企业内部控制简报

（2015 年第 1 期）

企业内部控制标准委员会 秘书处 签发人：杨敏

[编者按]：为宣传国内外有关内部控制理论研究成果和实务操作，进一步推动我国企业内部控制规范体系建设，企业内部控制标准委员会创办了《企业内部控制简报》。简报的主要内容包括：国内外有关内控标准制定机构和监管部门制定发布的文件、通知、公告、研究报告、最新动态等；国内外有关单位在内部控制体系建设、内控评价、内控审计等方面，具有创新性和可借鉴性的内部控制案例或实务操作；国内外有关方面在内部控制的本质特征、行为规范、机制原理等方面，具有开创性和突破性的内部控制理论研究成果；有关部门、行业或地区在推动企业内控规范实施工作中好的经验做法；其他有价值的内控研究成果。

欢迎有关单位或个人踊跃投稿。来稿请寄至企业内部控制标准委员会秘书处，并将电子版发送至 neikongjianbao@163.com。请在信封和电子邮件标题上标注“内控简报投稿”字样。邮寄地址：北京市西城区三里河南三巷 3 号财政部会计司综合处（企业内部控制标准委员会秘书处）（收），邮编：100820。

目　录

内控简讯

财政部关于印发企业内部控制标准委员会主席、副主席、委员、秘书长名单的通知

（财会〔2014〕26号）

自2006年企业内部控制标准委员会成立以来，在各委员单位的大力支持下，委员们认真履行职责，充分发挥专业指导和组织协调作用，为制定和完善我国企业内部控制规范体系发挥了重要作用。为充分利用企业内部控制标准委员会这一平台，进一步推动我国企业内部控制规范体系的建立健全及有效实施，我部对企业内部控制标准委员会进行了充实调整，在各委员单位推荐的基础上，经企业内部控制标准委员会主席批准，现将新的企业内部控制标准委员会主席、副主席、委员、秘书长名单予以印发。

企业内部控制标准委员会主席、副主席、委员、秘书长名单

主　席：

余蔚平　　财政部部长助理

副主席：

刘新华　　中国证券监督管理委员会副主席

陈尘肇　　审计署副审计长

周慕冰　　中国银行业监督管理委员会副主席

王祖继　　中国保险监督管理委员会副主席

孟建民　　国务院国有资产监督管理委员会副主任

朱宏任　　工业和信息化部总工程师

委　员（以姓氏笔画为序）：

王晓华(女)　财政部税政司副司长

方红星　　东北财经大学会计学院院长

方春生　　中国石油化工集团公司企业改革管理部副主任

邓力平　　厦门国家会计学院院长

白　涛　　中国人寿保险（集团）公司副总裁

冯来法　　国家电网公司财务资产部副主任

刘新宇　　宝钢集团有限公司风险控制总监

刘慧清(女)　深圳证券交易所副总经理

许世龙　　中国航天科技集团公司财金部部长

许科敏　　工信部中小企业司副司长

李扣庆　　上海国家会计学院院长

李福申　　中国联合网络通信集团有限公司副总经理、总会计师

杨　敏(女)　财政部会计司司长

杨雄胜　　南京大学会计与财务研究院院长

吴奇修　　财政部监督检查局局长

吴晓辉　　招商银行法律合规部总经理

何肖锋　　保监会发展改革部副主任

沈　翎(女)　中国五矿集团公司总会计师

肖雪峰　　财政部资产管理司副司长

张天强　　财政部驻浙江省财政监察专员

张克慧(女)　神华集团有限责任公司财务总监

张连起　　瑞华会计师事务所技术管理合伙人

陈毓圭　　中国注册会计师协会副会长兼秘书长

欧阳宗书　　财政部会计司副司长

郑　鑫　　中国农业银行内控合规部总经理

周明笙　　安永（中国）企业咨询有限公司合伙人

赵立新　　证监会上市部巡视员

郝爱群　　银监会银行监管一部巡视员

胡绳木　　中国大唐集团公司总会计师

都本正　　中国航空工业集团公司审计部部长

聂　颖　　中国航空集团公司总法律顾问

贾文勤(女)　证监会首席会计师兼会计部主任

徐　明　　上海证券交易所副总经理

高一斌　　北京国家会计学院院长

曾晓安　　财政部经济建设司司长

赖永添　　财政部条法司副司长

廖家生　　国资委财务监督与考核评价局副局长

滕铁骑　　中国第一汽车集团公司副总经理、总会计师

魏明海　　中山大学副校长

魏　强　　审计署企业审计司司长

秘书长:

杨　敏(兼) 财政部会计司司长

中国企业内部控制标准委员会与美国科索委员会

签署合作备忘录

2015 年 2 月 11 日，中国企业内部控制标准委员会与美国科索委员会（COSO）签署合作备忘录，两国内部控制标准制定机构将建立定期工作会议制度，并将在内部控制的标准制定、学术研讨、知识共享、人才培养等领域开展交流活动。

美国科索委员会是世界上最具影响力的内部控制和风险管理标准制定机构，其内控标准得到了许多国家内控标准制定机构的认可和借鉴，并在世界范围内各类型组织中得到广泛应用。中国财政部和中国企业内部控制标准委员会一直与美国科索委员会保持工作联系。2014 年 1 月，美国科索委员会主席何逸夫（Robert Hirth）先生拜访财政部余蔚平部长助理时，提出了中美在内部控

制领域建立定期沟通交流机制的建议。2014 年 10 月，美国科索委员会的创始成员单位——美国管理会计师协会（IMA）总裁兼首席执行官杰弗里·汤姆森（Jeffrey Thomson）先生拜访财政部会计司，进一步就中国企业内部控制标准委员会与美国科索委员会建立定期沟通交流机制以及中国参与 COSO 相关标准制定等事宜进行交流与会谈，并就双方合作的具体事宜达成初步共识。随后，经过多轮的磋商，中国财政部会计司司长、中国企业内部控制标准委员会秘书长杨敏和美国科索委员会主席何逸夫于 2015 年 2 月 11 日共同签署了《中国企业内部控制标准委员会与美国科索委员会合作备忘录》。双方在合作备忘录中表示，中美两国将进一步深化在内部控制领域的交流与合作，共同致力于建立高质量的内部控制标准，促进内部控制在各类型组织中的广泛运用，推动内部控制在保障资本市场健康发展和提升企业经营管理水平及风险防范能力方面发挥积极作用。

《中国企业内部控制标准委员会与美国科索委员会合作备忘录》的签署，标志着中美在内部控制领域的交流与合作取得重要进展，有利于我国准确了解国际内部控制标准的最新发展动向，进一步完善我国内部控制规范体系；有利于我国全面参与国际内部控制标准的制定，提高我国在国际内部控制领域的影响力和话语权；有利于打造我国全方位、多领域的会计对外交流格局。

此外，美国科索委员会于2014年10月启动了《风险管理——整合框架》的修订工作。按照合作备忘录的规定，美国科索委员会专门邀请我国参与相关修订工作，这是第一次外方主动邀请我国参与国际内控标准制定工作。

财政部启动小型企业内部控制规范研究制定工作

在我国，小型微型企业数量庞大，已成为国民经济的重要支柱，是经济持续稳定增长的坚实基础。截至2013年年底，全国各类企业总数为1528万户，其中小型微型企业1170万户，占到企业总数的77%，将个体工商户纳入统计后，小型微型企业所占比重达到94%[1]。据统计，我国中小企业创造的最终产品和服务价值相当于国内生产总值(GDP)总量的 60%,纳税占国家税收总额的50%,完成了 65%的发明专利和 80%以上的新产品开发[2]。党中央、国务院高度重视小型微型企业的发展，出台了一系列财税金融扶持政策，取得了积极成效。但受国内外复杂多变的经济形势影响，小型微型企业经营压力大、成本上升、融资困难等问题仍很突出。因此，在当前中国经济进入新常态的大背景下，大力支持小型企业发展，从内控角度为其提高经营管理水平、提升风险和舞弊防

1. 《全国小型微型企业发展情况报告》，国家工商总局全国小型微型企业发展报告课题组
2. 《全国小型微型企业发展情况报告》，国家工商总局全国小型微型企业发展报告课题组

范能力提供指导和帮助，对保障广大小型企业持续运营，培育小型企业不断发展壮大，促进国民经济健康发展具有重要意义。

截至2014年底，企业内部控制规范体系已经在我国1400余家主板上市公司和113家中央企业范围内得到平稳有效实施，而中小板、创业板上市公司和广大非上市小型企业尚未实施企业内控规范体系。财政部等五部委发布的企业内部控制规范体系主要适用于大中型企业，小型企业实施这一套体系的成本偏高，理论界和实务界对制定出台小型企业内部控制规范呼声很高。为此，近期财政部将联合有关部门，组织有关内控咨询专家，成立专门工作小组，研究小型企业内控规范的体例体系、主要内容、实施要求等，择机发布实施《小型企业内部控制规范》，为下一步中小板和创业板实施内控规范以及广大中小企业开展内控体系建设提供制度依据和参考。《小型企业内部控制规范》的制定将充分考虑小型企业的资源限制，坚持成本效益原则，侧重于财务报告内部控制，重点突出实用性和可操作性，引导小型企业在有限的资源下防范各类风险，切实降低小企业的内控实施成本，有效提升小企业管理水平和风险防范能力。

国际视野

网络时代的内部控制[1]

（Mary E.Galligan & Kelly Rau）

一、网络时代的商业变革

当组织考虑如何应对日益严峻的网络安全风险时，无论是COSO内部控制整合框架（“2013框架”）还是企业风险管理整合框架（2004）均提供了评价风险和管理风险的有效方法。事实上，这两个框架都系统性地引导组织通过COSO的视角以相似的路径去应对网络风险。随着各公司致力于实施2013框架，在本文中，我们结合2013框架阐述如何使用COSO框架以协助组织管理网络风险和实施控制。

1992年内部控制整合框架（1992框架）发布时，商业运营环境同现在相比截然不同。 例如:

• 1992年在全世界范围内仅有不到1400万互联网用户，而今天有接近30亿的用户。

1.2015年1月，美国科索委员会（COSO）发布了《网络时代的内部控制》参考性文件。该文对于企业应用COSO内部控制框架（2013）防范网络风险具有指导性作用。该研究由美国科索委员会委托德勤Mary E.Galligan总监和Kelly Rau高级经理承担。在美国科索委员会授权下，财政部会计司联合德勤（中国）翻译了该文。在翻译审校过程中，中山大学林斌教授、普华永道（中国）武瑶女士、安永（中国）司婉玲女士给予了大力支持，在此表示感谢。

- 基于微软 DOS 系统的美国在线（AOL） 刚刚被发布。
- 微软 IE 浏览器尚不存在。
- 最流行的手机是“大哥大”。
- 电话和传真是商业沟通中最为主要的方式。

在过去的二十年间，信息技术（IT）让商业运营模式发生了翻天覆地的变化，网络驱动成为商业运营的基本环境。客户订单使用电子数据在互联网中进行交互处理从而没有或很少有人工参与；业务处理往往是通过内部网络外包给服务供应商；越来越多的员工远程工作或在家工作，而不再需要到办公室；仓库中的库存情况通过使用射频识别（RFID）标签进行跟踪；伴随网上银行的出现，几乎所有的银行都向客户提供网上银行服务。

随着商业和技术的发展，2013 框架也在不断完善。更新和发布 2013 框架的一个根本的驱动因素就是帮助组织利用和依靠不断发展的技术以实现内部控制目标。2013 框架在许多方面进行了改进，并考虑了组织应如何管理 IT 创新的思考:

- 市场和运营的全球化趋势;
- 更加复杂的业务流程;
- 法律、条例、规章和标准的要求及复杂性;
- 使用和依靠不断发展的技术;
- 预防和发现舞弊行为的要求。

自从1992框架发布以来，商业模式的创新已经与网络形成了错综复杂的联系。然而，互联网设计的初衷是共享信息，而不是保护信息。每天都有许多重大网络事件被媒体报道出来。虽然某些行业受到网络攻击的事件在新闻中占据更大的比重，但其实所有行业都有可能受到网络攻击。在特定的时点，哪些数据、系统和资产是有价值的，将取决于网络攻击者的动机。随着网络事件持续对受害公司的财务状况产生负面影响，并持续引起额外的监管审查，网络漏洞将继续成为媒体报道的高频事件。

此外，信息技术将继续改变全球经济中的商业运营模式。随着数字化的普及，特别是企业与外包服务供应商的外部合作伙伴共享数据的情况越来越普遍，信息技术的应用增加了业务复杂性及不稳定性，使企业更加依赖信息技术相关的基础设施，而这些基础设施却不完全受企业控制。即便企业与外部机构（如服务提供商，供应商，客户）建立了相互信任的关系，能够确保日常的信息共享及电子化沟通，一旦出现问题，企业还是需要为这些不在其控制范围内的信息技术承担责任。随着公司不断利用新技术和继续聘用外部机构开展运营，网络攻击者将利用新的漏洞对企业进行攻击，这就促使企业开发新的信息系统和控制手段以规避风险。

虽然企业为了保护业务，在内部和外部共享技术信息时非常谨慎，但网络袭击者却在网络的另一边肆意地进行操作。他们没

有限度地公开分享信息，而不惧怕任何法律后果，而且经常大量进行匿名操作。网络攻击者几乎可以利用技术攻击任何地方的任何类型的数据。

即使没有这无处不在的网络威胁，保护所有的数据也是不可能的，特别是考虑到组织的目标、流程和技术如何持续革新以支持其业务。每次革新都将有可能暴露风险——尽管通过周密的安排，革新可以降低风险，但仍不可能完全规避风险。此外，网络攻击者也在不断升级，寻找新的方法来发现信息系统的弱点。结果就是，事实上网络风险是不可避免的，因此，管理网络风险是必要的。。一旦明确对组织至关重要的数据，管理层必须投入成本，建立安全控制措施以保护其最重要的资产。通过采用一系列措施使组织具备安全性、警惕性、可恢复性，组织将对实现战略投资的价值更有信心。

为了能够以安全的、警惕的和可恢复的方式管理网络风险，组织可以通过内部控制要素来分析网络风险。例如:

• 控制环境 —— 董事会是否了解组织的网络风险概况以及是否了解组织如何应对面临的不断变化的网络风险?

• 风险评估 ——组织及重要的利益相关者是否对其运营、报告以及合规目标进行评估，并收集信息以了解网络风险对这些目标的影响?

• 控制活动 ——组织是否制定了控制活动，包括信息系统一般控制，使组织在风险承受水平内管理网络风险？该控制活动是否通过正式的政策和程序进行实施？

• 信息与沟通——组织是否明确了网络风险内部控制所需要的信息？组织是否已确定了支持内部控制持续运行的内部和外部的沟通渠道和方案？组织将如何应对、管理和沟通网络风险事件？

• 监督活动 ——组织如何选择、制定以及执行与网络风险相关的控制设计及执行的有效性的评估？当缺陷被识别后，如何进行沟通并优先进行整改？组织通过哪些措施来监督网络风险？

当公司通过 COSO 框架的视角去管理网络风险时，董事会及高级行政人员能更好地沟通他们的运营目标、关键信息系统的定义以及相关的风险承受水平。这使组织内的其他人，包括 IT 人员，可以对网络风险进行详细的分析，包括最有可能受攻击的信息系统、可能的攻击方法和最有可能被攻击者利用的信息。由此实施适当的控制活动以应对这些风险。

在讨论每一个内部控制要素时，我们将展现每个要素之间是如何相互关联的，以及如何基于内外部信息开展持续的、动态的风险评估。

控制环境和监督活动要素是考虑网络风险的基础。为了使组织具备安全性、警惕性和可恢复性，这两类要素必须存在并持续

运行——若非如此，组织可能无法充分理解网络风险，部署有效的控制活动，并对网络风险做出适当的应对。因此，本白皮书的主要重点将放在风险评估、控制活动以及信息与沟通要素，我们将在本文的结束语中讨论对于控制环境和监督活动方面的思考。

二、基于 COSO 的网络风险评估

任何一个组织都会面临一系列由外部和内部因素引发的网络风险。我们可以通过评估对实现组织目标存在的不利影响和事件发生的可能性来评估网络风险。恶意行为，尤其是那些受经济利益驱动的行为，往往出于对成本和利益的权衡。实施网络攻击的犯罪者及其动机可以分为以下几类:

• 敌对国家和间谍——敌对国家以军事和获得竞争优势为目的寻求知识产权和交易机密，窃取国家安全机密或知识产权。

•有组织的犯罪者——运用精密工具窃取钱财或公司客户的私人敏感信息（如盗用身份信息）。

• 恐怖分子——以团体或个人的形式利用互联网对包括金融机构在内的重要基础设施进行网络攻击。

• 黑客 ——以团体或个人的形式，通过窃取或公开组织敏感信息发布社会或政治言论。

• 内部人员——组织内部受信任的个人出售或公开组织敏感信息。

控制活动能够防范、发现和应对网络风险，而风险评估结果最终会影响组织在控制活动上的资源分配，因此对于风险评估过程本身也必须要进行投资。组织资源有限，因此针对控制活动的投资决策必须依据相关的高质量信息，优先为对组织来说最重要的信息系统提供资金支持。

评估组织网络风险需要首先理解信息系统对组织的价值。该价值可通过评估其对组织目标的潜在影响来衡量。

原则 6[1]　组织应设定清晰明确的目标，以识别和评估与目标相关的风险。

2013 框架在原则 6 中提供了若干关注点，为组织在网络风险评估过程中评估组织目标提供了参考。这些关注点分为以下五类:

- 经营目标
- 外部财务报告目标
- 外部非财务报告目标
- 内部报告目标
- 合规目标

网络风险评估会帮助管理层作出用以支持组织目标实现的信息系统控制活动的决策部署，因此高级管理层和其他重要的利益相关方需要引导风险评估过程，根据组织目标确定需要被保护的信息系统。很多组织没有花费足够精力了解对组织来说最重要的

1.源自《内部控制——整合框架》（2013）中列示的 17 项内部控制原则。下同。

信息系统，他们也不了解信息在哪里储存、如何储存。这会导致组织企图保护所有方面，从而导致过度保护某些特定的信息系统，而又对其他的信息系统保护不足。

信息系统的价值评估需要业务和信息技术人员的高度配合。因为在有限的时间、预算和可利用的资源下，组织无法采取措施应对所有风险，因此管理层需要确定组织可接受的风险承受水平，重点保护最重要的信息系统。

原则 7　组织应对影响其目标实现的风险进行全范围的识别和分析，并以此为基础来决定应如何管理风险。

原则 8　组织应在评估影响其目标实现的风险时，考虑潜在的舞弊行为。

应用原则 6 进行目标识别后，组织应当清晰地理解对于实现目标具有重要影响的信息系统。然后应用原则 7 和原则 8，进行更深入的风险评估，引导组织评估网络风险影响的严重程度和可能性。在高级管理层的领导下，通过业务和 IT 利益相关方的配合，组织能够有效评价影响组织目标实现的风险。

为了使风险评估过程有效，相关人员必须了解组织网络风险概况，这包括了解哪些信息系统容易成为攻击者的目标，了解哪些攻击行为容易发生。会造成组织付出高额代价的攻击一般是组织最为关注的部分，组织应该了解并时刻警惕这些网络威胁。

保持警惕意味着在组织中建立危险意识，有些行为模式预示着重要资产损失，在组织中应当提高发现这种行为模式的能力。组织必须将其整合到整体风险评估过程中，以便识别在哪些节点实施控制，以保护资产安全。

与仅广泛关注网络风险相比，关注行业特定的网络风险更为重要。网络攻击者对于各行业有特定的攻击目标。比如，在零售行业，有组织的攻击者主要利用信息系统中的薄弱点，窃取能够用来获利的特定信息（如信用卡数据或个人身份验证信息）。石油天然气行业容易成为敌对国家为窃取勘探地战略数据而攻击的目标。化工企业由于其产品带来的环境问题也容易遭受黑客攻击。

无论出于哪种动机，网络攻击者都是坚持不懈的、技术娴熟的、有耐心的。他们会通过收集暴露组织信息系统和内部控制弱点的信息来分阶段进行攻击。通过仔细识别其动机和可能的攻击方式，以及所用的技术、工具和流程，组织可以更好地预测风险，设计有效的控制措施，并在网络攻击发生时最小化潜在风险，保证重要资产的安全。

原则 9　组织应识别并评估对其内部控制体系可能造成重大影响的改变。

任何组织都会存在变化的情况，在评估网络风险时，应当预测这些变化。组织会不断发展，包括目标、人员、流程和技术都处在变化之中。网络环境也会发生变化，包括产生新的网络攻击

者、新的攻击方式。尽管网络风险评估主要关注组织目前状况，但评估过程必须是动态且持续的，需要考虑内部和外部威胁的变化，据此调整组织管理网络风险的方式。

在组织寻求发展、创新及成本优化的过程中，往往伴随着经营模式创新与科技创新。然而，这些创新也会带来新的网络风险。比如，网络、移动设备、云技术和社交媒体技术的采用会增加被网络攻击的风险。相似地，外包、离岸和第三方合作会导致潜在的、超出组织控制范围的网络漏洞。这一趋势促使网络生态链条的不断发展，同时也给网络攻击者实施攻击提供了更大的平台。对于可能影响内部控制体系发生变化的评估需要考虑人员的变动。业务层面人员的流动对于组织实施网络风险相关控制活动的有效性有很大影响。

风险评估需要不断更新，以反映那些会影响组织为保护关键信息系统而实施的相关控制的变化。监控变化中的威胁情况以及风险评估过程将产生信息，高级管理层及利益相关方必须分享并讨论这些信息，以制定避免组织暴露于网络风险之中的最佳决策。

三、识别并执行网络风险控制活动

原则 10　组织应该选择并执行那些可以将影响其目标实现的风险降至可接受水平的控制活动。

原则 11　针对信息技术，组织应选择并执行信息技术一般控制以支持其目标的实现。

原则 12　组织应通过政策和程序来实施控制活动。政策是建立预期，程序是将政策付诸行动。

控制活动由组织中的员工实施，帮助确保管理层方针得到有效执行，以降低影响组织目标实现的风险。这些控制活动需要在政策中明确，以确保控制活动在组织中执行一致。

如前文所述，网络风险不可避免，但组织可以通过设计和执行适当的控制措施来管理网络风险。当组织通过风险评估流程考虑到可能的攻击方式和路径时，组织可以更有效地降低潜在的网络漏洞对实现组织目标的影响。意识到网络风险不可避免，并实施适当的风险评估后，组织应当按层级建立多层控制防线，防止攻击者在攻破第一道防线后继续侵入信息系统。

由于网络风险可能暴露在组织内部和外部的多个切入点上，因此，可以同时应用预防性和发现性控制，以降低网络风险。有效的预防性控制能够未雨绸缪，使得攻击者无法接触到组织内部信息技术环境，保证信息系统安全。此外，在组织内部信息技术环境中实施预防性控制，对攻击者侵入网络环境设置障碍，可以延缓了攻击的速度。即使被入侵，这些控制会使组织及时发现，并尽早采取整改措施修正漏洞和评估潜在损失。实施整改措施后，管理层需要研究入侵发生的根本原因，进而完善控制措施以预防和发现未来可能发生类似攻击。

除了预防性控制和发现性控制，为降低网络风险而部署的控制活动还应包括与其他业务控制相联系的信息技术一般控制（GITC）。信息技术一般控制会帮助预防或发现网络入侵，使得组织面对灾害具备快速反应及恢复能力。发现网络攻击事件时，应当及时与组织中的相关人员进行沟通，以采取进一步降低风险的措施。由于风险评估是基于对组织目标的理解开展的，需要关键利益相关方参与其中，因此组织应当编制基本的联络图，明确当网络攻击事件发生时，哪些人员应得到及时的通知。

尽管2013框架提供了原则和关注点以指引组织建立有效的控制活动，它并没有涵盖组织应当采取的具体控制措施。每个组织都是由具有不同技术、不同经验的人员构成，这些经验技术会影响他们的职业判断，进而影响内控。当评价组织是否设计并实施适当的控制以应对网络风险时，可以将控制活动与网络风险管理相关的标准和框架对比。以下提供了一些网络风险相关标准和框架指引，可以帮助组织评价控制的充分性，以确保组织安全、警惕和可恢复。

网络风险相关的标准和框架指引

COBIT　由ISACA编制，协助管理层弥补在控制要求、技术问题及业务风险之间的缺口。

ISO　国际标准化组织编制了ISO 27000系列，为组织实施支持信息安全准则的流程和控制制定标准。

NIST 美国商务部国家标准与技术研究所于2014年2月发布“关于提高关键基础设施网络安全”的框架（第一版）。该框架依据现有标准、指引和操作实务，引导组织降低网络风险的潜在影响。

四、形成并沟通相关的高质量信息，以管理网络风险和控制

信息与沟通要素有三项原则，包括:（1）识别相关的高质量的信息;（2）确定信息在组织内部的沟通方式;（3）确定组织与外部的沟通方式。所有其他内部控制要素均依赖于信息与沟通要素提供的相关的高质量信息。尽管在应用2013框架时，所有的关注点都需要考虑，但某些关注点就网络风险及其控制而言更加重要。这些关注点会在本部分中重点强调。

原则 13 组织应获取或生成和使用相关的高质量信息来支持内部控制的持续运行。

1.识别信息需求

组织的控制活动决定了信息需求。信息的形式可以是报告、控制分析中的数据、显示组织商业结构概况的图表。

识别对于内部控制较为重要的信息需求和进行网络风险分析，在风险评估过程是密不可分的。比如，网络风险评估需要的是逐层的信息，通过高层级的信息来引导更为详细的风险评估程序。

最终，组织需要明确信息系统及其价值，通过实施与其价值匹配的控制措施保护其不受网络攻击。为了达到该目标，业务人

员和信息技术人员（包括外部服务供应商）必须首先对商业结构的整体框架达成共识，包括相关的对组织重要的商业目标和子目标。依据这些信息，组织可以延伸风险评估范围，深入了解可能受到攻击的信息系统及攻击方式。一旦完成风险评估，组织将沟通这些信息，确保所设计的流程和控制能够用来应对这些风险。

尽管该概念容易理解，但由于人员、流程和技术会随着组织目标不断发展，组织仍需将信息要求（以及相关的风险分析和应对）记录为正式文档，以帮助确保流程和控制的实施与相关的高质量信息保持一致，从而能够持续反映那些由于组织目标的变化，而导致的人员、流程和技术的变化。

2.将相关数据转化为信息

在当今商业环境下，具有警惕性的组织能够收集到大量的信息系统活动日志数据。安全运营中心每天产生大量预警数据，以及数万至数百万个预警事件。为了对网络风险保持警惕，将原始数据转换成有意义的、可操作的和可靠的信息就变得极其重要。

对很多组织来说，通过识别风险事件的预警模式将原始数据转化为信息是很困难的。每天、每周、每月都会产生大量信息，从中找出预警信息是很有挑战性的。进一步讲，通过观察单一事件，通常无法识别网络风险事件。往往经过一段时间，从多渠道整合信息，才能识别风险并采取措施处理被发现的网络事件。由于控制依赖于及时的、相关的、高质量的、完整的信息，如果组

织无法将原始数据转换成可用于自动或人工控制的可操作信息，组织将无法采取恰当措施。

3.从内部和外部来源获取数据

如前文所述，对于信息的需求使得信息来源于内部或外部。尽管网络风险分析和控制的主要信息来源会从内部产生，但组织仍需考虑需要从外部获取数据。下列外部数据来源的示例未必全面，但很可能适用于大多数组织。

• 商业或行业的外部数据：从网络角度看，行业中所有公司的发展模式和趋势是类似的。行业中各公司信息系统的价值及运用的技术也是类似的。这种一致性会影响网络攻击者的行为和采取的攻击方式。尽管与外部共享信息需要谨慎，但与可信任的同盟或同行业组织共享信息并讨论网络事件发生趋势，能够帮助组织预防和发现网络风险事件。

• 政府机构外部数据：尽管获取政府机构外部信息需要得到政府的安全等级权限，但这些信息对实施控制以应对网络风险具有重要意义。针对日益严峻的网络风险威胁，许多政府部门支持通过提升流程和控制来免受侵害。

• 外部服务提供商外部数据：由于组织通常会将某些职能或流程外包给其他服务组织，从这些服务组织获得的网络事件信息可以帮助识别和控制网络风险。为了获得期望的外包服务效益，需要建立信任关系，将双方的信息系统相联接。尽管组织与外部

服务供应商基于自身的利益均想保护其信息系统，当网络事件同时威胁到双方及各自的经营目标时，双方都应意识到信息共享的重要性。如果某一方出现了会影响另一方业务运营的风险事件，一定程度的信息透明度和与该风险事件相关信息的共享可以增强双方的快速反应及恢复能力。

4.在处理过程中确保信息质量

网络时代的控制活动的设计依赖于信息，因此组织在实施控制活动时需要考虑信息的质量。正如应当在组织中广泛建立信息管理相关制度，这些制度也应应用于网络风险控制活动中。组织应当明确责任和义务，遵循数据治理相关要求，保护数据和信息避免未经授权的访问和修改，从而保证信息的质量。

组织生成并使用用以支持内部控制持续运行的相关的高质量信息的能力依赖于数据治理。在利益相关方中建立共识并由管理层牵头实施，对建立有效的数据治理机制至关重要。一旦组织建立了有效的数据治理项目且能够持续实施该项目，则能够获得高质量的信息。信息质量能够提升组织的内控体系，完善与网络风险相关的内部控制。

原则 14　组织应在内部对内部控制目标和责任等必要信息进行沟通，从而支持内部控制持续运行。

5.沟通内部控制信息

（1）全体员工。保持安全性、警惕性、可恢复性是组织的责任，每位员工在保护信息系统安全中扮演不同的角色。尽管某些员工有明确责任负责管理网络风险和控制，组织中的每位员工都应对保护信息系统保持警惕。组织应当制定并实行全组织范围的沟通计划，提升每位员工的网络风险和控制意识。

信息沟通能够帮助加强内控链条中的薄弱点——人。由于人性使然，人成为了内控中最薄弱的环节，尤其考虑到人的好奇心带来的后果时:

当人们收到被认为是可信任的同事、顾客、供应商或其他商业伙伴的邮件时，人们会怎么做？如果邮件看起来是正式的，仅仅点击一个链接就可能导致网络入侵。

当人们发现地上有一个U盘，人们会怎么做？当他们把U盘插到电脑上想查看是谁的U盘时，在U盘中预先加载的程序会导致公司面临网络攻击者的威胁。

人的特性比如好奇心和对他人的信任，为网络攻击者提供了攻击组织内控薄弱点的机会。针对这种情况，比较有效的方式是定期对员工进行培训，提升网络安全意识，降低攻击者从普通员工入手进行网络攻击的可能性。 用不同的方式来实现沟通计划，能够最大限度的提升员工网络风险意识和责任感。持续的沟通（如直播会议，全公司范围发送消息）为员工提供了相关且及时的信

息传递机制。例如新员工培训和年度培训项目可以帮助组织完成相关信息传递。

（2）对于网络风控有明确管理和监督责任的人员。正如之前控制活动要素中提到的，管理层应当选择、执行和部署内控，以保护信息系统。内控信息应当内部共享，使管理层和员工能够履行网络控制责任。

由于网络系统的复杂性，维护正式的网络控制的文档是十分重要的。没有支持内部控制预期的正式文档，组织有效管理网络风险的能力就会急剧降低。组织需要正式的文档来评估控制设计和实施的有效性，以保护组织的信息系统。

（3）董事会。当前，董事会比以往任何时候都需要了解那些可能影响组织实现其目标的网络趋势。董事会在以下方面发挥了重要的作用：通过了解网络风险，保持组织安全性、警惕性和可恢复性；基于已设定的风险容忍度，确定应对网络风险的预防性和发现性控制措施已实施；并且明确对于管理层所确立的风险应对流程和程序的期望。

董事会和管理层（包括高级管理层和运营管理层）的有效沟通，对董事会履行内部控制监督职责至关重要。为了保持董事会层面的有效沟通，复杂的信息技术内容，需要转换成有意义的、可操作的信息。

尽管董事会成员或其他下属委员会中有网络和（或）信息技术专家，但大部分董事会成员对于网络和信息技术的相关知识是有限的。董事会成员的这种差异使得对信息需求的解释和定义显得极为重要，以确保董事会能够履行监督职能。

根据董事会对信息要求的定义，组织可以利用相关的信息技术框架和标准，从而将技术性很强的内容转换为无论信息技术背景还是业务背景的人员都能够理解的内容。这些框架和标准在上文控制活动要素中有所涉及，包括 COBIT、ISO 以及 NIST 发行的网络安全框架等其他近期颁布的框架和标准。

尽管董事会层面的定期沟通会涵盖网络方面的讨论，也应当建立其他沟通渠道，以确保及时沟通出现的重要网络事件。当发生影响组织目标实现的重大网络风险事件，且组织可能需要就该事件与外部沟通时，及时与董事会进行沟通，并提供当时可获得的高质量信息，是组织具备快速反应及恢复能力的体现。

原则 15 组织应就影响内部控制持续运行的事项，与外部进行沟通。

（4）外部机构。在网络安全大环境下，政策和标准的应用是有效管理和控制外部沟通的重要手段。外部沟通会涉及到股东、所有者、客户、商业伙伴、监管者、金融分析师、政府机构和其他外部机构。就网络风险而言，与外部机构沟通的两个驱动因素：

- 确保由外及内的沟通能够影响网络风险评估和控制。

• 通过由内及外的沟通向外部相关方传递与网络事件、活动相关的信息，或者其他可能影响外部相关方与组织互动的情况。

通过与外部机构对组织的沟通，组织可以获得有价值的信息。尽管管理层必须确认这些信息的质量，但通常来说，由外对内的沟通会为网络风险评估和内控提供有价值的信息。

相反地，由内及外的沟通能够向外部机构提供有价值的信息。这是组织所具备的可恢复能力的一种体现。如果没有使用恰当的控制，这种沟通可能会损害组织的利益。当组织向外界提供信息后，组织对于这些信息的控制能力有限，这些信息可能会被其他组织获得且利用。

在权衡外部沟通的利弊，并减少其可能导致的对组织的负面影响时，面对名誉损害、股价变动、潜在诉讼致使客户或其他利益相关方受损，甚至是暴露更多机会给网络攻击者等后果，制度与标准对管理风险的重要性就显而易见了。

五、控制环境和监督活动——缺乏有效的公司治理将无法管理网络风险

控制环境和监督活动要素是组织有效管理网络风险的基础。

正如 2013 框架中所述“控制环境是一套标准、流程和结构，能够为组织实施内部控制提供基础。董事会和高级管理层应在高层建立基调，强调内部控制的重要性（包括期望的行为准则）。”

董事会和高级管理层有权力和责任明确公司的首要任务。如果组织没有将安全性、警惕性和可恢复性设定为首要任务并在组织内部进行沟通，组织将无法部署足够的资源来保护其信息系统并适当地应对网络事件。

应对复杂的网络风险对于董事会和管理层来说是一个艰巨的挑战。为了履行其管理网络风险的责任，信息技术的主题需要被纳入组织目标中并得到优先关注。尽管一些组织可能有专业人员可以就信息技术如何影响一个组织的流程和目标进行解释，但许多组织仍需要外部专家的帮助引导战略决策，以使组织变得更安全、更警惕和更具可恢复性。

为了有效的将资源优先部署到应对网络风险中，得到专业的网络风险管理专家的援助是至关重要的。董事会和管理层必须认识到并被告知信息系统的价值是与组织目标相一致的。根据这些信息，他们可以设定自身的风险承受水平，并确保将足够的资源用以保护对组织目标至关重要的信息系统。

正如 2013 框架在监督活动所述“主体应通过持续评估、单独评估或者两者的组合，以确认内部控制的五个要素，包括实现每个要素中原则的控制活动是否存在并持续运行。对监督时所发现的问题应进行评估，并及时沟通缺陷，如有重大事项应向高级管理层和董事会报告。”

专业的网络风险管理人员对于组织的监督活动也非常重要。为了减少潜在的网络风险暴露，组织应对控制活动的设计和执行有效性开展持续评估和单独评估。如果负责监督活动的人员不具备足够的网络风险控制能力，那么事先考虑解决方案就很重要，或者在组织内部培育这种能力，或者引入外部专家进行协助。

如前文所述，很多公司的信息技术环境延伸到其他组织。在这种情况下，监督第三方或其他外包服务供应商的网络控制活动就很重要。如果供应商不能提供审计报告或报告不能充分说明网络控制的情况，组织应努力采取措施以了解这些控制，从而确保其具备安全性及警惕性。

如果管理层将网络风险管理列为首要任务并通过监督活动认真评估网络控制，组织在面对可能影响其目标实现的网络风险变化时，将能更好地进行部署内部控制，以确保网络风险变化是可控和（或）可预期的。

对管理层同等重要的是，发现缺陷时进行有效沟通。对于问题的有效沟通是分析产生问题的根本原因并修正控制活动，实施有效整改计划的必要前提。此外，为了加强组织的警惕性，应采取措施以确保内部控制的责任人切实承担起保护信息系统的责任。

六、结束语

通过从 COSO 框架的角度分析网络风险，很多组织可能会重新考虑他们应如何应对变化来提高他们的控制手段，以减少网络风

险对组织目标的影响。即使组织目前没有将安全性、警惕性和可恢复性设定为网络风险管理的优先目标，那么最终它也会成为优先目标。如果以被动的方式管理网络风险，网络攻击造成的损害可能导致非常严重的后果，甚至可能导致组织破产或停止运营。随着时间的推移、技术的发展以及黑客手段的日益成熟，网络风险只会变得更加难以管理。从现在开始，在网络风险管理方面进行投入，并使其得到与其他目标类似的优先关注，对组织具有战略意义。如何开始将取决于组织的实际情况。2013 内部控制整合框架可以用来作为一个转型的指南，支持组织在网络驱动的环境中设计、评估并保持控制环境的安全性、警惕性和可恢复性。

报： 部领导，企业内部控制标准委员会主席、副主席

送： 企业内部控制标准委员会委员，部内各司局，各位司领导，企业内部控制标准委员会咨询专家（电子版）

2015 年 3 月 6 日　（印 80 份）