KPMG

毕马威内部审计

2017年十大关注点

kpmg.com

关注重点，发挥内审影响力

在这瞬息万变的世界中竞争生存，企业必须努力应对几乎每天都会出现的新挑战，例如网络威胁、新兴及潜在的颠覆性技术、业务绩效风险等。在这个日趋复杂的环境里，内部审计（“IA”）扮演着重要的角色，能协助企业管理复杂多变的业务趋势所涉及的各类风险。

为发挥重要影响力，内部审计部门需要持续关注这些不断涌现的各种业务问题，以有效地监控各项相关风险和它们对公司的潜在影响。为了给企业创造最大价值，内部审计部门必须善于择机识别公司现状中潜在的问题以降低风险、加强内控、寻找可提高效率的潜在空间，并同时兼顾成本效益。

为了帮助内部审计部门实现上述目标，毕马威对各个行业的公司内部审计部门开展了调研工作，并于《毕马威内部审计：2017年十大关注点》中总结了调研结果。本报告概述了内部审计需要重点关注的领域，从而有效地协助企业增值创益，并在公司内部最大程度地提升内审的影响力。

2017年十大关注点

1. 综合管控
2. 网络安全
3. 新兴技术
4. 战略协同
5. 合规遵循
6. 第三方关系
7. 数据分析和持续审计
8. 反贿赂/反腐败
9. 绩效风险
10. 文化风险

《毕马威内部审计：2017年十大关注点》列出了2017年内部审计的十大关注点，希望协助公司的内部审计部门将宝贵的资源更加合理地分配到对公司影响最大的重要领域以建立广泛的竞争优势，包括改善内部控制环境、加强风险管理流程，以增强审计委员会的信心。

01 综合管控

驱动因素：

— 风险形势瞬息万变，更加上企业需要独到的专业见解以做出有效决策

— 与管控服务提供者携手合作，以得出有关风险的一致观点

— 在企业内部全面简化风险评估和管控活动，以提高效率，尽量增加风险管理的覆盖范围

— 将有限资源分配到公司风险最高的领域

随着风险形势不断变化，董事会和高级管理层希望所有管控部门能一起携手合作，就机构的风险情况提供综合的视角。许多公司未能开发系统化的流程来预测新的和将会出现的风险，导致不能尽早识别关键风险以做出有效管理。此外，传统的风险管理控制模式通常独立进行，彼此之间缺乏良好协调。如果企业能够有效预测和应付风险形势的变化，在不同的管控职能之间制定良好协调的应对措施，尽量增加企业风险管理的覆盖范围，便能够为高级管理层和董事会提供独到的见解和视角，以做出更加有效的业务决策和风险管理。

内部审计可以提供以下协助：

— 领导或支持不同风险管控部门之间在风险评估、规划、工作执行和汇报方面的协调工作，从而减少对业务部门的干扰

— 协调企业内部的公司治理、合规和审计等职能，根据企业面对的风险制定和执行全面的管控计划

— 评估新兴的业务趋势及其风险，判断其对企业发展经营的影响

— 鼓励增加利用数据和分析，就最新风险形势提供最佳的见解

02 网络安全

驱动因素：

— 预防因数据泄露而导致的高昂代价和严重后果，例如：司法调查、法律罚款、补偿客户损失、后续整改工作、中高级管理层消耗的时间精力、潜在的业务及客户流失等

— 避免公司因客户数据泄露而遭受的声誉损失

— 防止知识产权和公司资产的损失，以及公司其他专有信息的泄漏

在当今这个持续互联的世界，网络安全对很多公司而言至关重要。网络安全的问题频繁出现在很多企业的董事会议程上，数据安全威胁问题现已几乎成为每周的新闻头条。网络威胁形式的日益变化，技术的快速更新，法规环境的变化，社会变迁及企业的变革等因素，致使对于网络安全相关问题的关注度不断增加。此外，黑客的技术能力不断提高而且资金充裕，他们不断地寻找新的方法，不仅通过网络直接地瞄准目标公司，而且还利用主要供应商及技术伙伴间的联系进行黑客活动。因此，疏忽安全防范的后果将是灾难性的，公司的利润和声誉将受到严重的影响和挑战。有鉴于此，所有公司更应保持时刻的警惕并定期更新网络安全保护标准。

内部审计可以提供以下协助：

— 以行业准则为指引审阅企业的网络安全风险评估、网络安全流程及控制措施，以保护其知识产权，并且提供改善建议

— 针对已修订的技术安全模型的应用情况进行评估，例如多层防御，强化检测方法以及在离线状态下对数据的加密等

— 安排提供健全的培训和课程计划，包括模拟的网络诱骗钓鱼式攻击，让员工在全面的网络安全保障计划中发挥关键作用

— 对第三方安全服务供应商进行评估，识别其是否充分、完整地评估了最新的风险并采取应对措施

03 新兴技术

驱动因素：

— 规划采用和实施云计算以作为传统电脑系统的替代方案

— 鉴于技术高速发展，员工期望的变化以及不断出现无法有效预测的挑战，需要重新审视传统的灾难恢复和业务持续发展的方案

— 考虑机器人和其他技术，以减少对手工劳动力的依赖

移动计算、远程计算、云计算、社交媒体和大数据使我们能前所未有地存取、使用和管理信息，并彻底改变了营商环境。新兴技术使全球各地企业的员工能轻而易举地取得各种信息，让企业能够更有效地运作，从而影响着人们的生活和工作方式。在现今的商业社会，企业拥有无数机遇发掘和利用这些新兴技术以推动市场和行业的改变和创新。然而，每项新技术的演变发展均会带来风险，企业必须高度关注有关的风险管理，在尽量提高新技术的效用和减轻新技术在实施和使用上的风险之间取得适当平衡。

内部审计可以提供以下协助：

— 根据行业准则，评估企业目前使用的技术系统和新兴技术系统

— 评估因采用技术方案可能导致的业务模型变化以及控制架构的相关变化

— 审阅有关技术管理的政策和程序，包括治理和控制、数据完整性、安全和隐私以及供应商管理合规性等

— 评估灾难恢复和业务持续发展方案，包括管理层就 “拒绝服务” 类攻击所造成的威胁，检讨测试有关方案所采用的方法

— 考虑数字劳工和相关举措所需的治理和控制措施

04 战略协同

驱动因素：

— 确保内部审计与公司的战略重点保持一致，并且与公司的组织变革和其他重大变革保持相关性

— 确保内部审计能有效参与公司的关键战略措施，包括事前咨询，事中监督或事后评价手段

在全球化临界点的趋近、西方经济增速持续放缓、技术和能源支出大幅变化以及监管合规带来的挑战等多个重要因素驱使下，很多企业开始考虑转型以寻求更广阔的发展前景。当公司转型和其他目标指向其战略目标和具体举措时，内部审计部门应积极参与并考虑其对相关风险治理及内部控制的影响。当努力实施战略转型并迎合新的商业模式时，企业可能会忽略针对转型后新商业模式的内部控制措施做出适当调整。内部审计为战略变革提供了独特的视角，并且应该在关键的战略举措中得到更为积极的体现。

内部审计可以提供以下协助：

— 确保内部审计资源被分配到公司最重要的目标和举措上

— 加强关注公司治理范围外通常与内部审计职能关联性不大的领域，例如某些管理流程、信息技术和数据管理及操作风险等

— 决定公司如何评估与重大战略举措相关的风险，以及如何管理与这些举措相关的变化

— 收集内部和外部变化迹象，以供企业战略部门参考

— 协助深入分析战略决策和风险事件，为管理层的未来决策提供独到见解

05 合规遵循

驱动因素：

— 确保遵循持续大量新增的国内外各类监管要求

— 严格控制因遵循持续新增的监管要求所导致的合规成本的增加

— 建立策略以减少合规活动对业务运营的限制

— 确保收购兼并后的运营合规

无论何种行业的公司，都需要保持对国内外新增监管法规要求的持续关注。这些新增的监管法规要求加重了首席合规官及相关员工的工作负担，同时也增加了疏漏遵循某些合规要求的可能性。另外，满足这些新的法规要求会大幅增加公司的合规预算，同时增加了内部架构和信息需求的复杂性。与此同时，企业收购及兼并活动不断增加，公司同样需将自身的合规职能与被收购方及兼并方的合规职能有效整合以确保公司合规职能的统一性。

内部审计可以提供以下协助：

— 总结会对公司产生影响的监管机构及其监管要求

— 评估公司在全球范围内的合规管理方式，包括其如何整合所并购公司的合规管理要求

— 评估公司对任何明显违规事件的反应

— 确保向员工和其他利益相关方提供的合规培训，与其角色和所处地区相匹配

— 到访各营运地点执行合规部门指示的工作，以尽量减少业务部门重复执行有关工作的情况，并同时确保能实现有关目标

06 第三方关系

驱动因素：

— 第三方业务伙伴关系不断增加所涉及的风险，加强对第三方关系的监管

— 增加收入及缩减成本

— 提升合同和服务供应商的治理

— 创建更有效的缔约方自身汇报流程

— 预防或及时发现第三方业务伙伴的风险管理疏漏

为提高生产效率和适应不断转变的业务模型，越来越多公司会依赖第三方执行关键业务职能。但是，引入第三方合作会产生各种新的风险敞口，并可能导致服务、合规和其他方面出现疏漏，从而导致罚款、诉讼、操作禁令及声誉受损等问题。由于外部环境或协议条款的复杂性，业务伙伴可能会在不经意间违规或违约。例如，第三方如果可以进入公司的网络，则会增加数据泄露的风险；又如公司可能未意识到第三方合作伙伴聘用的转包商不能符合公司的业务合规要求。再如，第三方可以在政治风险不确定的领域经营，将合作双方暴露在更大的风险敞口下。综上所有因素，公司需要确保在力争从外部关系中获取最大利益的同时，又应兼具恰当的控制手段，从而降低有关的风险和责任。

内部审计可以提供以下协助：

— 审视对第三方身份的识别、尽职调查、筛选及准入审批流程和控制措施

— 评估管理层对于第三方关系的合同管理流程

— 监督与第三方管理相关的监管要求的发展

— 加强执行第三方审计权利条款，并确保有关条款的一致性

— 加强第三方对公司信息数据安全要求的遵循

— 开发、实施并调校一套全周期的、供第三方业务伙伴提供数据的监管系统

07 数据分析和持续审计

驱动因素：

- 可进行实时、持续的风险管理
- 提升审计的整体效率（频率、范围等）
- 通过分析关键数据，对关键风险领域进行更深入的挖掘
- 可在早期发现潜在的欺诈和错误
- 充分利用ERP单一平台系统可带来的效益

在过去几年中，数据分析彻底改变了公司进行自身评估和监控的方式，尤其是有效扩大了审计范围，并且提升了审计执行的深入程度。数据分析和持续审计可以帮助内部审计部门简化和提升审计流程，带来更高质量的审计结果，并为业务提供实质的价值。传统的审计方式是具有周期性的，包括人为地识别控制目标，评估和测试控制，以及在有限的样本量里抽样去衡量控制的有效性或业务运营表现。相比较而言，现在的审计方式更注重利用可持续的数据分析，提供更透彻并具备风险导向的审计方式。伴随着有效的数据分析，企业具备审查每宗业务交易的能力，不再是仅针对样本，而是对更广泛的控制领域进行有效的分析。内部审计部门需要与公司整体进行协调，致力于强化战略发展、提升企业整体凝聚力，通过发挥数据分析所带来的优化作用，为企业带来整合性的优势。

内部审计可以提供以下协助：

- 协助建立自动化的数据提取、转换及上传功能，并由业务部门根据特定风险指标监控由系统生成的分析数据和仪表盘
- 持续评估公司风险管理实践与公司整体战略目标的契合情况，并在此基础上持续监控公司战略目标与风险管理实践，制定风险管理的优先次序
- 提高审计程序的数据分析能力，以核实相关数据分析并汇报业务层面的风险
- 实施自动化的审计，将重点集中于根本原因分析和管理层对风险的应对措施，包括业务异常情况和风险触发事件
- 建议持续采用一贯的分析手段，包括通过描述、诊断、预测和既定元素等方法进行风险分析

08 反贿赂/反腐败

驱动因素：

— 识别新出现的监管与合规风险，例如因企业扩张进入新兴市场，或来自与第三方及收购兼并业务的合规风险

— 就现有的反贿赂及反腐败合规活动的有效性，向利益相关方进行汇报

— 当出现潜在的违规情况时，确保公司拥有足够的调控能力

通过落实一套有效的反贿赂及反腐败合规方案，并根据公司特定风险情况进行适当调校给企业带来的效益显而易见。公司制定的明确限定违禁行为的管理制度、高级管理层推行反贿赂反腐败工作的承诺、定期开展的培训、与第三方商定的审计条款，以及合规人员的警惕性，均可以有效阻止贿赂和腐败，从而降低监管执法所带来的高昂成本和损失。为了防止意外发生，一套完善和得到良好落实的反贿赂反腐败合规程序可以在最大程度上协助企业避免法律诉讼，甚至大幅降低罚款和损失金额。

内部审计可以提供以下协助：

— 将公司现有的反贿赂反腐败措施与最佳实践规范指引进行差距分析

— 保障公司所采用的预防性和检查性控制手段设计和运作的有效性

— 通过将反贿赂反腐败的流程嵌入现有的/定期进行的审计和第三方监管活动中，提升内部审计活动的效力

— 通过数据分析和第三方审计识别贿赂和腐败风险

— 引入或借用相关资源对潜在违规事件进行调查

— 通过测试和评估公司的反贿赂反腐败程序以做出持续改进

09 绩效风险

驱动因素：

— 确保财务业绩与经营和战略互相关连

— 为管理层提供独到见解，以管理和尽量降低绩效不佳的风险

— 整合风险管理和绩效管理方案，确保可以明智有效地驾驭风险

— 提高内部审计作为企业战略伙伴的意识

股东对业务绩效的期望与日俱增，管理绩效不佳的风险变得越来越重要。股东期望内部审计职能专注于运营事宜，并真正了解企业成功和获利的要素。内部审计目前比以往任何时候更加需要协助企业评估风险，识别和发展可持续产生利润的模式。内部审计站在企业风险分析的最前沿位置，需要分析企业战略、运营、财务和合规等各项风险，它们均会影响企业的业绩。风险分析结果可以在定量和定性上联系到收入、运营开支和投资等价值驱动因素，令内部审计见解在提升绩效上发挥不可或缺的作用。

内部审计可以提供以下协助：

— 将内部审计资源分配予各项企业举措，发挥内部审计活动在合规以外的效益

— 评估企业的绩效衡量方式，识别改进机会

— 实施全面评估方案，以评估管理层是否能有效地管理绩效不佳的风险，其中除财务和合规外，还将注意力集中在运营和绩效的审计活动上

10 文化风险

驱动因素：

— 监管审查更加严格，各界对企业文化的期望不断提高

— 跨国企业不断增加，造就更加多样化的文化规范和实践

— 业务单位之间缺乏相互联系，导致存在管治差距

— 更加严格的企业管治、监督和问责要求

— 审计结果和内部控制事宜

许多不当行为事件影响了公众对企业的信任，因此企业文化风险成为了管理层关注的议题。即使企业制定了明确的业务战略，但如果企业文化不能提供适当的支援和配合，企业取得成功的机会也会相当渺茫。企业可通过观察、监督和不时调整企业文化以减少不当行为的发生，鼓励员工做出配合企业战略的行为。广泛的企业文化方案可有助处理企业管治、合规和风险管理等具体事项，亦可集中了解企业如何做出决策以满足不同利益相关者的要求、这些决策如何影响当前和未来的企业文化。

内部审计可以提供以下协助：

— 评估公司的企业文化在组织规范方面的推动力

— 审阅绩效指标是否能配合企业战略，确保良好的行为得到激励和奖励

— 就企业文化的演变和与合规活动的配合，以及财务目标和业务及营运模式的配合提供保证

— 通过数据分析和第三方审计识别企业文化风险

— 领导或参与涉及潜在不当行为事件的调查

— 通过测试和评估企业文化的演变计划，推动持续改善

联系我们

上海

胡丽芬
合伙人
风险管理咨询
电话: +86 (21) 2212 2603
lifern.woo@kpmg.com

陈晓红
合伙人
风险管理咨询
电话: +86 (21) 2212 2780
grace.xh.chen@kpmg.com

沈奇伟
总监
风险管理咨询
电话: +86 (21) 2212 3640
michael.shen@kpmg.com

葛怡婷
总监
风险管理咨询
电话: +86 (21) 2212 3295
joyce.ge@kpmg.com

北京

梅放
合伙人
风险管理咨询
电话: +86 (10) 8508 7188
frank.mei@kpmg.com

徐捷
合伙人
风险管理咨询
电话:+86 (10) 8508 5952
jessica.xu@kpmg.com

李斌
合伙人
风险管理咨询
电话: +86 (10) 8508 5975
johnson.li@kpmg.com

王霞
总监
风险管理咨询
电话: +86 (10) 8508 5113
shirly.wang@kpmg.com

香港

马绍辉
合伙人
风险管理咨询
电话: +852 2978 8236
paul.mcsheaffrey@kpmg.com

宋家宁
合伙人
风险管理咨询
电话: +852 2978 8101
jianing.n.song@kpmg.com

李懿玲
总监
风险管理咨询
电话: +852 2143 8764
alva.lee@kpmg.com

侯爵维
总监
风险管理咨询
电话: +852 2685 7780
jeffrey.hau@kpmg.com

广州/深圳

梁安超
合伙人
风险管理咨询
电话: +86 (755) 2547 3338
kelvin.oc.leung@kpmg.com

杜小娅
总监
风险管理咨询
电话: +86 (755) 2547 1168
daisy.du@kpmg.com

kpmg.com/socialmedia