ICS XX.XXX.XX
A XX

团　　体　　标　　准

T/CCPITCSC XXX—2018

合规风险识别、评价与控制指引

The Guidance for Compliance Risk Identification, Assessment and Control

（征求意见稿）

2018－XX－XX 发布　　2018－XX－XX 实施

中国国际贸易促进委员会商业行业分会 发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国国际贸易促进委员会商业行业分会提出并归口。

本标准起草单位：

本标准主要起草人：

本标准为首次发布。

合规风险识别、评价与控制指引

1 范围

本标准规定了合规风险的识别、风险评价以及风险控制的指引，帮助组织做好合规管理工作。

本标准适用于各类组织，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成，无论该组织是否为法人，公有或私有。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

ISO19600:2014 Compliance Management System ——Guidelines（《ISO19600:2014 合规管理体系——指南》）

ISO37001:2016 Anti-Bribery Management System

GB/T 27921-2011 风险管理 风险评估技术

GB/T 27914-2011 企业法律风险管理指南

GB/T 35770-2017 合规管理体系 指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

合规风险 compliance risk

合规风险是不合规的作为或不作为导致的对于合规目标所造成的不确定性。本指引所指的合规风险包括：法律风险、违规风险、欺诈风险、操作风险和其他风险。

注 1：本标准所指的合规风险是“大合规”意义下的风险，是指组织违反其所面临的违反法律、法规等禁止性及义务性规定所给组织带来的风险，同时也包括组织及组织内外部合规义务人违反控制性合规义务所造成的所有的不合规风险，包括但不限于法律风险（指违反法律规定所造成的风险——如违反反腐败反贿赂法律、贸易禁运/国际经济制裁/出口管制、洗钱、不正当竞争、垄断/反托拉斯、倾销、信息违规使用的相关法律法规）、违规风险（比如违反国家重大政策、公司内部规定、道德规范等所造成的风险）、欺诈风险（比如组织内部员工受贿、利益冲突所造成的风险。组织并不会因为内部员工的欺诈行为而遭致处罚，但组织会因此遭受经济损失、名誉损失或其他损失）、操作风险（比如组织的工作人员因为操作不当而引发的风险，比如生产安全责任事故）、其他风险（比如组织的工作人员因为没有设置适当的流程或设置的流程不当导致组织没有能够及时识别并管控市场风险等）。

注 2：合规风险包括固有合规风险和剩余合规风险。固有合规风险是组织在没有对应的合规风险管理措施，处于无管控状态下面临的全部合规风险。剩余合规风险是在组织当前已有的合规风险管理措施管控下，仍然还存在没有被有效管控的部分合规风险。本指引没有特别指出时，合规风险均指固有合规风险。

3.2

风险源 risk resources

组织活动中可以引发合规风险的因素，包括但不限于组织运转过程中存在违法违规、制度缺陷、技术缺陷、监控缺失等一切可以引起与合规义务不一致的行为及其他因素，都是合规风险源。

3.3

风险及风险源代码 code for risk and risk resources

风险与风险源代码是检索合规风险与风险源的重要工具。组织的合规风险与风险源的清单较长时可以用代码进行检索。

注：当一个组织有很多分支单位比如分公司或子公司，特别是有海外公司用中文以外的语言进行交流的时候，集团公司和分公司以及子公司采取相同的代码来指代同样的风险和风险源，往往能够迅速地让大家在对话和交流时同频和提高效率。

3.4

风险识别 risk identification

风险识别指查找、辨别、列举和描述组织运转过程中可能发生的风险源或相应的风险事件或者潜在风险因素的过程。在识别合规风险源时应把与合规义务不一致的、导致不合规效果的因素描述出来，同时也可以对具有典型意义的合规风险源进行列举。

注1：对合规风险源的列举和描述指把引发风险的风险源给一一列举出来或者描述清楚。比如组织在做环境与健康安全（EHS）合规审核时，组织要检查所有危险品的堆放是否都有二次围堰以防止危险品一旦泄露因为没有围堰阻挡而直接流入或被雨水冲入下水从而造成水源污染，因此没有二次围堰、二次围堰有缺陷的或者没有采用方法防止水源可能遭致污染的危险品堆放都不合规。其中，“没有二次围堰或二次围堰有缺陷”是对合规风险源的列举；“没有采用方法防止水源可能遭致污染的危险品堆放”是对合规风险源的描述。

注2：合规风险是不合规的作为或不作为导致的不确定性对于合规目标的影响，而此种不确定性源于合规义务人没有遵守一个合规义务，从而发生不合规，甚至违规的现象。识别合规风险的目的是让合规义务人在合规风险发生之前，预先识别出风险源，并以此作为风险评价及风险控制的前提。

注3：风险的三要素是风险存在的环境、发生的诱因以及发生后造成的影响，即风险识别的通用语言是“在……的情形下，因……的原因，导致（或可能会导致）……的后果”。一般来说合规风险识别既需体现风险源的概念，也应当体现组织环境、风险影响等概念和方法。因为这些概念和方法在《GB/T 35770-2017 合规管理体系指南》以及相应的国际标准中都有所体现和描述，本指引就不再重复。

注4：风险识别的方法包括但不限于以下：

——基于案例证据的方法（检查表法以及对历史案例的辨析、评估）；

——系统性的团队方法（一个专家团队遵循系统化的过程，通过一套结构化的提示和问题来识别风险）；

——数据统计归纳推理方法（危险与可操作性分析方法，现金流分析法）；

——操作技术分析法（利用各种支持性的技术来提高风险识别的准确性和完整性，包括头脑风暴法、场景模拟等）；

——合规风险源间接识别法（通过识别合规风险源来找到合规风险的方法，包括但不限于利益冲突、制度缺陷、技术缺陷及监控缺失）；

——合规义务梳理识别法（通过识别梳理合规义务来逆向找到合规风险的方法）；

——权力识别分析法（利用权力清单在组织内部生产经营活动中的分布规律，基于岗位职责或者流程环节分析）。

注5：本标准所建议的风险识别的主要方法是通过风险实证识别和通过对重大合规义务归纳识别。本指引还建议使用对通过权力岗位进行风险识别的方法来识别风险。

3.5

风险实证 risk case studies

风险实证指通过案例辨析、场景模拟等方法对合规风险和风险源进行直观和客观的说明和验证，同时也是确定合规管理措施对合规风险是否有效的过程。

注：组织在做风险识别的时候，其赖以识别风险的最直观来源往往是组织内外部的案例学习，包括但不限于尽职调查、来自于组织内外部的举报、组织内部的审计发现、自我检查发现的问题等等。在实务中，经常出现的一个问题是组织对发生在组织内外部的案件置若罔闻，这种情况无论是故意还是疏忽都表明该组织对风险实证的工作没有做到位。

3.6

实质性合规义务 substantive compliance obligations

实质性合规义务指以禁止性及义务性规定为基础而产生的合规义务。在合规审核时应根据实质性义务做实质性测试。

注1：实质性合规义务所对应的是禁止性的规定（法律或者公司的规章制度禁止某个行为）或者是义务性的规定（某某必须或者应当履行某个义务）。违反了这些规定会给合规主体和义务人带来法律责任、经济或者名誉上的损害。

注2：实质性合规义务具有普适性——所有适合的合规义务人都必须遵守。

3.7

控制性合规义务 control compliance obligations

为了达到管理某个合规风险的目的而为相关合规义务人所预先设定或者应当设定但没有设定的行动方案。在做合规审核时，应根据控制性义务做控制性测试。

注1：内控制度是为了让合规义务人遵守实质性合规义务、避免合规风险的发生而制定的控制要求，从而也是控制性合规义务的来源。相应地，控制性合规义务本身是一种合规义务，其本身是和实质性合规义务相对应的一个概念，是为了防止风险的发生，从而建立一套风险防控的流程而形成的义务。比如一个组织为了防止行贿行为的发生，要求凡是跟政府官员之间往来的费用都必须经审批才可以发生，则审批这一行为本身是一种控制性合规义务。没有履行该控制性合规义务不会直接产生法律责任，但因为没有履行该控制性合规义务，则可能为合规义务人不履行其应当遵守的实质性合规义务大开方便之门。

注2：控制性合规义务不具有普遍性，各个组织在做好风险管控的前提下，可以根据自身的大小和特点选择性使用并达到有效地控制风险的目的。

3.8

合规义务人 compliance obligee

合规义务人指合规义务的具体责任人。合规义务人不仅包括组织本身，还包括组织内部的工作人员以及组织外部的第三方及其工作人员。

注1：组织是法律或其他规范下所拟制的虚拟对象，其合规性需要通过工作人员的行为来体现和实现。因此，本指引旨在通过规范组织内部工作人员的行为来达到组织合规的目的。

注2：这里所说的组织还包括与组织所进行的合规管理工作相关的第三方组织及其内部工作人员。比如组织不能行贿也不能通过第三方比如经销商行贿，那么组织就应当对第三方经销商及其工作人员设定合规义务。

3.9 **风险评价** risk assessment

对已经识别出的风险从风险源频率、风险发生的严重程度以及风险发生的可能性等维度进行评估以确认合规风险的风险敞口。

3.10 风险敞口 risk exposure

风险敞口指风险发生的后果的严重性，以及其后果发生的可能性的综合量值。风险敞口包括固有合规风险敞口和剩余合规风险敞口。

注：固有合规风险敞口即固有合规风险的量值；剩余合规风险敞口即剩余合规风险的量值。

3.11 风险控制 risk control

风险控制是内部控制的一种，是在一定的环境下，组织为了提高合规风险管理效率、充分有效地获得和使用各种资源，达到既定管理目标，而在组织内部实施的各种制约和调节的组织、计划、程序和方法。

注1：风险控制是合规“管理体系”的一部分。“管理体系 management system”是“组织（2.1）建立方针（2.8）和目标（2.9）以及实现这些目标（2.9）的过程（2.10）的相互关联或相互作用的一组要素。”（参见《GB/T 35770-2017 合规管理体系 指南》第2.7条。）。

注2：本指引所说的风险控制更多的是指风险控制手段的模块化建设——一个组织在解决一个复杂问题时自顶向下逐层把系统划分成若干模块的过程。每个模块各有多种属性，但都反映了组织内部有关合规风险管理的特性。

4 通过风险实证识别风险

4.1 风险实证是确证风险存在的过程。通过案例辨析、场景模拟等方法对合规风险和风险源进行直观和客观的说明和验证，同时也是确定重大合规风险管理措施对合规风险是否有效的评价基础。

4.2 风险实证的来源是过去已经发生了的事实，包括但不限于组织内外部案件、案例、调查结论、经过核实的举报内容或者不合规行为发生的场景模拟等等，在与组织生产经营活动、产品、服务及运营方面联系起来之后，分析出违规的起因，从而确认可能发生不合规行为的情形。这些具有实证意义的历史数据和模拟数据，其可以明确地告知和提示哪些风险源会引发合规风险、哪些合规义务人会容易产生违规行为，以及帮助发现其他风险源。

注：风险实证的来源包括但不限于以组织法务调处、内外部审计、内控评价以及舞弊调查等为渠道的风险识别，以面向业务部门合规访谈为导向的风险识别，通过建立面向全员的合规信息报告（举报、风险信息上报）为渠道的风险识别，以调查问卷为渠道的风险识别。通过案例辨析、组织总结、模拟、专业方法工具等，确定本组织对某合规义务所面临的合规风险，进行的全面梳理、辨别与查找。

5 通过对合规义务的归纳识别风险

识别和确定组织要遵守的合规义务是组织对合规风险的全面梳理，也是合规风险评价的基础。确定合规义务的重要成果之一是组织所面对的重大合规义务清单。

注：《合规管理体系指南》第3.6条指出：组织应通过将其合规义务与其行为、产品、服务和运营相关各方面进行比对，以识别出不合规行为可能发生的情况，从而识别出相应的合规风险。

5.1 重大合规义务

5.1.1 重大合规义务与组织所面临的重大风险高度相关，一旦违反这些义务就会引发重大合规风险或者让风险管控失去控制。

5.1.2 相对于某一个方面的合规风险源，组织外部及内部会有很多的法律及规定，相应地也有很多的控制性合规义务，包括组织承诺的和强制的合规义务。如果要把所有的合规义务都确定下来，是不现实的、也是没有必要的。其次，确定合规义务如果不按轻重缓急予以区分，则会在总体上降低合规义务人对合规风险、尤其是重大合规风险的敏感度。因此，一个组织在确定与合规风险相关联的合规义务时应将重大的合规义务优先确定下来。

5.2 确定重大实质性合规义务

实质性合规义务来源于法律法规及公司的规章制度，但又不同于法律法规及公司的规章制度。相较于后者而言，实质性合规义务更加接近行动指令和要求。相比较具有普适性的法律法规而言，实质性合规义务与企业的实际情况更加紧密关联从而各具特点。

注1：以《反垄断法》当中的“转售价格维持”（Resale Price Maintenance）为例，《反垄断法》第14条明确规定：禁止经营者与交易相对人达成下列垄断协议：（一）固定向第三人转售商品的价格；（二）限定向第三人转售商品的最低价格；（三）国务院反垄断执法机构认定的其他垄断协议。但是，《反垄断法》对于“转售价格维持”的禁止性规定从合规管理实务的角度来说要达到防控“转售价格维持”的风险的目的还缺乏可操作性，组织还需要根据自己的实际情况将其翻译成可以实际遵守的合规义务。以下是某快销品行业的企业就“转售价格维持”合规所梳理的重大实质性合规义务。

注2：为了避免涉嫌转售价格维持：

——不得在与经销商、零售商的任何形式的协议中规定经销商、零售商应按照某一价格销售或不得低于某一价格销售；

——不得要求（不论是书面、口头还是暗示）经销商、零售商按照某一价格销售或不得低于某一价格销售；

——不得对经销商、零售商的价格调整进行干涉，不得因其价格原因而停止供货、解除合同、取消返利、折扣、费用或采取其他惩罚措施；

——不得在任何内部文件或对外文件、邮件往来中涉及对经销商销售价格或零售商零售价格的控制，不得使用“破价”、“红线价”等涉嫌价格管控的词语；

——不得在发现经销商、零售商销售价格低于预期时，向其发出书面函件、电子邮件或进行口头警告，不得在与经销商、零售商人员的对话中涉及价格控制内容；

——不得与经销商或零售商商定转售价格、促销价格或要求经销商或零售商在进行价格调整前取得我们组织同意；

——除非获得经销商书面授权且明确声明经销商对价格有最终决定权，不得代经销商与零售商商定供货价格；

——不得因为经销商、零售商“破价”或“低于建议价格”销售而对他们予以处罚；

——不得强制经销商、零售商执行建议转售价格或建议零售价格或对它们施加压力，使得它们不得不这么做（比如，反复地将将建议价格发给经销商、零售商，以至于看起来是在威胁它们）。不得将建议转售价格或建议零售价格变为固定价格或最低价格；

——不得以设置转售价格浮动空间、利润率的形式固定经销商、零售商的销售价格或设置价格下限。

5.3 确定控制性合规义务

5.3.1 确定控制性合规义务的来源包含但不限于组织为了管理某个合规风险已经制定有的以及应当制定但却没有制定的内控流程所生成的义务。

5.3.2 控制性合规义务不求是否全面或者重大，而在于是否有效地管控风险。

注1：我们同样还以5.2中所提及的转售价格维持为例，组织为了避免涉嫌转售价格维持，规定了十项实质性的合规义务。为了让这十项合规义务落实到位，组织规定了如下内控流程：

——组织法务必须对公司的销售人员进行《反垄断法》培训，并对这十项合规义务逐条予以解释和说明；

——销售部门每一个季度都要在销售工作会议上和每一个销售人员一起复习这十项合规义务；

——组织法务在审查经销合同时必须严格对照上述十项合规义务来审查合同。

注2：虽然组织规定了上述三项规定，但组织的转售价格维持现象还是屡禁不止，组织的合规人员通过在同行业对标发现其他组织针对转售价格维持现象还规定了处罚措施：组织对于屡教不改的合规义务人将会采取扣发奖金等处罚措施——这些处罚措施虽然在组织内部还没有制定与实施，但这些措施以及与其相关的合规义务应当写入重大的控制性合规义务清单，成为相关合规义务人应当履行的合规义务。

5.4 合规义务的维护

5.4.1 合规义务的维护即合规义务的更新。

5.4.2 组织应当及时跟进、学习并了解对其所适用的法律法规并把这些法律法规中对组织所适用的实质性合规义务解析出来。

5.4.3 组织还应当与同行业的其他组织不断地进行交流以做好对标等工作，从而不断地把合规管理当中的最佳实践给吸纳进组织，为组织有效地管控合规风险打好基础。

5.4.4 组织尤其应当关注其为控制某个合规风险所制定的控制性合规义务是否能够有效地控制该风险、在实务当中是否能够得到有效的执行。如果有关的控制性合规义务不能有效地控制风险或者不能得到有效的执行，那么组织应当考虑采取其他什么样的管控措施、是否应当设计、增加或者调换一个或多个内控模块从而更加有效地控制合规风险。

5.4.5 与合规义务的更新相关的活动包括但不限于以下内容：

——组织宜有适当的过程识别新的和变更的法律、法规、准则和其他合规义务，以确保持续合规。

——组织宜有过程评价已识别的变更和任何变更的实施对合规义务管理的影响。

5.4.6 获取关于法律和其他合规义务变更信息的过程包含但不限于以下内容：

——列入相关监管部门收件人名单；

——成为专业团体的会员；

——订阅相关信息服务；

——参加行业论坛和研讨会；

——监视监管部门网站；

——与监管部门会晤；

——与法律顾问洽商；

——监视合规义务来源（如：监管声明和法院判决）。

5.5 合规建设性的指导

5.5.1 合规义务是合规义务人的底线，合规义务人一旦违反了合规义务就会引发合规风险。所以实质性合规义务的表述往往是禁止性或者义务性的表述，比如义务人不得做什么样的行为或者应当做什么样的行为。

5.5.2 在实务中，为了更好地帮助合规义务人履行合规义务，组织除了设定禁止性的规定之外，还可以提供一些建设性的指导，以帮助义务人员进一步做好合规工作。

注：我们还以“转售价格维持”为例，组织除了设定5.2.中的禁止性规定之外，还可以提供建设性的指导：

——尊重经销商、零售商的经营自由和独立地位，不干涉、不限制其销售价格或零售价格（法律虽未禁止设置最高价格，但应非常小心，应提前取得法务批准）；

——只能建议经销商的转售价格或零售商的零售价格，且明确建议价格仅供参考，经销商、零售商有决定其价格的自由；

——可以设定最高转售价格，但前提条件是该最高转售价格的设定不是实际上在设定最低转售价格或对转售价格进行限制。

6 具体合规义务人

6.1 识别具体合规义务人的目的

合规义务落实到具体的执行责任人符合合规风险管理的精准化要求，可避免合规管理职责不清、权责不分、互相扯皮的现象，可以让组织把有限的合规资源用到最需要合规风险管理的岗位或部门。

6.2 具体合规义务人识别方法

6.2.1 确定实质性义务下的合规义务人

组织应当确定实质性合规义务的具体执行岗位或部门。

注：某组织受美国《反海外腐败法》管辖，其在中国的控股子公司既有B2C业务，也有B2B业务。同样是该子公司的销售部门，负责B2B的销售主管和人员相比较B2C的销售主管和人员而言最有可能违反行贿风险下的合规义务，那么负责B2B的销售主管和人员就应当被列为行贿风险下的合规义务人，而负责B2C的销售主管和人员就不应当被列为《反海外腐败法》下贿赂风险下的合规义务人。但是，如果B2C的销售主管和人员因为其他原因与政府官员打交道比较多，比如某负责B2C的主管负责与政府部门打交道拿公司的直销牌照，那么与政府机关打交道的负责B2C的主管也当被列为《反海外腐败法》下贿赂风险下的合规义务人。

6.2.2 确定控制性义务下的合规义务人

组织应当确定具体负责履行某个控制性合规义务的岗位或部门。

示例：同样以上述的6.2.1的例子为例，该公司规定凡是与政府官员发生的费用都必须由公司的合规官事先进行审批。就这个控制性合规义务而言，该公司的合规官就是合规义务人。

6.3 合规义务人排序

在确定合规义务人时，可以把合规义务人按照其合规义务的大小或者是潜在的合规责任的大小做一个排序。排序可以采用损失减少原则即指一个有效率的合规体系在众多义务人中分摊责任时，应当让能够以最低代价来减少甚至避免损失的一方作为首要的合规义务人并承担主要责任。

注：比如在贿赂风险管理的过程中，贿赂风险的合规义务人可能包括：销售部门的主管和业务人员（其在销售的过程中不能私下通过财物等手段获得或者保有业务）、合规总监（其负责审查所有的发生在政府官员身上所发生的费用）、财务总监（其负责审批费用的报销）。这三类人当中能够用最小的代价来减少贿赂风险带来的损失的一方应当是销售部门的人员，其对贿赂风险的防控简单到不去做就可以了，而其他两方合规义务人对贿赂风险的防控需要公司花费人力、物力及财力进行审查。因此，销售部门的主管和业务人员应当列为首要合规义务人，并承担主要责任。

7 基于岗位权力的合规风险识别法

7.1 岗位职责清单

基于岗位的合规风险识别，即围绕岗位上履行的职责内容来识别分布在岗位职责中的合规风险。它们将直接或者间接地影响某个管理目标的实现或者合规目标的实现。岗位上明确了哪些职责，合规风险也隐藏其中。因此，要识别出岗位职责里存在的合规风险，需要将岗位职责内容逐一列出，并将每一岗位职责对应的业务目标和合规目标列出，具体见附录 A《岗位职责清单表》。

7.2 识别岗位职责对应的权力

7.2.1 岗位上不同的岗位职责，组织可能赋予了对应的不同业务执行权力。权力是引致合规风险发生的重要因素。

7.2.2 识别岗位职责对应的权力，需要用到一个工具模型，即企业“八项权力模型”。

7.2.3 引致合规风险的主要风险源是权力的不正当使用。组织内部的不合规、违规，进而发展为贪污腐败、犯罪等问题，96%出现在拥有以下“八项权力”中一项或者一项以上的业务领域和岗位。在组织生产经营岗位上的人，存在一个不合规、违规铁三角定律：权力+不良动机+业务机会=合规风险发生，权力+不良动机+业务机会是发生合规风险的充分条件（不是必要条件），导致了组织人员在岗位履职过程中的大多数违规行为。存在于组织的“八项权力”包括以下具体内容。

——审核权：包括直接行使和直接影响改变审核权两个方面，如决策权、审批权、审核权等具有行政审核性质的核准工作（授权各级领导的签字权），或者本人作为其更高直线分管领导，能够直接影响和改变权力的行使，如本人是组织上级集团的部门、组织领导。

——市场客服与销售权：包括直接行使和直接影响改变市场客服与销售权两个方面，如向客户介绍产品、服务功能、销售政策、价格优惠条件、销售合同签订、售后服务、维修、保养、新旧置换等客服、销售性质的相关业务活动以及围绕客户在采购、决策、放行、计量、财务资金和与这些活动密切相关的客户内部关键商务信息所实施的公关、影响活动，或者作为其直线分管范围,能够直接影响和改变这些权力的行使方向，如市场客服与销售分管领导、组织上级集团的部门、组织领导。

——人事权：包括直接行使和直接影响改变人事权两个方面，如雇佣、招聘、任免、考核、人员奖励与处罚、职称评定、岗位选拔等人事活动，或本人作为其直线分管范围,能够直接影响和改变权力的行使，如人事分管领导。

——采购权：包括直接行使和直接影响改变采购权两个方面，如确定供应商、分包商、租赁商合格名册、确定采购方式、采购策划、确定采购文件、确定投标人、确定价格和中标人、分包商、租赁商选择、签合同、合同变更等与采购有关的业务活动，或本人作为其直线分管范围,能够直接影响和改变权力的行使，如采购分管领导。

——放行权：包括直接行使和直接影响改变物料设备进出放行权两个方面，如质量检测、安全管理、仓储管理、品控管理、物料设备使用管理、技术审核、专业评审、专业认证、监督权、进出门管理等进出、放行、许可、专业技术复核性质的业务，或本人作为其直线分管范围,能够直接影响和改变权力的行使，如质量、技术、安全分管领导。

——计量权：包括直接行使和直接影响改变工作量、物资计量权两个方面，如货物计数、采购结算、开具验收单、物料领用、消耗计量、工作量计量、分包量计量、容积测量、计时计件等计数计量相关业务，或本人作为其直线分管范围,能够直接影响和改变权力的行使，如物资、设备分管领导。

——财务资金权：包括直接行使和直接影响改变财务资金权两个方面，如收款、付款、费用开支、费用报销、后勤账务管理、津贴福利管理等经手钱财业务，或本人作为其直线分管范围,能够直接影响和改变权力的行使，如财务、资金分管领导。

——拥有关键信息权：拥有、知晓、掌握、创造关键商业信息，或在行使前面七个方面的权力时候

掌握的需要保密的信息，如公司内部商业秘密、工作策略、工作战略、重要人事安排、重要工作部署、采购分包其他投标人、标底、预算等信息。

以上八个方面的权力是企业在生产经营过程中赋予各岗位的权力,在这些权力行使的过程中,最容易导致不合规、违规、腐败风险发生，识别了以上八个方面的权力在企业各岗位的分布情况，就能够找到合规风险存在的地方。

然后根据每项岗位职责和基于合规风险分布特征的“八项权力识别模型”，识别每项职责内容中的权力，根据权力内容，确定对应的合规风险点。具体见附录 B 《基于岗位的合规风险识别矩阵图》。

7.3 基于流程权力合规风险识别法

7.3.1 对组织行为过程进行流程化描述

基于流程的合规风险识别，即围绕流程来识别流程中某些步骤可能存在的合规风险。这些风险将直接或者间接地影响流程目标的实现，或者合规目标的实现。要识别出流程里存在的合规风险，首先需要将流程制度按照流程图的形式进行描述。

流程是组织为实现决策/业务的某一特定目的所采取的一系列有控制的步骤、活动与方法的集合。从该定义可知，流程是明确了 1 个特定目的和步骤、组织、活动、控制记录、工作标准、工作方法等 6 个方面共同构成的 1+6 个基本要素。其中，特定目的即流程特定“管理目标”，步骤即流程里的“工作步骤”，组织即流程里每个工作步骤的“责任主体”（责任部门和责任岗位），活动即流程里每个工作步骤的“工作任务”，控制记录即流程里每个工作步骤应该形成的规范格式的“工作记录”，工作标准即流程里每个工作步骤的工作任务的“工作标准”，工作方法即流程里每个工作步骤的工作任务的“工作方法”。这些基本要素构成了现代组织流程的 1+6 标准结构，具体见附录 C。将组织的流程制度按照附录 C 表格进行分解描述，将组织“看不见”的文本流程制度展开为可以“看见”的“流程图”，再根据“流程图”识别流程运行环节对应的权力。

7.3.2 识别流程运行环节对应的权力

识别流程运行环节对应的权力，应通过此“流程图”和基于合规风险分布特征的“八项权力模型”（参见 7.2“识别岗位职责对应的权力”),，从而识别流程运行各环节的具体权力内容，再根据权力内容，确定对应的合规风险点。具体内容详见附录 D《基于流程的合规风险识别矩阵图》。

8 风险评价

风险评价既是对风险敞口定量的过程，也是就风险管理分配资源的依据。风险敞口越大给合规主体所带来的风险越大。合规风险评价需要识别所有会给组织造成较大损失和损害的风险并从风险源频率、风险造成损害的严重程度以及风险发生的可能性等维度对风险敞口的大小进行定量分析。

8.1 评价风险维度

评价风险维度指衡量风险敞口的维度，其通常包括风险源频率、风险严重程度、风险发生可能性。

8.2 对风险源频率的衡量

风险源隐含在组织业务活动中,组织隐含风险源的业务活动频率越高,合规风险发生的机会就越高,从而风险源频率就越高。

8.2.1 衡量系数

风险源频率大小取值范围可以按照按照 1-6 系数的标准来衡量：1 或 2 代表风险源频率低；3 或 4

代表风险源频率中等；5 或 6 代表风险源频率最高。

8.2.2 衡量标准

以组织业务活动频率为衡量标准
——每年发生一次和两次业务活动的和每季度发生一次、两次业务活动的，为低频率；
——每月发生一次、两次业务活动的，为中频率；
——每月发生三次及以上的业务活动，为高频率。

8.3 对风险严重程度的衡量

衡量风险敞口的一个重要维度是风险发生的后果严重程度。

8.3.1 衡量系数

风险严重程度取值范围可以按照 1-6 系数来衡量：1 或 2 分代表后果严重程度小（比如，不会触发刑事责任、经济损失低于预先设定的阀值、给组织造成的名誉损失也低）；3 或 4 代表后果严重程度中等；5 或 6 代表后果严重程度最大（比如会触发刑事责任、经济损失高于预先设定的阀值、给组织造成的名誉损失也大）。

8.3.2 衡量标准

衡量标准因风险的不同而不同、因组织的具体性质和大小而异。
常见的衡量标准包括但不限于以下内容：
——是否会触发刑事责任；
——经济损失大中小的阀值分别是什么；
——给组织造成名誉损失的可能性大小。

8.4 对风险发生可能性的衡量

衡量风险敞口的另一个重要维度是风险发生的可能性。

8.4.1 衡量系数

风险发生的可能性大小可以按照 1-6 系数的标准来衡量：1 或 2 代表可能性小（比如政府执法严厉程度不高；同行业发生类似案件的情况也不多；被检查单位制定有完善的内控制度并严格实施该内控制度）；3 或 4 代表可能性中等；5 或 6 代表可能性最大（比如政府执法非常严厉；同行业发生类似案件的情况很多；组织内部已经有举报；被检查单位没有制定内控制度，或虽然制定有内控制度，但没有严格实施）。

8.4.2 衡量标准

衡量标准因风险的不同而不同、因组织的具体性质和大小而异。
常见的衡量标准包括但不限于以下内容：
——政府执法严厉程度怎样；
——同行业发生类似案件的频率；
——被检查单位是否制定有完善的内控制度并严格实施该内控制度。

8.5 对风险敞口的衡量

风险敞口的衡量是把风险源频率乘以衡量风险严重程度的系数，再乘以衡量风险可能性的系数所得

到的结果。风险敞口=风险源频率 X 风险严重程度系数 X 风险可能性系数，按照 1-216 的标准取值范围来衡量：1-8 代表风险小；9-64 代表风险中等；65-216 代表风险高。

示例：

合规风险识别				风险实证	实质性合规义务（重大）	控制性合规义务（重大）	具体合规义务人			风险评价			
风险代码	风险名称	风险源代码	风险源	案例案件、场景模拟／来源	合规义务／来源	合规义务／来源	合规义务人	合规义务人	合规义务人	风险源频率	后果严重程度	发生可能性	风险敞口
01	行贿风险	a	贿赂医院医生	XYZ 公司被判对非国家工作人员行贿罪	合规义务／法律及规定（略）	合规义务／法律及规定（略）	销售总监及部门	市场推广部门	合规部门	3	6	4	72

9 合规风险控制

内部控制是在一定的环境下，组织为了提高经营效率、充分有效地获得和使用各种资源，达到既定管理目标，而在组织内部实施的各种制约和调节的组织、计划、程序和方法。风险控制的策略包括风险规避、风险转移、风险管控、风险接受等。

9.1 内部控制构成

9.1.1 合规内控需要组织从合规风险管控的角度提出控制要求并制定出内控标准，通过针对流程中的内部控制措施进行有效设计并执行来落实。合规内部控制标准不是用来取代组织现有的制度、流程，而是作为合规管理参照工具，审视组织现有内控标准是否满足合规内部控制要求，以及内控制度在管控合规风险时是否执行到位。

9.1.2 合规内部控制的主体内容由总体控制和具体控制两部分构成。

——总体控制目标反映合规方面的共性要求，旨在就制度程序、决策授权、岗位职责分离等方面作出总体要求，保障内部控制有效的同时实现整体合规目标。总体控制更加宏观抽象，是组织战略目标的一部分。

——具体控制针对涉及的具体业务面临的具体合规风险，应满足细节性合规控制要求，每项内部控制标准均需要与相关的合规风险建立勾稽关系。具体业务综合概括起来主要涉及组织架构、发展战略、人力资源、社会责任、组织文化、资金活动、采购业务、资产管理、销售业务、研究与开发、工程项目、担保业务、业务外包、财务报告、全面预算、合同管理、内部信息传递、信息系统等十八个方面。

9.2 内部控制措施

9.2.1 无论是内部控制的总体控制还是具体业务控制，内部控制标准实施主要依靠各项内控措施来保障，一般常见的合规内部控制措施包括但不限于以下几种：不相容职责分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制和绩效考评控制等。

——不相容职责分离控制：组织应全面系统地分析、梳理业务流程中所涉及的不相容职务，实施分离措施，形成各司其职、各负其责、相互制约的工作机制。如资金支付的审批与执行，工程项目的招标与验收付款等岗位职责相互分离。

——授权审批控制：组织应根据常规授权和特别授权的规定，明确各岗位办理业务和事项的权限范围、审批程序和相应责任。组织应当编制授权表，明确各项常规授权和特别授权，在涉及重大业务和事项时，采取集体决策审批或联签制度，任何个人不得单独进行决策或者擅自改变集体决策。如涉及企业股份制改革、战略投资扩张等重大事项时必须召开股东大会对议案投票。

——会计系统控制：组织应严格执行国家统一的会计准则制度，加强会计基础工作，明确会计凭证、会计账簿和财务会计报告的处理程序，保证会计资料真实完整。组织财务部门应依法合理设置会计人员架构，配置专业会计技术人员负责会计相关工作。

——财产保护制度：组织应建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全。

——预算控制：组织实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束。

——运营分析控制：组织应建立运营情况分析制度，科学设置考核指标体系，对组织内部各责任单位和全体员工的业绩进行定期考核和客观评价，将考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据。

9.2.2 合规风险管理中应当根据业务情况，结合不同风险的应对策略，综合运用上述控制措施，对各项业务和事项实施有效控制。在面对重大风险时，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。

9.3 内部控制措施执行评价测试

9.3.1 组织首先应在围绕自身合规方面涉及的内部控制要素确定合规内部控制具体内容，进而确定后续内部控制评价具体内容，对内部控制措施和所涉及业务流程和运行情况进行全面评价。

9.3.2 在针对内部控制中内部环境评价时，组织应当以自身组织架构、发展战略、人力资源、企业文化、社会责任等方面为依据，对内部环境的设计及实际运行情况是否符合当前合规管理的需要进行认定和评价。

9.3.3 在结合本组织的内部控制制度方面，对上述的经营管理的合规方面的风险识别、风险评价、风险分析、风险应对策略等流程和措施进行认定和评价，判别合规风险管理程序足够科学有效。

9.3.4 组织应当组织开展控制活动评价，对内部控制活动的控制措施的设计和运行情况进行认定和评价，判断是否存在运行缺陷和控制不足等状况。

9.3.5 在信息与沟通评价方面，应当结合本组织的内部控制制度，对信息收集、处理和传递的及时性、内控机制的健全性、财务报告的真实性、信息系统的安全性，以及利用信息系统实施内部控制的有效性等进行认定和评价。

9.3.6 组织结合自身内部控制制度，对内部控制监督机制的有效性进行认定和评价，重点关注监事会、审计委员会、内部审计机构等是否在内部控制设计和运行中有效发挥监督作用。

9.3.7 合规内部控制实施的评价工作最终应形成工作底稿，详细记录组织合规内部控制的执行和评价工作内容，包括评价要素、主要风险点、采取的控制措施、有关证据资料以及认定结果等。

9.4 合规内控缺陷的认定及整改

9.4.1 按照组织内部控制本质不同，可以把合规内部控制缺陷分为设计缺陷和运行缺陷。

——设计缺陷指组织缺少在合规风险管理过程中为实现合规目标的必须控制，或者现存的内控并不合理及未能满足控制目标。例如，未建立出纳和会计的岗位分离制度。

——运行缺陷是指设计合理及有效的内部控制，但在实际运作过程中没有被正确地执行。例如，组织采购人员未严格按照采购询价制度中供应商名单制度进行采购询价。

9.4.2 按照两者对组织的合规管理影响程度可以分为重大缺陷、重要缺陷和一般缺陷。

——重大缺陷是指一个或者多个控制缺陷组合，可能严重影响内部整体控制的有效性，进而导致组织无法及时防范或发现严重偏离整体控制目标的情形。

——重要缺陷是指一个或多个一般缺陷的组合，其严重程度低于重大缺陷，但导致组织无法及时防范或发现严重偏离整体控制目标的严重程度依然重大，需引起管理层关注。一般缺陷是指除重要缺陷、重大缺陷外的其他缺陷。

9.4.3 针对不同控制缺陷的整改应制定不同的整改方法，对需要整改的内控设计缺陷，组织需要在已有的内控管理制度中补充相关规定或修改原有规定，按照组织既定的管理制度报批程序对做出的补充或者修改进行审批。

附 录 A
（规范性附录）

岗位职责清单表

岗位名称		
职责项数	岗位职责内容清单	对应业务目标和合规目标
1		
2		
3		
4		

附 录 B
（规范性附录）

基于岗位的合规风险识别矩阵图

表4 基于流程的合规风险识别矩阵图

步骤编号				1	2	3	4	5	6	7	8	9	10	11	12	13	14	16
管理目标	管理目标	业务需求发起部门、岗位	1	业务启动														流程主控部门
		业务主要承办部门、岗位	2		业务计划	业务总方案		业务子方案		实施步骤一	实施步骤二	实施步骤三	关键实施步骤		完成步骤		业务交底	
		业务主要参与、配合承办部门、岗位	3				评审		评审					评审		会签		
		业务专家委员会评估、认证	4															
	目标计算公式	公司内部专职监督部门、岗位	5															签发人
		上级专业管理部门、岗位/专业分管领导	6				审批		审批					审批		审批		
		工作任务	1															
		工作记录	2															
		工作标准	3															
		工作方法	4															
权责清单	八项权力识别	市场客服与销售权	1															
		审核权	2															
		人事权	3															
		采购权	4															
		放行权	5															
		计量权	6															
		财务资金权	7															
		拥有关键信息	8															
权力对应的合规义务	合规义务梳理	国家法律法规社区规定	1															
		伦理道德规范要求	2															
		企业承诺	3															
合规风险识别（ISO19600 4.6）	不合伦理道德规范风险	商业贿赂风险	1															
		操纵市场价格风险	2															
		不道德欺诈风险	3															
		不廉洁、腐败风险	4															
		舞弊风险	5															
		对产品不负责任风险	6															
		违背企业核心价值观风险	7															
		血汗工厂蔑视人权风险	8															
	不合企业自行承诺风险	与相关方信息沟通风险	9															
		相关方要求识别响应风险	10															
		产品技术风险	11															
		产品质量风险	12															
		售后服务风险	13															
		产品功能持久性风险	14															
		产品节能风险	15															
		产品绿色风险	16															
		产品智能化风险	17															
		产品人性化设计风险	18															
		产品技术专利风险	19															
		产品知识产权风险	20															
		商业秘密风险	21															
		资产保值增值风险	22															
	不合国家法律法规社区规定要求风险	违反法律法规风险	23															
		生产安全风险	24															
		职业健康安全风险	25															
		环境风险	26															
		社会责任风险	27															
		风俗信仰文化冲突风险	28															
		社区冲突风险	29															
		社会治安风险	30															
		政治风险	31															
		其他风险	32															

附 录 C
（规范性附录）

组织行为过程流程图

流程管理目标					目标计算公式		
步骤	责任主体			工作任务	工作记录	工作标准	工作方法
	某业务部业务主办	某业务部主管	某业务分管领导				
1							
2							
3							
4							

附 录 D
（规范性附录）

基于流程的合规风险识别矩阵图

表2 基于岗位的合规风险识别矩阵图

编号				1	2	3	4	5	6	7	8	9	10	11	12	13	14	16
岗位名称	岗位职责清单																	岗位所在部门
																		部门负责
	对应业务目标和合规目标																	
权责清单	八项权力识别	市场客服与销售权	1															
		审核权	2															
		人事权	3															
		采购权	4															
		放行权	5															
		计量权	6															
		财务资金权	7															
		拥有关键信息	8															
权力对应的合规义务	合规义务梳理	国家法律法规社区规定	1															
		伦理道德规范要求	2															
		企业承诺	3															
合规风险定义（ISO19600 4.6 ）	不合伦理道德规范要求风险	商业贿赂风险	1															
		操纵市场价格风险	2															
		不道德欺诈风险	3															
		不廉洁、腐败风险	4															
		对产品不负责任风险	5															
		舞弊风险	6															
		违背企业核心价值观风险	7															
		血汗工厂蔑视人权风险	8															
	不合企业自行承诺风险	与相关方信息沟通风险	9															
		相关方要求识别响应风险	10															
		产品技术风险	11															
		产品质量风险	12															
		售后服务风险	13															
		产品功能持久性风险	14															
		产品节能风险	15															
		产品绿色风险	16															
		产品智能化风险	17															
		产品人性化设计风险	18															
		产品技术专利风险	19															
		产品知识产权风险	20															
		商业秘密风险	21															
		资产保值增值风险	22															
	不合国家法律法规社区规定风险	违反法律法规风险	23															
		生产安全风险	24															
		职业健康安全风险	25															
		环境风险	26															
		社会责任风险	27															
		风俗信仰文化冲突风险	28															
		社区冲突风险	29															
		社会治安风险	30															
		政治风险	31															
		其他风险	32															