

2009 年 9 月

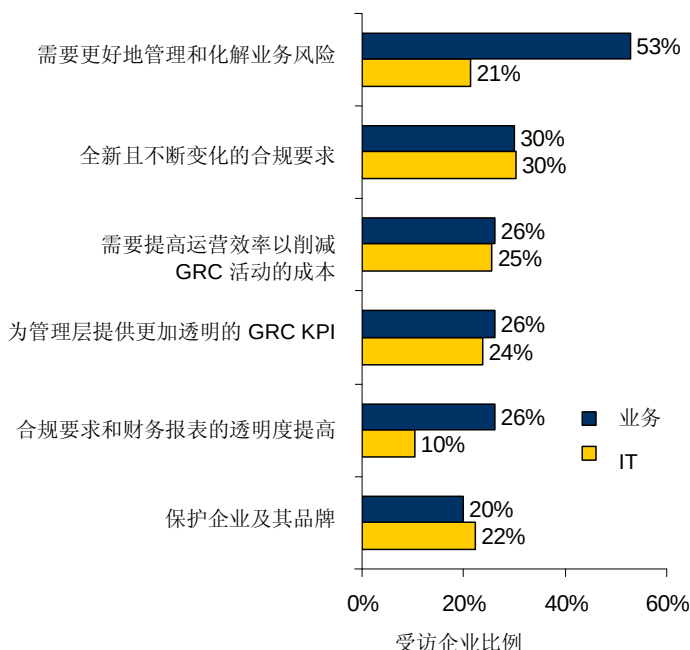
GRC 战略—找出业务和 IT 之间的最佳平衡点

日益繁杂的法规要求、透明度的需要以及更好地管理和消除风险的愿望等多种因素，使得监管、风险和合规 (GRC) 成为业务和 IT 高管的头等大事。业务性质的日益复杂和千变万化常常使高管们感觉到自己就像在掌控一艘即便抛了锚也不平静的船。此外，变化的节奏也不断加快，使得这艘船成了一艘需要不断修正飞行速度的宇宙飞船。企业人士对如何恰当地进行职责划分 (SoD) 并对关键的信息资产进行访问控制感到压力重重。业务经理和 IT 安全经理必须共同协作，并不断控制访问和授权，防止欺诈和错误，同时又要要有清晰的透明度，因为这是企业具备充分监控能力、以确保其赢利和合规的前提。

风险及合规推动业务转型

多重压力促使业务向 GRC 促进型转变。

图 1：两大压力



来源：Aberdeen Group，2009 年 5 月

分析师点评

Aberdeen 视点为您提供了解析师从调查研究、访谈和数据分析中所得出的综合观点。

定义

- ✓ **监管**是指用于业务决策和管理的框架、政策、规程、控制、决策级别等
- ✓ **风险管理**是指发现、依次排列和消除对组织有潜在影响的风险
- ✓ **合规**是指在既定的时限内达到并保持政府法规、行业规则和内部制度的要求
- ✓ **IT GRC**是指与组织所使用的 IT 技术有关的统一、综合和内部关联的监管、风险管理和合规方法
- ✓ **企业风险管理**是指整个企业的风险评估和战略管理

业务和 IT 经理通常有不同的想法。图 1 同时揭示了业务经理和 IT 经理所感到压力的相似之处和不同之处。上页图表显示，在 IT 经理看来，没有一个因素是主导性的；而业务经理则认为，更好地管理和消除业务风险是显而易见的主导因素。这些业务风险通常分四大类：*财务、战略、运营和其他类*，而 IT 经理则很少直接将这些风险联系起来。不过，IT 在解决众多重要风险因素中具有根本性和基础性的作用，而且无论哪个企业，其业务的各方面都离不开 IT 的支持。IT 监管、风险管理和合规 (IT GRC) 的重要性的日益提高反映出人们对 IT 战略价值的认识不再仅仅局限于技术本身，而且还包括如何最有效地加以应用和管理。从图 1 可以很明显看出，在一流企业的首席信息官 (CIO) 和 IT 管理层能够更加清晰地了解企业业务状况的同时，很多人仍然没有承认和意识到自身在管理和消除风险以及提供合规和财务报表的透明度方面所应当起到的作用。

相应的行动

尽管业务和 IT 高管感受到的压力可能各不相同（图 1），不过制定一个综合性的“持续性”合规架构的总体策略则明显异曲同工。然而，这两个不同的部门通常对于 GRC 和 IT 支持之间的联系并不十分清楚。一流企业的某些特性（包括流程和控制的集中化和自动化）反映了这样一个事实，即其目标不仅仅是很好地解决自身的合规、监管或风险管理的问题，而且还要更为有效地发挥 IT 在支持实现业务目标和管理财务、战略和运营风险方面的作用。

例如从为用户提供访问企业应用和/或其中的敏感数据权限的简单流程（概念上）来说，通常这种访问权限是专门基于角色和职能分配的。用户可以根据当前的职位获得许可，并访问应用程序和数据。如果该用户被分配为其他角色或分配到其他部门而使访问级别发生改变时，能否保证现在将其删除呢？事实上，当员工离开企业时，能否确保有删除该用户访问权限的流程呢？提供流程的自动化程度越高，需要承担责任的可能性就越低。有 70% 的一流企业对主要的自动化控制功能和流程实现了集中管理，而其他企业（非一流企业）则只占到 22%。

一流企业的特质

有效的战略执行可以实现更好的合规和促进业务转型。通过在组织内部的所有适当层面上进行技术和内嵌 GRC 的整合，运营成本和 GRC 成本都能得到削减。

一流企业标准

- √ 找出现有风险管理流程中的缺点
- √ 能够将风险管理评估数据转变为可付诸行动的建议
- √ 适应新规则要求的灵活性

表 1：业务和 IT GRC 的竞争性框架

	一流企业	业内平均企业	落后企业
政策和流程	建立并推行一致的 IT 风险及合规管理政策和规程（在所有地区和业务部门）		
	72%	49%	45%
	正式的职责划分		
	67%	33%	29%
	对业务和 IT GRC 活动采取“持续改进”的方法		
	55%	28%	24%
组织	对 IT GRC 活动负有主要责任的高管或团队		
	85%	55%	49%
	支持工作流程、风险管理和合规控制以及沟通渠道的正式组织架构		
	58%	35%	33%
监控和衡量	一致的流程优先性评估，以确保大多数重要的合规流程能经常受到监控		
	61%	33%	29%
	一致的流程优先性评估，以确保大多数与财务有关的风险管理流程能经常受到监控		
	39%	35%	19%
	一致的监控，以确保技术控制的政策导入和审计结果能够实现且准确		
	55%	24%	20%
	对合规管理、审计和报告解决方案结果的定期核查		
	58%	31%	29%
	对历史风险管理数据的常规分析，以发现异常情况		
	58%	28%	14%
	职责划分监控		
	76%	31%	26%

来源：Aberdeen Group，2009 年 5 月

政策和流程

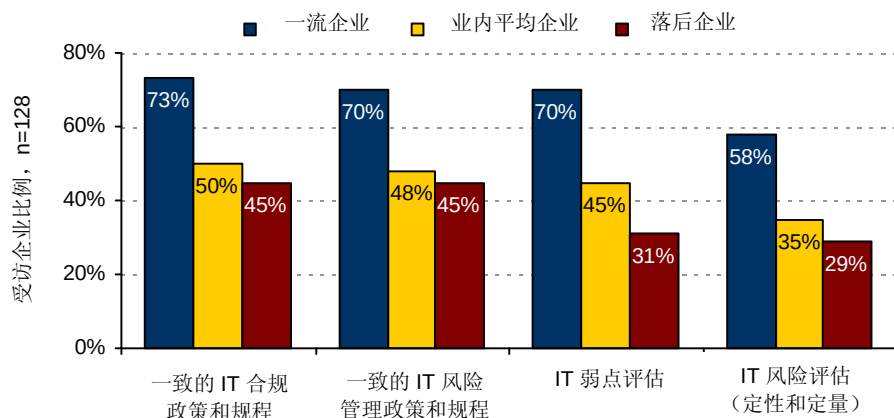
一致的合规和风险管理政策是 GRC 战略成功的基础。没有这些政策，高管们的宇宙飞船就会迷失方向，消失在茫茫宇宙中。正式的职责划分是这些政策的核心，不过还需要对访问控制进行严格的掌控。这些职责的制定是一项业务决策，而应用程序及其数据的访问则需要发挥 IT 的作用。从访问申请到批准和文件记录的授权流程自动化程度越高，就可以在不牺牲安全性和控制的前提下实现更高的成本效率。一致的政策和规程，再加上对弱点和风险的定性和定量两方面的定期评估，是一流企

“从访问申请到批准和文档记录，SAP BusinessObjects Access Control 和 SAP NetWeaver Identity Manager 几乎实现了整个授权流程的自动化，从而帮助我们节省了投入。”

~ Reinhard Falke
业务流程及 IT 总监
Vibracoustic GmbH & Co. KG

业 GRC 战略的鲜明特点（图 2）。对这两方面进行一致和常规评估的一流企业至少是落后企业的 2 倍，由此可以看出这并不是一项简单的工作。

图 2：一致的政策；定期评估



来源：Aberdeen Group，2009 年 5 月

组织方面

由于弱点和风险管理的内在困难性，因而更加需要建立这些企业内部重要活动的基本负责制。Aberdeen 各方面的数据都得出了相同的结论：管理层重视和高管负责制是一流企业的主要特征：85% 的一流企业为企业的 IT GRC 活动指定了主要责任高管或团队。此外，在终端用户培训的投入方面，好、坏消息并存。好消息是：对企业政策、实践和道德表现预期方面的沟通手段进行投入的一流企业数量是落后企业的 1.7 倍左右。坏消息是：仅有约 2/3 (64%) 的一流企业目前进行了这方面的投入。

在较为成功的 IT GRC 活动中，组织架构在 workflows、问题上报和问题解决方面是相互关联的（图 9）。一流企业通过沟通和明确企业对于可接受的风险参数的看法，对赋予各个员工的职责和授权给予支持。这些最佳实践对于集中化和自动化都较低的大多数早期 GRC 活动是否更为重要尚无定论，尽管研究显示，职责分散及沟通不畅通常是相伴而生的。

技术还可以成为加强组织内部联系的催化剂。GRC 和 IT GRC 并非两个互不相干的问题。通过采用共同的平台，IT 和业务部门的专业人员可以阅读同一页文件的内容，使用数据和信息相同的语言进行交流，从而有助于消除组织内部的鸿沟，并支持内部协作。

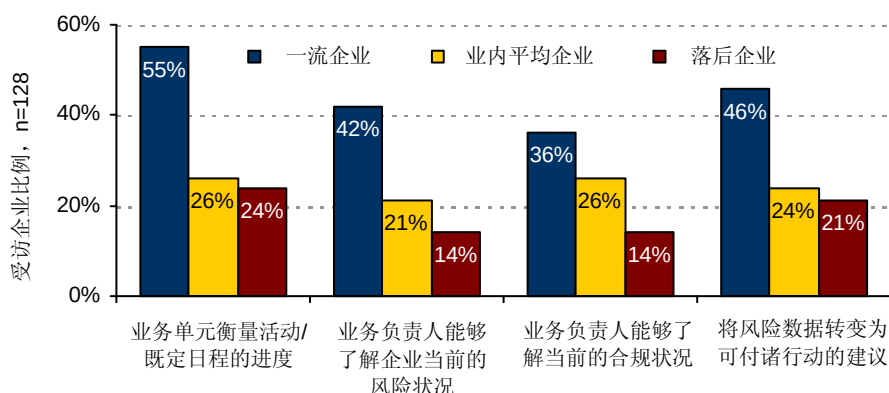
一流企业 GRC 活动的负责人通常为最高层人员，即大多数一流企业的相关领导或主要负责人都是 CEO、首席合规官、CIO、CFO、CTO、

首席风险官或 COO。在所有受访人员的反馈中，GRC 活动的领导和作用情况各异。有趣的是，研究显示，一流企业的 GRC 活动的预算决策权主要是在 CIO 和 CEO 层面—而非 CFO，并综合最高级别的业务和 IT 负责人的意见。

衡量和监控

了解当前的风险和合规状况、针对已制定的战略日程的进展以及将风险数据转变为可付诸行动的建议（图 3）是真正需要加以“监管”的地方。

图 3：增强透明度及可付诸行动的建议



来源：Aberdeen Group，2009 年 5 月

我们要求受访人员对过去 12 个月以来企业所经历的与 IT 监管、风险管理和合规有关的多个方面的变化程度进行估计。表 2 列举了一流企业与业内平均企业和落后同行相比，其 GRC 活动在为企业提供更高透明度以及为决策提供更多信息方面所带来的某些优势。从表 2 中的发现可得出如下主要结论：

- 在风险发现、评估和主次排列能力方面，一流企业的收获更大
- 一流企业的风险管理活动能够让管理层更好地接触和了解当前的风险状况，并与主要利益相关者更好地沟通风险方面的情况
- 一流企业能够更好地将风险评估数据转化为可付诸行动的建议，从而加快了决策速度
- 在与合规相关的跟踪和报告方面，一流企业显然比其他企业做得更好，而且在适应新法规要求方面也更加灵活
- 一流企业的合规活动能够让管理层更好地接触和了解当前的合规状况，并与主要利益相关者更好地沟通合规状态方面的情况

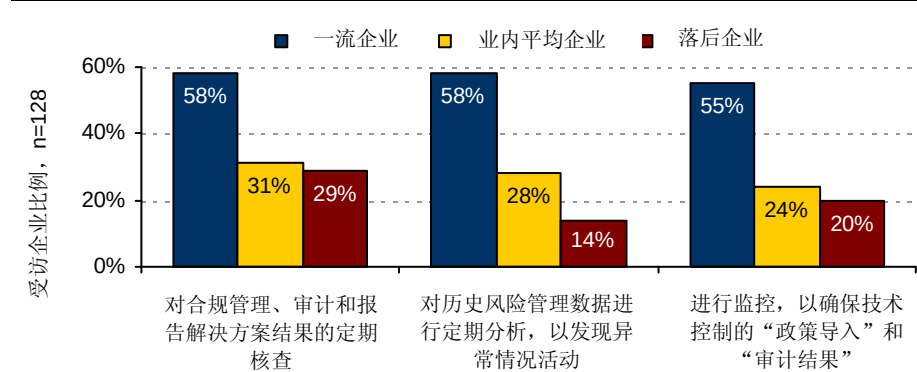
表 2：透明度的平均年比变化

风险管理和合规能力	一流企业	业内平均企业	落后企业
能够清晰、及时地与股东和董事会沟通风险情况	8.9%	4.9%	0.7%
能够在更好地了解当前风险极限的情况下，迅速作出重要业务决策	9.8%	4.8%	-2.0%
合规跟踪和报告的效率	12.0%	7.5%	1.9%
适应新法规要求的灵活性	11.5%	4.8%	0.0%
管理层能够掌握企业当前的合规状况	12.2%	5.0%	1.0%
就当前合规状况与董事会和股东进行沟通	9.3%	4.8%	0.1%
由于能够更好地了解企业当前的合规状况，从而可以迅速作出重要的业务决策	8.9%	4.9%	-0.8%

来源：Aberdeen Group，2009 年 5 月

一流企业不仅在情况搜集方面是其他企业的两倍，在核查和分析所搜集的情报方面也是如此（图 4）。近 3/5 (58%) 的一流企业能定期核查、审计和报告合规和风险管理解决方案的结果，而相比之下，其他企业还不到 1/3。

图 4：定期监控、分析和核查



来源：Aberdeen Group，2009 年 5 月

技术能力

在监管和合规情况下加强商业决策依据的需求以及受企业风险容忍度的限制，最终会使企业对一种或多种专项技术进行评估、选择和部署。这些选择（包括实施的政策、规划、流程和组织要素）对于企业能否成功地把握好业务决策和 IT 决策的平衡至关重要。

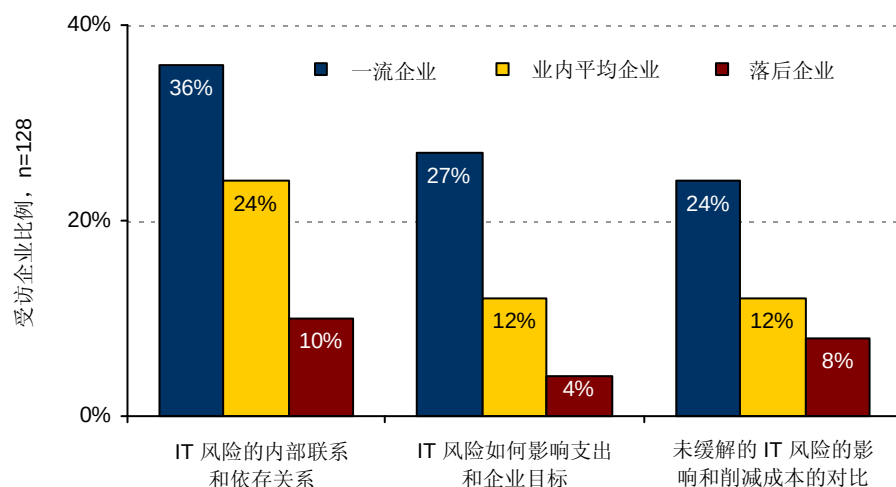
“我们最早的 IT 监管会议极其耗时，因为信息准备主要依靠人工进行。而讨论基本上也是主观性的，比如对于更快完成日本子公司结账的 SAP 项目以及改善与增值经销商之间交易环节的安全网络端口项目这二者哪个更为重要。不过我们还是成功地让公司的业务领导介入到思考中并共同参与到战略、财务、运营、合规和风险事务当中。这已经是而且仍将是 IT GRC 的真正胜利。”

~ 某中型高科技企业 CIO

多种旨在保证 GRC 活动持续性的工具陆续出现。安全性、流程控制和访问控制是首要问题。不过，分析和商务智能能力在为企业当前合规状况和各种风险参数状况的透明信息方面也具有重要作用。在监控和验证内部政策和外部规范要求方面所能实现的控制手段自动化程度越高，就能削减更多的成本。

建立内部联系及 IT 风险之间依存关系的模型、了解它们对预算和企业目标的影响，以及对消除风险的有关成本和好处进行假设性分析的能力，都是最新出现的方法，但它们的使用比例在表现最好的企业中要高得多（图 5）。我们在与选定调查对象的单独访谈中发现，大多数企业的决策层目前需要对此进行开放式讨论、凭直觉感知并最终形成判断，尽管所有人都对分析功能更强的方法的吸引力很快表示认同。

图 5：建立风险、依存关系、成本和目标的模型



来源：Aberdeen Group，2009 年 5 月

用企业级数据仓库来保存所有有关控制和既定规程的适用合规法律和法规以应对法规的修改，这已经超越了初级阶段，而反映自己具备这种技术能力的一流企业占到了 58%，明显超出其他企业 34% 的水平。与之相似，55% 的一流企业拥有所有风险和风险相关信息的统一集中的数据共享平台，而其他企业只占到 26%。我们还发现了另一项显著差别，大多数 (76%) 一流企业具备了保存可追溯审核记录的能力，从而能够为分析、审计、报告或调查提供相应支持，其在这方面是业内平均企业和落后企业的 2 倍之多。

不过为了更加清晰、准确和完整地掌握情况，通常需要将零散的合规数据整合成一个根据角色定制的综合视图或高管指示板。具有这方面能力的一流企业仍然是其他企业的 2 倍多，不过仍有很多可以改进的余地，因为只有 30% 的一流企业有这方面的投入。

案例聚焦：Valero 能源公司

Valero 能源公司是位于美国德克萨斯州 San Antonio 的财富 500 强企业。Valero 拥有庞大的炼油系统，日产能力将近 300 万桶。公司的炼油设施分布在美国、加拿大和阿鲁巴岛，并拥有管道和码头等中转物流系统。Valero 还拥有约 5,800 多个本品牌的零售和批发站点。Valero 的员工约有 22,000 人，总资产达 370 亿美元。作为北美地区最大的炼油厂，Valero 经过不断地兼并，目前的年销售收入已经从 1997 年的 50 亿美元上升到 2008 年的 1,100 亿美元。

Bill Weber 是 Valero 公司的 SAP 经理，负责 SAP 的财务应用和 GRC 事务。他和公司的 Sarbanes-Oxley 合规副总裁 Jack Ligon 从目前 SAP GRC 应用系统投入伊始便一同合作，而首次合作始于一个旨在解决职责划分 (SoD) 问题的项目，这些问题是在 Valero 推行其 SOX 404 内部控制程序时发现的。“我们怀疑自己的问题和很多企业有明显不同。员工加入公司后，便拥有访问数据和功能的权限。当他们进入角色并逐步成长后，就需要更多的访问权限。然后他们可能会被调换到公司的其他岗位。在某些情况下，他们保留了现有的访问级别，并升入新的级别。最终有些人则余留了一些不再需要的访问权限，包括某些相互冲突的活动... 因而造成了 SoD 问题。” Ligon 这样认为。

当 Valero 开始寻求解决这些问题的良方时，曾考虑过各种方案。“我们曾考虑过开发自己的 SoD 矩阵，但我们意识到这要花费大量的精力，而且很容易出现遗漏。” Webber 说。“因而我们选择采用 SAP BusinessObjects Access Control。”

Ligon 继续解释道，“通过 Access Control 和其他 SAP 工具，我们分析了用户的访问要求，并设计了全新的 SAP 角色，从而大大减少或消除了 SoD 冲突。所有用户的现有访问功能均予以取消，并代之以新设计的角色。我们找到了缓解控制方法来解决绝大多数仍然存在的 SoD 冲突，而我们的外部审计机构也认为，年底时的残留冲突并无大碍。所有冲突最终都得以消除或缓解，而我们现在每天都运行 Access Control 报告，以显示没有未消解的 SoD 冲突。”

Valero 首先从 SAP 所产生的 SoD 规则集合入手。Weber 说：“这些（规则集合）是一个很好的开始。它们比我们自己创建的内容更为全面。不过最终，我们的 SoD 规则集合应当具有 Valero 的特色。因此我们通过取消那些对于 Valero 来说风险相对较低的 SoD 规则，从而对此进行吸收和发展。此外，我们对与 Valero 有关的所有最新的 Access Control SoD 规则集合进行了评估。例如，我们最近取消了与巴西银行交易代码有关的 SoD 规则，因为我们在巴西没有业务。”

Valero 还应用了其他 Access Control 模块为用户提供相关权限，从而使 Valero 能够评估在对 SAP 的安全性进行改动之前，新的用户访问请求是否会造成 SoD 冲突。其他模块可以允许可能需要进行系统维护的临时性升级访问。Valero 同时还开始使用了 SAP NetWeaver Identity Management。

“我不认为有人会把它当成
“一次性”买卖。业务是在
不断变化的。”

~ Jack Ligon
SOX 合规副总裁
Valero Energy Corporation

关键提示

在平衡 GRC 活动的业务和 IT 前景方面，一流企业取得了巨大进步，这为其带来了战略和运营两方面的好处，包括：

- 在风险发现、评估和主次排列的能力方面年比取得重大进步
- 让业务负责人更好地访问和了解当前的风险状况
- 与主要利益相关者更好地沟通风险和合规状态方面的情况
- 更好地将风险评估数据转化为可付诸行动的建议，从而加快了决策速度
- 在与合规相关的跟踪和报告方面年比取得重大进步
- 适应新法规要求的灵活性更强

Aberdeen 目前的研究成果显示，业务和 IT GRC 活动的相关性在不断加强，直接原因在于其能够更有效地应用和管理 IT，从而为企业带来最大的战略价值。对于所有正在寻求转变业务流程以削减成本、提高监管及合规，并消除和管理风险的所有企业，我们有如下建议：

- 在 GRC 方面进行持续改进。
- 整个企业范围内的运营标准应当一致并强制实行。对 IT 流程采用与财务控制相同的尽职和控制水平。
- 确认安全性和访问控制以得到有效管理和保持。有效监控并控制用户使用权限的提供，且更为重要的是，在员工调整岗位或角色亦或离开公司时，需要取消访问权限。这些流程的自动化程度越高，安全危害的可能性就越低，从而更可能降低成本。
- 有效利用分析和 BI 工具进行衡量和监控，以清晰了解监管、风险和合规的状况。

更多有关本文或其它研究课题的内容，请访问 www.aberdeen.com。

相关研究

<u>IT GRC: 《管理风险、提高透明度和降低运营成本》</u> ; 2009 年 5 月 <u>《统一 GRC 解决方案, CFO 们准备好了吗?》</u> ; 2008 年 4 月	<u>《您的 GRC 战略是否具有智能? 整合分析功能, 实现准确、实时的透明度和决策》</u> ; 2008 年 7 月 <u>《SAP 的统一 GRC: 困惑时期的全盘答案》</u> ; 2009 年 3 月
作者: Cindy Jutras, 研究发展部副总裁兼研究员 (cindy.jutras@aberdeen.com)	

自 1988 年起, Aberdeen 的研究成果帮助世界众多企业迈入了企业行列。通过对 644,000 多家企业的绩效研究, Aberdeen 在为企业提供发展精要方面独树一帜, 这些成果是企业领先他人并获得成功的法宝。这就是我们的研究成果吸引了全球 40 多个国家的 220 万读者的原因, 他们中有 90% 是财富榜 1,000 名的企业, 93% 是科技 500 强企业。

作为 Harte-Hanks 旗下的公司, Aberdeen 在为全球化营销公司出谋划策方面发挥着重要的作用。Aberdeen 的分析及独特的 Harte-Hanks“客户优化”流程观点(信息—机会—洞查—接触—交流)延伸了客户价值, 并突显出 Harte-Hanks 作为市场策略者的形象。更多内容请访问 Aberdeen 公司网站 <http://www.aberdeen.com> 或致电 (617) 723-7890; 如欲了解 Harte-Hanks 的更多内容, 请致电 (800) 456-9748 或访问 <http://www.harte-hanks.com>。

本文为 Aberdeen Group 的基本研究成果。Aberdeen Group 以客观事实为依据进行研究工作, 并提供最符合当时出版情况的分析结果。除非另有说明, 否则本出版物的全部内容属于 Aberdeen Group, Inc. 的版权, 任何人未经 Aberdeen Group, Inc. 书面许可, 不得擅自复制、散布、存档或以任何形式进行传播。