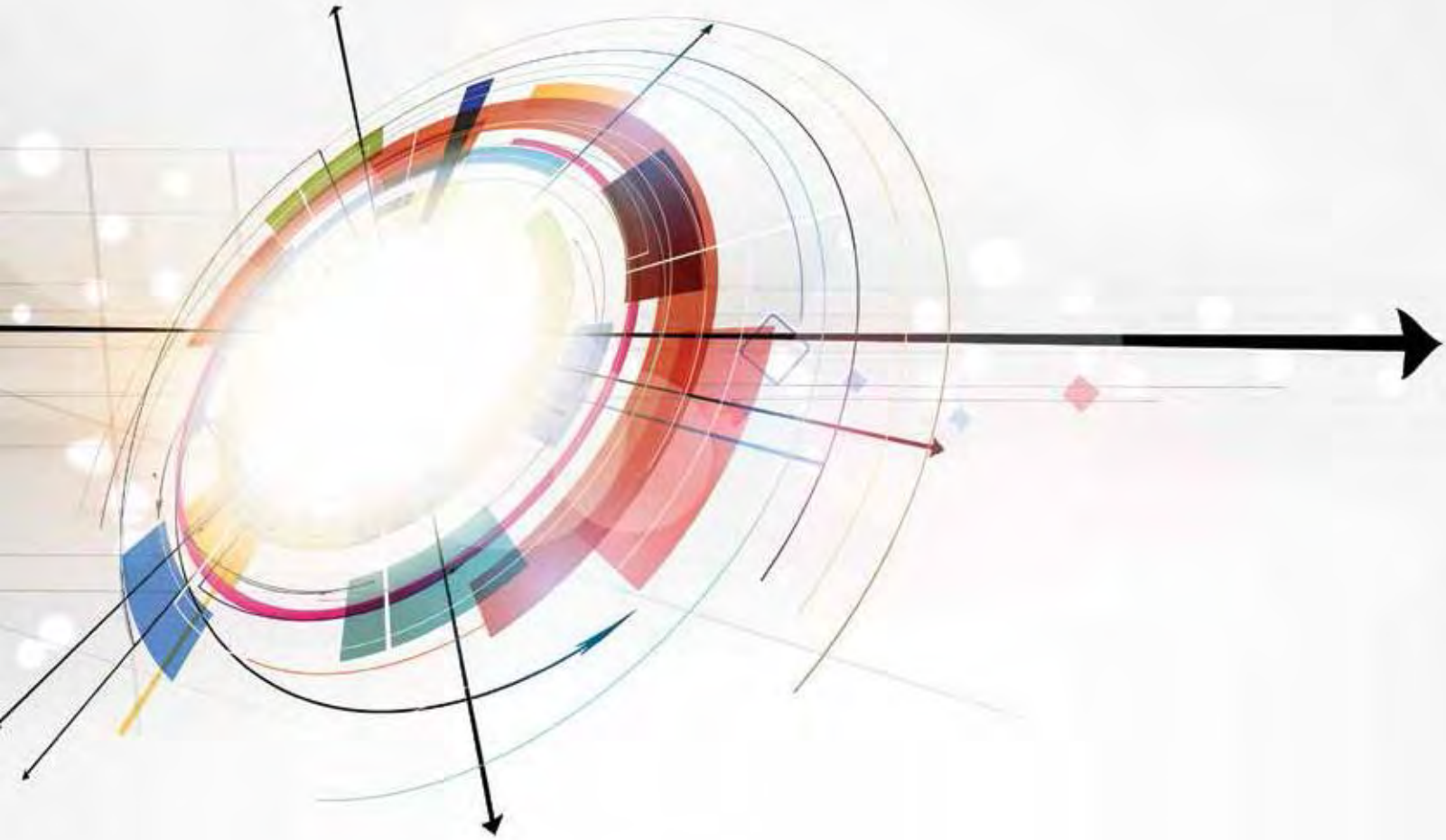

全球视角与见解

2018:首席审计执行官面临的主要风险

The Institute of Internal Auditors

前期报告

请访问以下链接，获取前期全球视角和见解报告 www.theiia.org/gpi.

读者意见反馈

请将问题和建议发送至 globalperspectives@theiia.org.

目录

前言 ..... **Error! Bookmark not defined.**

人才管理 ..... **Error! Bookmark not defined.**

数据分析 ..... **Error! Bookmark not defined.**

网络安全 ..... **Error! Bookmark not defined.**

监管措施 ..... **Error! Bookmark not defined.**

加密货币 ..... **Error! Bookmark not defined.**

《通用数据保护条例》 10

变革应对 ..... **Error! Bookmark not defined.**

结语 19

前言

在已经到来的 2018 年，我们将会看到一系列全新的法律法规、看法见解、更加先进的科学技术以及前所未有的新风险。如今的商业环境与以往大不相同，各种因素之间的关系更加复杂，彼此之间联系也更加紧密。组织不仅需要面对新的未知风险，也会拥有前所未有的发展机遇。展望新的一年，组织在面对这些机遇和挑战——其中有些已经被预见到，有些则是 2018 年出现的全新课题——的时候，需要制定着眼全局的审计计划，并根据实际情况迅速做出相应的调整，尤其是在遇到重大变革的情况下。

从组织的角度看，内部审计拥有一套体系完善，规定严格的工作方法，能够帮助组织在完成既定目标的过程中评估和提升组织的风险管理、控制和治理程序。监管部门和审计委员会要求内部审计对组织的风险管理措施进行确认，评价其是否能够帮助组织合理应对竞争对手、科技发展、市场走向的变更以及监管措施的发展等因素带来的威胁。（详情请参考：《内部审计未来发展趋势：发展新趋势和主要影响内部审计发展的关键领域》）

不论从事哪个行业，组织都需要内部审计为其提供更多有价值的战略支持，因此审计人员必须确保审计工作范围涵盖所有的关键风险因素，尤其是战略风险和运营风险。内部审计必须提高适应能力，积极应对不断变化的风险环境。

风险永远处在发展之中，因此对于组织任何层面的工作来说，即便制定了完善的审计计划，也必须保持高度的灵活性，根据新的风险情况及时作出调整。国际内部审计协会（IIA）各分会确定了首席审计执行官（CAE）（在内部审计和整个组织层面）面对的最主要的五大风险：人才管理、数据分析、网络安全、监管要求以及应对变革本文将围绕这些风险展开探讨。

人才管理

人才管理一直都是 CAE 和内部审计从业人员十分关注的问题。在过去的几年中， CAE 们一直苦于难以找到有能力适应新环境、应对新风险的人才。坦白讲，目前适合内部审计发展需求的人才数量十分有限。而且，如何在工作环境中满足年轻员工的特殊需求，也是一项十分严峻的挑战，千禧一代渴望在工作中得到更多的支持和认可，具体需求也有所不同，他们对工作环境有一些特定的要求，往往愿意追求更加灵活的工作安排。（详情请参考：《缩小内部审计人才差距的四大战略》）

“放眼未来，内部审计必须要解决的五大问题之一是要提高灵活性。我们必须在内部审计业务中保持灵活的工作方式，做到及时发现并解决新兴风险，对风险进行持续评估，并根据实际情况对审计范围作出相应的调整。而且我们必须能够及时发现能力方面的缺陷，并迅速采取补救措施。只有通过实施不断发展变化的人才管理战略，内部审计部门才能在未来取得成功。”

理查德 • 钱伯斯
IIA 秘书长兼 CEO

015 年，IIA 开展的一项全球性调查显示，超过 40%的受访者将“吸引和留住人才”视为内部审计发展的重中之重，超过半数的受访者认为“知识不足”（*knowledge gap*）是造成审计人才匮乏的主要原因。2017 年 IIA 开展的首席审计执行官服务中心®（AEC®）调查中，受访的近 200 位首席审计执行官里大多数人（79%）都认为人才管理是内部审计职业面临的极为重要的风险。毕马威（KPMG）调查显示，董事会也将人才——特别是人才的缺乏——视为一项“企业风险”。在全球化发展过程中，组织需要员工的支持才能继续走下去，因此人才管理对于组织来说十分关键。由于全球人才短缺，为组织发展和培养未来的领导者变得更加困难，因此可能会造成组织的领导能力下降；除此以外，由于员工没有能力承担重要职责，组织经营战略的实施情况就可能会受到质疑。越来越多的组织发觉自身没有能力培养年轻员工，而且难以留住高端人才和专业型人才，造成了智力资本和竞争优势的流失。未来，随着退休人数不断增长，技术能力匮乏的危机会更加显著。（详情请参考：《董事会会议疑问：人才管理…还是人才危机？》）

新兴风险的出现更是雪上加霜。包括数据分析、第三方管理、网络安全、可持续发展以及政治因素等其他不确定因素在内的新兴风险使得组织对内部审计的期望越来越高。内部审计再也不能像以前一样，只需要开展传统的财务和合规业务了。

虽然内部审计并不直接承担人力资源相关的工作，但是内部审计需要对管理层在人力资源相关风险的处置情况进行评估。如今组织要求内部审计人员在审计工作中采用关注全局的工作方式，对风险进行综合考虑，注重价值创造。因此，内部审计方面的高端人才、相关技能和优势能力都成了各个组织竞相追逐的对象。

如果缺乏足够的技能，内部审计就很可能会忽视具体风险和非传统风险，如科技、地缘政治、经济状况、制定企业报告以及国内外监管制度，或是出现审计不透彻、不深入的问题。《缩小内部审计人才差距的四大战略要素》一文认为，突破财务、运营和一般 IT 技能等传统领域的发展能力和对全局的把控能力，对于内部审计来说十分关键。

内部审计只有不断拓展自身能力范围，全面考虑组织面临的各类风险，并据此承担相关工作任务，才能更好地为组织服务。为此，内部审计需要引进高素质的人才，利用他们先进的批判性思维能力、敏锐的商业头脑、特定领域的专业技能或是特定行业的专业知识开展业务。传统风险以外的的新兴风险将会对审计工作的各个方面产生影响，因此内部审计必须不断努力拓展自身技能的宽度和深度。

CAE 必须要领导审计人员不断取得更加丰富的经验和技能，并在评估和执行审计计划时将风险“新常态”纳入考虑范围。传统的审计培训仍然不可或缺，但是只有通过坚持继续教育和实践相结合，提高适应能力，加强软技能的培养以及学习有关流程和运营方面的知识，才能在所有的商业环境中做到游刃有余。

合理管理各个类型的人才对于内部审计的成功来说也十分关键，不仅可以弥补短期人才缺失，而且还能带来更加长远的益处。为了进一步优化人才管理战略，CAE 和高级管理层需要全面考虑各方面的因素，制定并采取完善的应对措施，重塑和强化员工队伍建设。为了提升效率，使得内部审计能够以最佳状态应对风险的到来，CAE 必须采取适当的战略，包括衡量现有员工缺乏哪方面的能力、未来加入团队的人才应当具备哪些能力的真实需求，以及员工需要从领导者那里获得哪些信息才能获得成长和成功。

一套完善的人才管理战略是建立在多种工作方法之上的。CAE 不可能通过招聘解决人才缺失的问题。目前，我们最缺乏的还是那些有能力应对未来风险的人才——即具备数据科学、创新思维、分析/批判性思维、沟通以及其他技能的人才。内部审计需要制定一个高效的战略，其中包括要充分理解所需的技能和要素，并不断努力寻找、培养和留住组织的高端人才。

发展目标

- 内部审计的综合能力和内部审计的工作范围一样由风险决定。
- CAE、审计委员会和高级管理层充分了解支持组织完成目标所需的技能以及内部审计人员的总成本。
- 内部审计部门内部执行一套统一的绩效管理流程。
- 内部审计领导有能力指导和培养新一代的员工，以及其他新加入内部审计团队的人员。
- 为所有的内部审计人员制定正式的职业发展规划。
- 建立内部审计新员工的培训制度，并为每一位内部审计人员持续提供有关组织文化、风险偏好和战略导向的培训。

具体行动

- 对风险评估和审计计划进行检查，确定执行计划所需的相关技能。对现有技能和所需技能的差异进行分析，并制定弥补差异的战略措施。
- 对绩效评估的结构进行调整，将具体工作所需的能力和具有可行性的目标纳入其中，在制定可行性目标时，确保其能够反映组织的战略规划以及专业人员（如数据分析师）的薪资结构。

审计重点

IIA 准则 1210：专业能力

内部审计师必须具备履行其职责所必需的知识、技能和其他能力。内部审计部门整体必须具备或获得履行其职责所必需的知识、技能和其他能力。

IIA 准则 1230：持续专业发展

内部审计师必须通过持续专业发展来增加知识、提高技能和其他能力。

审计重点

IIA 准则 1220：应有的职业审慎

内部审计师必须具备并保持合理的审慎水平和胜任能力所要求的谨慎和技能。但是，应有的职业审慎并不意味着永不犯错。

1220.A2 – 在履行应有的职业审慎时，内部审计师必须考虑利用技术的审计方法和其他数据分析技术。

- 对现有员工进行技能培训，不仅可以避免大的人事变动，还能将现有的企业知识和新获得的技能融合在一起。
- 不断招聘具有新技能的人员。寻找具备各种教育经历和工作背景的人才，不局限于财务和会计方面的人才。将第三方服务供应商作为快速获取应对复杂和特殊风险所需技能的有效资源。
- 建立一套高效的入职培训程序。

数据分析

数据分析是收集和分析数据，并利用分析结果帮助决策的过程（《内部审计》第四版，11-2，内部审计基金会，2017）。组织运营产生的数据存储量不断增长，给内部审计工作带来了两个关键性的挑战。一方面是如何帮助董事会和管理层了解数据收集、管理、保护和运用的方式，另一方面是该如何从内部审计的角度出发充分利用数据，在现有的审计程序中运用分析工具，实现常规审计自动化以及重点关注新兴风险领域。（详情请参考：《风险聚焦：2018 内部审计热点话题》）

简单来说，数据分析就是将大量的数据拆散，然后将数据以小单位进行重组，以便于从数据中提取各类信息。因此，内部审计可以对各类风险及风险之间可能存在的相关性进行分析，提供洞见和预测，并就利益相关者关心或感兴趣的问题提出报告。对数据分析及相关风险进行管理有时难度的确很大。通过数据分析，提取有意义的洞见，并将其付诸实践也并非易事。只有具备合适的人才、工作模式、工作流程以及必要的科技手段，才能保证数据分析的有效性。

随着管理层和董事会需要立即处理的数据越来越多，他们必须认识到大量的数据会给组织带来数据相关的各类风险。每一个数据分析项目都需要解决以下几方面的风险（详情请参考：《理解并管理分析项目的风险》）：

- **数据和信息质量风险 —**只有保证数据的质量，才有利于决策者进行沟通，促进对复杂状况的理解。

  所有的数据和信息必须具备清晰的定义和质量标准。
- **数据和信息合规风险—**违反官方和认证机构（通常与政府、联邦和国际组织相关）的要求会给组织带来负面影响，如罚款、承担额外工作或是个人责任。
- **数据和信息治理风险—**在组织合适的层级中运用风险管理准则和工作流程，对数据和信息进行严密的控制，以保证数据和信息的保密性、安全性、质量和可审计能力。
- **对分析风险不恰当或不成熟的运用 —**如果没有时间用来收集、处理和解读数据，之前没有有关决策的先例，历史数据是误导性信息，或是无法衡量关键的变化因素或不确定因素程度极高时，分析理论是无法发挥作用的。

- **与组织文化产生矛盾，因而造成负面影响的风险** —在非数据导向型组织文化中开展分析项目会给组织领导带来重大风险；分析项目中应该加入对组织决策系统和组织文化中数据导向程度的评估。
- **数据道德风险** —数据分析项目应该要和组织的核心价值、决策机制以及组织行为保持一致。组织必须要采取相应的控制措施，保证数据收集和使用符合道德要求。

内部审计要时刻关注组织进行大数据项目可能面临的危机，尤其是组织员工缺少某项技能的情况。组织对数据分析的需求不断增长，而且不久之后，数据分析一定会成为每一个组织不可或缺的一部分。虽然充分参与大数据项目能够帮助组织紧跟潮流，提升竞争能力，对于组织发展至关重要，但是对于以下相关风险还是需要保持关注：

- 数据安全。
- 数据保密。
- 成本。
- 数据的不可靠性、不确定性、不充分性和不相关性。
- 分析流程的不可靠性、不确定性、不充分性和不相关性。

科技的迅速发展导致如今的世界瞬息万变，如果我们没有做好充足的准备，就无法妥善应对快速变化的局面。科技发展会产生庞大的数据，内部审计可以利用这些数据对风险进行更加全面的评估，提升审计成果的质量，还可能会提升确认服务的水平。

近期开展的案例分析结果显示，数据分析给内部审计带来的好处包括提升内部审计的有效性和工作效率，使内部审计更加关注战略风险，扩大审计范围，在内部审计长期发展过程中大大节省时间和成本。然而，想要真正达到以上这些效果，内部审计必须首先对数据分析项目是否能够帮助内部审计完成首要的发展目标，并开展有益的活动进行评估。

数据分析是内部审计的关键性工具，能够为内部审计提供隐藏在数据中的深度洞见，还可以提供更多有效的测试。许多内部审计团队尚未采用更加复杂的数据分析技术；他们依然依赖于原始的以电子表格为基础的工具和应用。另外，审计委员会的支持也很关键。内部审计应确保审计委员会了解数据分析的重要性。（详情请参考：《数据分析：是时候迈出第一步了吗？》）。

为了建立和维护数据分析程序，CAE 们应该与利益相关者进行讨论，了解利益相关者想要达到的结果，确定数据分析的目标以及所需的能力和技术。

缺乏具备处理大数据所需相关能力的人才是建立有效的数据分析程序的主要障碍，也是内部审计一直面对的风险。专业人才的短缺使得内部审计分析程序不如人意——不一定是程序本身存在问题，而是因为程序没有得到最大化利用。大数据工程和其他新出现的业务项目一样都存在风险。但是如果没有能够管理大数据的人才，大数据风险因素的程度就会大大提高。

发展目标

- 内部审计深入理解数据分析和相关技术，充分了解先进技术如何才能强化内部审计的效率和效果。
- 扩大数据分析使用范围会产生新的风险，内部审计要对管理层如何应对这类新风险进行评估。
- 内部审计要以组织的整体利益为出发点，充分利用数据分析程序的先进性。（例如，对有关高风险的计划、行为、评估以及针对组织指定的风险评估流程的准确性等工作进行确认和监督。）
- 内部审计能够利用科技手段提前确定可能出现的异常情况和舞弊风险的类型，并将关键发现与组织进行沟通。
- 内部审计能够利用科技手段，在更短的时间内，利用更低的人力成本，强化组织整体的风险覆盖率。

部分内容引用来源为：《为内部审计团队建立数据分析的第一步》

具体行动

- 确定数据分析项目的基本需求和具体需求，由此确定何种分析结果最有利于内部审计完成审计目标。
- 了解分析项目能够为组织和内部审计在创新和发展机遇方面带来哪些好处。确定为了更好地施行分析项目，达到预想的结果需要哪些技能。
- 将数据分析视为一项关键的业务，合理安排审计业务，寻找最具可持续性的高质量工作方法，帮助组织管理整体的合规和控制框架。
- 对分析项目的具体规则、数据点、数据代码和项目设想进行管理，有助于准确确定和判断违规行为和舞弊类型。

网络安全

网络犯罪不仅会给组织造成大范围的信息泄露，也会持续不断地盗取个人身份信息，其犯罪手段复杂，资金充足，是组织不可忽视的天敌。当前世界互联互通，造成关系越来越复杂，风险层出不穷，给网络犯罪培育沃土。网络犯罪技术范围不断扩大，技术能力也不断发展，想要跟上网络犯罪发展的步伐还有很多工作要做。

制定抵御网络攻击计划，并确保计划有效实施是一项全天候 24 小时的工作。需要确定的不是是否会出现网络攻击，而是网络攻击出现的时间。网络风险意识和准备应对网络风险是两个截然不同的概念。我们都了解风险概念，但是我们需要每天面对的是风险本身。因此我们需要做好充足的准备工作，其中包括要具备在攻击之前就将其整体瓦解的能力，也包括抵御攻击，减轻影响，并快速恢复的能力。哪怕是面临再小的网络攻击，组织都需要具备抵御、应对和恢复能力来保护网络安全——即“网络韧性”。

由于网络安全问题的担忧不断增长，利益相关者希望能够更加清楚地了解组织网络安全风险管理程序，董事会也希望内部审计能够就网络风险和网络程序提供独立、客观、全面的洞见。因此，内部审计必须了解可能存在的风险，并在提高组织网络韧性方面发挥重要作用。

网络安全风险不仅会受到外部因素影响，组织员工和商业伙伴的行为也有可能对网络安全造成威胁。因此，对组织文化和网络风险评估进行恰当、有效地管理对于提升网络韧性至关重要。董事会习惯于将“风险文化”纳入组织文化范畴，因为“风险文化”是整个组织采取所有决策、行为和风险应对措施的基础。内部审计可以在进行标准的运营审计和财务审计时，通过收集数据和非正式评审对组织的风险文化进行审计。

通过这种方式，内部审计能够帮助管理层加强对所有领域，甚至是工作需求、流程和能力受到组织文化影响的领域中，网络安全控制有效性的理解。文化会影响组织的生产能力、价值观念、态度和工作方法，而文化也是在多种不同因素影响下形成和发展的；因此，内部审计可以利用评估组织其他领域的工作方法对组织文化进行评估（详情请参考：《内部审计未来发展趋势》）。内部审计可以通过了解评估组织文化的工作方法，并帮助管理层了解组织文化的重要性来达到内部审计价值的最大化。

为了能够抵御包括文化在内的网络安全相关风险，领导团队一定要制定防御措施，并在培训项目中充分应用，确保在组织运行中得到持续地体现。因此，组织所有者、供应商、合作伙伴还有承包商等都要接受培训，根据网络安全措施和网络安全协议的内容，确定自身的具体职责。

内部审计在制定风险评估战略时一定要充分考虑网络安全相关的所有风险因素，并保证评估战略符合政策和内部控制的规定。内部审计要制定详尽的审计方法，努力满足组织和利益相关者在网络相关领域的需要。为了确保工作有效性，内部审计至少需要在审计工作中安排控制活动，创造控制环境，制定风险评估、沟通交流、监管措施以及评估网络安全措施的工作框架（详情请参考：《风险聚焦：2018 内部审计热点话题》）。

作为组织的第三道防线，内部审计要与管理层和董事会在制定网络安全战略和政策方面相互协作，共同提高组织确定和应对网络安全风险的能力。内部审计还需要合理利用与审计委员会和董事会的关系，确保他们充分参与风险应对工作；除此之外，还要确保将网络安全风险正式融入审计计划之中，并且要（通过内部培养或通过合包方式）掌握执行审计计划的必要能力。新出现的科学技术和发展趋势会影响组织网络安全风险的具体内容，因此，内部审计还需紧跟先进技术的发展趋势，对组织易受攻击水平，以及可能会影响网络安全计划的风险行为进行评估。

“即便不是技术专家，组织高管也可以在网络风险监控中发挥重要作用——但是每个董事会都可以利用这个机会来提升网络监控的有效性。”

《网络风险监控手册》，美国企业董事联合会(NACD), 2017

来源：《监管工作的重要性：网络风险管理检查》

发展目标

- 组织具备应对网络风险的文化。
- 内部审计中对于网络安全检查和准备工作至关重要的关键要素：
  - 保护和发现：内部审计提供一套全面的工作方法，帮助组织确定可能会受到攻击的领域；还将数据分析纳入内部审计职责范畴，随时发现错误并向组织汇报。
  - 业务持续性：在管理层为应对和克服可能会对组织持续运营造成影响的风险，如网络安全、自然灾害或换届等制定应对计划时，内部审计与管理层协同合作，向管理层提供相应的意见和建议。
  - 危机管理/沟通交通：内部审计通过提供有关有效性和时效性的确认，并对计划执行情况进行分析和判断，帮助组织制定危机管理计划，做好沟通交流的准备工作。
  - 持续发展：内部审计主要通过提供洞见，为更好地完成抵御网络攻击的准备工作提供更加完善的战略和准则来增加自身的价值。

具体行动

- 根据组织的网络韧性对组织文化进行评估。
- 对安全模型和网络安全工作流程进行风险评估，并提出修改建议。
- 同 IT 部门以及第三方合约商合作，利用数据渗透测试的方法对第三方是否具备满足现有协议要求的能力进行评估。
- 分析网络韧性差异，提出补救意见并跟踪补救措施的实施。
- 通过强调网络安全监督和应对的重要地位来影响组织文化。
- 保证定期对业务持续发展计划进行测试，并针对确定的纰漏采取修正措施。
- 在整个组织内建立强大的网络文化和风险文化，这将在未来影响和改善组织的网络安全措施和准则。

监管措施

全球范围内的组织都面临新的或是经过修订的监管要求，设计这些监管要求在一定程度上是为了保护消费者或公众的利益。其中最受关注的监管要求内容将重点放在金融风险和控制、数据保密和安全方面，将会对所有行业的组织产生影响。

加密货币

据 CNBC 的报道，由于近期电子货币交易额大幅上涨，加密货币价值可能已经超过千亿大关。比特币价值浮动较大：2018 年初，比特币价值在 6,000 美元到 10,000 美元之间浮动。加密货币交易平台 Gatecoin 亚太地区事业发展部领导 Thomas Glucksmann 表示：“通过提高对加密货币交易的监管意识，扩大机构资本准入并促进重要科技领域的发展，能够促进今年市场回暖，并将加密货币的价值推向新高。今年（2018）年底比特币一定会突破 50,000 美元大关。”

全球范围内，随着在区块链技术和加密货币交易方面的参与度逐渐提升，主要的金融机构需要了解如何才能妥善应对由于员工利用个人账户进行数字货币交易引发的冲突。数字货币价格高涨不仅使投资商和银行充满兴趣，也引起了合规部门的密切关注。如果金融机构的员工也参与——或是想要参与——加密货币投资的话，会影响交易的公平性。一般来说，证券发布之前必须对可能引起利益冲突的内部员工进行利益核查；然而，这一政策在加密货币交易方面的实施难度会更大，因为加密货币是通过碎片式的网络进行交易的——有些情况下是匿名交易——因此很难追踪交易来源。

审计重点

IIA 准则 2130：控制

内部审计部门必须评估控制的效果和效率，并促进控制持续改进，从而协助组织维持有效的控制。

2130.A1 –内部审计部门必须评估控制的效果和效率，并促进控制持续改进，从而协助组织维持有效的控制：

- 组织战略目标的实现。
- 财务和运营信息的可靠性和完整性。
- 运营和程序的效率和效果。
- 资产的安全。
- 对法律、法规、政策、程序及合同的遵循情况。

除此以外，全球监管机构对此没有设立清晰的规定，使金融机构设立内部规定更加困难。有些人将加密货币视为一种商品，还有些人表示某些加密货币可能是证券属性，但又不能明确是哪些加密货币。对于近期比特币以及其他数字货币价值的大幅度波动，全球监管机构表示十分担忧，可能会采取更加强硬的监管措施。（详情请参考：《加密货币交易成为主流，合规部门忧心忡忡》）

“《通用数据保护条例》的重要程度越来越显著，从确认服务的角度来说，审计委员会希望内部审计从一开始就对项目本身进行评估，但接下来希望我们能够以最新的法律法规为基础建立自身的工作程序，从而确保工作流程正确无误，符合监管规定。”

某跨国银行集团CAE

来源：《风险聚焦：2018内部审计热点话题》

《通用数据保护条例》

一部分国家的政府正在不断加强对数据保密的监管力度。其中最显著的是欧盟和中国。

历时四年的准备工作和讨论，欧盟《通用数据保护条例》，其中包括数据保护指令 95/46/EC，终于在 2016 年 4 月通过了欧盟议会的批准，并将于 2018 年 5 月正式生效。目前，数据泄露危机正逐年增长，侵略性和应对成本也在不断提高。2017 年数据泄露情况增长尤为显著，较 2015 年至 2016 年度增长了 40%。（其他细节请参考下一页“2017 数据泄露”。）

虽然许多公司的保密政策是按照旧的指令制定的，但是新的《通用数据保护条例》生效之后，其中许多新的欧盟数据保护规定将会实施，也将根据新的条例对数据控制商和数据处理商的违规行为进行罚款或处罚。简单来说，所有在欧盟境内从事商业活动以及处理有关欧盟居民个人数据的组织（当地组织或跨国企业）都必须遵守新规。

对于违反主要规定且具有重大破坏性的事件，监管部门有权对其处以 2000 万欧元或者全球上一年度总收入 4%的处罚。新规中对于处罚有明确的规定（例如，如果没有按要求做好记录（第 28 条），没有发现有关泄露事件的官方监管和数据项目，或是没有进行影响评估，企业将会面临 2%的处罚。）需要注意的是，新规不仅适用于控制方，也适用于数据处理方，也就是说，云服务提供商也必须遵守《通用数据保护条例》的规定。还有一类违反新规的情况分别是没有遵守处理个人数据的核心准则、侵犯数据项目的权利以及将个人数据泄露给第三方国家或其他国际组织，此类事件都会对确保数据保护水平产生影响。（详情请参考：《欧盟全面数据保护法规》）

2017 数据泄露		
时间	**组织**	**违规/泄露事件**
2017 年 1 月 8 日	电子竞技娱乐协会(ESEA)	共有 1,503,707 条包含个人/隐私信息的数据记录泄露。
2017 年 2 月 2 日	Xbox 360 ISO 和 PSP ISO	120 万 Xbox 360 ISO 用户和 130 万 PSP ISO 受到影响；个人/隐私信息失窃。
2017 年 3 月 15 日	邓白氏公司（Dun & Bradstreet）	Dun & Bradstreet 网络中有超过 3300 万家企业（包括美国国防部和美国邮政）的联系方式；个人/隐私信息泄露。
2017 年 4 月 6 日	自愿联邦奖学金（ FAFSA）：美国国内税务局（ IRS）数据检索工具	100,000 名纳税人/学生个人/隐私信息失窃。
2017 年 5 月 10 日	布朗士黎巴嫩医院	2014 至 2017 年共有至少 7,000 名患者的个人信息受损，信息内容包括瘾症、神经和医学健康诊断、HIV 症状以及攻击报告。
2017 年 6 月 20 日	Deep Root Analytics	美国共和党国家委员会签约数据厂商 Deep Root Analytics 将个人/隐私信息存储在一个云服务器，但未设立密码保护措施，信息暴露时间长达 2 个星期，大约有 1.98 亿美国市民受到影响。
2017 年 7 月 13 日	威瑞森（ Verizon）	由于数据存储服务器安全性出现问题，造成 1400 万用户信息泄露；泄露的数据属于用户登录信息，是在用户通过手机连接 Verizon 网站时产生的。
2017 年 8 月 30 日	Online Spambot	Online Spambot 是一个机器人程序，它从一个不安全的服务器上盗取了 71,100 个邮箱和密码信息。
2017 年 9 月 7 日	伊奎法克斯公司（Equifax）	黑客攻破了网络软件的薄弱环节，导致 143,00 万客户受到影响；包括社交安全账号以及信用卡账号在内的个人/隐私信息泄露。
2017 年 10 月 12 日	君悦酒店	酒店借记卡和信用卡支付系统受到非法攻击，全球共有 11 个国家 41 家酒店受到影响，泄露信息包括信用卡账号、内部验证码和持卡人姓名等。
2017 年 11 月 21 日	优步	5,700 万司机和用户的个人信息泄露，信息内容包括姓名、邮箱和手机号码
2017 年 12 月 10 日	TIO Networks (PayPal 子公司)	约 160 万用户信息受到影响，信息内容包含银行账户信息、支付卡信息、密码、用户名和社会安全号码。

来源：**《2017 数据泄露事件——史上最严重的一年》**

审计重点

IIA 准则 2120：风险管理

内部审计活动必须评估风险管理过程的有效性，并对其改善作出贡献。

2120.A1 –内部审计必须评估下列与组织治理、运营及信息系统有关的风险：

- 组织战略目标的实现。
- 财务和运营信息的可靠性和完整性。
- 运营和程序的效率和效果
- 资产的安全。
- 对法律、法规、政策、程序及合同的遵循情况。

虽然“用户许可”的定义和情况都有严格的规定，之前，数据控制方可以在一些情况下仅靠模糊的许可和系统默认授权进行操作。2018 年，欧盟《通用数据保护条例》强化了对用户授权具体情况的规定，组织不允许再使用冗长的模糊不清的条目和满篇都是法律术语描述的情况，而是根据新条例的要求，为了提高数据处理工作的效率，简化有关用户许可的规定。有关用户许可的规定一定要与其他情况区分开，并用简单直白的语言进行表述。用户许可的撤销要和授权一样简单易行。此外，一旦用户撤销许可，数据程序有权清除个人信息，不再对数据进行处理。（详情请参考：欧盟《通用数据保护条例》对组织运营的十大影响）

《通用数据保护条例》将会对德国的网络安全监管产生重大影响。2017 年 5 月德国立法部门对《联邦数据保护法》进行了修订，将于 2018 年 5 月和欧盟的《通用数据保护条例》同步生效。新修订的法规要求严格，罚款最高可达 300,000 欧元，这意味着德国对于网络安全标准的要求越来越严格，承诺要保护用户，保证关键基础设施领域服务提供商和运营商网络信息的安全。新法案共包含 85 个条款，其中一些条款与欧盟《通用数据保护条例》交互参照。修订法案生效之后，关键基础设施运营商必须在两年内，根据新法案的具体要求，采取适当的组织和技术安保措施和其他符合最新发展趋势的措施。此外，关键基础设施运营商必须定期递交履行安保要求的证明，一旦出现任何重大变革必须立即向联邦信息安全办公室报告，因为这些变革会影响 IT 系统、要素和工作流程的可获性、完整性、可靠性和保密性，可能或已经导致运营商负责的关键基础设施项目功能失效或受损。（详情请参考：《德国网络安全法案需知》）

中国虽然已经就信息安全出台了严格的法律、规定和监管措施，但又制定了补充法案（2017 年 6 月生效），新法案融合了欧盟的《通用数据保护条例》相关条款，弥补了网络安全和数据保护之间的差异。《中华人民共和国网络安全法》在许多方面都和《通用数据保护条例》内容一致（详情请参考：《风险聚焦：2018 内部审计热点话题》）。《中华人民共和国网络安全法》修正案更加注重个人信息和隐私的保护，以及个人信息收集和使用的标准化问题。例如，之前外资企业可以在境外传输信息，但现在法律规定，敏感信息必须存储在国内，而且违反法律将会面临严苛的惩罚措施，如暂停商业活动。罚款金额最高可达 1,000,000 人民币。（其他细节请参考下一页“《中华人民共和国网络安全法》修正案”）

《中华人民共和国网络安全法》修订案		
条款	**最终版本**	**重要修订内容**
31	国家对***公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务***等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。	此条款确定了关键信息基础设施保护的重点行业和领域。
43	个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。***网络运营者应当采取措施予以删除或者更正。***	此条款赋予公民更多保护个人信息的权利，而且通过增加网络运营商的责任以确保能够及时修正出现的错误。
46	任何个人和组织应当对其使用网络的行为负责，不得实施诈骗以及其他违法犯罪活动。	此条款强调个人和组织应在网络使用方面承担责任。
76(5)	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于***自然人***的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。	此条款将个人信息保护的范畴从“公民”扩展至“自然人”。

但是也有一些人并不认同《中华人民共和国网络安全法》。根据 2017 年 5 月《纽约时报》报道，“一个代表欧洲、美洲和亚洲企业的商业游说组织联盟呼吁中国延缓新法律的实施，与此同时，欧盟驻中国商会也向中方争取更多的时间，以确保企业能够满足新增的‘重要合规责任’。”

63	对违反本法第二十七条规定，从事危害网络安全的活动的人可以根据案情处五日以上十五日以下拘留，并处十万元以上一百万元以下罚款。	违反《网络安全法》最高罚款金额可达 1,000,000 人民币。

来源：**《中国网络安全法综述》**

无论是在欧盟、中国还是其他许多国家，组织都能明显感觉到数据隐私监管力度加强带来的影响。为了满足法律的要求，董事会在组织内部要求不断强化组织治理框架，而监管部门、投资商以及其他利益相关者也在不断督促董事会调整组织结构，确保整体流程的工作效率（详情请参考：《公司治理、风险管理和内部审计审计》）。新法规的实施使风险管理、控制和治理程序更加复杂，造成成本增加，也给组织带来了很大的压力。

随着董事会压力增加，内部审计面临压力也随之增长。组织对内部审计的期待越来越高。组织意识到内部审计的建议和确认有利于组织将变革力量转换为机遇，而且还能保证符合不断变化的监管要求。（详情请参考：《毕马威内部审计：2016 年十大关键风险》）

审计重点

IIA 准则 2210：业务目标

必须为每项业务确定目标。

2210.A3 –评估治理、风险管理和控制需要依据适当的标准。内部审计师必须确认管理层和/或董事会制定适当标准的程度以确定目标和目的是否实现。如果标准适当，内部审计师必须使用该标准进行评估。如果不适当，内部审计师必须与管理层和/或董事会进行讨论，并确认适当的评估标准。

IIA 准则 2050：协调和信赖

首席审计执行官应当与其他内部和外部确认和咨询服务的提供方式共享信息、相互协调，并考虑利用他们的工作成果，以确保适当的工作覆盖面，并尽可能减少重复工作。

应对变革性力量的关键在于提升治理、风险管理、监管合规水平以及工作绩效的平衡。应对这些挑战有利于保护和增强工作价值，提升运营效率。

发展目标

- 评估项目和战略时要阐明风险偏好。
- 确保整个组织都了解目前的国家和国际监管要求。
- 针对目前的国家和国际监管要求制定应对措施。
- 与内部和外部确认服务提供商协作。

具体行动

- 了解国际合规框架和确认标准。
- 罗列现有监管组织及其要求。
- 对组织管理全球合规活动的工作方法进行评估，其中包含对新并购组织的整合。
- 对组织如何应对关键的非合规情况进行评估。
- 检查合规培训项目，并对不同岗位的工作分别进行评估。
- 与内部和外部确认提供方协作，确保工作覆盖面，将重复性工作比例降至最低。
- 根据组织的利益和工作重点定制交通方式，鼓励组织建立合规文化。
- 对组织履行监管合规责任的工作进行评估

变革应对

新的时代已经到来，组织面临着新的机遇和挑战。如今科学技术发展日新月异，变得越来越快，越来越强，涉及领域越来越广泛，也越来越深入；科技无所不达，渗透进世界的每一个角落，达到了前所未有的程度。内部审计人员每天都面临新的机遇，能够向利益相关者提供洞见和先见之明，但他们可能还不具备创新相关的技能，如批判性思维和创造力。长此以往，如果内部审计人员缺乏创新能力，他们就无法妥善应对突发事件，或是缺乏对现状的清晰认知。内部审计人员必须根据实际情况调整使用科技手段的工作方法——灵活处理，积极应对，能够快速根据创新发展调整工作导向。

虽然创新科技在很多方面都能够为内部审计人员的审计工作提供机遇，但是创新常常伴随着新的风险、威胁和*变革*，这些也会成为内部审计担心的问题。例如，（以前）内部审计只需关注风险本身即可，但是现在内部审计需要能够快速*确定*可能出现的变革，并决定哪些方面需要立即采取应对措施或是额外的关注。

组织关注创新的主要原因之一是可以帮助组织远离竞争——而内部审计可以引领这一变革。2018 北美内部审计脉搏调查报告结果显示，创新意味着内部审计有两个选择：要么提升自身能力，满足组织赋予的越来越重要的职责；要么继续墨守成规。后者可能更会导致未来工作的失败，因此内部审计必须对创造性观点（甚至是颠覆性观点）保持开放的态度，做好准备，将工作重心放在与风险相关的有效管理工作上面。

挑战不能避免。改变工作方法确实会增加管理工作的困难程度；预算可能会受到商业环境的约束，组织也可能会面临缺少具备所需技能人才的问题。但是，好在内部审计不是单打独斗。内部审计可以从其他商业团体、组织或内部审计中学习经验，他们可能已经掌握了具体的工作技巧，能够对创新流程进行有效管理。

创新——只要采取正确的发展方式——对于内部审计和整个组织而言极具价值：

- 降低成本。
- 增加价值。
- 实现增长和改善绩效。
- 缩短推出新产品和服务的周期。
- 提升用户体验和满意程度。
- 增强组织灵活度和敏锐度。
- 提升利益相关者满意程度。

创新不仅能够提升审计工作的效率和效果，而且能够提升组织敏锐程度，帮助组织面对变革时做出更加迅速有效且重点突出的反应。（详情请参考：《2018 北美内部审计脉搏调查报告：内部审计转型的当务之急》）国际内部审计师协会（IIA）北美理事会主席 Shannon Urban 鼓励内部审计进行创新，认为创新不仅是业务提升的关键，也是满足利益相关者不断变化的需求的必要手段。虽然创新可能会有一定的困难，让人难以接受，但是创新的脚步从不会停止，而且需要具备决心和勇气。创新的回馈是相当丰厚的。如果内部审计想要充分了解利益相关者的需求，并在将来做好利益相关者的服务工作，创新是必由之路。（详情请参考：《创新型内部审计人员》）

发展目标

- 内部审计了解商业环境的变化情况。
- 内部审计致力于建立创新文化，强化自身能力和绩效。
- 内部审计致力于通过创新掌握最佳的工作方式，提升工作质量。
- 内部审计希望通过创新提升工作效率。

“我坚信内部审计能够为组织的成功起到至关重要的作用。但是我也认同，这与内部审计承担的具体任务有关。我们必须重树创新内部审计的决心。内部审计一定要将创新作为工作的核心内容，才能保证跟上组织发展的步伐。”

Shannon Urban

IIA 北美理事会主席
(2017 – 2018)

来源：《内部审计师》

具体行动

- 设计实施新创意，将创新作为内部审计工作的核心基础。
- 承担领导职责，参与业务变革，对环境的变化进行监控，并提供范围更加广泛的应对措施和意见。
- 建立并投资维护良好关系。与业务部门保持联系，掌握最新的创新发展情况。
- 确定需要额外关注的变革，并以此了解风险的发展情况。
- 针对与变革性事件相关的新兴风险提供洞见。
- 寻找并吸引具有应对新兴风险所需能力的人才，确保能够灵活果断地应对风险。
- 与其他风险管理和合规职能部门合作。

结语

报告中重点强调的风险——虽然是 IIA 各分会确定的主要风险——但是不代表组织或内部审计面临的所有风险。除此以外，分会也根据审计委员会、预算、三道防线以及战略的需求确定了相应的风险——这些都是组织治理的关键领域，需要内部审计进行充分了解和检查。风险会阻碍组织完成使命和战略目标，威胁组织的整体价值。因此，内部审计的责任——作为值得信赖的顾问，协助风险管理、控制和治理程序工作——要求内部审计对所有的风险机遇进行全面的考虑，并提供正确的建议。

全世界范围内的组织都需要内部审计职能，以及内部审计评估。为了能够充分参与组织的各项活动，成为值得信赖的顾问，内部审计必须充分考虑完成自身目标以及组织目标过程中可能遇到的风险。因此，内部审计必须重视审计结果，为了组织的整体利益而不断提升自身价值。这需要内部审计具备应对挑战和困难的能力，如批判性思维能力；还需要保持独立性和客观性；保持敏锐度；重视抵御风险的*领导能力*——真实存在或是理想状态；组织随时有需要时能够及时做出反应，保证工作“时效性”；提供组织所需的确认服务；了解所有系统、工作流程、监管要求和运营之间的相互关联性。

IIA 分会

IIA 各分会是 IIA 发展的基石。 IIA 与全球 170 多个国家和地区的分会合作，共同致力于完成内部审计的使命，促进内部审计职业发展，为全球超过 190,000 的会员提供服务。

关于国际内部审计师协会（IIA）

国际内部审计师协会（IIA）是在内部审计行业得到最广泛认可的国际组织，是内部审计的倡导者，并提供教育服务、内部审计标准、实务指南和资格证书。国际内部审计师协会成立于 1941 年，如今会员人数超过 190,000，遍布 170 多个国家和地区。协会全球总部设在美国佛罗里达州的玛丽湖。更多信息，请登录 www.globaliia.org。

免责声明

《全球视角和见解》中所含观点并不一定完全代表接受访谈的人员及其雇主的观点。

版权

The Institute of Internal Auditors

globaliia.org