IT审计之当今首要技术风险观（精辑版）

国际信息系统审计协会（ISACA）和甫瀚咨询发布的年度调查显示：
网络安全、隐私、数据及监管合规是当今IT首要风险事项

ISACA

protiviti
Global Business Consulting
甫瀚

为了解当今IT审计中最受关注的技术风险，国际信息系统审计协会（ISACA）与甫瀚咨询联合推出年度《IT审计技术风险调查》。来自全球的7,500余位IT审计领导者与专家参与了本次调查，调查结果显示：**网络安全、隐私、数据及监管合规几大方面为当今IT首要风险事项**。

调查概要

不确定的全球经济、动荡的地缘政治局势、旷日持久的新冠疫情、持续变化的监管要求、日益演变的技术风险考量等种种因素，给IT审计领导者及其职能带来了众多挑战。而各行各业（如电信、物流、高科技、医疗保健、金融服务等）均面临着同样的境况。

总体而言，企业员工的持续远程办公会带来一系列技术及安全挑战。网络攻击隐患不可忽视，网络安全风险仍是今年的重点防范领域。同时，数据治理及数据完整性、监管合规方面的风险亦需持续关注。

ISACA与甫瀚咨询合作发布此份调查报告，旨在通过本篇调研与大家分享IT审计领域随着年度变化的动态风险全貌。

主要调查发现

IT审计最为关注网络安全相关的风险事件 — 各行业和类型的企业均将“网络安全”列为最高风险等级。相关网络事件，如数据隐私、安全事件管理、灾难恢复、访问风险和第三方风险，也被列为企业的核心关注点。这些风险因素，极可能导致企业名誉受损、收入及客户流失、受到合规处罚及审查。快速演变的合规环境，加之持续改变的业务流程和IT环境，使网络安全风险的应对日益复杂。

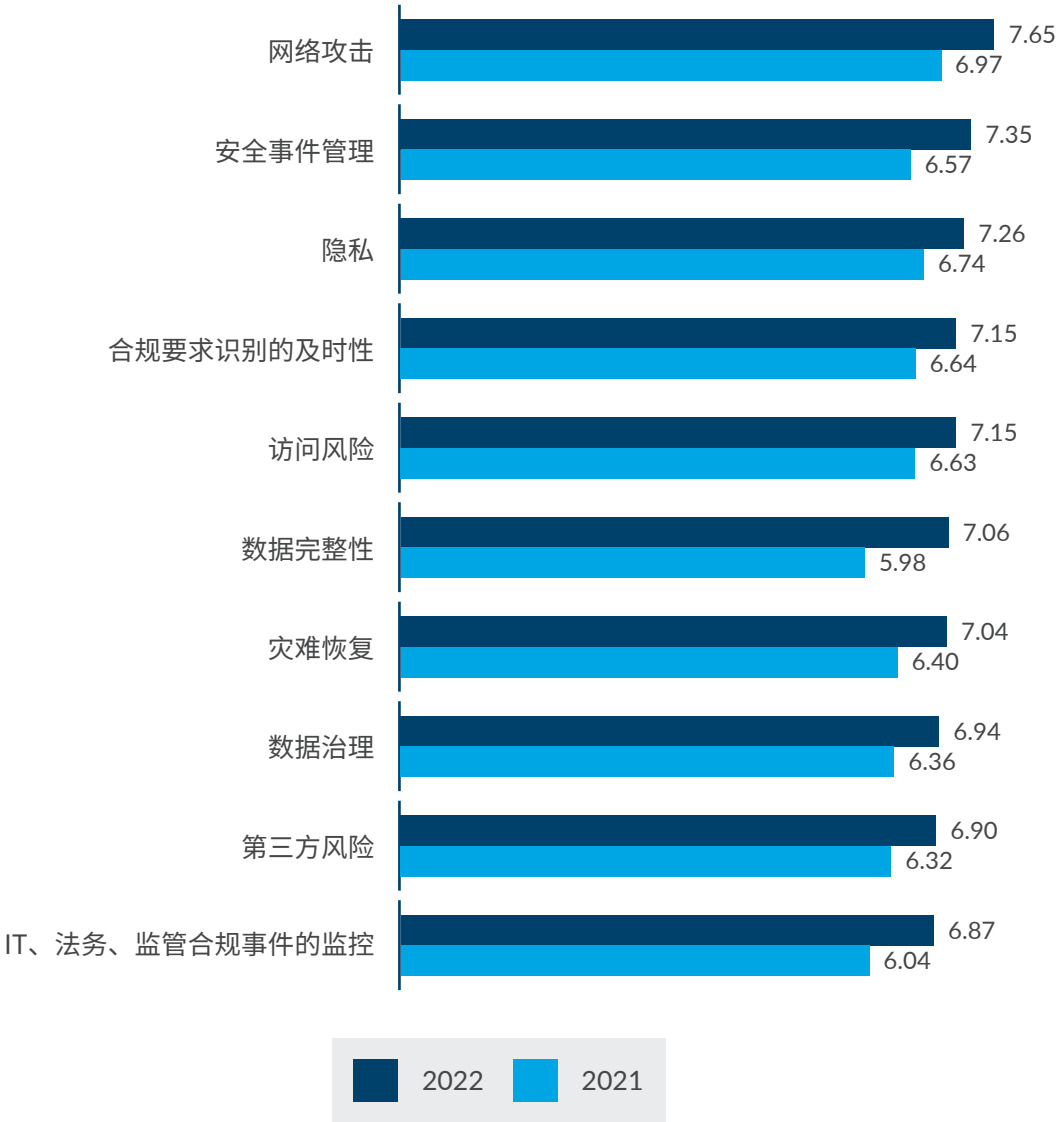
数据治理及数据完整性亦需加以详细审视 — 企业正从多渠道收集和使用海量的数据，并把这些数据共享给更多的第三方。企业从这些数据中获得的益处越多，越说明其很大一部分价值与管理和保护好这些数据密不可分。这也解释了为何IT审计领导者将识别数据相关的风险因素评为高风险等级的原因。鉴于企业高频、大规模的内部变更及转型，以及不可预测的外部干扰和善变的环境，与数据相关风险的控制则较为困难。

监管合规方面的压力及风险正迅速增长 — IT 审计团队和其他部门（如法务部门、合规部门、IT 部门），一直致力于跟上新数据隐私和数据安全的规则以及不断变化的法律监管合规要求的步伐。各种监管要求，如数据隐私和安全、行业标准、国家及地区要求、甚至突如其来的经济制裁等，对企业数据管理及技术相关活动的影响与日俱增。

年度首要技术风险

IT审计领导者及其团队对企业面临的重大技术风险有着清晰的认知，本调查以10分制的标准评估了风险的重要程度，结果表明：2022年各大风险领域的得分，相比上一年有显著增长，人们对当下技术风险的认知之深、之重，有显而易见的提升趋势。以下列示了2022年全球前十大首要技术风险及排名：

2022年前十大首要技术风险 – 全球



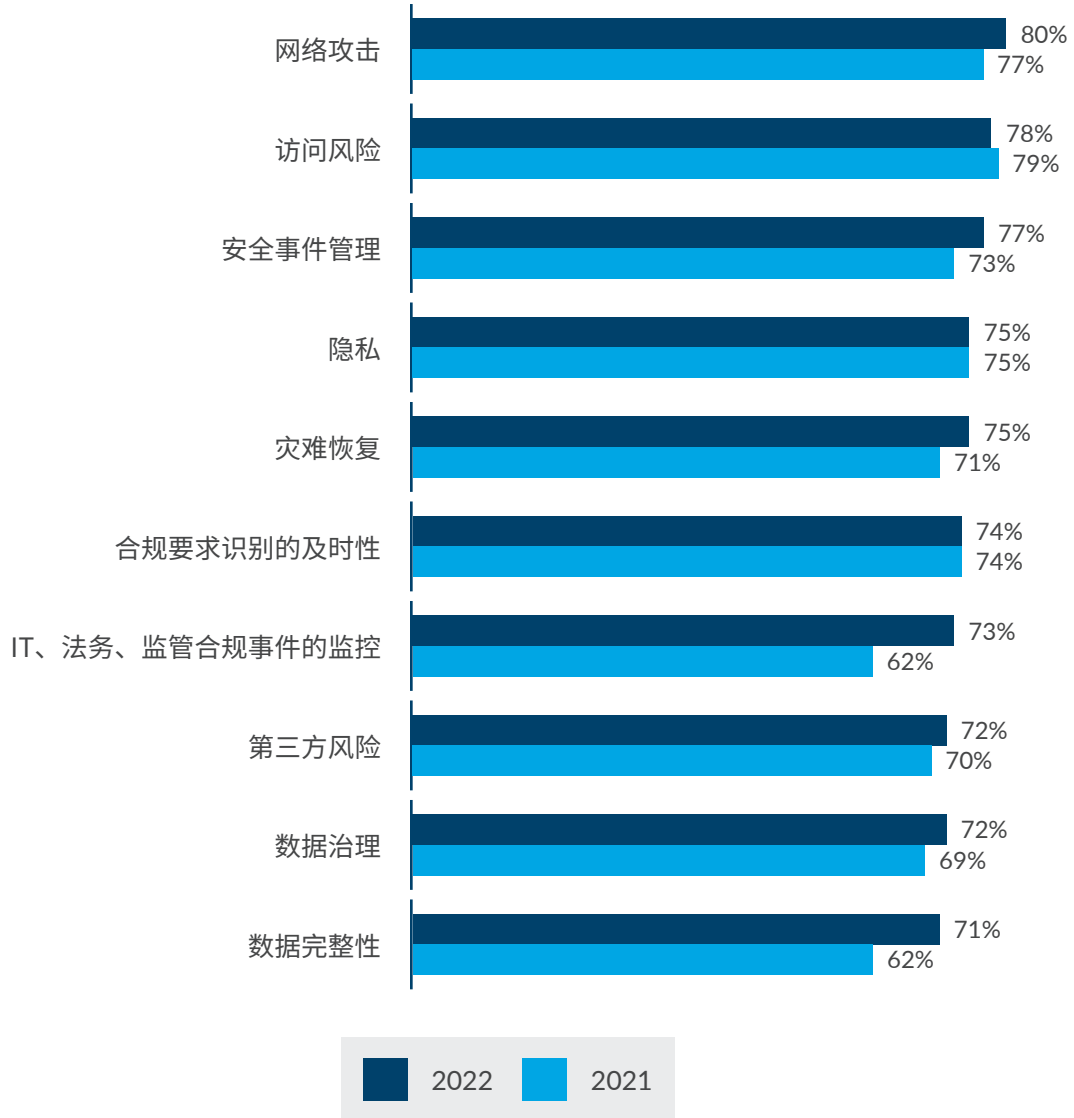
上述十大首要风险，均被列入企业的绝大多数审计计划（平均每10个企业中有7个企业会将其纳入审计计划）。

IT审计团队不是管理网络安全风险的第一道防线，但其必须评估网络安全管理手段的效力，以确保企业具备适当的控制和防御能力。IT审计团队应执行适当的网络安全评估，从而可了解企业所面临的网络安全风险是否被有效地防范。

由于企业内部的变化（如数字化转型、云迁移、混合工作模式）和外部的影响（如战争引发的全球效应、供应链剧变、网络攻击），使得数据治理和数据完整性相关的风险难以定性，这在一定程度上阻碍了企业治理和保护其数据，加上企业越来越依赖第三方的现状以及数据隐私法的陆续颁布，使得数据治理和数据完整性被大范围地纳入企业审计计划。

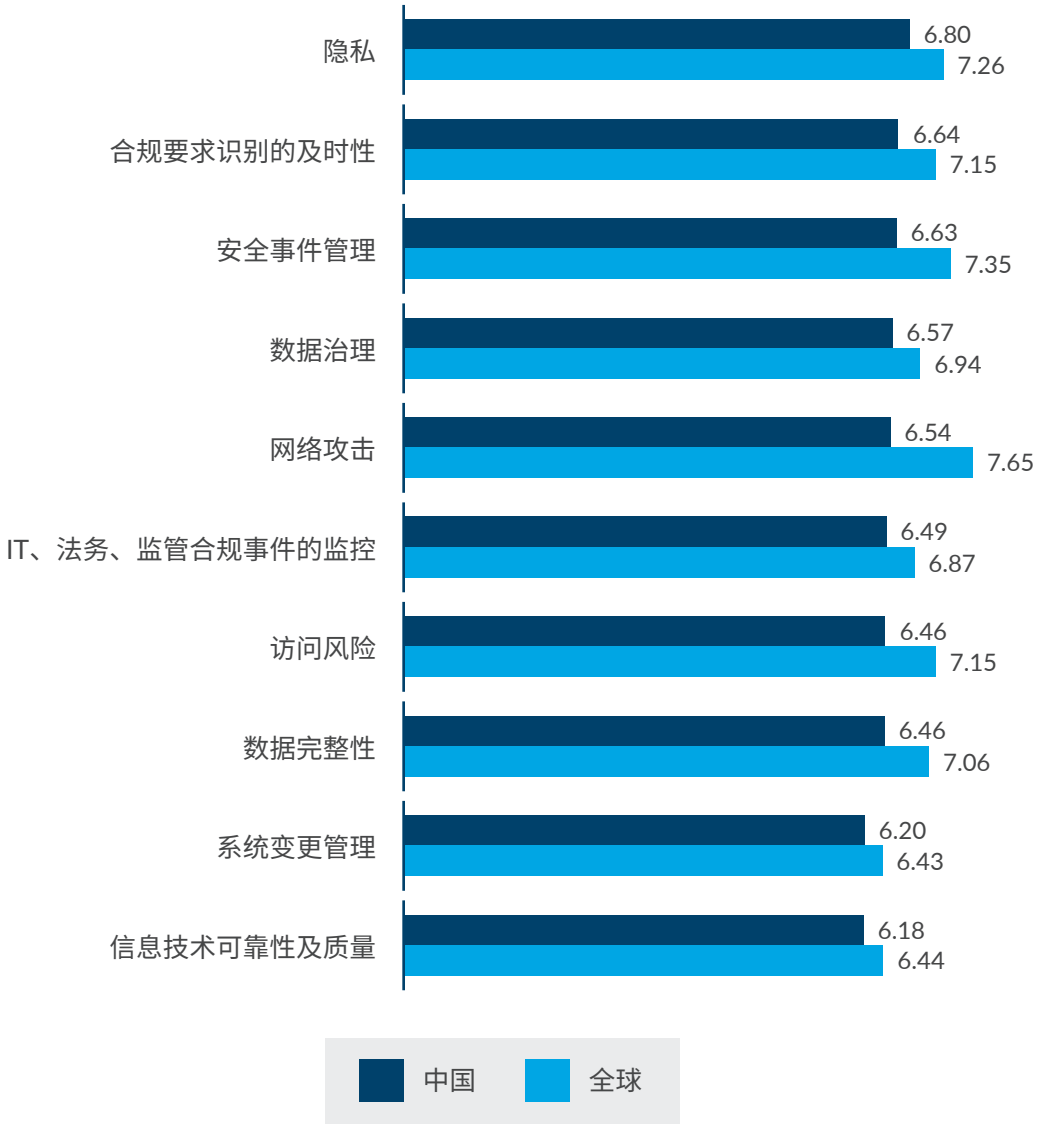
合规方面，IT审计团队更加重视合规要求的发展变化及相应的影响，亦需要通过汇报数据、系统、流程、控制及专业的人才，有效评估急速变化的合规风险。

纳入审计计划中的常见首要技术风险 – 全球



此处我们特别呈现中国地区的调查结果与全球综合数据的对比。根据下图可以看出，中国地区的前十大首要风险及风险排序与全球综合数据有所差异。隐私风险成为最受瞩目的焦点；数据治理及 IT、法务、监管合规事件的监控跃居前位；灾难恢复、第三方风险未进入前十，取而代之的风险要素是系统变更管理、信息技术可靠性及质量。该统计结果表明的趋势与中国企业信息技术快速更新迭代以及 IT 管理成熟度阶段等特点紧密相关。

2022年前十大首要技术风险 — 中国



关于本次调查

本次调查于2021年第四季度启动，是ISACA与甫瀚咨询合作展开的第十次年度IT审计技术风险研究，共计约7,591名企业高管和专业人士参与了我们的线上问卷调研，受访者包括首席审计执行官、IT审计副总裁、IT审计总监。

受访者按照10分制就每一项技术风险对企业的重要性进行评估，1分表示重要程度极低，10分表示重要程度极高。除了全球综合统计数据外，本次调查还基于行业、国家地域等不同维度，给出直观的风险重要程度排名。行业方面，涉及快消零售、能源和公用事业、金融服务、医疗保健、生产制造、国营产业、科技媒体及通讯7个行业。国家方面，涉及澳大利亚、中国、德国、香港特别行政区、印度、意大利、日本、中东、荷兰、新加坡、瑞士、英国、美国13个国家和地区。

本次调查采用自愿原则，故可能存在因参与者和未参与者在观点和认知上的不同而产生的调研结果偏差。另外，由于有些参与者只回答了部分问题，各地理区域的数据统计也可能存在不均衡因素。尽管会有以上固有限制，我们依然相信本次调查结果可为当今企业的IT审计实务提供有价值的洞见。

关于甫瀚咨询

甫瀚咨询（www.protiviti.com）是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2022年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，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。

关于国际信息系统审计协会（ISACA）

ISACA®（www.isaca.org）是一个全球性的组织，推动个人和企业在不断发展的数字世界中取得信任。50多年来，ISACA致力于为全球的技术领域专业人士和企业提供知识、资格认证、教育、培训和交流社群，以促进他们的职业发展和企业转型，从而建立一个更值得信赖和更具公序良德的数字世界。作为全球知名的专业协会和学习组织，ISACA拥有165,000多名成员，遍布在信息安全、治理、鉴证、风险、隐私和质量等数字工作领域。ISACA在全球188个国家和地区设有225个分会。通过其基金会One In Tech，ISACA支持缺少资源和话语权的人群获得IT教育和职业发展机会。

isaca.org

protiviti.com / protiviti.cn