浅析贿赂风险识别、分析和评价的方法

雒宏伟（上海天祥质量技术服务有限公司）

在《中国认证认可》2017 年 11 期发表

摘要：贿赂风险的识别、分析和评价是反贿赂管理体系的建立和贿赂风险控制的基础和依据。本文分别阐述了贿赂风险识别、分析和评价的方法，并对影响贿赂事件发生的四个基本要素：预期的不当收益、外部威胁、内部的脆弱性和预期后果进行了分析，还结合一些高风险过程对贿赂风险进行举例说明；最后举例说明了风险分析和评价的方法。

关键词：ISO37001 贿赂风险

Simple Analysis of Approaches to Identification, Analysis and Evaluation of Bribery Risks

LUO HONGWEI Intertek China

Abstract: Identification, analysis and evaluation of bribery risks are the basis of developing ABMS and bribery risk controls. This article states the approaches to identification, analysis and evaluation of bribery risks, in which analyzes four elements effecting bribery occurrence including anticipated undue advantages, external threats, internal vulnerabilities and anticipated consequences, as well as examples bribery risks regards to high-risk processes. At the end the methods of risk analysis and evaluation are exampled.

Keywords: ISO37001 Bribery Risk

ISO37001:2016 反贿赂管理体系标准的基本原则之一是“基于风险”。预防贿赂的发生的前提是了解组织现在和预期将要存在的贿赂风险，才能针对存在的贿赂风险采取必要的措施进行控制从而防止贿赂的发生；另一方面组织不可能杜绝贿赂的发生，不可能因为反贿赂而不计成本的投入过多的资源或者采取过于复

杂的管理措施影响正常业务的开展,因此对贿赂风险的处置和资源投入必须要与与贿赂风险的风险级别相适应。高风险高投入,低风险可能只能维持现有的措施。已识别的贿赂风险到底哪些是高风险（不可接受的风险）、哪些是低风险（可接受风险），就需要对已识别的风险进行分析，排列优先顺序，确定风险等级，然后通过与组织建立的风险评价准则进行对比,确定组织需要处置的不可接受风险和中等风险。从以上分析我们可以看出贿赂风险的识别、分析和评价是反贿赂管理体系的建立和贿赂风险控制的基础和依据。下面我们将讨论贿赂风险识别、分析和评价的方法。

一、贿赂风险识别

ISO37001:2016 **给出的“风险”的定义是：**

“不确定性对目标的影响。”

注 1：影响指对预期的偏离——正面的或负面的。

注 2：不确定性是指对某一事件、其后果或可能性方面的信息缺失（即使是部分缺失）、理解或了解不足的状态。

注 3：风险通常用潜在“事件”（见 ISO 指南 73:2009，中 3.5.1.3 的定义）和“后果”（ISO 指南 73:2009，中 3.6.1.3 的定义）或二者的结合来表示风险。

注 4：风险通常以事件后果（包括情况的变化）与相关的事件发生的“可能性”（见 ISO 指南 73:2009，3.6.1.1 中的 3.6.1.1）的组合来表示。

这也是 2012 年以后新发布或换版的 ISO 管理体系标准给出的风险的定义。标准虽然没有给出明确的“贿赂风险”的定义，但是基于“风险”的定义，我们可以认为组织的目标包括质量、环境、职业健康安全、信息安全和资产等管理方面的目标，反贿赂管理目标是组织众多管理目标的一个方面，因此我们可以认为影响反贿赂管理目标实现的组织的风险为“贿赂风险”。

虽然对于不同的组织和组织不同时期可能有不同的反贿赂管理目标,但是对贿赂发生的“零容忍”是所有组织反贿赂管理的基本原则。通过对所有发生的贿赂事件进行分析，我们可以看到影响贿赂事件的发生的四个基本要素（如图 1 所示）：

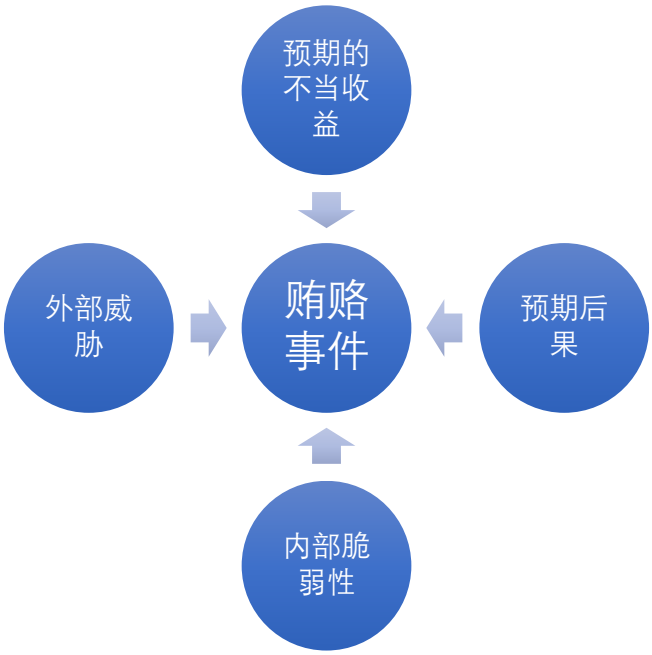
1、预期的不当收益。贿赂的目的是获得不当收益，因此预期的不当收益越多，贿赂的动力越大，发生贿赂的可能性也会越高，这也是为什么所有组织的采

购、人事、财务、福利、项目决策和审批过程是贿赂事件多发过程和重灾区。这些过程是大多数组织都普遍存在的过程,但并不是所有组织的所有这些过程都会有贿赂的发生，因为贿赂的发生还必须有威胁（行贿或索贿的人、组织、业务伙伴或者其代理)。

2、外部威胁（对组织、组织的员工、业务伙伴或者其代理行贿或索贿的人、组织、或其业务伙伴和代理)。不同国家、行业、地区、组织、部门、人员的对待贿赂的文化意识不同，主动行贿索贿的意愿和可能性不同，威胁程度不同，因此外部威胁同样影响了贿赂发生的可能性。高腐败感知指数越高的的国家和地区发生贿赂的可能性越大，同样与一些在贿赂方面有不良声誉的行业、组织、人员合作或交易发生贿赂的可能性较大。

3、内部脆弱性（组织存在的管理漏洞的大小)。脆弱性也是影响贿赂发生可能性的另一个重要因素。对于组织、组织的员工和代表组织的相关方受贿的情况，组织的脆弱性是指组织贿赂风险相关岗位的人员的反贿赂意识和组织反贿赂管理的漏洞；对于组织、组织的员工和代表组织的相关方行贿的情况，组织的脆弱性是指组织反贿赂管理的漏洞。大多数情况下，预期的不当收益是组织的性质、特点、权限、运营模式和业务发展情况等因素决定的，组织对其很难进行控制；对来自外部的贿赂威胁，组织只能施加影响而无法真正控制；而脆弱性完全由组织自身控制和决定的。组织反贿赂管理体系的建立和反贿赂管理制度的完善是降低脆弱性、防止和减少贿赂发生的重要手段，它直接影响贿赂发生的可能性。

4、预期后果。贿赂事件的后果包括：有形的后果（资产损失、业务中断、系统和功能有效性的破坏、经济损失等）和无形的后果（声誉损失、竞争优势丧失、不符合法规和监管要求、对人员安全和治安的威胁等)。



图一

通过以上对影响贿赂事件的四个基本要素的分析可以看出：因为预期不当收益的广泛存在，造成贿赂风险的广泛存在。贿赂风险识别和评价的是为了处置风险--控制和降低风险，而且风险处置只是针对的较高贿赂风险。贿赂风险的识别会占用组织大量的时间，因此从组织整体角度来看，贿赂风险的识别不是越全越好、越多越好，而是重点关注可能存在高贿赂风险的过程。正如前面所分析的，很多组织的采购过程、商务过程、人力资源管理过程、项目审批过程等都是存在较高预期不当收益的过程，组织应该先识别自身的存在高预期不当收益过程。组织还要考虑有些虽然预期不当收益不高，但是后果严重的过程，如影响到人身安全健康的产品和服务的技术标准的制定、修改以及关键社会服务设施的检查验收等相关过程，同时重点关注高腐败感知指数的国家和地区的相关业务过程。另外与第三方如公务人员、代理人、咨询师、分包商、家庭或亲属有关的贿赂风险也是贿赂风险识别的重要内容。如：

1、人力资源管理过程的贿赂风险：

- 选择和雇佣工作能力不足的应聘者；
- 因为与政府或公务人员的关系或被公务人员要求而被推荐或雇佣；
- 选择和雇佣与公务人员有紧密的家庭关系或业务、财务关系的人员；
- 故意重复支付给受到关照的员工；

- 付给受关照员工过多或过高的报酬等。

2、商务活动的贿赂风险：

- 向当地或国外公务人员行贿以确保获得政府合同；
- 向代理人、咨询师、中介、竞争对手员工行贿，以获得合同或订单；
- 向审计或监管部门的人员行贿以篡改数据和组织产品或服务的可靠性和质量状况等
- 高管和销售团队为了获得合同或订单，直接或通过其他人向供应商、顾客或其他组织的官员、员工或代表提供看起来可能影响与组织的关系的旅游、礼物、招待等

3、采购过程

- 接受供应商贿赂，选择一个没有足够能力的供应商；
- 接受外包方贿赂，持续接受外包方较差的工作和服务绩效；
- 在合同期间供应商有腐败行为或者没有遵守反腐规定却没有立即终止合同等。

另外，组织贿赂风险识别也是一个动态的过程，应随着组织战略目标、业务活动过程、组织架构、管理制度、业务伙伴、法律法规和相关方要求等因素的变化对贿赂风险的识别进行更新。

二、贿赂风险分析

从风险定义中“注 4”知道“贿赂风险是贿赂事件后果和贿赂事件发生可能性的组合”。影响贿赂事件发生的因素中，前三个因素：预期的不当收益、外部威胁和内部的脆弱性影响了贿赂发生的可能性，再考虑贿赂事件后果的大小，我们就可以确定贿赂风险的等级。另外考虑到贿赂风险识别、分析和评价的的目的处置风险、防止贿赂的发生，对于一些容易发现和预防的贿赂，组织可以及时采取措施防止贿赂的发生；相反对于隐蔽、不容易发现和预防的贿赂，组织更应该采取必要措施处置贿赂风险。因此贿赂风险分析方法可以在考虑：**后果的严重程度（S）**和**发生的可能性(O)**的基础上，增加**发现和预防贿赂发生的能力(D)**。风险值是通过风险优先级数来表示。

后果的严重程度 Severity （S） 1-10

发生的可能性 Occurrence（O）1-10

发现和预防的能力 Detection（D） 10-1

风险值 Risk Priority Number（RPN）= S x O x D

影响的严重程度可以定义为：

1- 无：无影响；

2- 非常小：非常小的影响；

3- 较小：普通客户会注意到的影响；

4- 非常低：弱点会被识别；

5- 低：降低的绩效水平；

6- 中：对体系的可操作性的中等影响；

7- 高：减少的主要职能；

8- 非常高：主要职能缺失；

9- 危险：警告情况下，故障会危及机器或操作者；

10- 危急：故障会无警告危及机器和操作者。

发生可能性可以定义为：

1- 微小：非常不可能发生，1:500,000；

2- 低：1:150,000；

3- 低：不可能发生，1:15,000；

4- 中：1:2000；

5- 中：中等机会发生，1:400；

6- 中：1:80；

7- 高：发生的可能性高，1:20；

8- 高：1:8；

9- 非常高：几乎一定发生，1:3；

10- 非常高：大于1:2。

发现和预防发生的能力可定义为：

1- 几乎必然：当前控制措施一定能发现或预防问题；

2- 非常高：当前控制措施发现或预防问题的可能性很高；

3- 高：当前控制措施发现或预防问题的可能性高；

4- 中度高：当前控制措施发现或预防问题的可能性中度高；

5- 中：当前控制措施发现或预防问题的可能性中等；

6- 低：当前控制措施发现或预防问题的可能性低；

7- 非常低：当前控制措施发现或预防问题的可能性非常低；

8- 微小：当前控制措施发现或预防问题的可能性微小；

9- 非常微小：当前控制措施发现或预防问题的可能性非常微小；

10- 无：不能发现或预防。

当然，虽然上述例子中**后果的严重程度（S）**和**发生的可能性(O)**和**发现和预防贿赂发生的能力(D)都采用了10级量表，但是我们也可以采用不同级数的量表来分析。**

三、贿赂风险评价

贿赂风险评价涉及将分析过程中确定的贿赂风险水平与组织建立的风险评价准则进行对比。根据比较，考虑风险处置的需求，并将重点放在确定的中、高风险上。例如风险评价准则如下：

RPN 1-149 低风险

RPN 150-250 中风险

RPN>250 高风险（危险）

最高管理者将贿赂风险可接受水平定为“**RPN 1-149** 低风险”。如果贿赂风险水平为“RPN190-250 中风险”，则考虑需要实施额外的预防、发现和应对措施。一旦风险水平增加到“RPN 大于 250 高风险”时，就应实施风险控制措施，然后再实施进一步的风险评价，确定减少的 RPN 并估计降低后的风险水平，以评价控制措施的有效性。除了上述定量的贿赂风险评价方法，组织可以基于反贿赂管理的经验、相关方和法律法规的要求，通过定性的方法确定一些高贿赂风险作为补充。贿赂风险的识别、分析、评价和处置过程的表格如下（作为参考）：

风险	影响区域	后果	后果的严重度 (S)	发生的可能性 (O)	当前控制措施	发现和预防的能力 (D)

续

初始风险优先级 RPNi=S*O*D	建议的措施	风险所有者	预定日期	采取的措施	New (S)	New (O)	New (D)	降低的 RPN RPNr= S*O*D

总之，贿赂风险的识别、分析和评价是建立反贿赂管理体系和处置贿赂风险预防贿赂发生的基础，虽然 ISO37001:2016 反贿赂管理体系标准并没有给出具体的方法，组织当然可以采用与本文不同的其他方法，但是组织需要有系统的贿赂风险识别、分析和评价的方法，同时与组织其他管理体系的风险评价方法保持一致。

参考文献

【1】 ISO，ISO37001:2016 Anti-bribery management systems—Requirements with guidance for use

作者简介

雒宏伟，工商管理博士。研究方向 :道路交通安全管理、资产管理、反贿赂管理 。INTERTEK 集团上海天祥质量技术服务有限公司 ISO37001、ISO39001 和 ISO55001 项目经理。