

Powerful Insights. Proven Delivery.™
敏于知 达于行

浅谈目前互联网企业 内审职能的热点问题

甫瀚 | protiviti®
风险与商业咨询。
内部审计。



随着经济环境逐步回暖，企业都有新一轮的投资计划，以寻找业绩增长机会，把握“先行者”优势，抢占市场先机。这对于以技术为资产的互联网企业而言尤为重要。在瞬息万变、日新月异的环境中，质量、变通力和创造力都是互联网企业不可或缺的成功要素。

然而，目前市场仍存在很多不确定因素，互联网企业在迈向成功的道路上仍会面临相关风险所带来的种种挑战，比如如何保障互联网信息的数据安全等。这使得企业在寻求业绩增长的同时，必须小心谨慎，在成本管理、增加收入以及风险应对能力上取得适当平衡，这是企业能否傲视同侪的关键所在，而内部审计职能将在协助其管理未来变化中发挥关键作用。内部审计能为企业提供保障，确保现存的以及新兴风险能够得到识别、监控和管理，从而让企业安心实施其业务战略。

本文针对若干互联网企业内审职能目前所遇到的几个热点问题予以探讨，重点在于内部审计在其中所扮演的角色和能够发挥的作用。

一、内审部门在数据安全与隐私保护方面的主要职责

谷歌在为其谷歌地图街景服务拍摄街道照片时，使用的软件可截获附近无线网络用户电子邮件账户名和密码等敏感个人信息，从而在全球超过30个国家通过未加密的无线网络收集了个人数据，引起众怒。

据《福布斯》杂志报道，过去一年维基解密（WikiLeaks）总共披露了76,000份阿富汗战争的机密文件和392,000份伊拉克战争的文件，这被视为史上最大宗的军事泄密事件。

Facebook推出的个人化功能让用户能直接从Facebook链接各大媒体及其他第三方合作网站，但同时也将用户个人资料一并分享到第三方网站，Facebook用户因担心隐私问题，发起抗议。

随着互联网和日常生活的联系日渐紧密，互联网公司的数据安全和隐私保护成为公众关注的焦点。数据的安全与隐私的保护不再仅仅是单纯技术的问题，而是互联网公司面临的商业发展与业务经营的关键问题。互联网行业因其自身业务性质以及不断创新的商业模式，引起公众的广泛关注，随着广大用户的安全意识、隐私观念的提高，互联网公司也被推向数据安全和隐私保护的风口浪尖。数据安全和隐私保护方面的风险也因此成为互联网企业面临的重大风险之一。

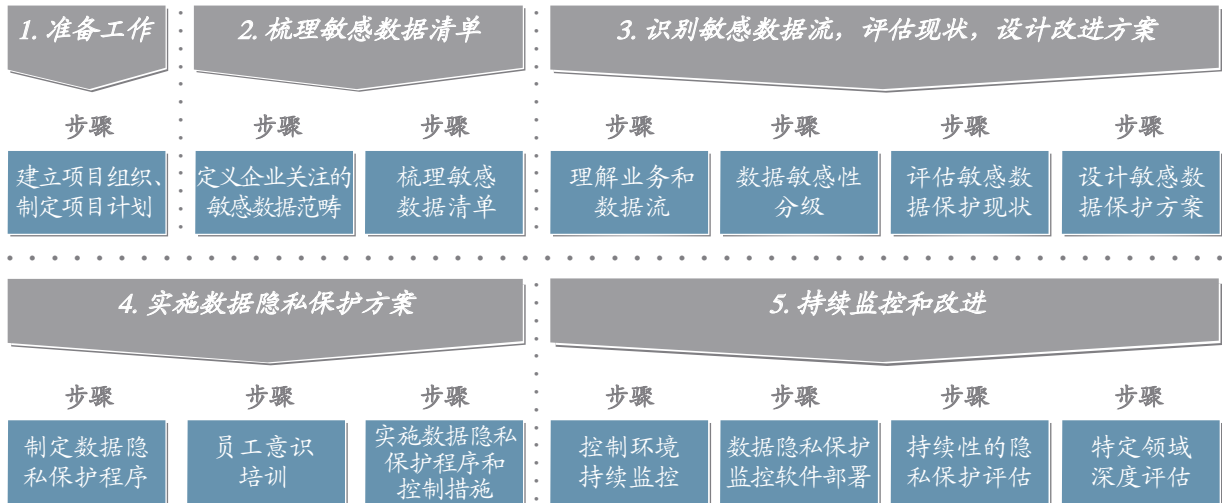
数据安全和隐私保护的风险分析存在于信息生命周期的各个环节，包括信息的收集、使用、传递、更改、存储和销毁。目前，企业在互联网中遭到泄露的信息包括——企业信息：商业机密、知识产权、财务信息、企业战略、薪酬信息和企业兼并信息等；个人信息：身份证号、银行账户信息、联系方式及其他非公开信息等；第三方信息：交易信息、报价信息和客户文档等。

实际上，敏感信息存在于企业各业务单元和业务流程中，敏感信息泄露所造成的危害和影响往往波及整个公司，因此，包括CISO（首席信息安全官）、CIO（首席信息官）、首席法务官、人力资源总监、IT安全总监/经理、内审总监、内控总监，以及涉及敏感信息处理的业务单元负责人均应对企业数据安全和隐私保护负责。数据安全和隐私保护是整个企业的职责。企业各个层面的决策者、管理者、执行者都应有数据安全和隐私保护的意识，并将这种意识贯彻到日常的工作中，大到一个公司商业决策、产品开发，小到日常工作中的一个细节操作环节都应注意对于数据安全和隐私保护的执行。数据不是静止于某一点或某一个部门，在数据与隐私内容处理的各个环节都可能存在保护不力、泄露、滥用的威胁，因此需要通过清醒的认识、明确的方法、有力的执行，对数据安全和隐私保护的进行控制。

根据内审的职责，结合以风险为导向的内部审计工作，我们认为，在现阶段，内部审计在数据安全和隐私保护方面的主要职责包括识别、分析与数据安全和隐私保护相关的风险，评估企业在数据安全和隐私保护方面控制的设计、执行效率、效果，并对这些方面持续监督，为企业在数据安全和隐私保护方面提供合理化的改进建议。内审应关注企业的数据安全和隐私保护策略和流程，可对控制设计的有效性进行评估，具体手段包括策略与流程审阅、数据安全和隐私保护项目审计和信息安全管理成熟度评估等。内审也应分别从外部和内部出发，以评估现有控制的执行有效性，包括技术性审计，如内外部渗透测试、内外部弱点扫描、网络与边界审计、无线网络审计、应用审计、系统审计等，也包括管理性审计，如业务流程审计、管理制度体系执行审计、社会工程学测试等。总之，内部审计工作作为企业风险管理最后一道防线，在数据安全和隐私保护方面承担了极其重要的职责。

甫瀚咨询将数据安全和隐私保护的实践经验与国内外先进理论结合起来，提出了数据安全和隐私保护的方法论。该方法论分为五个关键阶段（参见下页流程图），每个阶段均代表数据安全和隐私保护风险管理项目中的一项关键任务，包括：

1. 准备工作；
2. 梳理敏感数据清单；
3. 识别敏感数据流，评估现状，设计改进方案；
4. 实施数据隐私保护方案；
5. 持续监控和改进。



近年来，互联网企业对数据安全与隐私保护方面越来越重视，业务、信息技术、风险管理等相关部门也通过各种风险控制活动不断提升管控水平。同时很多企业已经将数据安全与隐私保护方面的风险与控制审计纳入内部审计的工作范围，在企业内部开展了不同层次、不同范围的审计工作，并通过培训、提供改进建议等方式与企业其他职能部门一起，为提高企业的数据安全与隐私保护水平而努力。

二、内部审计在工程项目中的角色和职能范畴

经济的飞速发展、社会的不断进步，以及用户的需求越来越高，都要求互联网企业必须在基础设施建设上投入更多资源，以不断开发新的产品和服务，从而保持竞争力。因此，互联网企业的工程建设项目日益繁荣，而与工程项目相关的固有风险也随之显现：工期延误、成本超支、质量不达标以及合同纠纷等等。

通过建立稳健的风险管理流程和内控目标，可监控工程建设活动、识别或防范资金外流，从而达到规避风险的目的，同时，亦可增加企业价值。

传统的内部审计主要是在工程后期的介入较多，但近年来，内审职能积极强化其对企业的增值效益，务求更有效地发挥实质性的监控和规范作用，因此很多内部审计从工程前端就开始参与其中，例如在工程预算或规划阶段提供帮助，为整个工程项目保驾护航。综合企业的经验，不难发现内部审计的职能发挥主要聚焦于风险管理和内部控制方面，贯穿于整个工程始末，包括前期准备阶段、建设实施阶段、工程竣工交付阶段，称为基建项目全过程跟踪审计。

基建项目全过程跟踪审计几大关键控制点：

- 建设资金投资立项决策
- 招投标过程
- 建筑施工合同管理
- 工程变更
- 工程资金使用
- 竣工交付验收决算

其中，工程招投标是建设工程项目中的一个重点环节，主要分四个阶段：预算阶段、供应商初选阶段、招投标阶段和合同签订阶段。内部审计部门参与整个的招投标过程，但应保持相对独立，即避免直接参与投票。通常来说，招投标环节的审计目标如下：1) 招投标程序包括资格预审、招标方式、开标、评标等过程是否合法、合规；2) 招标小组评标办法的有效性；3) 基建项目标底的客观性；4) 投标单位资格和

条件的真实性，防止施工单位之间串标，防止无资质或低资质等级的施工单位承包工程。内部审计部门需要帮助企业建立良好的控制环境，比如根据总体的建筑目标来评估风险，然后定义这些风险必需的控制点是什么，进而形成一套完整的内控标准，涵盖工程建设全过程的关键控制点，也就是说，建立一套内控架构标准，然后确保各部门均清楚知道需要关注的关键风险点何在，通过内控标准由各部门编制一些流程和规范甚至制定相应的措施，最后达到规避风险的目的。

比如，在选择供应商时，企业应制定一个统一的考查标准，在前期进行背景考查，比如供应商与公司员工是否存在利益冲突，以及供应商的经济状况和业绩纪录等。有的企业采取一个互相制衡的机制，由各个部门共同推荐一些供应商，然后从不同的角度进行分析和甄选，形成一种力量上的牵制。在招标阶段，招标文件应清晰列明各种条款和要求，例如投标人的资质、过往项目经验等。另外，必须根据公司的项目战略和侧重点，确定评标标准和规则。最后，合同须清楚列明项目条款和具体要求细节，避免双方出现歧义，产生合同纠纷。

某大型互联网公司实施了“流程质量保证检查”，在不同的阶段根据检查清单对流程制度进行审核，并出具检查报告。

某互联网企业的工程管理团队架构：

- 成立项目建设委员会，类似决策委员会，包括各个相关部门的经理，并从中指派一名项目经理与各部门进行协调，该名经理负责协调和管理整个工程项目的全过程；
- 法务部和财务部作为支持性部门，负责处理法律法规和财务等方面的要求，全程参与，有时也担当审核者角色；
- 内控和内审部门，负责对整个工程进行监督及咨询。

工程建设是专业的范畴，工程人员都是专业人员，因此内审人员的角色并不是要指导他们如何做工程，而是从规避风险和改善流程的角度出发，为他们提供一些指引和建议。例如，在项目前期识别和评估风险，制定内控标准，并按相关控制点编制流程和规范；监控流程的进行，在发现问题时提出警示；定期在项目的某些时点进行检查，确定流程的合规性、识别流程弱点并提出建议。

从大量的工程项目跟踪审计实践看，重视对内部控制审计，往往能收到事半功倍的效果，特别是内部审计职能从工程项目前期开始就参与到整个工程项目里来，对投资决策、工程管理、造价控制、财务管理等的真实性、合法性和效益性具有重要意义。

中国内部审计协会提倡建立“适时跟进、多方配合、审计指导、及时通报”的新型跟踪审计模式，以有效防范工程建设的跟踪审计风险。

三、内审团队的建设 and 培训

内部审计人员必须对业务有深入认识，才能识别业务中所存在的问题和风险，进而予以管理和监控。企业在配置审计职能时，应确保审计团队拥有适当的技能组合，该技能组合应根据企业的业务需要来确定。就互联网企业而言，其内审人员不仅需具备内审和内控的知识，也必须对互联网业务技术有一定程度的认识。如果内审人员对有关技术和业务运作一知半解甚至一窍不通，就很难跟技术人员沟通协调，更莫说提出具说服力和有效的建议。

以下列出了几种培养专业团队的途径，企业应根据自身实际需要予以筹划。

内部调职

最直接的办法是从公司内部发掘那些熟悉并了解公司业务的人才，然后向他们提供培训，传授所需的内审知识。

挑战：相对于内审部门，业务部门对员工来说更具挑战性和吸引力，待遇也比较好。因此可能只有后勤的部门员工对调职内审部门感兴趣，而后勤人员相对来说对业务运作没有实战经验和透彻的了解。

岗位轮换

长期或短期的岗位轮换计划，让内审人员到业务部门工作一段时间，实际了解业务的操作；而业务人员也有机会把他们的业务知识运用到内审部门。

优：轮岗制度不但能帮助管理层了解组织的内部控制环境和其他运营领域，也为员工提供在职培训和职业发展机会。这种灵活的机制和培训计划能够有助加强对组织的风险管理和内部控制体系的认识，并鼓励员工尽展所长、精益求精。

劣：可能引发利益冲突问题。例如，如果有人员是从组织中的其他现有业务职能调至内部审计部门，便有可能出现利益冲突，妨碍他们对从前共事的同事进行审计。又如，一位参与岗位轮换计划的内部审计人员在对某一业务单元或职能进行评估时心存偏袒，原因是他有意任职于该部门。

外部招聘

最常见的做法是从外部招聘富有经验并拥有适当技能的内审人员。

挑战：目前市场稀缺两者兼备的人才，既要有良好的内审知识和专业技术水平，也要懂一些互联网行业的业务特点和文化。

合包外包

企业应当确定应在内部配置哪些技能，如果开展某些审计项目所必需的技能与企业的标准能力组合不符，那么就应考虑以分包的形式执行这些审计工作。

优：与内审服务承包商或提供专门技能资源的外部组织合伙或合作，能够增强内部审计职能应对风险和满足客户期望的能力。此外，这些合包项目通常都能够有助于将外部知识引入组织内部，从而提高内审职能全职人员的能力水平。

劣：需要支出额外的成本。

外部培训

优：有关方面的专题培训，或举办研讨会、交流小组等，可以提升内审人员的能力水平。

劣：一些培训讲座泛泛而谈，往往不能针对实际问题，因而效果十分有限。

甫瀚咨询

www.protiviti.cn

大中华区办事处

北京

中国 北京 100022
朝阳区建国门外大街2号
银泰中心银泰写字楼
20楼2001单元
电话: (86.10) 8515 1233
传真: (86.10) 8515 1232

上海

中国 上海 200020
淮海中路381号
中环广场26楼
电话: (86.21) 5153 6900
传真: (86.21) 6391 5598

深圳

中国 深圳 518048
福田区中心四路1号
嘉里建设广场
第一座第十四层04室
电话: (86.755) 2598 2086
传真: (86.755) 2598 2100

香港

香港 湾仔
港湾道18号
中环广场21楼2102-3室
电话: (852) 2238 0499
传真: (852) 3118 7493

甫瀚 | protiviti®
风险与商业咨询。
内部审计。