在业务转型过程中
到达内部审计的临界点

2016年内部审计能力与需求调查报告（精辑版）

protiviti®

Face the Future with Confidence

甫瀚

Powerful Insights. Proven Delivery.®

敏于知　达于行

“临界点是指当某种思想、趋势或社会行为在越过某个门槛后，倾覆开来，然后像野火一样迅速蔓延的那一神奇时刻。”

—《临界点：区区小事如何成就云泥之别》，马尔科姆·格拉德威尔

前言

贵司的内部审计职能发展得如何？

该问题蕴藏着一个微妙但直白的挑战：一成不变是不够的。不论是C级管理层、董事会还是整个企业中的内部审计利益相关方，都在很大程度上依赖内部审计职能为他们提供保证及合规相关的活动。然而，这些贡献正越来越成为内部审计职能可发挥作用的冰山一角。在持续的业务转型过程中，利益相关方向内部审计团队寻求的信息日益增多，包括但不限于与长期战略密切相关的风险，或是潜藏于表面之下随时可能给企业带来灾难性影响的网络安全违规事件。

从战略的角度而言，其他威胁亦在远处若隐若现，包括有关数字化转型、移动技术以及持续监管变更的风险。而伴随物联网的逐渐崛起，谁又了解其中潜藏着多少数据保护风险？这些趋势在带来大量机遇的同时，亦裹挟着威胁而来。企业必须进行审慎的识别、评估和监控，方能胸有成竹地面对未来。

在我们开展内部审计能力与需求调查的第十个年头，我们认为内部审计已来到一个临界点。问题不再是你的内部审计职能是否在发展，而在于它的发展和转型速度有多快以及效果如何，从而在将来实现一种更具战略意义、协作性更强且更加以数据作为驱动的运作模式，同时确保内部审计获得最高质量的执行。

我们的主要调查发现：

- **网络安全措施的力度取决于董事会的参与及其在审计计划中的位置** – 网络安全并非信息技术问题——它是一项业务风险，需采取全面的、基于风险的方法来进行管理。最有效的网络安全审计能力一定是拥有企业的支持，董事会高度参与信息安全风险管理，并将网络安全风险纳入审计计划。
- **网络安全风险正成为内部审计计划的固定项目** – 近四分之三的企业已将网络安全风险纳入年度审计计划进行评估，而在2015年这一比例只有一半。
- **显著的审计优先事项包括移动应用、云计算、信息技术标准以及物联网** – 技术问题在内部审计师的优先事项名单中占据优势，包括新兴技术及趋势以及信息技术审计标准等。
- **是时候进一步提升企业的数据分析及技术驱动型审计能力** – 内部审计人员继续将数据分析和技术驱动型审计列为重大关注事项，但在经历了十年的停滞不前后，我们已到达需要取得更多进展的临界点。

在庆祝本报告发行十周年之际，我们谨对参与今年调查的逾1,300名首席审计执行官及内部审计专业人员表示深深的感谢。我们也谨向国际内部审计师协会（IIA）致以诚挚的敬意，感谢他们为推动内部审计在当今企业中的战略角色而在全球做出的杰出贡献。

网络安全与相关审计流程

网络安全与相关审计流程

- 拥有最有效的网络安全审计能力的企业将该风险纳入年度审计计划，并且其董事会高度致力于信息安全风险。
- 近四分之三的内部审计职能将网络安全风险的评估与审计纳入其审计计划——与2015年的调查结果相比进步巨大。
- 品牌和声誉受损、数据安全（公司信息）及数据泄露（员工个人信息）成为最大的数据安全风险。
- 资源/技能短缺及软件工具的短缺正在阻碍企业充分应对某些特定的网络安全领域。

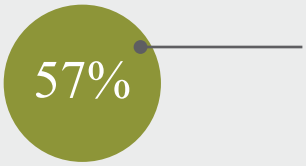
如今，网络安全已从信息技术风险上升为一项战略业务风险，并成为董事会定期应对的问题。好消息是根据我们的调查，许多企业，特别是其内部审计职能部门，已在网络安全能力的诸多方面取得重大进步。有关进步的最有力证据是：今年73%的受访企业将网络安全风险纳入年度审计计划，而在2015年的调查中该比例只占到53%。

然而，我们的调查结果显示，为避免遭受网络攻击的重创，企业尚需获得实质性进展。事实是，当涉及网络安全问题时，看得见的风险或许仅是冰山一角。

为弄清楚可能潜伏于表面之下的情况，不仅网络安全风险管理战略必须到位，还须确保有关战略行之有效。董事会不仅应当知晓网络安全风险的存在，还应积极参与到网络安全措施的制定中。内部审计部门应当把网络安全整合至其日常业务活动及其年度内部审计计划中。

与去年相似，我们的调查结果表明两大要素——“董事会高度参与网络安全管理”及“评估网络安全风险”被纳入当前审计计划，此两项是网络安全风险获得有效应对的关键成功因素。

重要信息



曾收到来自顾客、客户及/或保险提供商有关网络安全现状询问的公司比例

致首席审计执行官和内部审计专业人士的十大网络安全措施建议

1. 与管理层和董事会共同制定网络安全战略及政策。
2. 寻求机会加强企业识别、评估并将网络风险降至可接受水平的能力。
3. 认识到网络安全风险并非只是来源于外部，也要评估并降低员工或业务伙伴可能招致此类风险的潜在威胁。
4. 增进与审计委员会及董事会之间的关系：（a）强化董事会对网络威胁方面的意识和知识；（b）确保董事会始终高度参与网络安全事宜，并对变化的网络安全风险保持实时更新。
5. 确保网络安全风险被正式纳入审计计划。
6. 实时了解新兴技术及趋势对企业及其网络安全风险特征的影响。
7. 根据美国国家标准与技术研究院（NIST）的网络安全基础框架，来评估企业的网络安全程序。一旦发现该框架未能达至控制层面的情况，企业还需对网络安全程序额外进行ISO 27001及ISO 27002评估认证。
8. 寻找机会向管理层传达这样一个信息，即最强的网络安全防范能力应是人力与技术安全的结合体——集教育、认知、警觉以及技术工具于一体的相互融合。
9. 向高级管理层强调应将网络安全监督和网络事件视为其优先关注事项，而一个明确的自下而上的逐级汇报机制有助于实现并维持这一优先级。
10. 解决任何有关信息技术/审计人员配备不足、资源短缺，以及支持性技术工具不足的问题，因为这些问题都可能会妨碍对网络风险的有效管理。

一般技术知识

主要调查发现

- 与技术有关的风险，特别是网络安全风险，在内部审计师的诸多优先关注事项中脱颖而出。
- 来年要予以重点关注的领域包括ISO 27000、移动应用以及NIST网络安全框架。
- 本年度新增的两个调查领域——物联网和灵活的风险与合规，亦位列今年的内部审计优先关注事项之列。
- 过去十年来，最常被提到的优先关注事项明显侧重于信息技术。

总评结果 – 一般技术知识		
“改进需求”排名	受访者评价的领域	能力水平（5分制）
1	ISO 27000（信息安全）	2.4
2	移动应用	2.3
3	NIST网络安全框架	2.2
4	GTAG 16 – 数据分析技术	2.5
5（并列）	物联网	2.6
	灵活的风险与合规	2.3

内部审计措施建议
• 了解企业当前面临的战略风险，并预测12个月后的今天首要的战略风险会是什么。
• 与企业内的利益相关方建立并巩固协作关系，积极、全面地应对不断变化的业务风险。
• 鉴于网络安全已演化为一项重大业务风险，并日益成为董事会的关注对象，因此要认识该问题的战略性影响，并与企业内的利益相关方开展协作，对其不断变化的特性进行评估和监督，并为此投入必需的工具和专业技能。
• 协助企业确保其用来管理网络安全风险及其他重要技术（例如移动、分析、物联网）的方法是全面的、以风险为基础的。
• 确保舞弊检测和防范活动在企业技术、架构以及员工不断变动的情况下仍保持充足水平。

一般技术知识总评结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	ISO 27000（信息安全）	GTAG 16 – 数据分析技术	移动应用	社交媒体应用	社交媒体应用
2	移动应用	NIST网络安全框架	NIST网络安全框架	近期实施的IIA《标准》 – 职能性报告释义（标准1110） 近期实施的IIA《标准》 – 审计意见和结论（标准2010.A2和2410.A1）	云计算
3	NIST网络安全框架	移动应用	社交媒体应用	GTAG 16 – 数据分析技术 近期实施的IIA《标准》 – 总体意见（标准2450） 云计算	GTAG 13 – 舞弊防范和检测
4	GTAG 16 – 数据分析技术	实务公告 2320-4 – 持续保证	云计算	信息技术风险评估指南（GAIT） GTAG 13 – 舞弊防范和检测 ISO 27000（信息安全） COSO内部控制框架（2012草案版）	舞弊风险管理
5	物联网 灵活的风险与合规	信息技术风险评估指南（GAIT）	GTAG 16 – 数据分析技术	实务指南 – 评估风险管理的充分性 GTAG 6 – 信息技术漏洞管理与审计 舞弊风险管理	GTAG 16 – 数据分析技术

过去十年中入选首要关注事项频次最高的四大领域中的三个都带有明显的信息技术色彩——“ISO 27000（信息安全）”、“GTAG 16 – 数据分析技术”，以及“信息技术风险评估指南（GAIT）”。另外一项则是越来越需要利用技术及分析工具方能有效开展的“舞弊风险管理”。

2011	2010	2009	2008	2007
国际财务报告准则（IFRS）	信息技术风险评估指南（GAIT）	信息技术风险评估指南（GAIT）	ISO 27000（信息安全）	企业风险管理
GTAG 13 – 舞弊防范和检测				舞弊风险管理
ISO 31000（风险管理）	国际财务报告准则（IFRS）	国际财务报告准则（IFRS）	企业风险管理	COSO企业风险管理框架
行政诉讼中的刑罚（多德–弗兰克法案第929P条）	可扩展商业报告语言（XBRL）	可扩展商业报告语言（XBRL）	舞弊风险管理	国际财务报告准则（IFRS）
				六西格玛
六西格玛	ISO 27000（信息安全）	企业风险管理	COSO企业风险管理框架	格雷姆–里奇–比利雷法案（GLBA）
员工和董事的对冲（多德–弗兰克法案第955条）	信息及相关技术控制目标（COBIT）	ISO 27000（信息安全）	公允价值会计（FAS 159）	美国公认会计准则
GTAG 15 – 信息安全治理				

需要注意的是，虽然“分析技术”早几年并未纳入内部审计师的首要关注事项名单，但在过去五年却一直存在于首要关注事项中。

首席审计执行官在一般技术知识方面的评估结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	大数据/商业智能	NIST网络安全框架	移动应用	社交媒体应用	社交媒体应用
2	ISO 31000 （风险管理）	移动应用	云计算 NIST网络安全框架	近期实施的IIA《标准》－职能性报告释义（标准1110）	云计算
3	ISO 9000 （质量管理和质量保证）	GTAG 16－数据分析技术	GTAG 16－数据分析技术	COSO内部控制框架（2012草案版）	GTAG 13－舞弊防范和检测
4	GTAG 17－信息技术治理审计	信息技术风险评估指南（GAIT）	社交媒体应用	近期实施的IIA《标准》－审计意见和结论（标准2010.A2和2410.A1）	GTAG 16－数据分析技术
5	企业文化审计	ISO 27000 （信息安全）	GTAG 6－信息技术漏洞管理与审计	云计算 ISO 27000 （信息安全）	国际财务报告准则（IFRS）

过去十年来，首席审计执行官所重点关注的优先事项包括“ISO 27000”和“GTAG 16－数据分析技术”，以及“国际财务报告准则（IFRS）”，尽管后者的优先级别在近几年出现了情有可原的下降。

2011	2010	2009	2008	2007
国际财务报告准则（IFRS）	信息技术风险评估指南（GAIT）	国际财务报告准则（IFRS）	ISO 27000（信息安全）	COSO企业风险管理框架
GTAG 13 – 舞弊防范和检测	可扩展商业报告语言（XBRL）	信息技术风险评估指南（GAIT）	COSO企业风险管理框架	企业风险管理
			舞弊风险管理	
行政诉讼中的刑罚（多德–弗兰克法案第929P条）	国际财务报告准则（IFRS）	可扩展商业报告语言（XBRL）	企业风险管理	国际财务报告准则（IFRS）
员工和董事的对冲（多德–弗兰克法案第955条）				
GTAG 14 – 用户开发应用审计	信息及相关技术控制目标（COBIT）	企业风险管理	公允价值会计（FAS 159）	舞弊风险管理
GTAG 15 – 信息安全治理				
GTAG 3 – 持续审计	ISO 27000（信息安全）	ISO 27000（信息安全）	上市公司会计监管委员会（PCAOB）第5号审计准则	六西格玛
GTAG 12 – 信息技术项目审计			格雷姆–里奇–比利雷法案（GLBA）	

审计流程知识

主要调查发现

- 内部审计师对如何优化部署技术型审计继续保持关注，特别是统计分析工具，以期获得有关业务风险、流程及控制的更准确洞见。
- 信息技术审计的若干领域（包括安全性、持续性、程序开发和新技术）都被评为优先关注事项，这表明网络安全问题、数据共享以及其他新兴技术给企业带来的业务风险日益增多。
- 舞弊检测和调查亦成为重点关注领域，这或许是新技术及舞弊手段日渐复杂的又一佐证。
- 过去十年来有近一半的优先关注事项涉及技术型审计及分析。

总评结果 – 审计流程知识		
“改进需求”排名	受访者评价的领域	能力水平（5分制）
1	数据分析技术 – 统计分析	3.0
2	信息技术审计 – 安全性	3.0
3	信息技术审计 – 持续性	3.1
4（并列）	舞弊 – 舞弊检测/调查	3.1
	质量保证与改进程序（IIA标准1300） – 持续审核（IIA标准1311）	3.3
5	信息技术审计 – 程序开发	3.0

内部审计措施建议

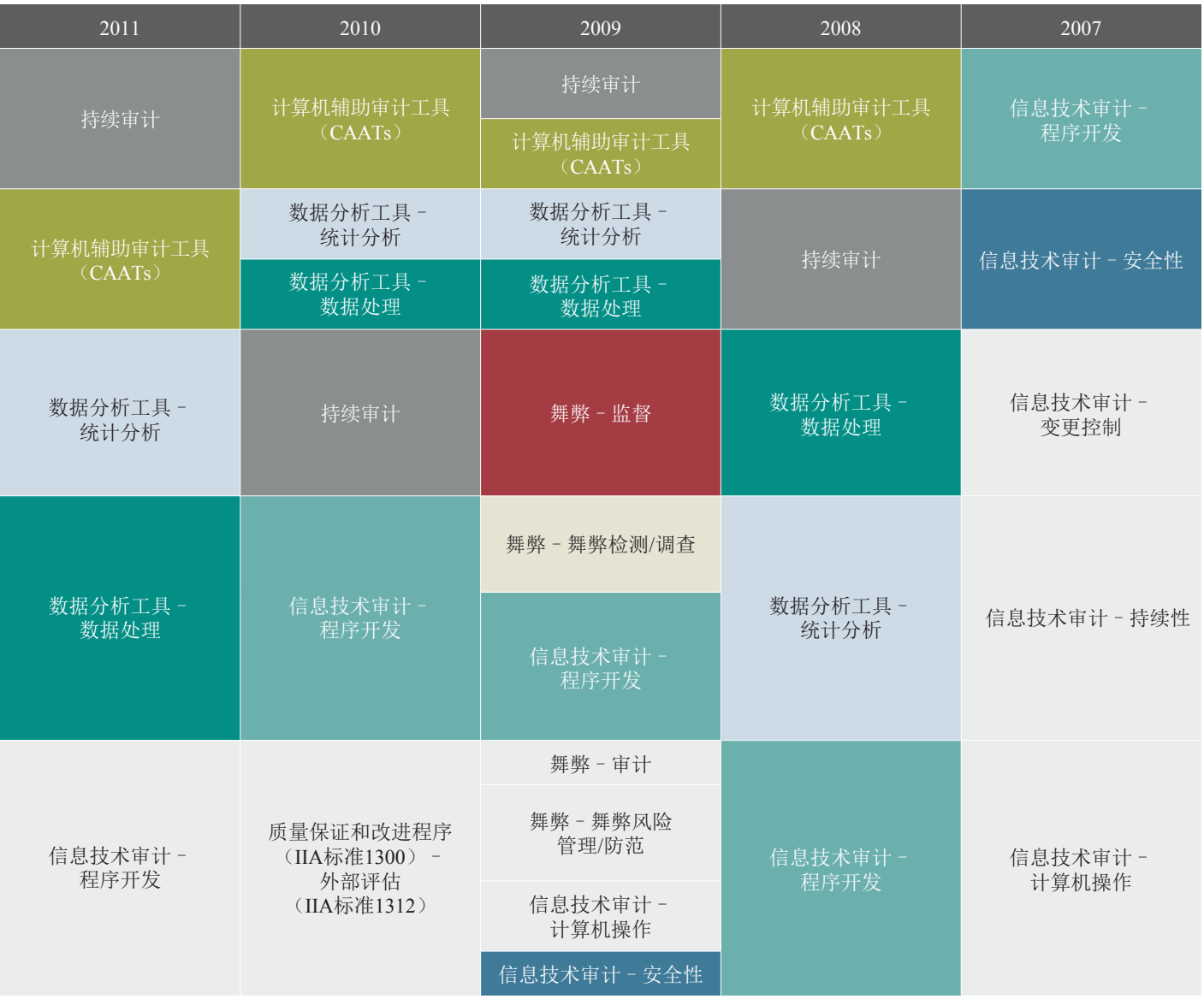
- 对内部审计职能开展的所有层面信息技术审计能力进行评估，包括安全性、持续性、程序开发、新技术、计算机操作、变更控制，以及信息技术治理。
- 根据所面临的企业风险及内部审计职能现有能力来判断信息技术审计的哪些层面需予以优先改进，然后制定相应计划并投入资源（人员扩充、培训和发展、新技术等）。
- 对于那些影响内部审计职能全面发挥其技术型审计应用及方法优势的障碍，予以识别并扫除。
- 确定如何加强内部审计部门的数据驱动化。
- 评估内部审计职能的现有专长能够在多大程度上为日益增长的信息技术审计及技术型审计需求提供支持；并考虑如何解决短期及长期的人才短缺问题。
- 通过开展战略性协作，与所有利益相关方建立持续合作关系，以及不断验证内部审计的洞见及专长价值，来持续提升内部审计在整个企业及董事会眼中的能力和地位。

审计流程知识总评结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	数据分析工具 - 统计分析	信息技术审计 - 安全性	计算机辅助审计工具（CAATs）	数据分析工具 - 数据处理 舞弊 - 监督	持续审计
2	信息技术审计 - 安全性	计算机辅助审计工具（CAATs）	数据分析工具 - 数据处理	信息技术审计 - 新技术 舞弊 - 舞弊风险评估	计算机辅助审计工具（CAATs）
3	信息技术审计 - 持续性	数据分析工具 - 数据处理	数据分析工具 - 统计分析	数据分析工具 - 统计分析 舞弊 - 舞弊检测/调查	持续监督
4	舞弊 - 舞弊检测/调查 质量保证与改进程序（IIA标准1300） - 持续审核（IIA标准1311）	在企业内部宣传内部审计	信息技术审计 - 新技术	舞弊 - 管理/防范 计算机辅助审计工具（CAATs）	数据分析工具 - 数据处理
5	信息技术审计 - 程序开发	舞弊 - 监督	数据分析工具 - 抽样	数据分析工具 - 抽样	数据分析工具 - 统计分析

在我们开展调查的过去十年中，盘踞首要关注事项时间最长的是“计算机辅助审计工具（CAATs）”和“数据分析工具”。此外，过去十年来近一半的优先关注事项均涉及技术型审计及分析。这是企业存在需整改缺陷的明确信号。

尽管内部审计职能一直致力于改进其对技术型审计工具的运用，但十年来的调查结果表明效果乏善可陈。让人疑惑的是为何内部审计组织一直未能解决该难题。与十年前不同，如今可用的数据分析及技术工具可谓不计其数，而且企业资源计划（ERP）系统在处理诸多类似活动方面也驾轻就熟。



不管存在何种组织性或文化性的冲突，最重要的一点，现在是时候拥抱变革并付诸行动了。一旦技术和数据驱动型企业在短时间内决定其内部审计职能必须拥有数据分析、持续审计及持续监督能力，那么，那些无法充分利用这些技术的内审组织将可能被迫达到其临界点。过去十年来的趋势一目了然。十年后的今天，企业很可能将无法再负担一个不具备该等能力的内部审计部门。

首席审计执行官在审计流程知识方面的评估结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	持续监督	信息技术审计 - 安全性	信息技术审计 - 新技术	数据分析工具 - 数据处理	计算机辅助审计工具（CAATs）
2	在企业内部宣传内部审计	计算机辅助审计工具（CAATs）	计算机辅助审计工具（CAATs）	信息技术审计 - 新技术	持续审计
3	质量保证和改进程序（IIA标准1300） - 外部评估（IIA标准1312） 舞弊 - 管理/防范	数据分析工具 - 数据处理	数据分析工具 - 数据处理	数据分析工具 - 抽样	数据分析工具 - 数据处理
4	信息技术审计 - 持续性	持续审计	在企业内部宣传内部审计	计算机辅助审计工具（CAATs） 数据分析工具 - 统计分析	持续监督
5	信息技术审计 - 新技术	数据分析工具 - 统计分析	数据分析工具 - 统计分析	舞弊 - 舞弊风险评估	数据分析工具 - 统计分析

对首席审计执行官而言，“数据分析工具”和“计算机辅助审计工具”在过去十年间的大部分年度中都被评为优先关注事项。首席审计执行官和其他内部审计领导应当识别并扫除那些影响其内部审计部门更有效地利用技术型审计的障碍。

2011	2010	2009	2008	2007
持续审计	计算机辅助审计工具（CAATs）	计算机辅助审计工具（CAATs）	持续审计	信息技术审计－程序开发
		持续审计		
数据分析工具－统计分析	持续审计	数据分析工具－数据处理	数据分析工具－数据处理	信息技术审计－安全性
数据分析工具－数据处理				
数据分析工具－抽样	数据分析工具－统计分析	数据分析工具－统计分析	计算机辅助审计工具（CAATs）	信息技术审计－计算机操作
				信息技术审计－持续性
信息技术审计－计算机操作	数据分析工具－数据处理	舞弊－监督	数据分析工具－统计分析	信息技术审计－变更控制
		舞弊－舞弊检测/调查		
舞弊－监督	质量保证和改进程序（IIA标准1300）－外部评估（IIA标准1312）	舞弊－审计	舞弊－监督	在企业内部宣传内部审计
		舞弊－舞弊风险管理/防范		

近几年出现的优先关注事项——“在企业内部宣传内部审计”，体现了首席审计执行官在向整个企业传递其职能价值方面所做出的坚持不懈的努力。

个人技能和能力

主要调查发现

- 发展与审计委员会的关系被评为改进需求最高的内部审计个人技能优先关注事项，演讲、建立人际网络，以及战略性思考紧随其后。
- 这些在过去十年间一直被列为优先关注事项的技能，对于在企业内部建立更加团结协作的合作关系，以及以一种最为有效的方式来宣传内部审计而言至关重要。

总评结果 – 审计流程知识		
“改进需求”排名	受访者评价的领域	能力水平（5分制）
1	发展与审计委员会的关系	3.1
2	演讲（公开演讲）	3.0
3	建立外部联系/人际网络	3.1
4（并列）	战略性思考 参加高压会议	3.5 3.2
5	处理冲突	3.1

内部审计措施建议
• 为更多的内部审计师提供向董事会审计委员会呈报的机会，以获取支持和信赖。
• 确认战略性思考的价值及内部审计专长在管理重大业务风险中的运用。
• 实施并推动有关培训活动，学习如何使用和掌握以新技术为基础的审计应用和方法。
• 作为一种获得个人发展机会和了解最新内部审计实务和思维的渠道，企业应鼓励内部审计师积极拓宽其在企业内部及外部的职业人际网络。

个人技能和能力总评结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	发展与审计委员会的关系	使用/掌握新技术及应用	演讲（公开演讲）	处理冲突	建立外部联系/人际网络
2	演讲（公开演讲）	说服开导	谈判	谈判	谈判
				说服开导	说服开导
3	建立外部联系/人际网络	发展与其他董事委员会的关系	说服开导	参加高压会议	处理冲突
			使用/掌握新技术及应用	演讲（公开演讲）	
4	战略性思考	战略性思考	处理冲突	战略性思考	演讲（公开演讲）
	参加高压会议		时间管理		
5	处理冲突	时间管理	发展与其他董事委员会的关系	发展与其他董事委员会的关系	参加高压会议
			建立外部联系/人际网络	使用/掌握新技术及应用	
				领导能力（在内部审计部门内）	
				时间管理	

十年的趋势表明，内部审计职能一直专注于提升个人演讲及说服开导技能，以期与企业内的所有关键利益相关方及董事会建立协作合同关系。

2011	2010	2009	2008	2007
处理冲突	演讲（公开演讲）	发展与其他董事委员会的关系	发展与其他董事委员会的关系	发展与其他董事委员会的关系
				谈判
演讲（公开演讲）	处理冲突	处理冲突	演讲（公开演讲）	领导能力（在内部审计部门内）
				演讲（公开演讲）
谈判	建立外部联系/人际网络	说服开导	发展与审计委员会的关系	建立外部联系/人际网络
		演讲（公开演讲）		
		战略性思考	建立外部联系/人际网络	
领导能力（在内部审计部门内）	说服开导	领导能力（在内部审计部门内）	与高级管理人员建立和谐关系	发展与审计委员会的关系
		建立外部联系/人际网络	时间管理	领导能力（在企业内部）
		时间管理		
建立外部联系/人际网络	战略性思考	发展与审计委员会的关系	变更管理	创建与时俱进的内部审计职能
			创建与时俱进的内部审计职能	说服开导
			领导能力（在内部审计部门内）	
			谈判	

首席审计执行官在个人技能和能力方面的评估结果 — 十年趋势

排名	2016	2015	2014	2013	2012
1	建立外部联系/人际网络	使用/掌握新技术及应用	演讲（公开演讲）	处理冲突	演讲（公开演讲）
2	战略性思考	发展与其他董事委员会的关系	发展与其他董事委员会的关系	发展与其他董事委员会的关系	发展与其他董事委员会的关系
				建立外部联系/人际网络	建立外部联系/人际网络
3	处理冲突	说服开导	使用/掌握新技术及应用	谈判	说服开导
				使用/掌握新技术及应用	使用/掌握新技术及应用
				时间管理	谈判
4	发展与审计委员会的关系	战略性思考	处理冲突	说服开导	处理冲突
	参加高压会议		说服开导		
5	变更管理	有效运用他人的专业技能	建立外部联系/人际网络	战略性思考	时间管理
			谈判		

过去十年中，首席审计执行官一直致力于提升内部审计对企业的战略贡献，方法包括但不限于与董事委员会建立关系（除审计委员会外），以及通过树立榜样来证明提高关系建立技能的重要性，比如演讲、处理冲突及战略性思考。

2011	2010	2009	2008	2007
发展与其他董事委员会的关系	发展与其他董事委员会的关系	发展与其他董事委员会的关系	发展与其他董事委员会的关系	领导能力（在内部审计部门内）
建立外部联系/人际网络	演讲（公开演讲）	演讲（公开演讲）	演讲（公开演讲）	谈判
时间管理		战略性思考		
领导能力（在内部审计部门内）	建立外部联系/人际网络	处理冲突	建立外部联系/人际网络	发展与其他董事委员会的关系
		时间管理		建立外部联系/人际网络
演讲（公开演讲）	时间管理	建立外部联系/人际网络	时间管理	演讲（公开演讲）
		谈判	书面沟通	创建与时俱进的内部审计职能
				领导能力（在企业内部）
战略性思考	处理冲突	创建与时俱进的内部审计职能	发展与审计委员会之间的关系	说服开导
			领导能力（在内部审计部门内）	

调查方法

超过1,300名（n=1,333）受访者完成了甫瀚咨询的审计能力与需求调查问卷，本次调查于2015年第四季度进行。

调查所包含的一系列问题被归为四大类：

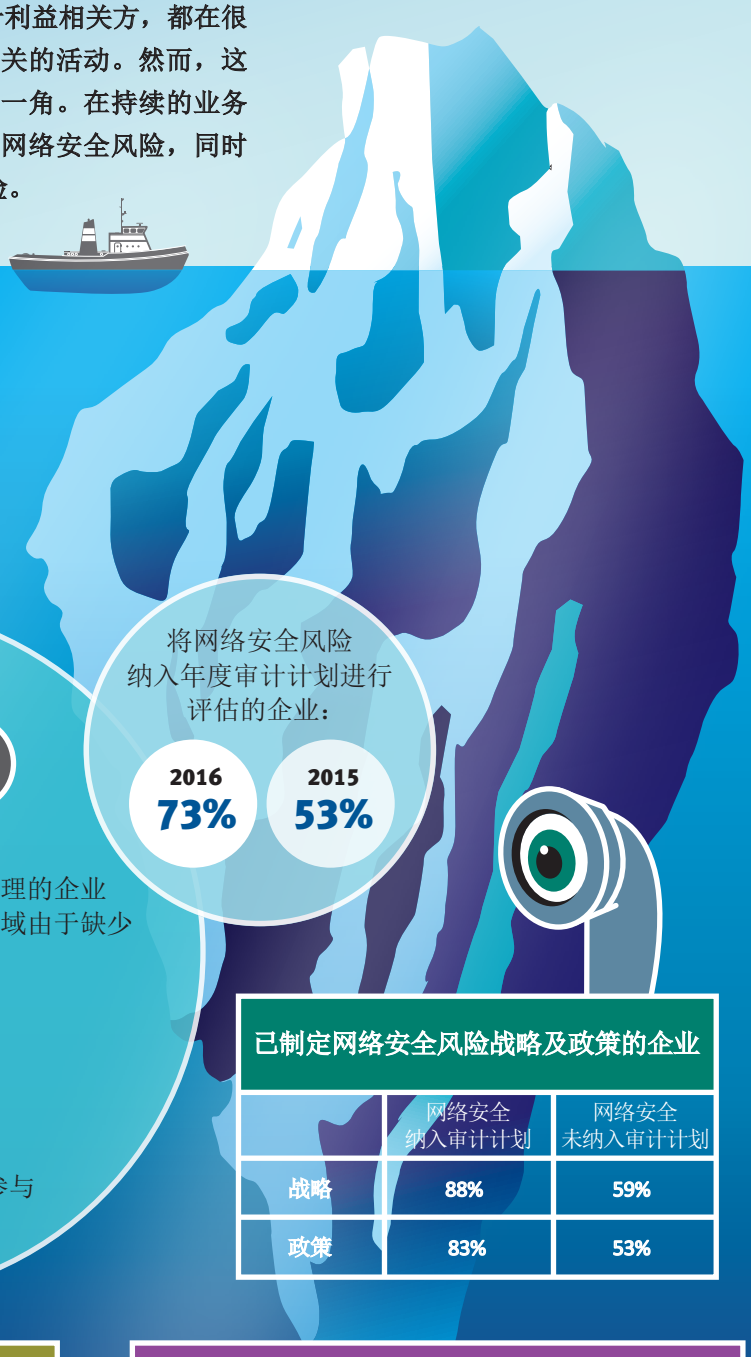
- 网络安全与相关审计流程
- 一般技术知识
- 审计流程知识
- 个人技能和能力

受访者回答了约200个领域的问题，以评估他们在这些领域方面的技能和能力。来自制造业、金融服务业以及医疗保健行业的受访者还对其所属行业的专有技能进行了评估。本次调查旨在了解当前各行业内部审计人员对必备技能的掌握情况，以及哪些知识领域最需要改进。

此外我们还请受访者提供了个人信息，如所在企业的性质、规模和所在国家，以及他们在内部审计部门的职位或职称等。这些信息有助于我们判断不同规模和性质的行业内不同资历水平的人员是否存在特殊的能力和需求。所有个人信息均为受访者自愿提供。

在业务转型过程中到达内部审计的临界点

不论是C级管理层、董事会还是整个企业中的内部审计利益相关方，都在很大程度上依赖内部审计职能为他们提供保证及合规相关的活动。然而，这些贡献正越来越成为内部审计职能可发挥作用的冰山一角。在持续的业务转型过程中，内部审计不仅要监控潜藏于表面之下的网络安全风险，同时还要致力于与新兴技术和企业长期战略密切相关的风险。



57

曾收到顾客、客户及/或保险提供商有关网络安全现状询问的公司比例

将网络安全风险纳入年度审计计划进行评估的企业：

2016	2015
73%	53%

董事会不同程度参与信息安全风险管理的企业占比，其中网络安全风险的若干特定领域由于缺少软件工具而未能获得充分应对：

18 董事会高度参与

51 董事会较少参与

已制定网络安全风险战略及政策的企业

	网络安全纳入审计计划	网络安全未纳入审计计划
战略	88%	59%
政策	83%	53%

2016年内部审计前十大优先关注事项 *

1. ISO 27000（信息技术）
2. 移动应用
3. NIST网络安全框架
4. GTAG 16 – 数据分析技术
5. 物联网
6. 灵活的风险与合规
7. ISO 14000（环境管理）
8. 数据分析工具 – 统计分析
9. 特定国家的企业风险管理框架
10. 大数据/商业智能

* 根据总体调查反馈

2016年首席审计执行官前十大优先关注事项

1. 大数据/商业智能
2. ISO 31000（风险管理）
3. ISO 9000（质量管理和质量保证）
4. GTAG 17 – 信息技术治理审计
5. 持续监督
6. 企业文化审计
7. 在企业内部宣传内部审计
8. 质量保证与改进程序
9. 舞弊 – 管理/防范
10. 信息技术审计 – 持续性

更多信息，请登录 Protiviti.com / IA Survey。

protiviti®
Face the Future with Confidence
甫瀚

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，帮助企业解决财务、信息技术、运营、治理、风险管理以及内部审计领域的难题。我们在20多个国家设有70多家分支机构，为超过60%的财富1000强及35%的全球500强企业提供咨询服务。我们亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。

甫瀚咨询荣幸地成为国际内部审计师协会（IIA）主要合作伙伴。超过700名甫瀚咨询专业人员是IIA的活跃会员，这些会员与IIA所在地方和国家的机构领导积极合作，提供领先思维、演讲、最佳实务、培训及其他资源，从而帮助促进内部审计职业的发展。

甫瀚咨询荣膺《财富》杂志2016年最佳雇主百强第57位，是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

内部审计和财务控制

不论客户公司如何、属于上市公司还是私营企业，我们都十分乐意配合其行政高管人员、管理层及审计委员会开展合作，协助执行内部审计工作。我们不但能够以完全外包的方式，协助公司启动和执行内部审计工作，也可以与公司现有内部审计部门合作，在内审团队人手不足或技能缺乏时，担当起有力的支持后盾。我们的专业人员已成功协助上百家公司制定了《萨班斯-奥克斯法案》首年合规计划，并帮助他们开展持续的合规工作。我们更能够协助公司采用以流程为基础的方案来执行财务控制合规工作，从而寻求提高工作效率、减轻工作负荷的有效途径，例如执行有效的风险评估、界定合适的审计范围，以及使用技术辅助手段。如此一来，客户的合规成本也将得以降低。我们拥有丰富的经验，已为数以百计的客户完成多项独立、专门的财务和内部控制咨询及控制检查服务项目，其中有些是一整套内部审计工作中的一部分，有些则作为独立的项目予以实施。在项目执行的整个过程，我们均会按照客户的要求，向其董事会、审计委员会或管理层直接汇报。

甫瀚咨询并非一间会计师事务所，这是我们重要的特征之一，使我们能够处在完全独立的立场为客户提供服务。甫瀚咨询可以调用所有的顾问来开展内部审计项目，这使我们得以随时为客户配备精通各种职能和流程领域的专家。此外，甫瀚咨询可以为公司的内部审计职能实施独立评估。根据国际内部审计师协会相关标准的要求，公司须每五年开展一次这样的评估。

我们所提供的服务包括：

- 内部审计外包与分包
- 财务控制与《萨班斯-奥克斯法案》合规
- 内部审计质量评估和转型
- 审计委员会咨询

甫瀚咨询 · 大中华区

北京

中国 北京 100004
朝阳区建国门外大街1号
国贸写字楼1座718室
电话:（86.10）8515 1233
传真:（86.10）8515 1232

上海

中国 上海 200020
黄浦区淮海中路381号
中环广场2618-38室
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1座1404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2103-04室
电话:（852）2238 0499
传真:（852）3118 7493

www.protiviti.cn
www.protiviti.com

protiviti®
Face the Future with Confidence
甫瀚