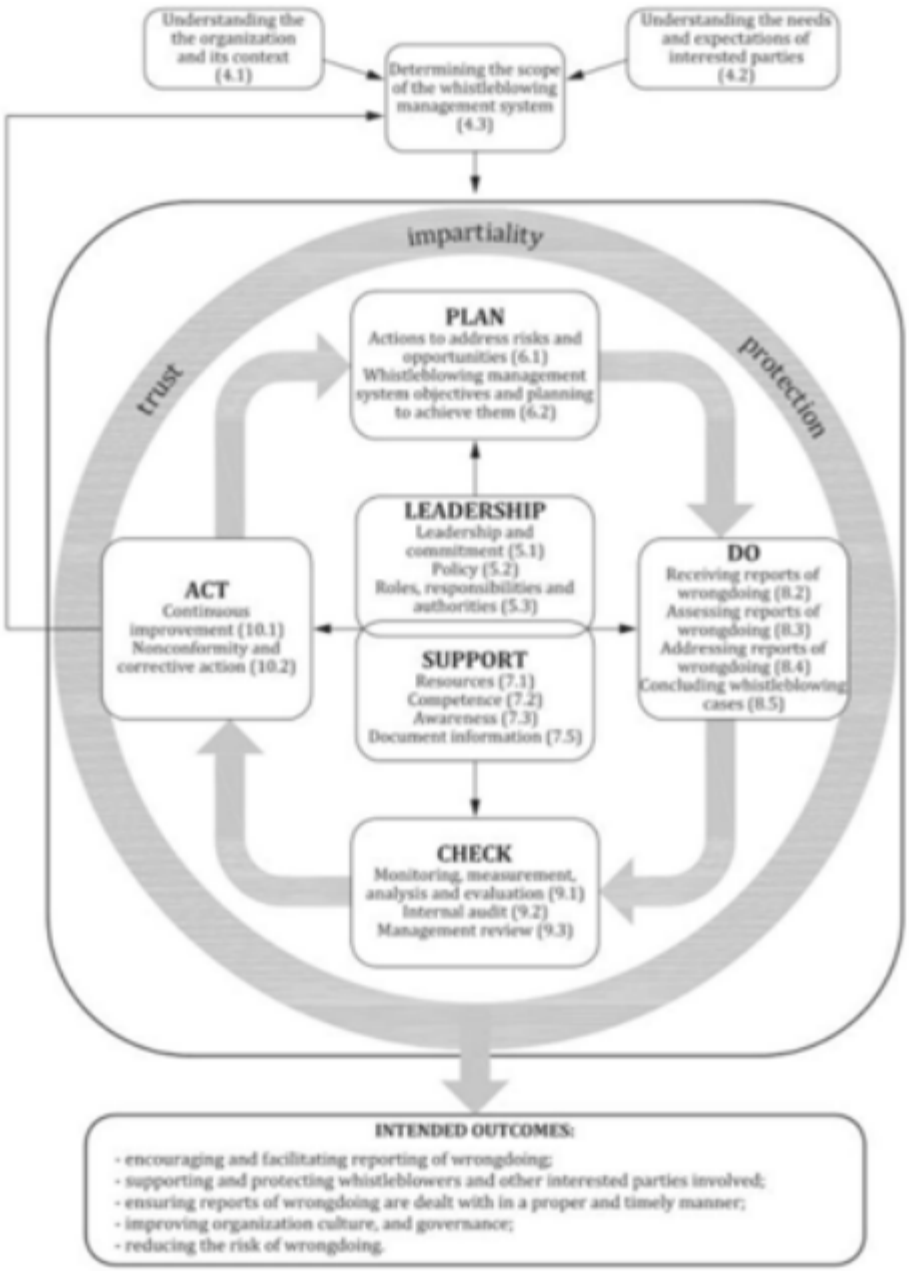


Figure 1 — Overview of a whistleblowing management system

前言

ISO（国际标准化组织）是世界范围内的国家标准机构（ISO 成员机构）联合会。制定国际标准的工作通常是通过 ISO技术委员会来进行的。对建立了技术委员会的主题感兴趣的每个成员机构均有权代表该委员会。与 ISO联络的政府和非政府国际组织也参加了这项工作。ISO 在电气标准化的所有问题上与国际电工委员会（IEC）紧密合作。

ISO / IEC 指令第 1 部分中描述了用于开发本文档的过程以及旨在对其进行进一步维护的过标准。本文档是根据 iso. ocg / directives

请注意，本何或所有此类专利权的在“简介”和/或 ISO收

本文档中使构成对本产品的认可。

有关标准的自愿性质的解释，与合格评定有关的 ISO特定术语和表达的含义，以及有关 ISO遵守《技术性贸易壁垒（TBT）中的世界贸易组织（WTO）原则》的信息，请参见 www. iso. org / iso / foreword. html。

关于本文档的任何反馈或问题应直接发送给用户的国家标准机构。这些机构的完整列表可以在 www. iso. org/members. htmL 中找到。

举报管理体系指南

1 范围

本文件根据信任、公正和保护的原则，在以下四个步骤中为建立、实施和维护有效的举报管理体系提供了指导：

a） 收到不法行为报告；

b） 评估不当行为报告；

c） 处理不当行为报告

d） 结束揭发

本文件的指导 规模、性质， 以及公共

这些指南的适 系统可以是独立的，也

2. 规范性引用

本文件中没有规范性引用文件。

3 术语和定义

以下术语和定义适用于本文件。

ISO和 IEC在以下地址维护用于标准化的术语数据库：

-ISO在线浏览平台：可在 https：//www. iso. org/obp

-IEC 电子百科：可在 https：//www. electropedia. org/

3. 1 管理系统

一个组织（3.2）的一组相互关联或相互作用的元素，以制定政策（3.7）和目标（3.25），以及实现这些目标的过程（3.27）

注 1：一个管理系统可以针对一个或多个专业。

注 2：管理体系要素包括组织结构、角色和职责、规划和运营。

注 3：这是协调结构的常见术语和核心定义之一适用于 ISO管理体系标准。

3.2 组织

有自己的职责、权限和关系以实现其目标的个人或群体（3.25）

注 1：组织的概念包括但不限于个体经营者、公司、法人团体、商号、企业、当局、合伙企业、慈善机构或机构，或其部分或组合，无论是否成立、公共或私人。

注 2：如果该组织是较大实体的一部分，则术语“组织”仅指在举报（3.10）管理体系（3.1）范围内的较大实体的一部分。

注 3：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3.3 全体人员

组织的（3.2）主管、官员、员工、临时员工或工人以及志愿者

[来源： ISO 37001: 2016, 3.25，条目的修改注释 1 和 2 已被删除。]

3.4 利益相关方（首选术语）

利益相关者（承认任期）

可能影响、受某项决策或活动影响或认为自己受其影响的个人或组织（ 3. 2）

注 1：利益相关方可以是组织内部或外部。

注 2：相关方可包括但不限于报告人、报告的任何主体、证人、人员（ 3. 3 ）、工

人代表、供应商、第三方、公众、媒体、监管机构和整个组织。

注 3：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。通过在条目中添加注释 1 和注释 2，对原始定义进行了修改。

3.5 高层管理人员

领导和控制一个组织的人或一群人离子（3.2）处于最高水平

注 1：最高管理层有权在组织内授权和提供资源。

注 2：如果管理体系（3.1）的范围仅涵盖组织的一部分，那么最高管理者指的是指导和控制该部分组织的人。

注 3：这是 ISO

3.6 管理机构

对整个组织（3.

注 1：无论是否

注 2：理事机构

人。

[来源： ISO/IEC 38500: 2015，2.9，修改了“对……负有最终责任”一词，替换了“对……的性能和合规性负有责任”，并增加了条目注释 1 和注释 2。]

3.7 政策

最高管理层（3.5）正式表达的组织意图和方向（3.2）

注 1：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 8 不法行为

可能造成损害的行为或疏忽

注 1：不当行为可包括但不限于以下内容：

-违反法律（国内或国际），如欺诈、腐败（包括贿赂）；

-违反组织（3.2）或其他相关行为准则，违反组织政策（3.Z）；

-严重疏忽、欺凌、骚扰、歧视、未经授权使用资金或资源、滥用权力、利益冲突、严重浪费或管理不善；

对人权、环境、公共卫生和环境造成损害或可能造成损害的作为或不作为

-安全、安全工作实践或公共利益。

注 2：不当行为或由此造成的损害可能发生在过去、目前或将来。

注 3：潜在危害可通过参考单个事件或一系列事件来确定。

3.9 告密者

报告可疑或实际不当行为的人（3.8），并有理由相信报告时的信息是真实的

注 1：合理信念是指个人基于观察、经验或已知信息而持有的信念，在相同情况下也会持有。

注 2：举报人的例子包括但不限于：

-组织内的人员（3.3）（3.2）；

-与组织建立关系的外部各方人员，包括法人，或

计划建立某种形式的商业关系 nship 包括但不限于客户、客户、合资公司

合资企业、合资企业合作伙伴、财团合作伙伴、外包供应商、承包商、顾问、分包商

-承包商、供应商、供应商、顾问、代理人、分销商、代表、 中介和投资者工会

代表等其他人士；

- 以前或将来担任本定义所述职位的任何人。

3. 10 告密

检举人（ 3. 9 ）举报涉嫌或实际不当行为（ 3. 8）

注 1：不当行为报告可以是口头、面对面、书面或电子或数字格式。注 2：常见的区别是：

-公开检举，检举人在不隐瞒其身份或身份的情况下披露信息

要求对其身份保密；

机密举报，举报者

-收件人知道这些 础的信息检举人的同意

-匿名举报，在没

注 3：组织（ 3. 2 或等效术语。

3. 11 举报管理职能

对举报（ 3. 10） 管理体系（ 3. 1 ）的运行负有责任和权限的人员

3. 12 分流

评估初始不当行为报告（ 3. 8），以便分类、采取初步措施、确定优先顺序和分配进一步处理

注 1：可以考虑以下因素：不当行为或疑似不当行为对人员（3. 3）、组织（3. 2）和相关方（ 3. 4）影响的可能性和严重性，包括声誉、财务、环境、人为或其他

损害。

3. 13 有害行为

可能对检举人（ 3. 9 ）或与检举有关的其他相关利益方（ 3. 4 ）造成损害的威胁、提议或实际、直接或间接的作为或不作为（ 3. 10）

注 1：伤害包括任何与工作相关或个人的不利后果，包括但不限于解雇、停职、降职、调动、职责变更、工作条件变更、不良绩效（3. 26）评级、纪律处分程序、晋升机会减少、拒绝服务、黑名单、，抵制、损害名誉、披露举报人身份、经济损失、起诉或法律行动、骚扰、隔离、施加任何形式的身体或心理伤害。

注 2：有害行为包括报复、报复、报复、故意作为或不作为，故意或不计后果地对举报人或其他相

注 3：有害行为还 中任何一个步骤的可

注 4：就本文件而言 与检举人在检举中的

注 5：其他相关利 向举报者提供支持的

3. 14 调查

系统、独立和文件化的过程（ 3. 27），用于确定事实并对其进行客观评估， 以确定不法行为（ 3. 8 ）是否已经发生、正在发生或可能发生，及其程度。注 1：调查

可以是内部调查，也可以是外部调查。这可以是一项联合调查。

注 2： 内部调查由组织（ 3. 2 ） 自身或外部代表进行。

注 3：外部各方也可以对该组织进行调查。

3. 15 审计

获取证据并对其进行客观评估的系统和独立流程（ 3. 27），以确定满足审计标准的程度

注 1：审计可以是内部审计（第一方）或外部审计（第二方或第三方），也可以是组合审计（组合两个或多个专业）。

注 2： 内部审计由组织（ 3. 2 ） 自身或外部代表进行。

注 3： “ 审计证据 ” 和 “ 审计标准 ” 的定义见 ISO 19011。

注 4：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 16 能力

运用知识和技能实

注 1：这是 ISO管

3. 17 一致性

满足要求（ 3. 28）

注 1：这是 ISO管

3. 18 不一致

不满足要求（ 3. 28）

注 1：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 19 纠正措施

消除不合格原因（ 3. 18） 并防止再次发生的措施

注 1：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 20 持续改进

提高绩效的经常性活动（ 3. 26）

注 1：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 21 文件化信息

组织（ 3. 2 ）需要控制和维护的信息及其包含的媒介

注 1：记录的信息可以是任何格式和媒体，也可以来自任何来源。

注 2：记录信息可参考：

-管理体系（ 3. 1 ），包括相关流程（ 3. 27）；

-为组织运作而创建的信息（文件）；

-取得成果的证据（记

附注 3ry：这是 ISO管

3. 22 有效性

计划活动的实现程度

注 1：这是 ISO管理体

3. 23 测量

确定值的过程（ 3. 27）

注 1：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 24 监控

确定系统、过程（ 3. 27）或活动的状态

注 1：为确定状态，可能需要检查、监督或严格观察。

注 2：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 25 目标

有待取得的成果

注 1： 目标可以是战略目标、战术目标或作战目标。

注 2： 目标可以与不同的学科（如财务、健康、安全和环境）相关，例如，它们可以是组织范围内的，或者特定于项目、产品、服务或过程（ 3. 27）。

注 3： 目标可以用其他方式表达，如预期结果、 目的、操作标准、检举（ 3. 10） 目标，或使用其他

注 4：在检举管理体 7） 设定， 以实现具体

注 5：这是 ISO管理

3. 26 绩效

可衡量的结果

注 1：绩效可以与定量或定性结果相关。

注 2：绩效可能与管理活动、流程（ 3. 27） 、产品、服务、系统或组织（ 3. 2 ）有关。

注 3：这是统一标准的通用术语和核心定义之一 ISO管理体系标准的结构。

3. 27 过程

一组相互关联或相互作用的活动，使用或转换输入以交付结果

注 1：过程的结果是否被称为输出、产品或服务取决于引用的上下文。

注 2：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 28 要求

明示的、通常暗示的或强制性的需要或期望

注 1：“一般暗示”是指组织（ 3. 2 ）和利益相关方（ 3. 4 ）的习惯或惯例是暗示考虑中的需求或期望。

注 2：规定要求是指文件化信息（ 3. 21） 中规定的要求。

注 3：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。

3. 29 风险

不确定性对目标的影响（ 3. 25）

注 1：影响是偏离预期的正面或负面。

注 2：不确定性是指与事件、其后果或可能性相关的信息、理解或了解不足的状态，甚至是部分。

注 3：风险通常以潜在事件（定义见 ISO指南 73）和后果（定义见 ISO指南 73）或两者的组合为特征。

注 4：风险通常表示为事件后果（包括环境变化）和相关发生可能性（定义见 ISO指南 73） 的组合。

注 5：这是 ISO管理体系标准协调结构的通用术语和核心定义之一。对原有定义进行了修改，在定义中添加了“关于目标 ”。

3. 30 责任

对他人履行责任的义务

4. 组织的背景

4. 1

组织举报管理体系预期结果

这些

a）

b）

c） 组织业务的性质、文化、规模和复杂性活动和业务；

d） 人员的性质和需求；

e） 组织的商业模式；

f）组织拥有控制权的实体和对公司行使控制权的实体

组织，包括该组织的受益所有人；

g） 组织的商业伙伴；

h） 该组织承担的公共利益义务或问题；

i） 适用的法定、监管、合同和其他义务和职责。

如果一个组织直接或间接控制另一个组织的管理，则该组织对该组织具有控制权。

4. 2 了解相关方的需求和期望

组织应确定：

a） 与举报管理体系相关的相关方；

b） 这些相关方的相关要求；

c） 哪些要求将通过举报管理系统解决。

4. 3 确定举报管理体系的范围

组织应确定举报管理体系的边界和适用性， 以确定其范围。

在确定该范围时，组织应考虑：

a） 4. 1 中提到的外部和内部问题；

b） 4. 2 中提到的要求；

c） 谁可以报告（内部/外部利益相关方）、来自何处（地区/地理位置）和什么系统涵盖了各类不当行为（见图 2）；

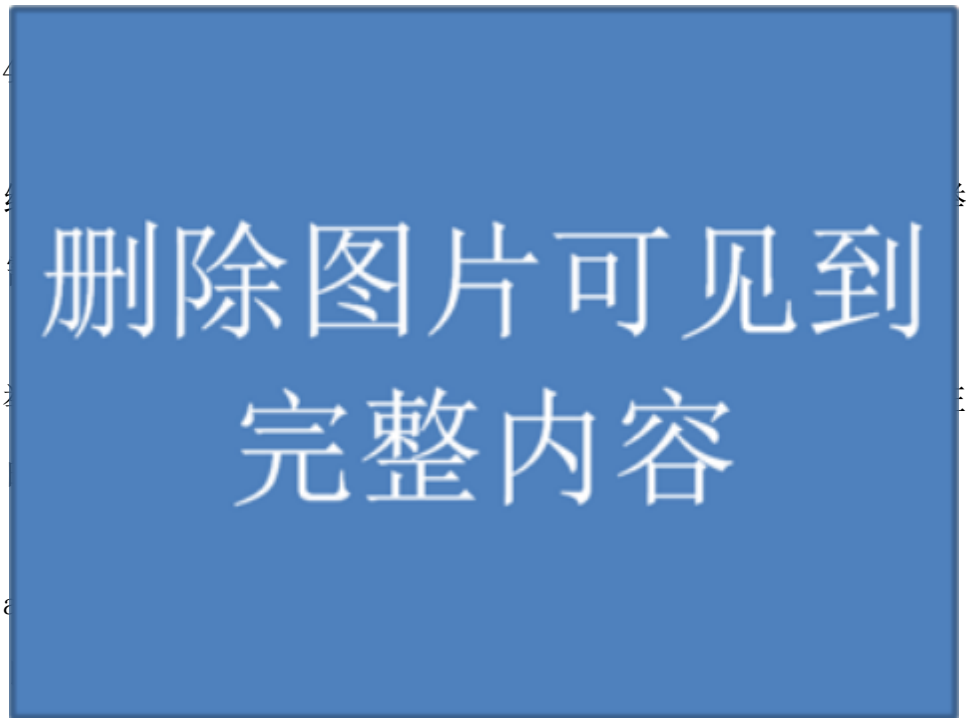
d） 任何合规风险评估或同等评估的结果（如有）。

组织可以参考 ISO 37301 进行合规风险评估，参考 ISO 31000 进行风险管理。

举报管理系统可以处理的不当行为类型（如果报告）对其范围很重要。并非向举报管理系统提交的所有报告都在其范围内，一份报告可以包括关于多种类型不当行为的信息，有些在范围内，有些在范围外。组织应确定现有或计划的其他流程将用于解决举报管理体系范围之外的举报不当行为（例如投诉、申诉），以及如何协调这些流程。如图 2 所示

范围应作为文件化信息提供。

图 2-举报管理系统与其他系统之间的关系组织过程和系统



4

组 举报管理体系，包括所

整个过程中提供适当

a 3 中包含的因素，可

b） 评估不当行为报告（分类）：举报管理系统应规定评估收到的报告的过程，包括优先级、完整性和信息的相关性。同时，应建立举报管理制度提供对损害风险以及保护和支持水平的评估

c ）处理不当行为报告：举报管理系统应提供进行公正及时的调查， 以及有效及时的保护和支持针对检举人和其他相关人员的适当措施和监控，包括报告的主题。这些保护措施可以预防和遏制补救损害。

d）检举案件结案：检举管理系统应提供关闭调查并根据建议和建议采取行动的机制根据解决步骤的结果做出决策。它还应确保支持措施可以继续并将继续下去

5. 1. 2 最高管理层

最高管理层应通过以下方式展示对举报管理体系的领导和承诺：

（a）确保举报政策和举报管理体系目标已确立，并符合公司的价值观、 目标和战略方向组织

b） 批准组织的举报政策；

c）确保举报管理系统的可访问性，并鼓励其使用；

d） 确保将举报管理系统要求整合到组织的业务流程，包括管理系统；

e ） 确保举报管理系统所需的资源可用，充分、适当和部署；

f ） 传达有效举报管理和遵守法律的重要性组织建立的举报管理体系要求；

g ） 在内部和外部传达举报政策（见 7. 4 ）；

h） 确保举报管理系统达到预期结果[见 6. 1]；

i ） 指导和支持人员为举报的有效性做出贡献管理制度；

j ）促进持续改进；

k） 支持其他相关角色， 以展示其在其工作领域的领导力责任

1 ） 致力于、促进和实践组织内的直言不讳/倾听文化，积极参与相关员工培训课程，并在征得其同意后公开赞扬该组织的举报人；

m）确保检举人和其他相关人员不会在工作中受到本组织的损害与举报的关系；

n） 按计划的时间间隔，接收和审查报告关于举报管理制度；

0）确保对使用该系统报告的事项进行公正调查，无论其身份如何举报者的身份、报告的主题以及所发现问题的影响。

注 1：本文件中提及的“业务 ”可以广义地解释为指那些对组织存在的目的至关重要的活动。

注 2：直言不讳/倾听的文化意味着提供一个值得信赖的双向环境，在这种环境中，任何相关方都有足够的信心，并被鼓励提出对不当行为或可疑不当行为的担忧，并且组织展示其接收、评估、处理和结束举报案件的承诺。

举报管理体系的可信度取决于相关方是否认为管理层致力于该体系，并将遵循程序。

5. 2 举报政策

最高管理层应制定举报政策， 以：

a） 符合组织的宗旨；

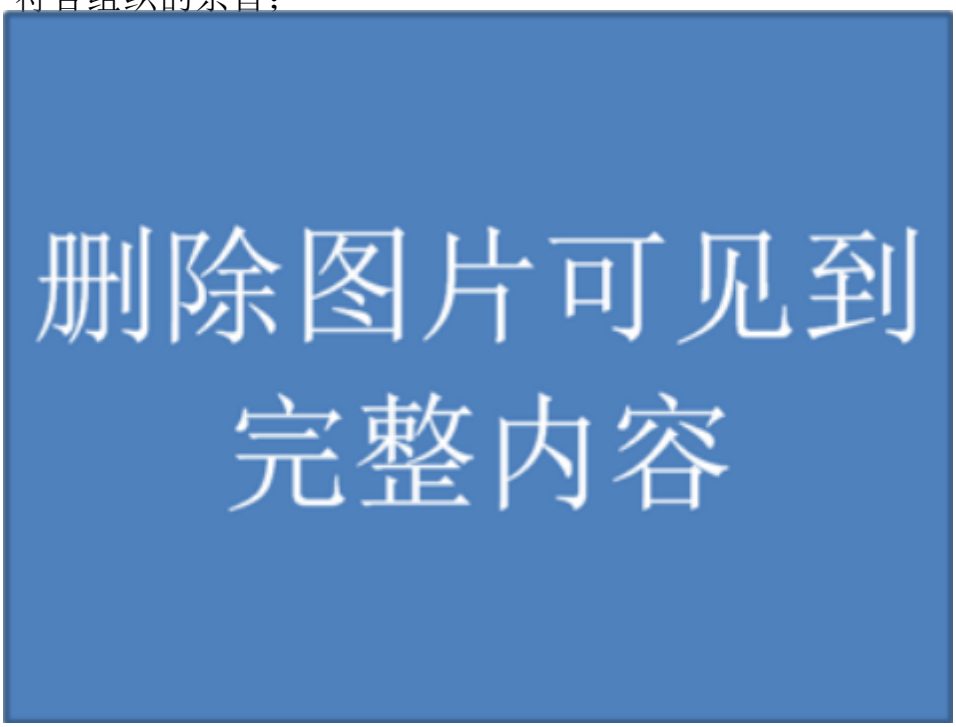
b）

c）

d）

e）

f）



g） 明确承诺建立直言不讳的文化；

h） 以易于理解的语言提供有关如何报告以及在何处寻求支持的指导或就举报过程提供建议；

i） 包括在整个举报过程中对信任、公正和保护的承诺；

j） 就举报不当行为的保密性作出规定；

k） 说明举报管理职能的权威性和独立性；

1） 解释不遵守举报政策的后果，例如明知故犯的虚假报告和采取有害行为可以受到纪律处分；

m）参考组织外部可用的其他报告渠道，例如作为监管者；

n）参考适用法律；

0)概述了举报管理系统的关键步骤，包括报告的发布方式接收、评估、处理和总结；