国际标准

ISO
37001

第1版
2016-10-15

反贿赂管理体系—
要求及使用指南

Anti-bribery management systems—

Requirements with guidance for use

ISO 37001-2016
©ISO 2016
本标准由雷泽佳翻译，13087319462，leizejia@126.com

目　次

前　言

国际标准化组织（ISO）是由各国标准化群体（ISO成员群体）组成的世界性的联合会。制定国际标准工作通常由ISO的技术委员会完成。各成员群体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与ISO保持联系的各国际组织（官方的或非官方的）也可参加有关工作。ISO与国际电工委员会（IEC）在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在ISO/IEC指引第1部分均有描述。应特别注意用于各不同类别ISO文件批准准则。本标准根据ISO/IEC导则第2部分的规则起草（见www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的ISO专利权声明清单中（www.iso.org/patents）。

本标准中使用的任何商品名称仅为方便用户而提供的信息，并不构成认可。

ISO与合格评定相关的特定术语和表述含义的解释以及ISO遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则关信息访问以下URLL：。

本标准由ISO/PC278反贿赂管理体系项目委员会负责编制。

引　言

贿赂是一种普遍现象。它会引发严重的社会、道德、经济和政治问题，破坏良好治理，阻碍经济发展，扭曲公平竞争。它侵蚀正义、危害人权，阻碍贫困的消除。它还会提高经商成本，在商业交易中增加不确定性，提高商品和服务成本，降低产品和服务质量，从而可能导致生命和财产损失，破坏机构公信力并妨碍市场公平、高效运行。

各国政府通过利用国际公约，如经济合作与发展组织的《关于打击国际商业交易中行贿外国公职人员行为的公约》和《联合国反腐败公约》及其国内法在治理贿赂上取得了一些成效。在大多数司法管辖区，个人的贿赂行为界定为犯罪，使组织和个人都为其贿赂行为承担责任正成为一种日益盛行的趋势。

然而，仅靠法律并不足以解决贿赂问题。组织有义务主动打击贿赂，这一目标能通过本标准期望提供的反贿赂管理体系，并通过领导层承诺建立诚信、透明、公开和合规的文化实现。组织文化的本质对反贿赂管理体系的成败至关重要。

管理良好的组织被预期制定由合适的管理体系予以支撑的合规方针，以确保其遵守法律义务和诚信承诺。反贿赂方针是整体合规方针的组成部分。反贿赂方针及支撑性管理体系帮助组织避免或降低卷入贿赂事件的成本、风险和损害后果，在业务往来中提升信任度和信心，并提高其声誉。

本标准反映了国际良好实践并能适用于所有司法管辖区，适用于所有领域的小型、中型和大型组织，包括公共、私营和非营利部门。组织所面临的贿赂风险根据组织规模大小、经营地域和所在行业、组织活动的性质、规模和复杂性等因素的不同而变化。本标准对组织贯彻执行方针、程序和控制措施予以规定，这些方针、程序和控制措施是合理的并与组织所面临的贿赂风险相对称。本标准所述要求的实施指南见附录A。

遵守本标准并不能确保杜绝涉及组织的、已发生或将发生的贿赂，因为贿赂风险无法完全消除。但本标准能帮助组织实施合理和适当的措施，用以预防、发现和应对贿赂。

在本标准中，以下书面表述适用：

——“应”表示要求；

——“宜”表示推荐；

——“可”表示许可；

——“能”表示可能性或能力。

信息标识为“注”的，为理解或明确相关要求的指南。

本标准符合 ISO 对管理体系标准的要求。这些要求包括高阶结构、相同的核心文本，以及附带核心定义的共同术语，为使实施多项 ISO 管理体系标准的用户受益而设计。本标准能与其他管理体系标准(如 ISO 9001、ISO 14001、ISO /IEC 27001 和 ISO 19600)及管理标准(如 ISO 26000 和 ISO 31000)一起使用。

反贿赂管理体系——要求及使用指南

1 范围

本标准为制定、实施、维护、评估以及改进反贿赂管理体系制定了具体要求并提供了指南。本体系能独立实施或纳入管理体系中整合实施。本标准解决与组织活动相关的下列贿赂：

——公共、私营和非营利部门中的贿赂；

——组织实施的贿赂；

——组织的员工代表组织或为其利益而实施的贿赂；

——组织的商业伙伴代表组织或为其利益而实施的贿赂；

——对组织实施的贿赂；

——对与组织活动相关的组织员工实施的贿赂；

——对与组织活动相关的组织商业伙伴实施的贿赂；

——直接和间接贿赂（如通过或由第三方给予或收受贿赂）。

本标准只适用于贿赂，为管理体系提出要求并提供指南，以帮助组织预防、发现和应对贿赂及遵守适用于其活动的反贿赂法律和自愿承诺。

本标准不专门针对欺诈、卡特尔和其他反垄断/竞争违法行为、洗钱或其他与腐败行为相关的活动（尽管组织可能会选择扩展管理体系范围，以囊括这类活动）。

本标准的要求是通用的，并旨在适用于所有组织（或组织的部分），不论类型、规模和活动性质，或是在公共、私营或非营利部门。这些要求的适用程度取决于 4.1、4.2 和 4.5 中列出的因素。

注 1：见指南 A.2。

注 2：用于预防、发现和降低组织实施贿赂风险的措施可能不同于用于预防、发现和应对向组织（或代表组织的员工或商业伙伴）实施贿赂的措施。见指南 A.8.4。

2 规范性引用文件

本标准无规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

贿赂 bribery

无论在何地违反适用法律直接或间接地提供、承诺、给予、接受或索取任何价值的不当利益（可以是财务的或非财务的），以引诱或奖励个人就其职责绩效（3.16）而言作为或不作为。

注：上述为一般定义。“贿赂”一词的含义由适用于组织（3.2）的反贿赂法律和由组织设计的反贿赂管理体系（3.5）进行规定。

3.2

组织 organization

为实现目标（3.11），由职责、权限和相互关系构成自身功能的一个人或一组人。

注 1：组织的概念包括，但不限于个体经营者、公司、集团、商行、企事业单位、权力机构、合伙企业、慈善机构或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

注 2：对于拥有一个以上运营部门的组织，其中一个或多个运营部门能被定义为一个组织。

3.3

相关方interested party

利益相关方 stakeholder

能影响、被影响或认为自己受到某个决定或活动影响的个人或组织（3.2）。

注：利益相关方可以是组织内部的或外部的。

3.4

要求 requirement

明示的和必须履行的需求。

注 1：“要求”在 ISO 管理标准体系中的核心定义为：明示的、通常隐含的或必须履行的需求与期望。“通常隐含的需求”不适用于反贿赂管理背景中。

注 2：“通常隐含”是指组织和相关方的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注 3：规定要求指明示的要求，例如：成文信息中规定的要求。

3.5

管理体系 management system

组织（3.2）建立方针（3.10）和目标（3.11）以及实现这些目标的过程（3.15）的相互关联或相互作用的一组要素。

注 1：一个管理体系可关注一个或多个领域。

注 2：管理体系要素包括组织结构、岗位和职责、策划和运行。

注 3：管理体系的范围可包括整个组织、组织中可被明确识别的职能或可被明确识别的部门，以及跨组织的单一职能或多个职能。

3.6

最高管理者 top management

在最高层指挥和控制组织（3.2）的一个人或一组人。

注 1：最高管理者在组织内有授权和提供资源的权力。

注 2：若管理体系（3.5）的范围仅覆盖组织的一部分，则最高管理者是指那些指挥并控制组织该部分的人员。

注 3：组织的形式，取决于其运营所遵照的法律框架及其规模大小、所属行业等。有些组织可能同时设有治理机构（3.7）和最高管理者，而有些组织则没有将职责分属于多个机构。这些关于组织及其职责的不同情况，能在适用第 5 章的要求时予以考虑。

3.7

治理机构 governing body

对组织（3.2）的活动、治理以及政策承担最终责任和行使权力的集体或机构，最高管理者（3.6）向其报告并对最高管理者问责。

注 1：并不是所有组织，尤其是小型组织都会有独立于最高管理者的治理机构（见 3.6 的注 3）。

注 2：治理机构包括但不限于董事会、董事会专业委员会、监事会、理事会或监察委员会等。

3.8

反贿赂合规团队 anti-bribery compliance function

拥有运行反贿赂管理体系（3.5）职责和权限的个人或群体。

3.9

有效性 effectiveness

完成策划的活动并实现策划结果的程度。

3.10

方针 policy

由最高管理者（3.6）或治理机构（3.7）正式发布的组织（3.2）的宗旨和方向。

3.11

目标 objective

要实现的结果。

注 1：目标可以是战略、战术的或操作层面的。

注 2：目标能涉及不同的领域（如财务、销售与营销、采购、健康与安全及环境的目标），且能应用于不同层面（如战略的、组织整体的、项目、产品和过程（3.15）。

注 3：目标能以其它方式表达，如：预期成果、目的、运行准则、反贿赂目标，或使用其他意思相近的词语（如：目的、终点或标的）。

注 4：在反贿赂管理体系（3.5）中，反贿赂目标由组织 L3.2）确定，与反贿赂方针（3.10）保持一致，以实现特定的结果。

3.12

风险 risk

不确定性对目标（3.11）的影响。

注 1：影响是指偏离预期，可以是正面的或负面的。

注 1：影响是指偏离预期，可以是正面的和/或负面的。

注 2：不确定性是指对某一事件、事件的后果或其发生的可能性缺乏（包括部分缺乏）信息、了解或知识的状态。

注 3：通常，风险以潜在事件（ISO 导则 73 中的定义）和后果（ISO 导则 73 中的定义）或两者的组合来描述风险的特性。

注 4：风险通常以事件后果（包括环境的变化）与相关事件发生的可能性（ISO 导则 73 中的定义）的组合来表示。

3.13

能力 competence

运用知识和技能实现预期结果的本领。

3.14

成文信息 documented information

组织（3.2）需要控制和维护的信息及其载体。

注 1：成文信息能以任何格式和载体存在，且来源不限。

注 2：成文信息是指：

管理体系（3.5），包括其相关的过程（3.15）；

—— 组织运行而创建的信息（文件）；

—— 结果实现的证据（记录）。

3.15

过程 process

将输入转化为输出的相互关联或相互作用的一组活动。

3.16

绩效 performance

可测量的结果。

注 1：绩效可能涉及定最的或定性的结果。

注 2：绩效可能涉及活动、过程（3.15）、产品（包括服务）、体系或组织（3.2）的管理。

3.17

外包 outsource

安排外部组织（3.2）承担组织部分职能或过程（3.15）。

注 1：尽管外包的职能或过程在管理体系范围内，但外部组织在管理体系（3.5）范围之外。

注 2：ISO 管理体系标准的核心文本包括本标准未使用的、与外包相关的定义和要求，因为已在商业伙伴（3.26）的定义中包括外包商。

3.18

监视 monitoring

确定体系、过程（3.15）或活动的状态。

注：确定状态，可能需要检查、监督或密切观察。

3.19

测量 measurement

确定数值的过程（3.15）。

3.20

审核 audit

获取审核证据并予以客观评价，以判定审核准则满足程度的系统的、独立的、形成文件的过程（3.1.5）。

注 1：审核能为内部审核（第一方）或外部审核（第二方或第三方），还能为多体系审核（合并两个或多个领域）。

注 2：内部审核由组织（3.2）自行实施执行或由外部其他方代表其实施。

注 3:“审核证据”和“审核标准”的定义见 GB/T19011.

3.21

合格 conformity

满足要求（3.4）。

3.22

不符合 nonconformity

不满足要求（3.4）。

3.23

纠正措施 corrective action

为消除不符合（3.22）的原因并防止其再次发生所采取的措施。

3.24

持续改进 continuous improvement

提高绩效（3.16）的循环活动。

3.25

员工 personnel

组织（3.2）的董事、高级职员、雇员、临时人员或工人和志愿者。

注 1：不同类型的员工会形成不同类型和程度的贿赂风险（3.12），并能由组织的贿赂风险评估和贿赂风险管理程序区别对待。

注 2：临时人员或工人的指南见 A.8.5。

3.26

商业伙伴 business associate

组织（3.2）已经或计划与其建立某种业务关系的外部组织。

注1：商业伙伴包括但不限于客户、顾客、合资企业、合资伙伴、联盟伙伴、外包商、承包商、咨询师、分包商、供应商、销售商、顾问、代理人、分销商、代表、中介和投资方。这个是特意宽泛的定义，并宜根据组织的贿赂风险'3.12）情况进行解释以适用于有相当可能使组织面临贿赂风险的商业伙伴。

注2：不同类型的商业伙伴会形成不同类型和程度的贿赂风险，组织（3.2）对于不同类型的商业伙伴的影响力也不同。不同类型的商业伙伴能由组织的贿赂风险评估和贿赂风险管理程序区别对待。

注3：本标准中的“商业”能宽泛地解释为表示与组织生存目的相关的活动。

3.27

公职人员 public official

无论是经任命、选举或继任而担任立法、行政或者司法职务的人员；或者为包括公共机构或者公营企业行使公共职能的任何人员；或者国内或国际公共组织的任何官员或代理人；或者任何公职候选人。

注：公职人员认定示例见附录A.2。

3.28

第三方 third party

独立于组织（3.2）的个人或机构。

注：所有的商业伙伴（3.26）均为第三方，但并非所有的第三方都是商业伙伴。

3.29

利益冲突 conflict of interest

商业、财务、家庭、政治或个人利益能妨碍个人在为组织（3.2）履职时的判断的情形。

3.30

尽职调查 due diligence

进一步评估贿赂风险'3.12）的性质和程度，以及帮助组织（3.2）作出与具体交易、项目、活动、商业伙伴（3.26）和员工相关决策的过程（3.15）。

4 组织环境

4.1 理解组织及其环境

组织应确定与其目的相关并影响其实现反贿赂管理体系目标能力的内部和外部因素。这些事项包括但不限于以下因素：

a） 组织的规模、结构及其委托决策权；

b） 组织运行或预期运行的地点和行业；

c） 组织活动和运行的性质、规模和复杂性；

d） 组织的商业模式；

e） 受组织控制的实体或控制组织的实体；

f） 组织的商业伙伴；

g） 与公职人员来往的性质和程度；

h） 适用的法律、法规、合同以及专业的义务和责任。

注：组织如果直接或间接控制另一个组织的管理活动，则该组织控制另一个组织（见 A.13.1.3）。

4.2 理解利益相关方的需求和期望

组织应确定：

a） 与反贿赂管理体系相关的利益相关方；

b） 这些利益相关方的相关要求。

注：在识别利益相关方的要求时，组织能区分利益相关方的强制性要求、非强制性期望或是对利益相关方的自愿承诺。

4.3 确定反贿赂管理体系的范围

组织应确定反贿赂管理体系的边界和适用性，以确立其范围。确定范围时，组织应考虑：

a） 提及的内部和外部因素；

b） 4.2 提及的要求；

c） 4.5 提及的贿赂风险评估结果。

范围应作为成文信息提供使用。

注：见指南 A.2.

4.4 反贿赂管理体系

组织应根据本标准的要求，建立、记录、实施、维护、持续评审并在必要时改进反贿赂管理体系，包括所需的过程及其相互作用。

反贿赂管理体系应包含识别和评价贿赂风险及防范、发现和应对贿赂的措施。

注 1：完全消除贿赂风险是不可能的，没有反贿赂管理体系能够防范和发现所有贿赂。

反贿赂管理体系应是合理和适当的，且考虑了 4.3 提及的因素。

注 2：见指南 A.3。

4.5 贿赂风险评估

4.5.1 组织应定期开展贿赂风险评估，应：

a） 考虑 4.1 列出的因素，识别组织可能合理预料到的贿赂风险；

b） 分析、评估和优先排序已识别的贿赂风险；

c） 评价组织现有控制的适合性和有效性以降低所评估的贿赂风险。

4.5.2 组织应对其方针和目标加以考虑，建立评价其贿赂风险等级的标准。

4.5.3 贿赂风险评审应：

a） 按照组织确定的时间和频率定期进行，以准确评估变更和最新信息；

b） 在组织的结构或活动发生重大变更时进行。

4.5.4 组织应保留成文信息，证明已开展贿赂风险评估，并用以设计或改进反贿赂管理体系。

注：见指南 A.4.

5 领导作用

5.1 领导作用和承诺

5.1.1 治理机构

当组织有治理机构时，该机构应通过下列方式证明其对反贿赂管理体系的领导作用和承诺：

a） 批准组织的反贿赂方针；

b） 确保组织的战略与反贿赂方针保持一致；

c） 按计划定期接收和评审关于组织反贿赂管理体系的内容和运行的信息；

d） 要求分配和指派充足且恰当的、有效运行反贿赂管理体系所需的资源；

e） 合理监督由最高管理者执行的反贿赂管理体系实施活动及其有效性。

注：组织如果没有治理机构，应由最高管理者实施上述活动。

5.1.2 最高管理者

最高管理者应通过下列方式证明其对反贿赂管理体系的领导作用和承诺：

a） 确保反贿赂管理体系（包括方针和目标）得到建立、实施、维护、评审，以充分处理组织的贿赂风险；

b） 确保反贿赂管理体系要求融入组织的过程；

c） 配置充足且恰当的资源以有效运行反贿赂管理体系；

d） 在内部和外部沟通反贿赂政策；

e） 在内部沟通有效反贿赂管理和满足反贿赂管理体系要求的重要性；

f） 确保反贿赂管理体系的恰当设计以实现其目标；

g） 指导和支持员工为反贿赂管理体系的有效性做出贡献；

h） 在组织内营造恰当的反贿赂文化；

i） 推动持续改进；

j） 支持其他相关管理岗位在各自职责领域证明其防范和发现贿赂的领导作用；

k） 鼓励对涉嫌和实际发生的贿赂使用报告程序（见 8.9）；

l） 确保员工不因善意或基于合理信念报告违反或涉嫌违反组织反贿赂方针的行为，或拒绝参与贿赂（即使组织可能因此丧失业务机会）而遭受报复、歧视或处分（见 7.2.2.Id）（个人参与违反活动的除外）；

m） 按计划定期向治理机构（若有）报告反贿赂管理体系以及对严重或系统性贿赂的指控内容和运行情况。

注：见指南 A.5。

5.2 反贿赂方针

最高管理者应建立、维护和评审反贿赂方针，方针应：

a） 禁止贿赂；

b） 要求遵守适用于组织的反贿赂法律；

c） 适合于组织目的；

d） 为设定、评审和实现反贿赂目标提供框架；

e） 包括满足反贿赂管理体系要求的承诺；

f） 鼓励出于善意，或基于合理信念私下提出疑虑，无需担忧遭受报复；

g） 包括持续改进反贿赂管理体系的承诺；

h） 解释反贿赂合规团队的权限和独立性；

i） 解释不遵守反贿赂方针的后果。

反贿赂方针应：

——作为成文信息以便于获取；

——以恰当的语言，在组织内以及与形成超过低贿赂风险的商业伙伴进行沟通；

——便于相应的利益相关方适时获取。

5.3 组织岗位、职责和权限

5.3.1 岗位和职责

最高管理者应承担遵守和实施 5.1.2 中所述的反贿赂管理体系的总体职责。

最高管理者应确保相关岗位的职责和权限在组织各等级内以及之间得到分配和沟通。

各级管理者应负责要求在其部门或团队内适用和遵守反贿赂管理体系的要求。

治理机构（若有）、最高管理者和其他所有员工应负责理解、遵守和适用与其在组织内职责相关的反贿赂管理体系要求。

5.3.2 反贿赂合规团队

a） 监督组织设计和实施反贿赂管理体系；

b） 向员工提供关于反贿赂管理体系以及贿赂相关事项的建议和指南；

c） 确保反贿赂管理体系满足本标准的要求；

d） 向治理机构（若有）、最高管理者和其他合规团队适时报告反贿赂管理体系的绩效。

反贿赂合规团队应资源充足并分配于拥有恰当能力、地位、权限和独立性的一个人（或多个人）。一旦需要提出与贿赂或反贿赂管理体系相关的任何事项或疑虑，反贿赂合规团队应具备直接且迅速接触

治理机构（若有）和最高管理者的渠道。

最高管理者能分配部分或全部反贿赂合规团队于组织外的人员。如分配，最高管理者应确保特定员工拥有针对那些向外分配的团队部分的职责和权限。

注：见指南 A.6。

5.3.3 授权决策

在最高管理者授予员工与超过低贿赂风险相关决策权限时，组织应建立和维护决策过程或一系列控制措施，要求决定过程和决策者的权限等级是恰当的，且没有实际或潜在利益冲突。最高管理者应确保定期审查这些过程，以作为其岗位和职责的一部分，实施和遵守 5.3.1 中所概述的反贿赂管理体系要求。

注：最高管理者或治理机构（若有）并不因决策授权而免除 5.1.1、5.1.2 和 5.3.1 中所描述的义务和职责，其潜在的法律责任也不会因此转嫁给被授权员工。

6 策划

6.1 应对风险和机遇的措施

组织策划反贿赂管理体系时，应考虑 4.1 提及的事项、4.2 提及的要求、4.5 识别出的风险以及需要应对的改进机遇，以：

a） 提供合理保障使反贿赂管理体系实现既定目标；

b） 防范或减少与反贿赂方针及目标相关的非预期影响；

c） 监视反贿赂管理体系的有效性；

d） 实现持续改进。

组织应策划：

——应对这些贿赂风险和机遇的改进措施；

——如何：

- 将上述措施纳入其反贿赂管理体系过程并加以实施；
- 评价上述措施的有效性。

6.2 反贿赂目标及实现策划

组织应在相关团队和等级中建立反贿赂管理体系目标。

反贿赂管理体系目标应：

a） 与反贿赂方针保持一致；

b） 可测量（若可行）；

c） 对 4.1 提及的适用因素、4.2 提及的要求和 4.5 识别出的贿赂风险予以考虑；

d） 可实现；

e） 可监视；

f） 可依照 7.4 沟通；

g） 可适时更新。

组织应保存反贿赂管理体系目标相关的成文信息。

在策划如何实现其反贿赂管理体系目标时，组织应确定：

——要做什么；

——需要什么资源；

——由谁负责；

——何时完成；

——如何评价和报告结果；

——谁来实施惩戒或处罚。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进反贿赂管理体系所需要的资源。

注：见指南 A.7。

7.2 能力

7.2.1 总则

组织应：

a） 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响反贿赂绩效；

b） 确保这些人员在接受恰当的教育、培训或经验的基础上胜任工作；

c） 在适用处，采取措施获得和维持必要的能力，并评价所采取措施的有效性；

d） 保存恰当的成文信息作为能力证据。

注：适用的措施能包括，例如：对员工和商业伙伴的培训、指导，或调岗；或雇用或签约。

7.2.2 雇用程序

7.2.2.1 对于所有的员工，组织应实施以下程序：

a） 雇用条件要求员工遵守反贿赂方针和反贿赂管理体系，并给予组织对不遵守的员工进行处分的权利；

b） 在开始雇用后的一段合理时间内，使员工接收或具备渠道获取反贿赂方针的副本及与该方针相关的培训；

c） 组织具备相应程序，以允许其对违反反贿赂方针或反贿赂管理体系的员工采取恰当的处分措施；

d） 员工将不会遭受报复、歧视或处分措施（例如：通过威胁、孤立、降级、限制晋升、调动、解雇、欺凌、侵害或其他形式的骚扰），因：

1）拒绝参与或回避任何其合理判断存在超过低贿赂风险、且该风险尚未被组织降低的活动；或

2）出于善意或基于合理信念对企图、实际或涉嫌贿赂或违反反贿赂方针或反贿赂管理体系提出疑虑或做出报告（个人参与违反活动的除外）。

7.2.2.3 对于所有面临超过低贿赂风险（经贿赂风险评估（见 4.5）确定）的职位以及反贿赂合规团队，组织应实施程序规定：

a） 在组织雇用人员、调动或晋升员工前对其开展尽职调查（见 8.2），以在合理范围内尽量确定对其进行雇用或调动是恰当的，以及对其将遵守反贿赂方针和反贿赂管理体系要求的信任是合理的；

b） 定期评审绩效奖金、绩效指标和其它薪酬激励因素，以核实合理的保障措施已落实以防范其助长贿赂；

c） 此类员工、最高管理者以及治理机构（若有），按与已识别贿赂风险相称的合理间隔定期提交声明，确认其遵守反贿赂方针。

注 1：反贿赂团队声明能为独立声明或为更宽泛合规声明过程的一部分。

注 2：见指南 A.8。

7.3 意识和培训

组织应为员工提供充足和恰当的反贿赂意识及培训，此类培训应对贿赂风险评估（见 4.5）结果予以考虑，适时应对以下事项：

a） 组织的反贿赂方针、程序和反贿赂管理体系以及员工的遵守义务；

b） 贿赂风险及贿赂对员工和组织能造成的损害；

c） 与员工义务相关的能发生贿赂的情形，及如何识别这些情形；

d） 如何识别和回应索贿或行贿；

e） 员工如何能帮助防范和避免贿赂，并识别关键贿赂风险指标；

f） 员工对反贿赂管理体系有效性的贡献，包括改进反贿赂绩效及报告涉嫌贿赂所带来的效益；

g） 不符合反贿赂管理体系要求的影响和潜在后果；

h） 员工如何及向谁能够报告疑虑（见 8.9）；

i） 便于获取的培训和资源信息。

应定期（按组织确定的计划）向员工提供适合其岗位、面临的贿赂风险和任何变更情形的反贿赂意识及培训。意识和培训方案应在必要时定期更新以反映相关新信息。

考虑已识别的风险（见 4.5），组织还应实施程序予以应对反贿赂意识和培训，以针对代表其或其利益，且能对组织形成超过低贿赂风险的商业伙伴。这些程序应识别商业伙伴（对其而言此类意识和培训是必要的）、培训内容和培训方式。

组织应保存培训程序、培训内容、培训时间和对象的成文信息•

注 1：针对商业伙伴的意识与培训要求能通过合同要求或类似要求进行沟通，并由组织、商业伙伴或为此目的所任命的其他主体实施。

注 2：见指南 A.9。

7.4 沟通

7.4.1 组织应确定与反贿赂管理体系相关的内部和外部沟通，包括：

a） 沟通什么；

b） 何时沟通；

c） 与谁沟通；

d） 如何沟通；

e） 谁来沟通；

f） 沟通使用的语言。

7.4.2 反贿赂方针应便于组织所有的员工和商业伙伴获取，并与超过低贿赂风险的员工和商业伙伴进行直接沟通，并应通过组织内部和外部沟通渠道适时发布。

7.5 成文信息

7.5.1 总则

组织的反贿赂管理体系应包括：

a） 本标准要求的成文信息；

b） 组织确定为反贿赂管理体系有效性所必要的成文信息。

注 1：不同组织的反贿赂管理体系成文信息的程度能不同，取决于：

—组织的规模及其活动、过程、产品和服务的类型；

—过程及其相互作用的复杂性；

—员工的能力。

注 2：成文信息能作为反贿赂管理体系的部分单.独保存，或能作为其他管理体系（例如：合规、财务、商业、审核）的部分保存。

注 3：见指南 A.17。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

a） 标识和说明（如标题、日期、作者、索引编号）；

b） 格式（例如语言、软件版本、图表）和媒介（例如纸质版、电子版）；

c） 评审和批准以确保适宜性和充分性。

7.5.3 成文信息控制

应对反贿赂管理体系和本标准要求的成文信息进行控制，以确保：

a） 在需要的场合和时机，均可获得并适用；

b） 予以妥善保护（如：防止泄密、不当使用或缺失）。

为控制成文信息，组织应适时应对以下活动：

——分发、访问、检索和使用；

——存储和防护，包括保持可读性；

——更改控制（如版本控制）；

——保留和处置。

组织确定为策划和运行反贿赂管理体系所必要的、外部来源的成文信息，应适时予以识别，并控制。

注：访问能意味若仅允许查看成文信息的决定，或允许并授权查看和变更成文信息的决定。

8 运行

8.1 运行策划和控制

组织应策划、实施、评审和控制满足反贿赂管理体系要求所需的过程，并实施 6.1 确定的措施，通过：

a） 建立过程的准则；

b） 根据准则实施过程控制；

c） 保留必要的成文信息，以确信过程已按策划执行。

这些过程应包括 8.2 至 8.10 提及的特定控制。

组织应控制策划的变更并评审意外变更的后果，必要时，采取措施降低任何不利影响。

组织应确保外包流程得到控制。

注：ISO 管理体系标准的核心文本包含本标准未使用的、与外包相关的要求，因为外包商已包括于商业伙伴的定义中。

8.2 尽职调查

在组织的贿赂风险评估（按照 4.5 开展）评估出超过低贿赂风险时（与以下方面相关）：

a） 特定的交易、项目或活动类型；

b） 与特定类型商业伙伴策划建立的或正在进行中的关系，或

c） 某些职位特定类别的员工（见 7.2.2.2），

组织应评估贿赂风险的性质和程度，其与属于那些类别的特定交易、项目、活动、商业伙伴和员工相关。该评估应包括任何必要的尽职调查，以获取充分信息评估贿赂风险。尽职调查应以界定的频率更新，以便能对变更和新信息予以准确考虑。

注 1：组织能断定对特定类别的员工和商业伙伴进行尽职调查是不必要、不合理或不适当的。

注 2：以上 a）、b）和 c）中列出的情况不构成穷举。

注 3：见指南 A.10。

8.3 财务控制

组织应实施财务控制，管理贿赂风险。

注：见指南 A.11。

8.4 非财务控制

组织应实施非财务控制，管理诸如采购、运行、销售、商业、人力资源、法律和监管活动等领域的贿赂风险。

注 1：任何具体交易、活动或关系能受财务和非财务控制。

注 2：见指南 A.12。

8.5 受控组织及商业伙伴实施反贿赂控制

8.5.1 组织应实施程序，要求其控制的所有其他组织：

a） 实施组织的反贿赂管理体系，或

b） 实施其自身的反贿赂控制。

在每种情形中仅达到合理的、且与受控组织所面临贿赂风险相称的程度，并考虑根据 4.5 开展的贿赂评估。

注：如果一个组织直接或间接地控制了另一个组织的管理活动，则该组织控制了另一个组织（见 A13.1.3）。

8.5.2 对于不受组织控制、贿赂风险评估（见 4.5）或尽职调查（见 8.2）对其识别出超过低贿赂风险的商业伙伴，且在该商业伙伴实施反贿赂控制将帮助降低相关贿赂风险时，组织应实施以下程序：

a） 组织应确定商业伙伴是否落实反贿赂控制，管理相关贿赂风险；

b） 在商业伙伴没有落实反贿赂控制，或无法核实其是否落实控制时：

1）在可行时，组织应要求商业伙伴实施与相关交易、项目或活动相关的反贿赂控制；

2）在要求商业伙伴实施反贿赂控制不可行时，此项应作为一项因素，在评价与商业伙伴业务关系的贿赂风险（见 4.5 和 8.2）以及组织管理此类风险的方式（见 8.3、8.4 和 8.5）时予以考虑。

注：见指南 A.13。

8.6 反贿赂承诺

对于形成超过低贿赂风险的商业伙伴，组织应在可行范围内实施程序要求：

a） 商业伙伴承诺防范涉及相关交易、项目、活动或关系的商业伙伴、其代表或为其利益进行贿赂；

b） 一旦涉及相关交易、项目、活动或关系的商业伙伴、其代表或为其利益进行贿赂，组织能终止与商业伙伴的关系。

在满足上述 a）或 b）的要求是不可行时，此项应作为一项因素，在评价与商业伙伴业务关系的贿赂风险（见 4.5 和 8.2）以及组织管理此类风险的方式（见 8.3、8.4 和 8.5）时予以考虑。

注：见指南 A.14。

8.7 礼物、款待、捐赠和类似的利益

在提供、给予或接受为或被合理视为贿赂时，组织应实施旨在防范提供、给予或接受礼物、款待、捐赠及类似利益的程序。

注：见指南 A.15。

8.8 管理反贿赂控制的不足

在对特定交易、项目、活动或商业伙伴关系开展尽职调查（见 8.2）后，证实现有反贿赂控制不能管理贿赂风险，且组织不能或不希望实施额外或加强性控制、或采取其他恰当措施（诸如变更交易、项目、活动或关系的性质）以使组织能够管理相关贿赂风险时，组织应：

a） 针对现有交易、项目、活动或关系的情形，采取适合于交易、项目、活动或关系的贿赂风险和性质的步骤，以在可行范围内尽快终止、中断、暂停或从其撤离；

b） 针对已提议新交易、项目、活动或关系的情形，推迟或拒绝继续。

8.9 提出疑虑

组织应实施程序，以：

a） 鼓励并使人员能够出于善意或基于合理信念，向反贿赂合规团队或向恰当的员工报告企图、涉嫌和实际贿赂，或任何反贿赂管理体系的违反活动或缺陷；

b） 除达到要求开展调查的程度外，要求组织对报告保密，以保护举报者或该报告中涉及或提及的其他人员的身份信息；

c） 允许匿名报告；

d） 禁止报复，并保护报告者，在其出于善意、或基于合理信念，对企图、实际或涉嫌贿赂、或反贿赂方针或反贿赂管理体系的违反活动提出或报告疑虑后，免遭打击报复；

e） 使员工如面临可能涉及贿赂的疑虑或情形，能够就下一步行动获得恰当人员的建议。组织应确保所有员工意识到并且能够使用报告程序，且意识到其在该程序下的权利和保护。

注 1：这些程序能与那些用于报告其它疑虑事项（例如：安全、渎职、不正当行为或其它严重风险）的程序相同或成为其中的部分。

注 2：组织能使用商业伙伴代表其管理该报告程序。

注 3：在某些司法管辖区，法律禁止上述 b）和 c）中的要求。在这些情形下，组织对其无力遵守予以记录。

8.10 调查和处理贿赂

组织应实施程序：

a） 要求评估，并适时调查任何经报告、发现或合理地涉嫌的贿赂、反贿赂方针或反贿赂管理体系的违反活动；

b） 要求采取恰当措施，一旦调查显示任何贿赂、违反反贿赂方针或反贿赂管理体系的活动；

c） 使调查者具备权力和能力；

d） 要求相关员工配合调查；

e） 要求将调查状态和结果适时向反贿赂合规团队和其他合规团队报告；

f） 要求保密执行调查及对调查输出进行保密。

调查应由非受调查岗位和团队一部分的员工执行并向其报告，组织能任命商业伙伴开展调查并将结果报告给非受调查岗位和团队一部分的员工。

注 1：见指南 A.18.

注 2：在某些司法管辖区，法律禁止上述 f）中的要求；在这种情形下，组织对其无力遵守予以记录。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a） 需要监视和测量什么；

b） 谁负责监视；

c） 需要用什么方法进行监视、测量、分析和评价，以确保结果；

d） 何时实施监视和测量；

e） 何时对监视和测量的结果进行分析和评价；

f） 应向谁以及如何报告此类信息。

组织应保留适当的成文信息，以作为结果的证据。

组织应评价举报管理体系的绩效和有效性。

注：见指南 A.19。

9.2 内部审核

9.2.1 组织应按计划定期开展内部审核，以提供信息，确定反贿赂管理体系是否：

a） 符合：

1）组织自身对其反贿赂管理体系的要求；

2）本标准的要求；

b） 有效实施和保持。

注 1：关于审核管理体系的指南已于 ISO 19011 中给出。

注 2：组织内部审核活动的范围和规模能，取决于包括组织的规模、结构、成熟度和所在区域在内的一系列因素的不同而变化。

9.2.2 组织应：

a） 策划、建立、实施和维护（多个）审核方案，包括频率、方法、职责、策划要求和报告，应对相关过程的重要性和以往审核的结果予以考虑；

b） 规定每次审核的审核准则和范围；

c） 挑选胜任的审核员并开展审核以确保审核过程的客观和公正；

d） 确保审核结果报告给相关管理者、反贿赂合规团队、最高管理者及，适时向治理机构（若有）；

e） 保存成文信息，作为实施审核方案和审核结果的证据。

9.2.3 这些审核应是合理、适当且基于风险的。此类审核应包括内部审核过程或其它程序，以评审针对以下内容的程序、控制和体系：

a） 贿赂或涉嫌贿赂；

b） 违反反贿赂方针或反贿赂管理体系的要求；

c） 商业伙伴未满足适用的组织反贿赂要求；

d） 反贿赂管理体系的缺陷或改进机会。

9.2.4 为确保这些审核方案的客观和公正，组织应确保这些审核由以下人员或部门之一进行：

a） 为这个过程建立或任命的独立团队或员工；

b） 反贿赂合规团队（除非审核范围包括对反贿赂管理体系自身的评价，或由反贿赂合规团队负责的类似工作）；

c） 来自非受审核部门或团队的恰当人员；

d） 恰当的第三方；

e） 由 a）至 d）任意组成的小组。

组织应确保审核员不审核他/她自身领域的工作。

注：见指南 A.16。

9.3 管理评审

9.3.1 最高管理者评审

最高管理者应按计划定期评审组织的反贿赂管理体系，以确保其持续的适宜性、充分性和有效性。

最高管理者评审应考虑：

a） 以往管理评审措施的状态；

b） 与反贿赂管理体系相关的内外部因素的变更；

c） 反贿赂管理体系绩效信息，包括以下各项体现的趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

4）贿赂报告；

5）调查；

6）组织所面临贿赂风险的性质和程度；

d） 为应对贿赂风险所采取措施的有效性；

e） 10.2 提及的、反贿赂管理体系的持续改进机会。

最高管理者评审的输出应包括与反贿赂管理体系的持续改进机会和任何变更需求相关的决策。最高管理者评审结果摘要应报告给治理机构（若有）。

组织应保存成文信息作为最高管理者评审的证据。

9.3.2 治理机构评审

治理机构（若有）应基于最高管理者、反贿赂合规团队提供的信息及其要求或获取的其他信息，对反贿赂管理体系进行定期评审。

组织应保存成文信息摘要作为治理机构评审结果的证据。

9.4 反贿赂合规团队评审

反贿赂合规团队应持续评估反贿赂管理体系是否：

a） 充分，以有效管理组织面临的贿赂风险；

b） 得到有效实施。

反贿赂合规团队应按计划定期和适时不定期，向治理机构（若有）和最高管理者、或向适宜的治理机构或最高管理者的委员会，报告反贿赂管理体系的充分性和实施，包括调查和审核的结果。

注 1：此类报告的频率取决于组织的要求，但建议至少每年一次。

注 2：组织能使用商业伙伴协助评审，只要商业伙伴的观察结果与反贿赂合规团队、最高管理者，及适时与治理机构（若有）恰当地进行沟通。

10 改进

10.1 不符合和纠正措施

发生不符合时，组织应：

a） 及时对不符合做出反应，适时：

1）采取措施控制和纠正不符合；

2）处理后果。

b） 评价是否需要采取措施，消除不符合的（多个）原因，以避免再次发生或在其他地方发生，通过：

3）评审不符合；

4）确定不符合的原因；

5）确定是否存在或能发生潜在的类似不符合。

c） 实施任何所需措施；

d） 评审所采取的任何纠正措施的有效性；

e） 如必要，修改反贿赂管理体系。

纠正措施应适合于所遭遇不符合造成的影响。

组织应保存成文信息，作为以下方面的证据：

——不符合的性质和随后采取的任何措施；

——任何纠正措施的结果。

注：见指南 A.20。

10.2 持续改进

组织应持续改进反贿赂管理体系的适宜性、充分性和有效性。

注：见指南 A.20。

附录 A （资料性附录） 关于使用本标准的指南

A.1 总则

此附录的指南仅用于说明，旨在为组织在实施反贿赂管理体系中采取措施的一些具体方面提供说明，本指南意不在提供全面或规范性的指导。组织实施符合本标准要求的反贿赂管理体系时不要求遵循下文所述步骤。组织采取的实际措施应与其所面临的贿赂风险的性质和程度（见 4.5 及 4.1 和 4.2 中的因素）相匹配并且合理。

关于反贿赂管理良好实践的进一步指导详见参考书目所列出版物。

A.2 反贿赂管理体系的范围

A.2.1 独立或整合式的反贿赂管理体系

组织可选择将反贿赂管理体系作为一个独立的体系或纳入整体合规管理体系的一部分（在纳入整体合规体系时，组织可参考 ISO 19600 的指南）加以实施。组织还可选择将反贿赂管理体系与其他如质量、环境和信息安全(组织可参考 ISO 9001、ISO14001 和 ISO/IEC 27001)等管理体系，以及 ISO 26000 和 ISO 31000 平行或作为其部分加以实施。

A.2.2 便利费和勒索费

A.2.2.1 便利费是指非法或非官方的付款，以换取付款方不付款也能依法享有的服务。它通常是向政府官员或拥有认证职能的个人支付数额相对较小的款项，用于确保或加速某项常规或必要行为，例如签证、工作许可证、海关放行或固话安装等。尽管便利费在性质上不同于为赢得业务而行贿，但是在大多数地区它们仍是非法的，且本标准也将其视为贿赂，因此,组织反贿赂管理体系应予禁止。

A.2.2.2 勒索费是指通过对员工健康、安全或自由实施实际或认为的威胁而强迫其给予的金钱，它不在本标准的关注范围内。人员的安全和自由是至关重要的，因此许多法律制度不将付款人因担心自身或他人的安全或自由而支付的勒索费视为犯罪。所以，组织可以制定政策允许员工为在避免自身或他人的健康、安全或自由受到直接危害时支付费用。

A.2.2.3 组织应向任何可能面临被索取这些费用的人员提供具体的指导，以帮助其避免和处理这些情况。这些指导意见可能包括：

a） 员工被索取这些费用时可以采取的具体措施：

1）当要求支付便利费时，要求其提供证明费用合法性的证明和正式收据，如果不能提供满意的证据，可拒绝付款；

2）当要求支付勒索费时，如果员工或他人的健康、安全或自由受到威胁，可同意付款。

b） 人员支付便利费或勒索费时应采取以下措施：

1）记录该事件；

2）向某一合适的经理或合规职能报告事件。

c） 员工支付便利费或勒索费时，组织应采取以下措施：

1）任命某一合适的经理调查事件（反贿赂合规职能或独立于员工所在部门的经理较为适宜）；

2）在组织的账户里如实记录此次支付行为。

d） 如果合适或法律有规定，应将支付行为向有关部门报告。

A.3 合理的和适当的

A.3.1 贿赂通常都是隐蔽的，很难预防、发现和处置。鉴于这些困难，本标准的总体意图是，组织的治理机构（若有）和最高管理者需要达到以下目的：

——真正致力于预防、发现和处置与组织的业务或活动相关的贿赂；

——且真正有意愿在组织内部采取措施以预防、发现和处置贿赂。

这些措施不能耗费大量金钱、增加负担或过于官僚化，否则组织可能负担不起或导致业务暂停。同时，这些措施也不能过于简单无效，否则贿赂很容易发生。这些措施必须与贿赂风险相适应，且具有可成功预防、发现和处置贿赂的可能性。

A.3.2 尽管需要执行的反贿赂措施的类型是国际认可的良好实践，且其中的某些内容已经在本标准中体现；但根据相关情况，需要实施的措施的实际细节差别极大。因此，列出特定情况下组织需要执行的具体措施是不可能的。本标准仅提出“合理的和适当的”要求，每种情况都可以根据实际情形进行判断。

A.3.3 以下例子介绍了如何根据不同的情形应用这些“合理的和适当的”要求：

a） 大型跨国组织可能拥有多个管理层以及成千上万的员工，因此，其反贿赂管理体系通常需要比只有少数员工的小型组织更加详细。

b） 与只在贿赂行为相对少见的低贿赂风险地区进行经营的组织相比，在高贿赂风险地区进行经营的组织需要针对其在这一地区的商业交易开展更加全面的风险评估和尽职调查程序，并实施更高层次的反贿赂控制措施。

c） 虽然所有的交易或活动都存在贿赂风险，但与向多个顾客销售小额物品或单一方进行多次小额交易的组织相比，参与大规模、高金额交易或商业伙伴众多的活动的组织实施的风险评估、尽职调查程序和反贿赂控制措施极有可能更全面。

d） 拥有众多商业伙伴的组织可能会认为：作为贿赂风险评估的一部分，其中某些类别的商业伙伴，如零售顾客，可能不会带来超出低贿赂水平的风险；因此，应在设计和实施反贿赂管理体系时将这一点考虑在内。例如，对于从组织购买消费品的零传顾客，尽职调查不可能是必要的或是适当和合理的控制措施。

A.3.4 尽管所有的交易都会有贿赂风险，但与低贿赂风险交易相比，组织应当对高贿赂风险交易实施更加全面的反贿赂控制措施。在这种情况下，组织应理解识别和接受低贿赂风险并不意味着组织可以接受贿赂发生的事实。也就是说，贿赂发生的风险（即贿赂是否会发生）不等同于贿赂的发生（贿赂的事实）。因此，组织可对贿赂持“零容忍”的态度，但可以允许在低贿赂风险或超过低风险的情形下开展商业活动（只要采取合适的缓解措施）。下文会对具体的管理措施进行进一步的介绍。

A.4 贿赂风险评估

A.4.14.5 所要求的贿赂风险评估是为组织构建反贿赂管理体系奠定坚实的基础，该评估过程确定了管理系统将重点关注的贿赂风险，艮卩：被组织视为贿赂风险的应是可降低贿赂风险的优先事项，反贿赂合规人员、资源和活动的控制实施与分配。组织如何进行贿赂风险评估、采用何种方法、如何对贿赂风险进行加权和优先排序，以及可接受的贿赂风险等级（如“风险偏好”）或容忍程度，均由组织自行决定。组织应基于其反贿赂方针和目标，建立评估风险的标准（低中高风险）。

以下提供了一些组织可以参考的方法：

a） 选择风险评估准则。如组织可以选择如“低”、“中”、“高”的三级标准，或者更具体的5级或7级标准或其他更详细的方法。这一标准通常要考虑多个因素，包括贿赂风险的性质、贿赂发生的可能性及发生时后果的严重程度；

b） 根据组织的规模和结构评估贿赂风险。与运营于多个地区的大型组织相比，位于同一地区且由少数人进行集中管理的小型组织控制贿赂风险的难度可能更低；

c） 检查组织运行或计划运行所在的地区或行业，并评估这些地区和行业为可能面临的贿赂风险。在开展评估时可使用一些合适的贿赂指标。组织可将高贿赂风险的地区或行业视为如“中”或“高”风险，从而实施适用于在这些地区或行业所开展的活动的较高级别的控制。

d） 评审组织活动和经营类型的性质、规模及复杂性。

1）与在多个地区开展多个大型建筑项目的组织相比，仅在一个地区开展制造业活动的组织的贿赂风险更容易控制；

2）有些活动的贿赂风险可能是特定的。例如，补偿性安排，它是指一个国家的政府在采购商品或服务时要求供应商按照合同价值的一定比例在采购国进行再投资的行为。组织应采取适当的措施确保这些补偿性安排不会构成贿赂。

e） 根据类别审核组织现有及潜在的商业伙伴，并评估其基本上面临的贿赂风险，例如：

1）组织可能有大量的客户，他们从组织购买小额的产品；他们对组织造成的风险实际上是最小贿赂风险。在这种情况下，组织可认为这些客户是低风险的，从而无须对其采取反贿赂控制措施。相反，组织可能需要关注向其购买高金额产品的顾客，他们可能会带有高贿赂风险（如以付款、审批等作为交换向组织索要贿赂）。这类客户可以被视为“中’‘或“高’’风险顾客，因此组织需要对其实施更高层次的反贿赂控制措施。

2）不同的供应商带来的贿赂风险也有所不同。如，业务广泛或可能与组织的客户、顾客或相关公职人员接触的供应商，可能带来“中”或“高”贿赂风险。而另一些供应商则可能是“低”风险的，如位于低贿赂风险地区、与交易相关的公职人员或组织的客户或顾客无接触的供应商。此外，还有一些供应商则可能是“超低“风险的，如低额少量物品的供应商、机票或酒店的网上订购服务等等。组织可能无须对这些低或超低贿赂风险的供应商实施反贿赂控制措施。

3）与组织客户或代表组织的公职人员往来的代理或中介很可能带来“中”或“高”贿赂风险，尤其是当其以佣金或提成获得报酬时。

f） 检查与可能带来贿赂风险的国内外公职人员往来的性质及频率。例如，与负责发放许可证或具有审批权的公职人员往来可能会产生贿赂风险。

g） 检查适用的法律、法规、合同以及专业责任与义务，如禁止或限制公职人员娱乐活动或使用代理。

h） 考虑组织对已评估风险的影响或控制程度。

以上所有贿赂风险因素均相互关联。例如，同一类别供应商可能带来的贿赂风险取决于其经营所在地。

A.4.2 评估相关贿赂风险后，组织可以确定适用于每一类风险的反贿赂控制措施的类型和程度，并评估现有控制措施是否适宜。如果不适宜，可予适当改进。例如，对位于高贿赂风险地区和属于高贿赂风险范畴的商业伙伴可进行高级别控制。组织可以决定对低风险活动或商业伙伴进行低级别的控制可予接受。本标准明确表示某些条款要求可不应用于低风险活动或商业伙伴（但是组织可自行决定是否采用）

•

A.4.3 组织可以改变交易、项目、活动或关系的性质以将贿赂风险的性质和程度降低到一定水平，从而可通过现有的、强化的或额外的反贿赂风险进行有效控制。

A.4.4 贿赂风险评估并不一定需要全面开展或非常复杂。风险评估的结果也未必需要证明其正确性（例如，评估认为是低风险的交易结果却发生了贿赂）。在合理可行范围内，贿赂风险评估的结果应反映组织面临的实际风险。这项工作宜设计为一种工具以帮助组织评估和需优先考虑的贿赂风险，并根据组织和环境的变化（例如：新市场和产品、法律要求和经验等）进行定期评审和修改。

注：更多的指南见 ISO 31000。

A.5 治理机构和最高管理者的岗位与职责

A.5.1 许多组织都有某种形式的治理机构，如董事会或监事会，他们对组织负有总体的监督责任，包括监督反贿赂管理体系。但是，治理机构通常不会对组织的日常活动进行指导，这是执行管理层（如首席执行官、首席运营官等）的职责，即本标准所称的“最高管理者因此，关于反贿赂管理体系，治理机构宜了解该体系的内容和运行情况，合理监督其充分性、有效性和实施情况，并通过管理评审程序定期了解体系绩效的相关信息（可指整个治理机构或其中的某一委员会，比如审核委员会）。在这方面，合规职能宜具有直接向治理机构（或合适的委员会）报告体系相关信息的权力。

A.5.2 一些组织，特别是小型组织，可能没有独立的治理机构，或者治理机构和执行管理层的职责均由一个团队甚至某个人来承担。在这种情况下，本标准中所指的最高管理者和治理机构的职责由该团队或个人承担。

注：领导层的承诺通常被称为“高层基调”。

A.6 反贿赂合规职能

A.6.1　反贿赂合规职能人员的数量取决于如组织规模、组织面临的贿赂风险程度以及该职能的工作量等因素。在小型组织中，合规职能可能只由一名员工兼任，该员工同时还需承担其他职责。当贿赂风险程度和总工作量较大时，合规职能可以委任一名员工全职负责。在大型组织中，合规职能则很可能是由数名员工担任；有些组织的合规职责则可由某一具有相关专业知识的委员会承担；有些组织可选择聘请第三方承担部分或全部反贿赂合规职能，只要组织某一经理保留对该反贿赂合规职责的总体责任和权限且可对第三方提供的服务进行监督，这种方式可以接受。

A.6.2　本标准要求反贿赂合规职能应该由具备合适能力、地位、权限和独立性的员工担任。

a）　“能力”是指承担反贿赂合规责任的相关员工必须具备符合这一职位要求的个人能力，有意愿和热情学习职位要求的相关素质，并能够准确履行职责；

b）　“地位”是指其他人可能听取并尊重承担合规职责的人员的意见；“权限”是指承担合规职责的相关员工得到治理机构（若有）和最高管理者赋予的足够权力，从而能够有效地承担合规职责。

c）　“权限”是指承担合规职责的相关员工得到治理机构（若有）和最高管理者赋予的足够权力，从而能够有效地承担合规职责。

d）　“独立性”是指负责合规职责的相关员工尽可能不参与有贿赂风险的组织活动。如果组织任命一个员工全职负责会更容易实现；但对于小型组织来说比较困难，他们通常是一个人同时负责合规职责和其它职责。若对合规职位进行兼职，合规职能人员不能由那些履行主要职责时可能存在贿赂风险的员工担任。在很难实现独立性的小型组织，这个合适的员工宜尽自己的能力区分合规职责与其他职责，以确保公正性。

A.6.3　为便于沟通相关信息，反贿赂合规职能直接向最高管理者或治理机构（若有）报告工作是很重要的。合规职能不必逐级先向其他部门主管报告，再由该主管向最高管理者报告；这样会影响合规职能向最高管理者报告的信息的完全性和清晰度。合规职能宜无需经过最高管理者同意便可直接与治理机构（若有）沟通和联系，可以向治理机构（比如董事会或监督委员会）报告或者向治理机构或最高管理者特别委托的委员会（比如审核或道德委员会）报告。

A.6.4　合规职能的主要职责是监督反贿赂管理体系的设计和实施，这不能与组织的反贿赂绩效和遵守可适用反贿赂法律的直接职责相混淆。每个员工都应以道德伦理规范来约束自己的行为，包括遵守组织的反贿赂管理体系以及反贿赂法律的要求。特别重要的是，为使组织所有部门均遵守相关规定，管理层应起表率作用。

注：更多指南见 ISO 19600。

A.7　资源

体系运行所需的资源取决于组织规模、业务性质以及面临的贿赂风险等因素。资源可包括：

a）　人力资源：确保组织有足够的人员能够投入足够的时间承担相关的反贿赂责任，以确保反贿赂管理体系得以有效运行。这包括配置足够的员工（无论是组织内还是组织外的）承担合规职能；

b）　物力资源：确保组织内部有可用的必要物质资源，包括配置反贿赂合规职能，以使反贿赂管理

体系能够有效运行。例如，办公空间、家具、计算机硬件和软件、培训材料、电话和文具等；

c） 财力资源：确保安排足够的经费预算，包括反贿赂合规职能的工作经费，以使反贿赂管理体系能够有效运行。

A.8 雇用程序

A.8.1 对员工的尽职调查

在签订劳动合同之前，组织应对新员工进行尽职调查；根据新员工职务和相应的贿赂风险，组织可采取以下措施：

a） 面试时与有聘用意向的应聘者讨论组织的反贿赂方针，判断其是否理解并认可遵守该政策的重要性；

b） 采取合理的步骤验证新员工的能力是否真实准确；

c） 采取合理的方式从新员工的前任雇主获得可靠的推荐信；

d） 采取合理的步骤确定员工是否曾经涉及贿赂事件；

e） 采取合理的步骤证明组织雇用新员工不是为了从前任雇佣关系中获取不正当的利益；

f） 采取合理的步骤识别未来该员工与公职人员的关系。

A.8.2 绩效奖金

补偿安排，包括奖金和奖励可能会甚至是无意中诱导员工参与贿赂。例如，如果某经理因为签订某项合同可以获得一笔丰厚奖金，这名管理人员可能会行贿，或对某个代理或合作企业的行贿活动视而不见，以确保获得合同奖金。当管理人员由于绩效原因压力过大时，也会发生相同的结果（例如，如果管理人员因为未实现过高的销售指标而可能被解雇）。因此，组织需要特别注意这些补偿因素，以确保尽可能合理地避免这些因素成为贿赂的动机。

同样，员工评价、晋升、奖金及其它奖励也可作为激励员工遵守组织反贿赂方针以及反贿赂管理体系的动力。此外，组织需要谨慎对待下列情况，即因为害怕失去奖金也可能导致员工隐瞒其违反反贿赂管理体系规定的行为。

员工应当意识到违反反贿赂管理体系以提升其在其它领域（如实现销售目标）的绩效不可取，这可能会使其遭受纪律处分。

A.8.3 利益冲突

组织宜识别和评估内外部利益冲突的风险。组织宜明确告知所有员工他们有义务报告任何实际或潜在的利益冲突，例如家庭、财务或与其工作相关的直接或间接的其他联系。这可帮助组织识别利于或不利于员工预防或报告贿赂的情况；如：

a） 当组织的销售经理与客户的采购经理有关联时；

b） 当组织的生产线经理在竞争对手的业务中有财务利益时；

组织宜更好地记录所有实际或潜在的利益冲突情形及是否采取措施减少冲突。

A.8.4 组织员工的贿赂

A.8.4.1　预防、发现和处置组织员工的贿赂（“内部贿赂”）所采取的措施与用以预防、发现和处置组织员工代表组织贿赂他人（“外部贿赂”）所采取的措施有所不同。例如，鉴于员工个人信息不受组织控制（如员工的个人账户以及信用卡的交易数据）、现行法律（如隐私法）或其他因素，组织发现或降低组织内部贿赂风险的能力可能受制于获取信息的难度。因此，组织降低外部贿赂风险的控制方法也多于内部贿赂控制。

A.8.4.2　组织员工的贿赂最容易发生在那些能够代表公司做出决策或影响决策的人身上（例如，能够从合同中获利的采购经理、审批工作的监督者、任命人事或审核工资或绩效的经理、负责发放执照和许可证的工作人员等）。由于不在组织管理体系控制措施范围内的员工很可能接受贿赂，因此对组织来说，预防和发现此种贿赂的能力就会受到限制。

A.8.4.3　除了 A.8.1 和 A.8.3 中所述的步骤外，本标准的下列要求可帮助降低内部贿赂风险：

a）　组织的反贿赂方针（见 5.2）宜明确禁止组织员工及代表组织工作的任何人索要和接受贿赂；

b）　指导和培训材料（见 7.3）应当强调禁止索要和接受贿赂，包括：

1）对涉嫌贿赂进行报告的指南（见 8.9）：

2）强调组织的非报复政策（见 8.9）o

c）　组织的礼物和款待政策（见 8.7）宜限制员工接收礼物和款待；

d）　在组织的网站上公布组织的反贿赂方针以及举报渠道，帮助商业伙伴设立期望值，以减少商业伙伴提供贿赂、或组织员工索要或接受贿赂的可能性；

e）　控制措施（见 8.4）中要求使用经过审批的供应商，竞标、签订合同和审批工作至少需两人签字批准等，从而降低审批风险，减少腐败行为。

A.8.4.4　为识别员工是否利用现行控制措施弱点而获取个人利益的情况，组织可执行相应审核程序。审核程序样例可以包括：

a）　审核工资文件，查看是否有虚假或重复的员工记录；

b）　审核员工的消费报告，查看是否有不正常消费；

c）　将员工工资的文件信息（如个人账户和地址）与组织供应商文件信息中的银行账户和地址进行对比，以发现潜在的利益冲突。

A.8.5　临时工或工人

在某些情况下，组织的临时工或工人由劳务公司或其他组织提供，组织宜确定是否按公司要求向存在贿赂风险的临时工或工人（如果有）进行培训和控制，或者通过提供临时工或工人的组织实施合适的控制措施。

A.9　意识和培训

A.9.1　培训的目的是确保相关员工根据其在组织内的职责或与组织的关系，了解以下信息：

a）　员工和组织面临的贿赂风险；

b）　反贿赂方针；

c） 反贿赂管理体系中与岗位相关的各方面内容；

d） 自身需要采取的与贿赂风险或涉嫌贿赂相关的任何必要的可预防措施，以及相关的报告和调查程序。

A.9.2 培训的形式和范围取决于组织的规模及其面临的贿赂风险。培训可以采取在线模式或面对面的形式（例如，课堂教学、研讨会、相关人员举行圆桌会议讨论或一对一谈话）。培训结果比培训方法重要，应确保所有相关人员理解 A.9.1 所列出的内容。

A.9.3 针对参与存在超出了低贿赂风险的业务和过程的治理机构、最高管理者、员工（不论其在组织内的岗位和职务高低）和商业伙伴，推荐对其进行面对面的培训。现场培训推荐给治理机构（如有），以及参与超出低贿赂风险的业务或过程的任何员工（不论其在组织内的岗位和职务高低）和商业伙伴。

A.9.4 如果被指派负责合规职能的相关人员不具备足够的相关经验，组织应能够为其提供必要的培训以确保充分履职。

A.9.5 可以进行独立的反贿赂培训，也可以把反贿赂培训作为组织整体合规和道德培训或入职培训的一部分。

A.9.6 培训的内容可以根据员工的岗位进行调整。对于岗位贿赂风险低的员工，只需对其进行简单的组织政策培训，以使其理解组织政策并在意识到潜在违规行为且了解应采取的行动。对于岗位贿赂风险较高的员工，则需要接受更为详细的培训。

A.9.7 培训宜保持常态化，以使员工可以及时了解组织政策和程序、与其职位相关的新动态及监管变化。

A.9.8 依据 7.3 的要求，将培训和意识要求应用于商业伙伴尤其具有挑战，因为商业伙伴的员工通常不直接为组织工作，且组织通常无法直接为这些人员提供培训。商业伙伴员工的实际培训通常由商业伙伴或为此目的雇佣的其他方提供。商业伙伴的员工意识到商业伙伴可能对组织构成超过低贿赂风险这一问题并接受合理的培训以降低风险，这一点很重要。7.3 的内容要求组织至少识别出应对其员工提供反贿赂培训的商业伙伴、培训至少应包含的内容及培训开展的方式。培训可由商业伙伴、指定的第三方进行，或者如果组织选择，也可由组织进行。组织可通过各种方式向其商业伙伴传达这些要求，如作为合同内容的一部分。

A.10 尽职调查

A.10.1 作为风险评估（见 4.5）的一部分，对特定交易、项目、活动、商业伙伴或组织员工开展尽职调查是进一步评估已识别的超过低贿赂风险的相关事项或人员的范围、规模和性质。同时，尽职调查也作为预防、发现贿赂风险的针对性附加控制措施，为组织是否推迟、中止、修改交易、项目或与商业伙伴或员工的关系提供决策依据。

A.10.2 关于项目、交易及活动，以下几点可助于组织评估：

a） 结构、性质及复杂性（如：直接销售或间接销售、折扣水平、合同签约，招投标程序）；

b） 筹资与支付安排；

c） 组织承诺与可用资源的范围；

d） 可控性与可见性程度；

e） 商业伙伴与其他相关第三方（包括公职人员）；

f） 所有相关方（e 中所述）与公职人员的关系；

g） 所有相关方的能力与资格；

h） 客户的声誉；

i） 所处地域；

j） 市场报告或新闻报道。

A.10.3 关于合理的对商业伙伴进行尽职调查：

a） 以下几点可助于组织评估与商业伙伴的相关信息，包括：

1）商业伙伴是否是合法的商业实体，可通过如公司登记文件、年度申请账户、纳税人识别号、在证券交易所上市等指标证明；

2）商业伙伴是否具备履行合同要求的业务所需的能力、经验和资源；

3）商业伙伴是否实施反贿赂管理体系以及实施的程度；

4）商业伙伴是否有贿赂、欺诈、不诚实或类似不良行为的名声，或因贿赂或类似犯罪行为被调查、定罪、制裁或禁止从业；

5）识别商业伙伴的股东（包括最终受益方）和最高管理者，他们是否：

i）有贿赂、欺诈、不诚信或类似犯罪行为；

ii）因贿赂或类似犯罪行为被调查、定罪、制裁或禁止从业；

iii）与可能导致贿赂的组织的顾客或客户或相关公职人员存在直接或间接的联系（包括其本身不是公职人员，但可能与公职人员、公职候选人员有直接或间接关系的人等）；

6）交易和支付安排的结构；

b） 尽职调查的性质、类型和程度将取决于组织获取充足信息的能力、获取信息的成本和内外部关系可能带来的贿赂风险的程度等因素；

c） 组织对商业伙伴进行尽职调查的程序应与其类似风险程度保持一致。和低风险地区或市场的低风险商业伙伴相比，组织需要对高风险地区或市场的高风险商业伙伴需要进行更严格的尽职调查；

d） 不同类型的商业伙伴可能需要不同级别的尽职调查，例如：

1）从组织潜在的法律和金融负债的角度来看，那些代表组织或为了组织利益而开展活动的商业伙伴往往会比那些仅向组织提供产品或服务的商业伙伴给组织带来更高的贿赂风险。例如，为帮助组织赢得合同，合同签约代理商就可能会向组织的客户的管理人员行贿；这就可能导致组织要对该代理商的腐败行为负责。所以，组织对代理商的尽职调查应尽可能全面。另一方面，向组织提供设备或原材料的供应商，如果其跟与组织活动相关的组织的客户或公职人员没有关联，则其以组织名义行贿的可能性较低，因此，对这类供应商的尽职调查程度可适当降低；

2）组织对商业伙伴的影响程度也会影响组织对其进行合理尽职调查的程度。对于一个组织而言，作为尽职调查的一部分，组织在确立与代理商和合资伙伴的合作关系之前就要求其提供详实的信息可能相对容易；因为在此之前，组织还有选择权。由于组织对客户或顾客可能没有足够的影响力，组织或难以要求顾客或客户提供相关信息或填写尽职调查问卷（例如，组织参与向客户提供服务的竞标）；

e） 组织对其商业伙伴的尽职调查可包括如下形式：

1）向商业伙伴发送调查问卷，要求其回答如 A.10.3.a 中所列的问题；

2）网络检索商业伙伴及其股东和最高管理者相关信息，以识别有无与贿赂相关的信息；

3）通过合适的政府、司法以及国际资源检索相关信息；

4）查看国家或当地政府或多边金融机构（例如世界银行）限制或禁止采购的公开黑名单；

5）向合适的第三方咨询商业伙伴的道德声誉；

6）委派拥有相关专业的其他人员或组织协助尽职调查；

f） 可以根据初步调查结果进一步询问商业伙伴（例如要求其对负面信息进行解释）。

A.10.4 尽职调查并不是万能的。没有负面消息并不能证明商业伙伴没有贿赂风险，有负面消息也不能说明商业伙伴一定有贿赂风险。但是，组织需要根据获取的事实认真评估调查结果并做出理性判断。尽职调查的总体目的是组织合理、适当地询问商业伙伴，考虑商业伙伴承担的活动及这些活动本身所具有的贿赂风险，从而合理判断如果组织与该商业伙伴合作将会面临的贿赂风险水平。

A.10.5 关于员工的尽职调查，见 A.8.1。

A.11 财务控制措施

财务控制措施是指组织为适当地管理财务交易并正确、完整和及时地记录这些财务交易而实施的管理体系和过程。根据组织和交易的规模，组织实施的用于降低贿赂风险的财务控制措施可包括：

a） 实施岗责分离制度，确保同一人员不能同时拥有提出用款和审批款项的权力；

b） 付款审批进行适当的梯度授权制（大型交易需要获得更高管理层批准）；

c） 确保组织有关审批程序已批准对支付人员的授权和工作或服务；

d） 付款审批至少要求两人签名；

e） 限制现金使用并采取有效的现金控制方法；

f） 确保记账时款项的分类并加以准确、清晰地描述；

g） 定期对重大财务交易开展管理评审；

h） 实施定期和独立的财务审核并定期变更实施审核的人员或组织。

A.12 非财务控制措施

非财务控制措施是指组织为合理管理其采购、运营、商业以及其它非财务业务而实施的管理体系和过程。根据组织和交易的规模，组织在采购、运营、商业和其它非财务方面实施的以降低其贿赂风险的管理控制措施可包括：

a） 使用通过资格预审的分包商、供应商和顾问。在资格预审过程中，需要评估其参与贿赂的可能

性。该过程可能包括 A.10 中规定的尽职调查；

b） 需评估以下内容：

1）商业伙伴（顾客或客户除外）对组织提供服务的必要性和合法性，

2）供应商的服务是否适当提供；

3）对商业伙伴提供服务的付款是否合乎情理或适当；避免商业伙伴利用组织向其支付的部分钱财以组织的名义进行贿赂的风险，这点尤为重要。例如，组织指定代理商帮助其销售并向其支付佣金或代理费，这样组织就必须确认其所支付的佣金与代理商所提供的实际服务是否成正比；并考虑在没有成功签订合同的情况下，代理所要承担的风险。如果组织向其支付了不合理的大额佣金或代理费，那么代理商就很有可能使用其中一部分去贿赂公职人员或者组织客户的员工，让其与组织订立合同；

c） 如果条件允许和合理，合同应该在开展至少有三名竞标人参与的公平和透明的竞标活动后订立；

d） 至少需要两人分别评估投标人和审批订立合同；

e） 实施岗责分离，使合同预算审批、合同预算需求、合同管理和合同审批的员工相独立；

f） 合同及合同条款修改或供应商审批文件要求至少有两人签名；

g） 对潜在高贿赂风险交易实施更严格的管理监督；

h） 保护投标和其它敏感价格信息的完整性，对人员获取相关信息进行限制；

i） 向员工提供合适的工具和模板（例如，实操指南、行为准则、审批层级、检查清单、表格、信息技术工作流等）。

注：更多控制措施和指南见 ISO 19600。

A.13 在受控的组织和商业伙伴中实施反贿赂管理体系

A.13.1 总则

A.13.1.1 提出这一要求（8.5）的原因是受控制的组织和商业伙伴都可能对组织构成贿赂风险。在这种情况下，组织要避免的贿赂风险类型如下：

a） 组织的子公司行贿，其结果可能由组织承担；

b） 合资企业或合资伙伴为组织参与的合资企业赢得工作而行贿；

c） 顾客或客户的采购经理向组织索贿以换取合同；

d） 组织的客户要求组织与特定的分包商或供应商合作，在该情形下，客户的管理人员或公职人员可能从中获得个人利益。

e） 组织的代理商以组织的名义向组织客户的管理人员行贿；

f） 组织的供应商或分包商向组织的采购经理行贿以换取合同。

A.13.1.2 如果受控制的组织或商业伙伴已对相关风险实施了反贿赂控制措施，那么组织相应的贿赂风险通常会相应降低。

A.13.1.3 8.5 的条款要求对是否受组织控制的组织予以区分；这一条款需求的目的，如果组织直接或间接地控制了另一个组织的管理层，则组织对其拥有控制权。例如：通过拥有董事会的多数投票或持有

大多数股权，组织可以控制一个子公司、合资企业或财团。仅是对另一个组织投入大量的工作不能表明组织对其拥有控制权。

A.13.2　受控组织

A.13.2.1　希望组织确保受其控制的组织实施合理和适当的反贿赂控制措施是合理的，受控制的组织既可以实施与组织一样的反贿赂管理体系，也可以实施自己的反贿赂控制措施。这些措施宜是合理的，与受控组织所面临的贿赂风险相匹配，并考虑了依据 4.5 执行的贿赂风险评估。

A.13.2.2　针对商业伙伴受组织控制的情形（例如：受组织控制的合资企业），那么，8.5.1 的要求适用于受控制的商业伙伴。

A.13.3　不受控的商业伙伴

A.13.3.1　对于不受组织控制的商业伙伴，组织可能不需要采取 8.5.2 要求的步骤要求商业伙伴在以下情形实施反贿赂控制。

a）　商业伙伴没有贿赂风险或贿赂风险程度较低；或

b）　商业伙伴所构风险超过低贿赂风险，但商业伙伴可以实施的控制措施未能降低相关风险，坚持要求商业伙伴实施无效的控制措施便毫无意义。然而，在这种情形下,组织宜在风险评估中考虑这一因素，以便形成如何以及是否与该商业伙伴维持业务关系的决策。

这体现了本标准的合理性和比例性。

A.13.3.2　如果贿赂风险评估（见 4.5）或尽职调查（见 8.2）显示不受组织控制的商业伙伴构成的贿赂风险超出了低贿赂风险，且商业伙伴实行的反贿赂控制措施能够降低贿赂风险,那么，组织需参照 8.5 的要求采取下列步骤：

a）　组织确定商业伙伴是否已采取适当的反贿赂控制以管理相关的贿赂风险。组织宜在进行合理的尽职调查后作出判定（见 A.10）。组织要尝试证实这些控制已控制与商业伙伴之间交易的贿赂风险，组织不需要证实商业伙伴的控制是否已控制其自身的其他贿赂风险。需要注意的是，控制的程度和组织核实这些控制需要采取的步骤宜合理，且与相关贿赂风险相匹配。如果组织已尽其合理可能确认商业伙伴确实采取适当的控制，那么，此类商业伙伴已满足 8.5 的要求。关于适当控制类型的评论见 A.13.3.4。

b）　如果组织确认商业伙伴未有适当的措施控制相关的贿赂风险,或者组织无法核实其是否采取了适当控制措施，那么，组织可以采取以下步骤：

1）如果切实可行（见 A.13.3.3）,组织要求商业伙伴在相关的交易、项目或活动中实施反贿赂控制（见 A.13.3.4）；

2）在要求商业伙伴实施反贿赂控制无法实现的情况下（见 A.13.3.3），组织在评估商业伙伴的贿赂风险及采取何种方式管理这些风险时应考虑这一因素。这并不意味着组织不能继续维持这个商业关系或开展交易。但是，作为贿赂风险评估的一部分，组织宜考虑商业伙伴发生贿赂的可能性，并在全面评估自身贿赂风险时考虑对商业伙伴缺乏有效控制的这一因素。如果组织确信商业伙伴的贿赂风险是不可接受的，并且通过其他手段也不能降低该贿赂风险（如改变交易的结构），那么，8.8 的条款要求适用

于这一情况。

A.13.3.3　组织要求一个不受其控制的商业伙伴实行控制措施是否可行视情况而定，例如：

a）　当组织对商业伙伴有较大影响时，这通常可以实现。如在组织委托代理商代表组织进行交易或委托分包商承担大量工作的情况。在这种情况下，组织通常能够将实行反贿赂控制措施的要求作为委托前提。

b）　当组织对商业伙伴的影响不够时，通常无法实现。例如：

1）项目的客户；

2）客户指定的特定分包商或供应商；

3）当重要的分包商或供应商的议价能力远胜于组织时（例如，当组织根据重要供应商的标准条款向其购买零部件时）；

c）　当商业伙伴缺乏实行反贿赂控制措施的资源或专业知识时，通常无法实现。

A.13.3.4　组织所要求的控制措施的类型视情况而定。所有反贿赂控制措施必须是合理的、与贿赂风险相匹配，且至少宜涵盖相关的贿赂风险。根据商业伙伴及其所面临贿赂风险的性质，组织可以采取如下步骤：

a）　对于业务往来多且其贿赂风险高的商业伙伴，组织可要求商业伙伴针对其对组织带来的贿赂风险实施与本标准要求等同的控制措施。

b）　对于业务往来一般且其贿赂风险一般的商业伙伴，组织可以要求该商业伙伴针对与交易相关的最低程度的反贿赂要求，如制定反贿赂方针、为其相关员工提供培训、委派相关管理人员承担相关交易的合规职责、对大额支付进行管理及制定报告路径等。

c）　对于仅有少量特定工作的小型商业伙伴（如代理商或小型供应商），组织可要求其为相关员工进行培训，并对大额支付、礼物和款待进行管理。

这些控制措施仅需要在与组织和商业伙伴的交易相关的活动中实施（虽然在实际中商业伙伴可能会对其全部业务实施控制）。

以上例子仅供参考。对组织来说，关键问题是要识别出与交易相关的重大贿赂风险；若可行，要求商业伙伴对这些重大的贿赂风险实行合理和适当的控制措施。

A.13.3.5　组织通常会将这些要求作为与不受其控制的商业伙伴进行合作的前提和/或作为合同文本的部分内容。

A.13.3.6　组织并不一定需要证实不受其控制的商业伙伴完全遵守这些要求。但是，组织宜采取合理的步骤使自己满意，即商业伙伴正在遵守（如通过要求商业伙伴提供其相关的政策文件）。针对高风险情形（如代理商），组织可以对其实行监督程序，如包括报告和审核权等。

A.13.3.7　由于实施反贿赂控制措施需要一定时间，因此，组织给予其商业伙伴一定的时间来实施这些控制措施是较为合理的。在此期间，组织可继续与其商业伙伴进行合作，但在风险评估和尽职调查中应考虑到商业伙伴缺乏控制措施这一因素。但是，组织宜考虑如商业伙伴无法及时有效实施所要求的控制，

要求有权终止相关合同或协议。

A.14 反贿赂承诺

A.14.1 要求提供反贿赂承诺仅适用于商业伙伴的贿赂风险超出组织可接受的低贿赂风险的情形。

A.14.2 在以下情况下，商业交易涉及的贿赂风险可能较小，例如：

a） 组织采购少量低值商品；

b） 组织在线直接从航空公司或酒店预定机票、房间；

c） 组织直接向客户提供低值商品或服务（如食物、电影票等）。

在这些情况下就不需要组织向这些低贿赂风险的供应商或客户索取反贿赂承诺。

A.14.3 当商业伙伴对组织构成的贿赂风险超出低贿赂风险时，组织宜在可行的情况下取得商业伙伴的反贿赂承诺：

a） 当组织能够影响商业伙伴时，要求这些承诺通常可行，因而可以坚持让商业伙伴做出这些承诺。例如，当组织任命某代理商代表其开展交易，或委托某分包商承担大量工作时，组织可以要求这些承诺；

b） 组织可能没有足够的影响力要求这些承诺，例如，与重要客户或顾客开展交易，或者当组织按照供应商的标准条款向其购买零件时。在这些情况下，不能要求其做出反贿赂承诺并不意味着项目或业务关系就不能进行开展，但是在贿赂风险评估和尽职调查中应考虑这一因素。

A.14.4 承诺应尽可能以书面形式表示，既可以是单独的承诺文件，也可以作为组织与商业伙伴所签订的合同的一部分。

A.15 礼物、款待、捐赠和类似利益

A.15.1 组织需要意识到只要是以贿赂为目的或是有贿赂意图的行为，即使不是受贿或者行贿方，收受礼物、款待、捐赠以及其他的利益均能够被第三方察觉（如商业竞争对手、新闻媒体、检察官或法官）。一个有效地控制机制能够尽可能地预防那些能被第三方察觉的以贿赂为目的收受礼物、款待、捐赠以及其他利益的行为。组织需意识到，即使给予和接受双方并非出于贿赂的目的，礼物、款待、捐赠以及其他利益都有可能被第三方（如商业竞争对手、新闻媒体、检察官或法官）认为是出于贿赂的目的。有用的控制机制能够尽可能地避免礼物、款待、捐赠以及其他利益可能被第三方合理地认为是出于贿赂的目的。

A.15.2 8.7 中的利益可包括，例如：

a） 礼物、娱乐和款待；

b） 政治或慈善捐款；

c） 客户或公职人员差旅费；

d） 宣传费用；

e） 赞助；

f） 团体利益；

g） 培训；

h） 俱乐部会员；

i） 个人喜好；

j） 保密和特权信息。

A.15.3 针对礼物和款待，组织可以实施的程序如下：

a） 通过以下措施管理礼物和款待的程度和频率：

1）全面禁止所有礼物和款待；或

2）允许礼物和款待，但应对以下这些因素设限：

i）费用上限（因地区及礼物和款待的类型而不同）；

ii）频率（相对较小的礼物和款待如果频率过高，其累计规模也不得忽视）；

iii）时间（例如：招标谈判期间及刚结束时）；

iv）合理性（考虑给予者或接受者的地点、行业和资历）；

v）接收人的身份（例如：负责合同签订或许可、证书或款项审批等的员工）；

vi）互惠款待（不允许组织内任何人接受价值超出其有权送出礼物、款待价值的礼物、款待）；

vii）法律和监管环境（一些地区和组织可能已颁布或采取措施）；

b） 礼物和款待的价值或频率超过限制，需要事先获得某一恰当的管理人员的批准；

c） 礼物和款待的价值或频率超过限制，要如实记录（如登记薄或分类账户）和监督并予公开。

A.15.4 针对政治或慈善捐款、赞助、宣传费用和团体利益，组织可以实施如下程序：

a） 禁止以意图或被合理怀疑存在意图影响招标或其它对组织有利的决策而进行支付；

b） 对政党、慈善机构或其他收款人开展尽职调查，确保支付的合法性，而非变相贿赂（例如，这可能包括在互联网上搜索或通过其它合适的查询途径以确定政党或慈善机构的负责人是否有过受贿行为或其它犯罪行为，或与组织的项目或客户是否有关联）；

c） 确保由合适的管理人员审批相关支付；

d） 要求公开披露支付信息；

e） 确保支付符合适用的法律、法规规定；

f） 避免在合同洽谈中或结束后立即进行捐款。

A.15.5 针对客户代表或公职人员的差旅费用，组织可以实施如下程序：

a） 确保支付为客户或公共机构相关程序和当地法律法规所允许；

b） 确保差旅费用是客户代表或公职人员适当履职所必须的（例如，检查组织工厂质量体系）；

c） 确保由合适的管理人员批准付款；

d） 如果可行，确保将所提供的差旅费用和款待告知公职人员的上级、雇主或反贿赂合规职责；

e） 限制与合理差旅路线直接相关的必要旅途、住宿和餐饮费用的报销；

f） 根据组织的礼物和款待政策，将差旅相关花费限制在一合理水平；

g） 禁止报销家属或朋友的费用；

h） 禁止报销度假或娱乐费用。

A.16 内部审核

A.16.1 9.2 的要求并不意味着组织必须有自己独立的内审部门，但要求组织需任命某一独立的、具备相应能力的部门或人员承担审核工作。组织可以雇佣第三方负责全部内审工作，或仅委托其负责现有工作的特定部分。

A.16.2 审核的频率由组织根据需求决定。每年可以选择特定项目、合同、过程、管理和体系进行审核。

A.16.3 审核可基于风险进行抽样，因此应优先选择高贿赂风险的项目进行审核。

A.16.4 通常需要提前做好审核计划，以给相关方准备必要的文件及预留充裕时间。但是，在某些情况下，开展突击审核会更加有效。

A.16.5 如果组织设有治理机构，治理机构也可在认为必要时指导组织确定审核对象和频率，以保持审核的独立性，并确保审核针对组织的主要风险。治理机构还可以要求查阅所有的审核报告和结果；即在完成审核后，应将识别出的特定高贿赂风险类型或贿赂风险指标向治理机构报告。

A.16.6 审核的目的是向治理机构（如有）和最高管理者确保已实施反贿赂管理体系且运行良好，可预防和发现贿赂，并对潜在的腐败人员起到警示作用（因为他们都知道，其负责项目或所在部门可能会被抽中审核）。

A.17 成文信息

7.5.1 的成文信息可包括：

a） 员工收到反贿赂方针的回执；

b） 针对所构贿赂风险超出低贿赂风险的商业伙伴制定的反贿赂方针条款；

c） 反贿赂管理体系的政策、程序以及控制措施；

d） 贿赂风险评估结果（见 4.5）；

e） 提供的反贿赂培训（见 7.3）；

f） 开展的尽职调查（见 8.2）；

g） 实施反贿赂管理体系的措施；

h） 给予和接收的礼物、款待、捐款和类似利益的审批和记录（8.7）；

a） 与下列情况相关的问题的措施和结果：

3）反贿赂管理体系的薄弱之处；

4）试图、涉嫌、或实际的贿赂行为；

b） 组织或第三方实施的监视、调查或审核的结果。

A.18 调查和处理贿赂

A.18.1 本标准要求组织实施关于调查和处理贿赂问题、或任何（举报、发现或合理怀疑的）违反反贿赂控制措施行为的适当程序。组织调查和处置特定问题的方法依不同情形而定。每种情形都有特殊性，因此，组织的应对措施宜因地制宜。相对于违反反贿赂控制措施的轻微情况，报告疑似贿赂的重大问题

需要更紧急、重要和详细的措施。以下建议仅作为指南，不宜将其当作规范性要求。

A.18.2　合规职能宜做好任何疑似或实际贿赂或违反反贿赂控制措施报告的接收工作。如果报告不是第一时间提交给合规职能，组织应确保有尽快报告至合规职能的程序。在某些情况下，合规职能自身也能够发现可疑或实际违规行为。

A.18.3　这一程序宜确定有权决定如何开展调查和处置问题的人员。例如：

a）　小型组织可以实施由合规职能将问题（无论其严重性）直接向最高管理者报告，以使其做出处置决定；

b）　大型组织可实施如下程序：

1）轻微问题由合规职能处理，并定期将总体情况向最高管理者报告；

2）重大问题由合规职能直接向最高管理者报告，以使其做出处置决定。

A.18.4　根据识别出的问题，最高管理者或合规人员（如果合适）宜评估已知事实和问题的潜在影响。如果没有掌握充足的事实以支撑决策，则宜启动调查程序。

A.18.5　调查宜由一名与该事件无关的人员执行，他可能是合规人员、内部审核人员、其他合适的管理人员或第三方人员。宜赋予调查人员合适的权力、资源，且能够直接向最高管理者报告，从而使调查有效开展。调查人员宜接受过培训或者参与过调查。调查宜尽快确认事实并收集必要证据，可通过以下手段：

a）　进行询问以确认事实；

b）　收集相关文件和其他证据；

c）　取得证人证词；

d）　若可行，以书面形式进行报告，并要求相关人员签名。

A.18.6　开展调查以及采取后续措施时，组织需要考虑相关因素，如：

a）　适用法律（需要提供法律意见）；

b）　人员安全；

c）　陈述时可能会有中伤风险；

d）　保护起草报告和本报告涉及的相关人员（见8.9）

e）　组织和个人潜在的刑事和民事责任、经济损失和名誉损害；

f）　向相关政府报告时给组织带来的法律义务或利益；

g）　在事实确认之前，对问题和调查事项进行保密；

h）　需要最高管理者要求所有人员全面配合调查。

A.18.7　调查结果宜向最高管理者或合规职责（如合适）报告。如果只向最高管理者报告的话，最高管理者也宜将结果同反贿赂合规职责进行沟通。

A.18.8　一旦组织完成了调查，并且/或取得了足以支持做出决策的信息，组织宜实施下列适宜措施。根据特定情形以及问题的严重程度，这些措施可以包括：

a） 终止、退出或修改组织参与的项目、交易或合同；

b） 偿还或退回任何不当的利益；

c） 惩处责任人（根据问题的严重程度，处分有轻微罪行警告、严重违规的开除及解雇等）；

d） 将有关事项向相关职权部门报告；

e） 如果贿赂已经发生，应采取行动避免或处理任何可能随之带来的违法行为（如，贿赂在账户中以其他名义记账时会出现虚构账目，在收入中扣除贿赂金额引发的偷税罪名，或者消除犯罪所得的不法收入等）。

A.18.9 由于程序本身会有一些漏洞，所以组织宜评审其反贿赂程序，以检查是否有潜在问题；如果有，组织宜立即采取适当的步骤改善该程序。

A.19 监视

反贿赂管理体系的监视可包括以下几点，例如：

a） 培训的有效性；

b） 控制措施的有效性，例如通过样本测试的结果；

c） 满足合规义务的职责分配的有效性；

d） 处理已识别不合规项的有效性；

e） 内部合规审核未按计划执行的情况。

合规绩效的监视可包括以下几点，例如：

——不合规和未遂事件（没有负面影响的“事件”）；

——未履行合规义务的情况；

——目标未完成的情况；

——合规文化现状。

注：见 ISO 19600。

组织可定期在全组织内或组织的部分内开展自评，以评估反贿赂管理体系的有效性（见 9.4）。

A.20 反贿赂管理体系计划与执行的变更

A.20.1 反贿赂管理体系的适用性与有效性宜通过几种方式进行常规和定期评价，如：由内审（见 9.2）、管理（见 9.3）与反贿赂合规职能（见 9.4）进行审核。

A.20.2 组织应考虑反贿赂管理体系评估的产出，并决定是否需要对体系进行变更。

A.20.3 为了帮助确认反贿赂管理体系保持完整性和有效性，单个因素的改变应考虑其与整个管理体系的从属关系，其变化是否对整个管理体系的有效性产生影响。

A.20.4 当组织决定需要变更反贿赂管理体系，系统执行时应考虑以下变化：

a） 变更目的以及潜在结果；

b） 反贿赂管理体系的完整性；

c） 资源获得性；

d） 职责与职权的分配与再分配；

e） 变更的速度、范围和时间。

A.20.5 针对评审出的不符合（见 10.1）以及需要持续改进（见 10.2）的结果，反贿赂管理体系宜执行以上流程（A.20.4）以增强其实施效果。

A.21 公职人员

许多反腐败法律对公职人员（3.27）的定义都很宽泛。

下列例举并不详尽，且并不是每一个例子都适用于所有的司法管辖区。在评估反贿赂风险中，组织应当考虑其往来或可能往来的公职人员类别，并在不确定的情况下寻求法律意见。

公职人员可包括以下方面：

a） 国家、州/省或市级的公务人员，包括立法机构人员、行政机构官员和司法人员；

b） 政党机关官员；

c） 公职候选人；

d） 政府工作人员，包括政府部门、政府中介、行政法庭和公共机构的工作人员；

e） 国际公共组织的官员，例如世界银行、联合国、国际货币基金组织等；

f） 国有企业工作人员，除非该企业在相关市场上以常规商业模式运作，例如其本质相当于民营企业，没有优惠补贴或其他特权，见“参考文献[17]”。

在很多司法管辖区，其反腐败法律中也把公职人员的亲属和与其关系紧密的人视为公职人员。

A.22 反贿赂举措

虽然在本标准中没有作出要求，但组织可发现参与和参考与组织的活动相关的、已形成良好实践的各个行业或其他反贿赂举措十分有用。

参考文献

[1] ISO 9000 质量管理体系—基础和术语

[2] ISO 9001 质量管理体系—要求

[3] ISO 19011 管理体系审核指南

[4] ISO 14001 环境管理系统—要求与使用指南

[5] ISO/IEC 17000 合格评定——术语和通用原则

[6] ISO 19600 合规管理理体系系—指南

[7] ISO 22000，食品安全管理体系—食品链中各类组织的要求

[8] ISO 26000 社会责任指南

[9] ISO/IEC 27001，信息技术—安全技术—信息安全管理体系—要求

[10] ISO 31000，风险管理—原则和指南

[11] ISO 导则 73 风险管理—术语

[12] ISO/IEC 导则 2 标准化与相关活动—通用术语

[13] BS 10500，反贿赂管理体系规范

[14] 《联合国反腐败公约》，纽 约，2004 年 。见 http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

[15] 经济合作与发展组织，《打击国际商业交易中贿赂外国公职人员公约》及相关文件。巴黎，2010 年

[16] 经济合作与发展组织，《内部控制、道德与合规良好做法指南》，巴黎，2010 年。

[17] 经济合作与发展组织，对《打击国际商业交易中贿赂外国公职人员公约》的评论，1997 年 11 月 21 日

[18] 联合国全球契约/透明国际，关于 10 次反腐败原则的报告指南，2009 年

[19] 国际商会、透明国际、联合国全球契约和世界经济论坛，抵制：抵制国际交易中的敲诈和索贿，公司员工培训工具，2010 年

[20] 国际商会，打击腐败规则，巴黎，2011 年

[21] 透明国际，反贿赂商业原则及相关工具。柏林，2013 年

[22] 透明国际，腐败感知指数

[23] 透明国际，行贿者指数

[24] 世界银行，全球治理指标

[25] 国际公司治理网络，ICGN 关于反腐败做法的声明和指南，伦敦，2009 年

[26] 世界经济论坛，《携手反腐，反贿赂原则》，世界经济论坛与透明国际和巴塞尔治理研究所合作的倡议，日内瓦

[27] COSO 内部控制——整合框架,2013 年 5 月