从网络安全走向协同合作：评估内部审计职能的优先事项

2015年内部审计能力与需求调查报告（精辑版）

protiviti®
甫瀚
风险与商业咨询。
内部审计。

Powerful Insights. Proven Delivery.®
敏于知　达于行

> 安全性，对我而言，是最重要的。我们借助计算机能够完成各种激动人心的事情，譬如安排日常生活、与朋友保持联系，一切都那么富有创造力——但是，如果我们不能解决安全问题，那将极大阻碍这一发展。
>
> — 比尔•盖茨

前言

2015年会重蹈2014年的覆辙，成为数据泄露事件泛滥的一年吗？不同规模的组织机构都正经历许多因网络安全问题所带来的挑战和入侵等麻烦事，信息技术（IT）部门对此显然承担主要职责。同时，内部审计人员通过与执行管理层和部门负责人紧密合作，确保日常业务流程中包含网络安全管理，也能够在保证组织运营安全方面扮演十分重要的角色。

在今年的内部审计能力和需求调查报告中，我们对网络安全风险的现状进行了专题阐述。调查结果发现，网络安全是企业内部审计计划中一个主要的关注点，但它远不止是内部审计职能中唯一紧迫的问题。

- **董事会的参与以及审计计划是有效网络安全管理的关键。**提到网络安全，表现最为出色的企业同时具备两个特点：董事会的高度参与并在年度审计计划中定义了网络安全的措施。
- **内部审计职能的优先级事项进一步增多。**网络安全问题，与新技术相关的风险（如社交媒体、云计算和移动应用），不断增加的监管合规需求，国际内部审计师协会（IIA）、ISO和COSO的新指引和新标准——这些和其他优先事项要求内部审计部门在帮助组织机构日益增长的发展需求时能更加灵活应变。
- **技术促使审计工作效率提高。**从冗长的事项清单上，优先处理紧急事项促使更多内部审计部门加大审计方法和工具的投入和利用。
- **更多关注于市场和合作。**内部审计主管和员工比之前更加关注于向组织机构内其他部门传递职能任务、价值以及与风险有关的关注点。他们也欲作为战略伙伴加强与执行管理层、其他职能部门主管和董事会的合作，从而帮助组织机构明白他们的风险并实现他们的战略目标。

我们真诚地感谢参与我们今年调研课题的800多名首席审计官和内审专业人士。我们也十分感激他们为此所付出的宝贵时间。最后，我们再次鸣谢国际内部审计师协会为推动当今商业环境下内部审计职能角色的发展所做出的贡献。

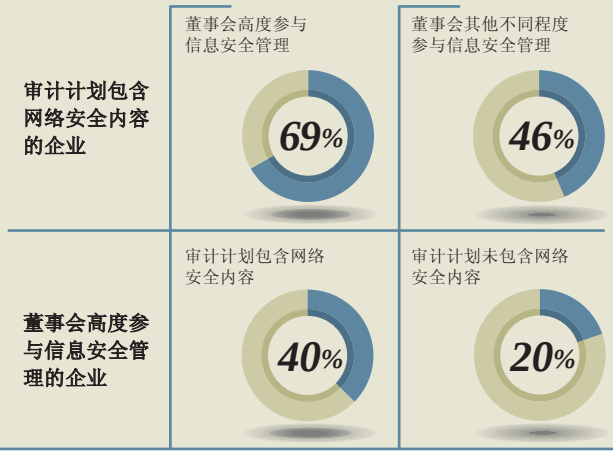
[1]《与比尔•盖茨一对一》，ABC新闻，2015年2月16日，www.abcnews.go.com/WNT/CEOProfiles/story?id=506354&page=1。

内部审计人员如何看待网络安全

2015年会重蹈2014年的覆辙，成为数据泄露事件泛滥的一年吗？

组织机构正经历许多网络安全挑战和侵袭的麻烦事。内部审计部门确保企业日常的业务流程中已包含网络安全管理，从而在保护组织安全运营方面扮演一个至关重要的角色。

董事会的参与程度和审计计划是网络安全管理是否有效的关键因素



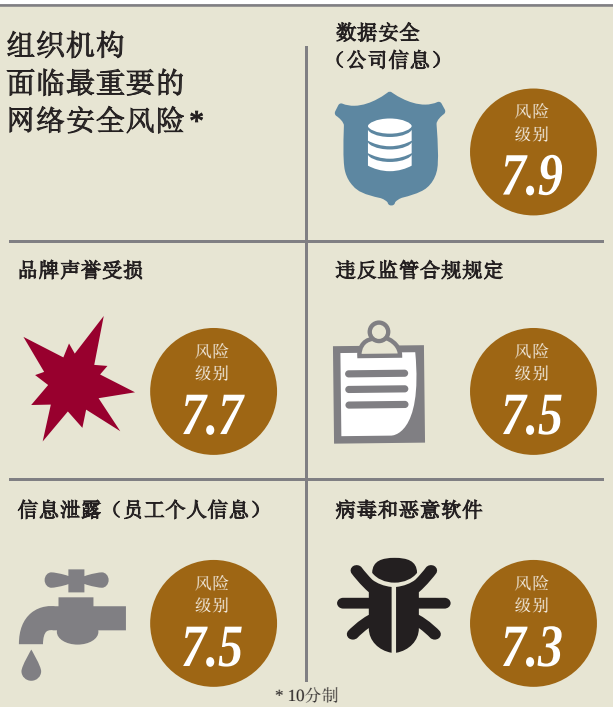
组织机构评估自己识别、评估和降低网络安全风险到可接受水平的能力“十分有效”。

	董事会高度参与的企业	董事会其他不同程度参与的企业	审计计划包含网络安全内容的企业	审计计划未包含网络安全内容的企业
识别	47%	19%	35%	20%
评估	43%	19%	31%	21%
降低	39%	15%	26%	18%

组织机构制定网络安全风险战略和相关政策

	董事会高度参与的企业	董事会其他不同程度参与的企业	审计计划包含网络安全内容的企业	审计计划未包含网络安全内容的企业
战略	75%	48%	70%	42%
政策	66%	46%	65%	39%

组织机构面临最重要的网络安全风险*



* 10分制

访问**protiviti.com/IAsurvey**，浏览《2015年内部审计能力和需求调查结果》的完整报告。
该报告还列出了针对首席审计官和不同组织规模的调查结果。

网络安全和审计程序专题报告

公司和个人机密信息，都处于受到外部网络攻击和内部员工或供应商剽窃的风险之中。

— 某中型保险公司首席审计官

主要发现

- 只有少于三分之一的组织机构，判断其在网络安全风险管理上达到“十分有效”的可接受水平。由此可见，网络安全风险管理的改进需求非常明显。
- 那些将识别网络安全风险列入审计计划，并且董事会能够积极参与到网络安全风险管理的企业被评为“表现突出”。
- 公司信息的安全性问题、品牌和声誉的损害、监管合规以及员工个人信息泄露等，这些事项均表明网络安全存在重大风险。

网络安全所引发的事件，所产生的影响和发生的频率都在持续攀升。实际上，那些被公开报导的网络攻击事件只是冰山一角[2]。因此，首席审计官和内审专业人士需要考虑的一个重要问题是：审计人员就网络安全问题应扮演的角色和承担的责任到底有哪些？

网络安全风险日益上升的重要性在今年的调查报告结果中得以佐证。内部审计主管和专业人士认为加强数据安全，遵循美国国家标准与技术研究院网络安全基础框架（NITS Cybersecurity Framework）提高网络安全的关键基础设施，掌握数据分析的新方法和审计技术应放在最优先的地位。我们在与首席审计官和内部审计主管的持续沟通中收到类似的反馈，意料之中的是，他们表示对网络安全和数据保密的议题有极大的兴趣。甫瀚咨询近期的其他研究[3]表明，同时美国董事协会[4]亦强调，网络安全已是董事会、执行管理层和内部审计部门议程上一项重大风险。

在本报告中，从网络安全和团队领导角度，我们评估了组织机构中网络安全风险的现状，识别了有效的网络安全风险管理能力的关键组成，同时揭示出一些区别和差异。我们总结了10条首席审计官和内审专业人士应考虑如何加强网络安全的行动措施建议。

[2] 《董事会视角：风险监督——管理网络安全风险》第44期，甫瀚咨询发布：www.protiviti.com/en-US/Pages/Board-Perspectives-Risk-Oversight-Issue-44.aspx。

[3] 参见ISACA及甫瀚咨询联合发布：《全球视野下的IT审计最佳方案》，www.protiviti.com/ITAuditSurvey；及参见甫瀚咨询发布：《跨越数据安全的鸿沟——甫瀚咨询2014年 度信息技术安全和查结果评估》，www.protiviti.com/ITSecuritySurvey。

[4] 《网络安全：董事会关注重点》，美国董事协会发表，2014 年，www.nacdonline.org。

致首席审计官和内部审计专业人士关于网络安全管理的10条行动措施建议
1. 与管理层和董事会共同商定网络安全战略和相关政策。
2. 寻求企业“十分有效”的能力，以识别、评估和降低网络安全风险到可接受水平。
3. 确认由于员工或商业伙伴的行为导致网络安全风险的威胁。
4. 增进与董事会的关系：a)加强董事会对网络安全风险的知识和意识；b)确保董事会始终高度参与网络安全工作，并且不断更新网络安全风险的内容变化和战略意义。
5. 确保审计计划中正式包含网络安全风险的内容。
6. 应与时俱进地理解新兴的技术和未来发展趋势，以及如何对公司和网络安全风险产生影响。
7. 根据美国国家标准与技术研究院的网络安全基础框架，评估企业的网络安全项目。一旦确认基础框架未能达到控制层级，则需要通过更多的诸如ISO27001和ISO27002的合规评估来加强保护。
8. 认识到关于网络安全的最强防范能力，是需要人力和技术安全方面的整合：包括教育、认知、警觉性、技术工具的互补融合。
9. 执行管理层需要优先考虑监控网络安全与网络事件响应，而一个明确的自下而上的逐级汇报机制有助于实现这个优先级。
10. IT/审计人员资源的短缺，代表了许多组织机构所面临的一个最重要的技术挑战，同时也成为有效应对网络安全风险的障碍因素。

网络安全管理“表现突出”的企业——董事会积极参与，审计计划列为网络安全管理重要关注点

通过对结果的分析，我们发现建立和维持有效的网络安全最重要的两个成功要素：

1. **董事会对网络安全管理的高度参与**
2. **评估网络安全风险列入当前的审计计划**

详细结果如下，同时可作为对网络安全调查结果进行讨论和分析的重要参考依据。

贵司董事会参与和业务有关的信息安全风险管理的程度如何？

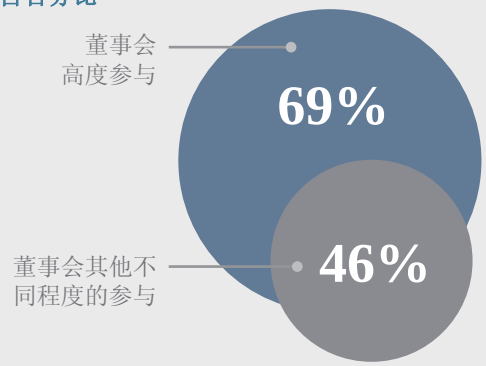
充分理解，高度参与	30%
一般理解，中度参与	41%
不太理解，较少参与	14%
不清楚	15%

评估和审计网络安全风险是贵司审计计划中的一部分吗？

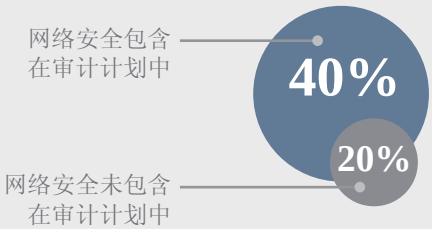
是的，已列入今年审计计划	53%
不是，但会列入明年审计计划	27%
没有计划将其列入审计计划	20%

关键因素

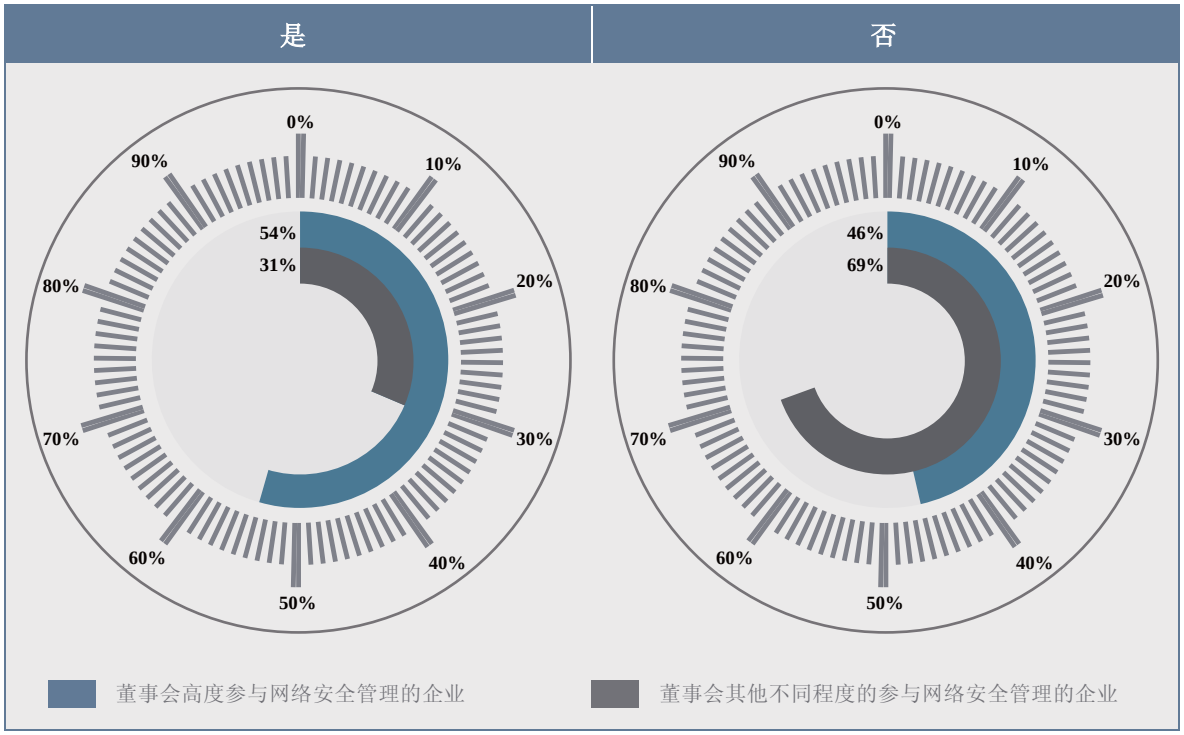
已在审计计划中包含网络安全审计的企业中，董事会不同程度参与信息安全风险管理的组织机构所占百分比



董事会高度参与信息安全风险管理的企业中，当年审计计划中是否包含网络安全的组织机构所占百分比



如果审计计划中已包含网络安全内容，贵司内部审计部门是否根据美国国家标准与技术研究院的网络安全基础框架评估组织机构的网络安全性？



网络安全的现状——一个内部审计人员的视角

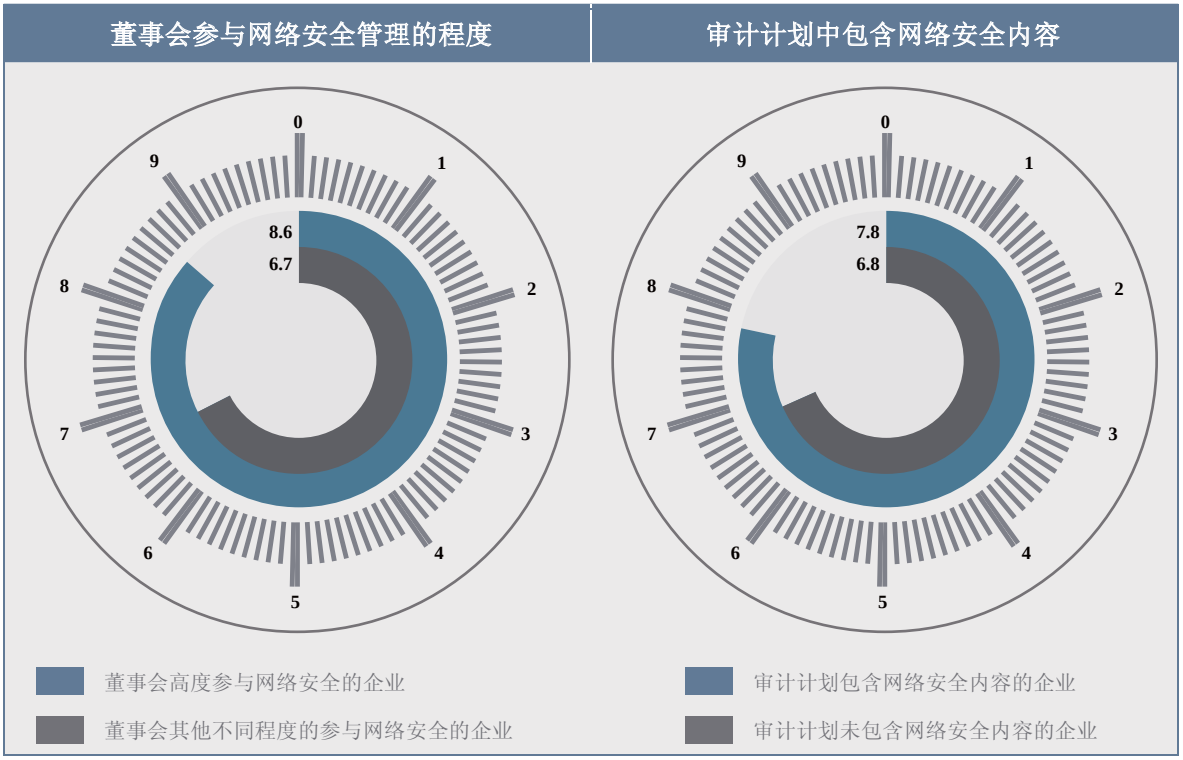
尽管“表现突出”的组织机构在这方面表现的更好，但是绝大多数组织机构对加强识别、评估和降低网络安全风险到一个可接受水平的能力有着明确的需求。

贵司评估自己识别、评估和降低网络安全风险到可接受水平的能力“十分有效”。

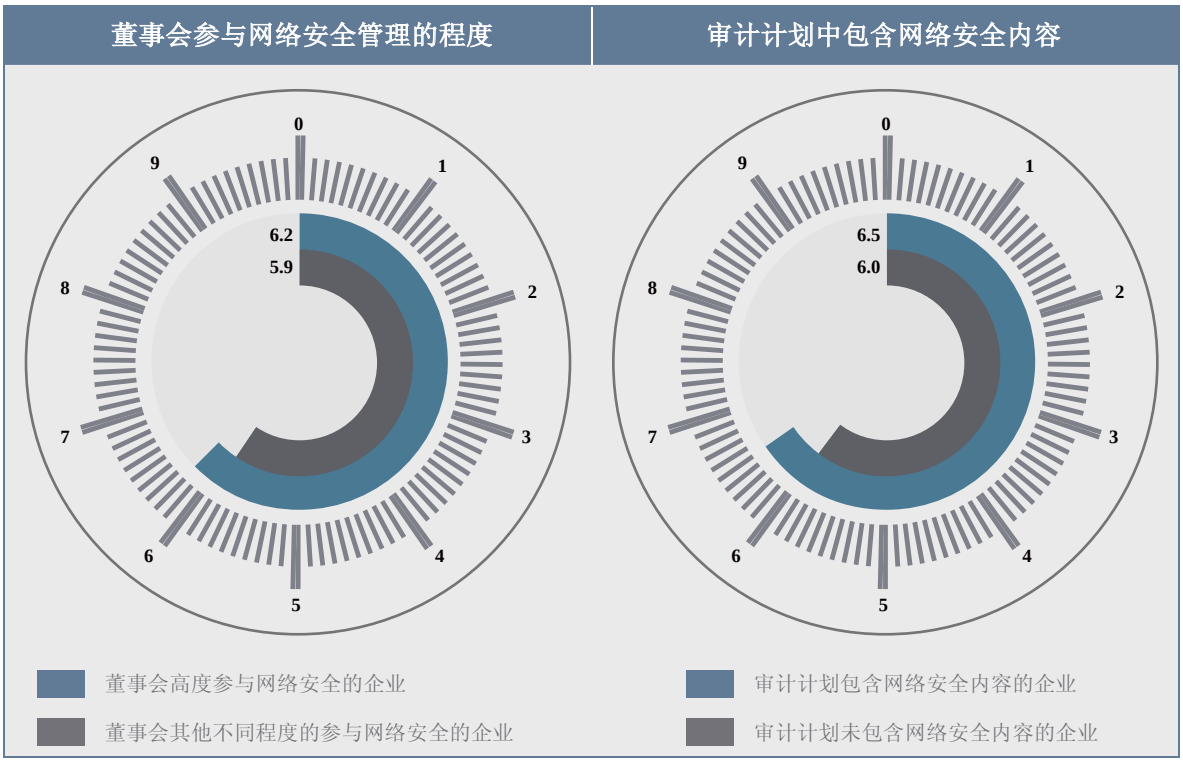
	董事会高度参与的企业	董事会其他不同程度参与的企业	审计计划包含网络安全内容的企业	审计计划未包含网络安全内容的企业
识别	47%	19%	35%	20%
评估	43%	19%	31%	21%
降低	39%	15%	26%	18%

对于企业信息安全风险的管理有相对较强的意识，尤其是“表现突出”的组织机构。然而，所有的调查对象对他们在预防员工或商业伙伴导致网络安全问题的能力上缺乏信心。（参见第5页图表）

受访者对高级管理人员就组织机构的信息安全风险意识进行评分，评分范围从1分到10分，其中“10”表示强烈意识，“1”表示没有意识。



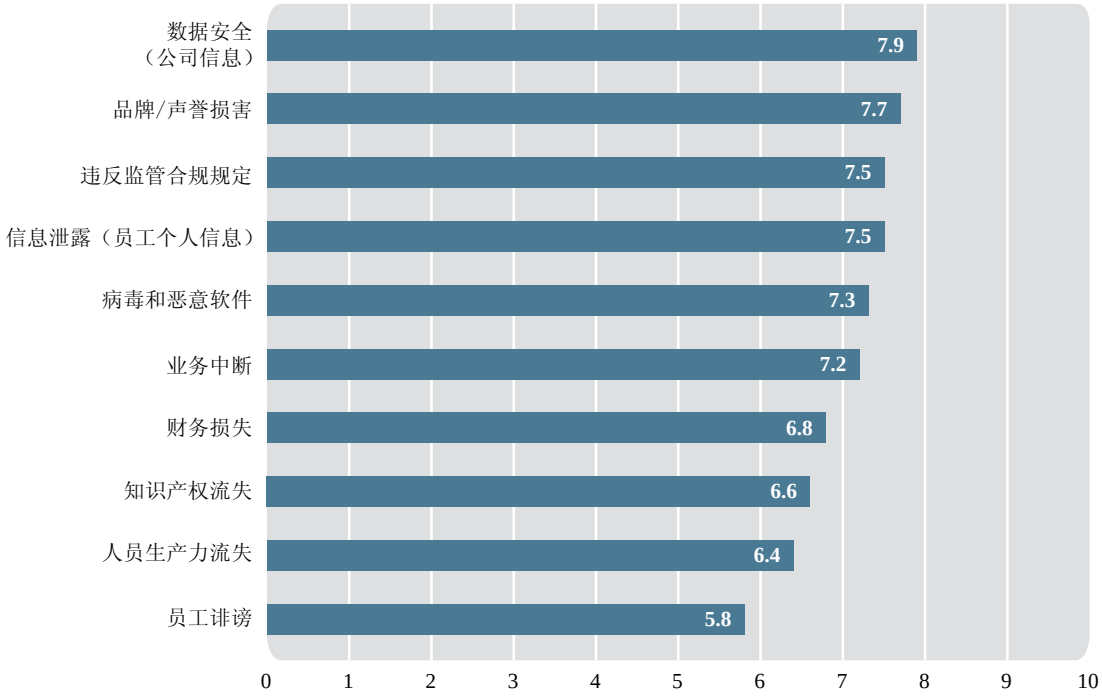
受访者对组织机构预防内部（员工或商业伙伴）行为造成违约可能的能力自信度，评分范围从1分到10分，“10”表示非常自信，“1”表示没有自信。



公司信息的安全性、品牌及声誉的潜在损害、监管合规与数据泄露，被视为最重要的网络安全风险。就应对网络安全风险的价值来看，组织机构能够尽早认识到他们识别问题、风险及内控问题的能力才是最重要的。

从以下几方面，对网络安全带给贵司的风险程度进行评分，“10”表示风险最高，“1”表示风险最低。

基数：全部调查对象



你认为目前网络安全风险管理对贵司哪方面的价值最大？

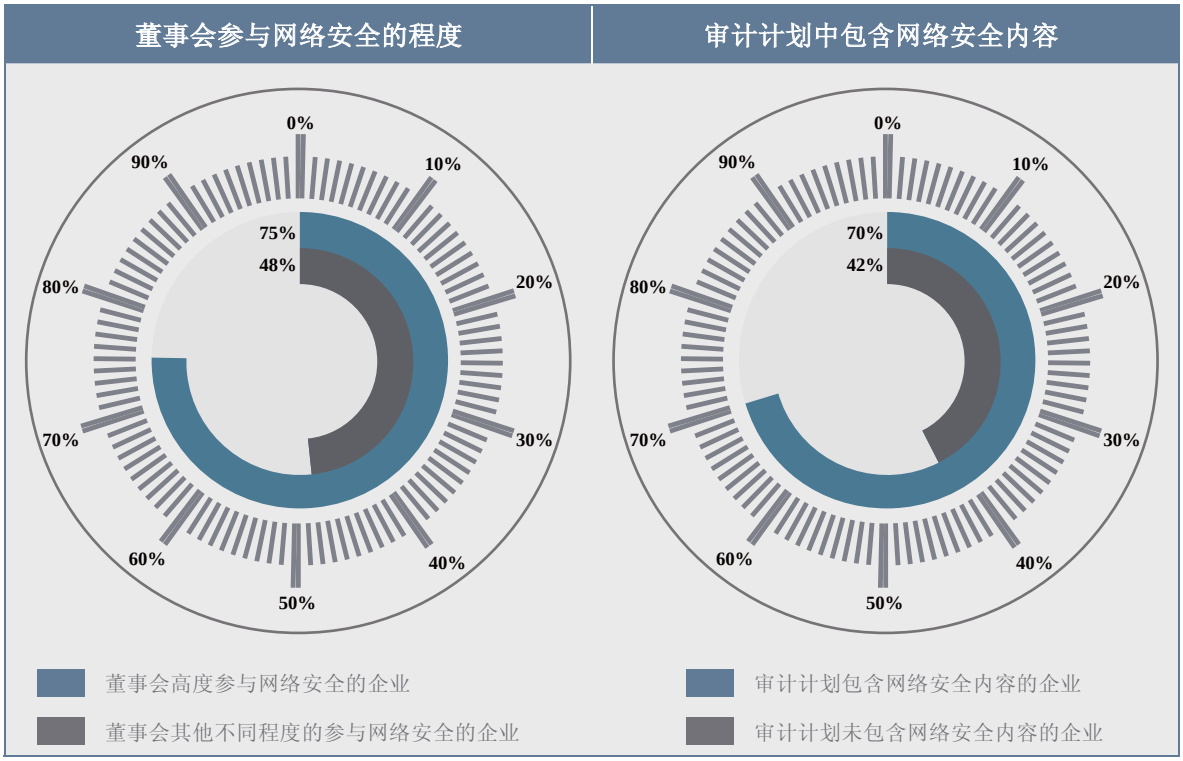
基数：全部调查对象

尽早的识别重大事项、风险和内控问题	40%
监管合规	16%
监控公司声誉风险	15%
整体商业战略	11%
验证内控的有效性	10%
改善运营绩效	5%
成本回收/节约	3%

评估网络安全管理最佳实践

总体来看，超过一半的组织机构制定了网络安全风险战略和相关政策，“表现突出”企业和其他企业之间拉开较远的距离。

贵司有否实施网络安全风险战略？*

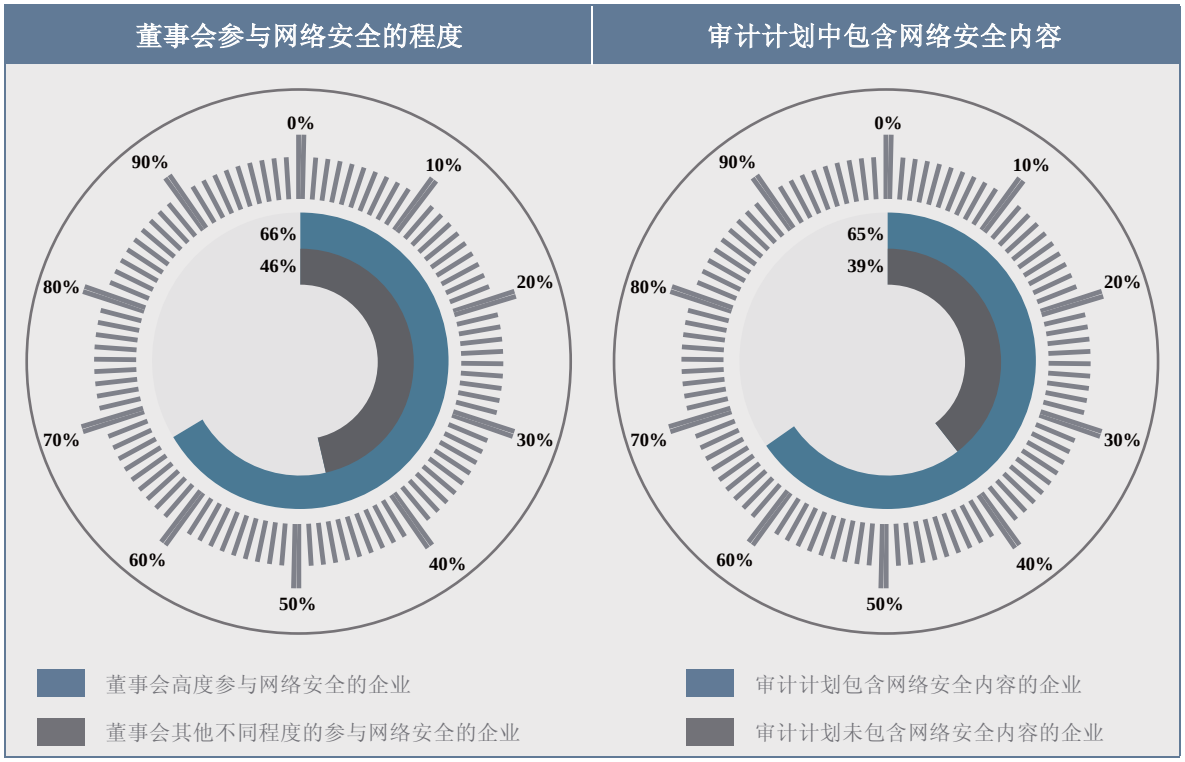


** 回答“是”的调查对象比例*

我们企业处理HIPAA健康医疗法案相关的保密数据，由于受保护的医疗数据和个人身份信息可能遭到破坏泄露，因此预防信息泄露的风险相当重要。

— 某中型技术公司首席审计官

贵司是否具备关于网络安全的政策？*



** 回答“是”的调查对象比例*

令人振奋的是，大部分组织机构通过一些风险评估，解决了网络安全风险的问题。在这些企业里，IT部门、外部审计人员、审计委员会和执行管理层是最重要的参与者（参见第9页图表）。

贵司是否从风险评估中识别出网络安全风险？

	董事会高度参与的企业	董事会其他不同程度参与的企业	审计计划包含网络安全内容的企业	审计计划未包含网络安全内容的企业
是的，独立于总体风险评估流程，加以识别区分	32%	22%	32%	17%
是的，作为总体风险评估流程的一部分，予以识别	63%	56%	65%	49%
没有	5%	22%	3%	34%

贵司有否实施网络安全风险战略？*

	重大	一般	较少	没有
审计委员会	17%	43%	28%	12%
公司IT部门代表	33%	47%	17%	3%
行政管理层	44%	41%	13%	2%
外部审计人员	20%	46%	28%	6%
人力资源部门	69%	27%	3%	1%
内审/IT审计部门	48%	38%	11%	3%
法务部门	31%	34%	19%	16%
业务人员	4%	27%	44%	25%
业务负责人/管理层	13%	38%	34%	15%
市场/公共关系/外部沟通部门	4%	23%	43%	30%
风险管理部门（独立于内部审计部门）	18%	38%	32%	12%
第三方服务商	13%	35%	28%	24%

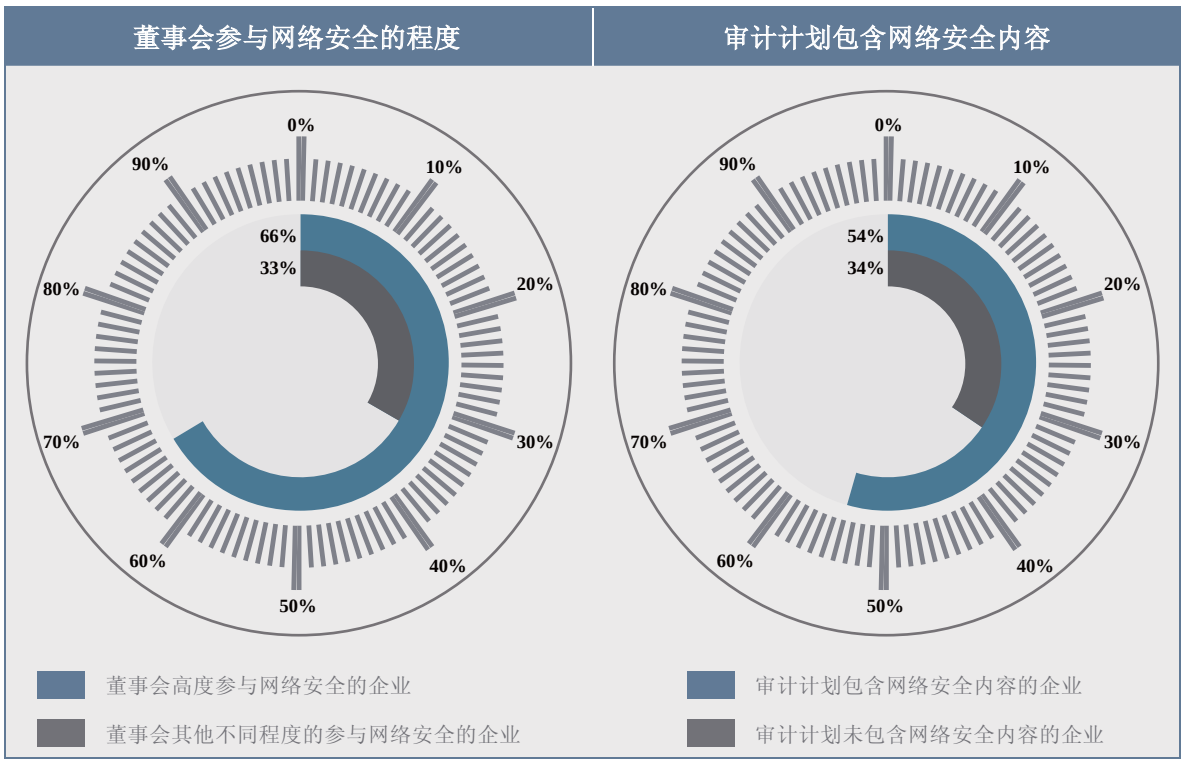
如果“是”：请列明以下个人或集体参与评估组织网络安全风险的程度。

	董事会高度参与的企业	董事会其他不同程度参与的企业	审计计划包含网络安全内容的企业	审计计划未包含网络安全内容的企业
审计委员会	81%	48%	66%	51%
公司IT部门代表	94%	73%	82%	78%
行政管理层	91%	81%	86%	83%
外部审计人员	81%	58%	67%	63%
人力资源部门	97%	96%	97%	94%
内审/IT审计部门	93%	82%	94%	73%
法务部门	85%	55%	70%	57%
业务人员	45%	23%	33%	26%
业务负责人/管理层	64%	44%	55%	44%
市场/公共关系/外部沟通部门	45%	18%	28%	24%
风险管理部门（独立于内部审计部门）	73%	46%	59%	51%
第三方服务商	59%	42%	55%	37%

** 调查对象回答“重大”和“中等”的加总百分比*

同样，我们乐观地发现许多企业的首席信息官会定期向审计委员会汇报关于网络安全和信息系统风险的总体情况。“表现突出”的企业又一次在这方面占比较高。

贵司首席信息官（或同等职位）定期参与审计委员会的会议并汇报信息风险的总体情况，并且特别重视有关网络安全问题？*



** 回答“是”的调查对象比例*

关键因素

由于缺少资源/技能，未能在审计计划中充分识别特定领域网络安全风险的组织机构的所占百分比。

30%

22%

由于缺少软件工具，未能充分识别特定领域网络安全风险的组织机构的所占百分比。

关于甫瀚咨询

甫瀚咨询（**www.protiviti.com**）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40%的财富1000强及全球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

不论客户公司规模如何、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–奥克斯利法案》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–奥克斯利法案》合规
- 内部审计质量评估和转型
- 审计委员会咨询

更多有关甫瀚咨询内部审计与财务控制解决方案的信息，请联络：

李维刚　董事总经理
+ 852.2238.0499
albert.lee@protiviti.com

Protiviti Greater China
甫瀚咨询 · 大中华区

Beijing 北京

Unit 718, China World Office 1
No. 1 Jianguomenwai Street
Chaoyang District
Beijing 100004, China
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
Tel / 电话: (86.10) 8515 1233
Fax / 传真: (86.10) 8515 1232

Shanghai 上海

Unit 2618-38, Central Plaza
No. 381 Huai Hai Zhong Road
Huangpu District
Shanghai 200020, China
中国 上海 200020
黄浦区淮海中路381号
中环广场2618-38室
Tel / 电话: (86.21) 5153 6900
Fax / 传真: (86.21) 6391 5598

Shenzhen 深圳

Unit 1404, Tower One, Kerry Plaza
No. 1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China
中国 深圳 518048
福田区中心四路1号
嘉里建设广场1座1404室
Tel / 电话: (86.755) 2598 2086
Fax / 传真: (86.755) 2598 2100

Hong Kong 香港

Suite 2103-04, Central Plaza
18 Harbour Road
Wanchai, Hong Kong
香港 湾仔
港湾道18号
中环广场2103-04室
Tel / 电话: (852) 2238 0499
Fax / 传真: (852) 3118 7493

www.protiviti.cn
www.protiviti.com

甫瀚 protiviti®
风险与商业咨询。
内部审计。