首次全面解析 2017 COSO 正式版《企业风险管理框架》（干货收藏版）

2017 年 9 月 6 日晚（美国时间 9 月 6 日早），全球风险管理行业翘首以盼的 COSO 更新版《企业风险管理框架》正式发布，距离 2016 年 9 月 30 日全球意见征集截止，已经过去了将近一年的时间。在这个过程中，笔者一直和 COSO 主席 Hirth 先生保持的紧密的沟通。当看到摘要中新框架与征求意见稿的变化如此巨大时，笔者大概理解了正式版迟迟没有推出的原因，COSO 内部肯定经历了大量的讨论、争议、妥协和坚持。

9 月 7 日一早，笔者便拿到了 COSO 正式发布的《企业风险管理框架》正式版，总共 201 页，这应该是中国第一份全文正式版文件。其中附录 B 中记录了定稿这个过程中关于对 1600 多条反馈建议的考虑、大量的不同意见的处理以及 40 多场研讨会，正好证实了笔者之前的猜测。针对 2016 年 COSO 发布的征求意见稿，笔者去年 12 月份曾专门翻译了其中精要并发布了征求意见稿解读（参见前期公众号文章）。

公众可以在 COSO 的网站上（ www.coso.org）免费下载公开的几个介绍文件： 1、企业风险管理框架 -摘要； 2、企业风险管理框架 -常见问题； 3、COSO 发布正式版企业风险管理框架的新闻稿。

下面，我们就正式版《企业风险管理框架》的相关背景和主要内容进行分析介绍。　　一、2017 正式版（第二版）《企业风险管理框架》与　2004 年《企业风险管理　-整合框架》的异同

2004 版框架发布据今已有十几年时间，　　这十几年间，　风险的复杂性发生了重大变化，由于新环境、新技术的不断演变，新的风险也层出不穷。　在此前提下，　COSO 在 2014 年启动了首次对风险管理框架的修订工作，新版本更新的内容主要包含：

变更了题目和框架展现方式；应用了要素和原则的编写结构；简化了企业风险管理的定义；强调了风险和价值之间的关联性；重新审视了企业风险管理整合框架所关注的焦点；检验了关于文化在风险管理工作中的定位；提升了对战略相关议题的研讨；增强了绩效和企业风险管理工作的协同效应；体现了企业风险管理支持更加明确的做出决策；明确了企业风险管理和内部控制的关系；优化了风险偏好和风险承受度的概念。

没有变化的部分是保留了　　2004 年出版的《企业风险管理　-应用技术》，只是对框架本身进行了更新，风险管理工作者仍然可以使用　2004 年发行的风险管理相关工具和技术。

二、正式版与征求意见稿的异同　　1、标题

首先，正式版框架的名字与征求意见稿发生了变动，从

Enterprise Risk Management-Aligning with Strategy and

Performance 变成了 Enterprise Risk Management-Integrating with Strategy and Performance，从“ Aligning ”到“ Integrating ”，虽然只变化了一个词，但含义大不相同，这个词的变化直接体现了整个框架从征求意见稿到正式版发布的核心理念的变化，对比两个文件的全文会发现，内容变化的核心正是体现了从“ Aligning ”到“ Integrating ”两个词义的不同。

“ Aligning ”可以意为协同、相协调、保持一致等，表达企业风险管理工作应该和企业战略与绩效相协同、相协调；

“ Integrating ”意为整合、集成、融为一体等，表达企业风险管理工作和企业战略与绩效是一个有机的、密不可分的整体；

仅仅一个词的变化，就把企业风险管理工作进行了重新定位，从作为一个看似独立的工作与战略和绩效相协同，到抛弃自我真正融入战略和绩效管理的工作中去，这种变化其实恰恰能描述我们一直以来倡导的风险管理工作融入企业管理和业务的最佳实践。

笔者期望可以用比较简单形象的表达方式让大家理解清楚其中的区别，如下图。

2、整体框架的展现方式

从征求意见稿到正式版，企业风险管理框架中的要素和原则从围绕企业战略和绩效，变成了贯穿融入企业战略、绩效和价值提升，也是对题目一词进行变更后，正文整体内容变化

的一个直接体现。

3、五大要素

五大要素的变化最明显的标志就是“ 去风险化 ”　　，五大要素中的“ 风险 ”一词均被去除，不再一味的强调风险视角下的企业治理及管理要素，而是直接从企业治理和管理的角度提出将风险管理内容嵌入，为风险管理工作的真正融入治理与管理打下了基础。

当一个组织可以接受卖什么不吆喝什么的时候，它的精神境界就提升了一个层次。

另外，把“ 执行中的风险 ”　（Risk in Execution ）直接改为了“ 绩效 ”，理解更为直接，而且避免了“ 执行中的风险 ”在全球不同区域的理解差异。　　4、基本原则

正式版将征求意见稿中五大要素的　　23 项基本原则改为了　20 项，因为在征求意见过程中有意见表示　　23 个原则太多了，并且部分内容不太实用。所以在治理和文化中有两条原则合并成了一条，更侧重核心价值的体现；同时，在战略和目标设定方面，原第　10 和 11 条原则合并成为一条，即设定商业目标；最后，在信息、交流和报告方面，利用相关信息和利用信息系统被合二为一，新原则更加关注信息和技术在支持企业风险管理上的应用。　　三、正式版的文件的结构　　正文的内容除了摘要部分，分为了第一册（　　Volume I）和第二册（VolumeII ），第一部分框架部分又分三块介绍了本框架的应

用环境、框架介绍和术语表；第二部分介绍了项目背景和框架修订的方法、公共评论的总结、风险管理工作的角色和责任、风险状况图示等。

四、主要观点

1、重新定义了风险及风险管理　　风险被重新定义为：

事项发生并影响战略和商业目标实现的可能性。　　对于风险的定义，非常高兴得看到，　由第一版只强调风险的　“ 负面性 ”，第二版已经将风险的范畴扩大到了对风险的“ 正面 ”和“ 负面 ”影响兼顾。

从个人角度而言，也有感到遗憾的地方，自从　　2009 年国际标准化组织发布　ISO31000　系列标准，　国际上对风险的定义就逐步趋同，风险—不确定性对目标的影响，况且这一标准是国际标准组织首次采纳中国提出的定义，　　COSO 此次并没有采用此定义，而是相对保守的采用了　　2000 年前后出现的典型的风险定义。　　企业风险管理被定义为：

组织在创造、保持和实现价值的过程中，结合战略制定和执行，赖以进行管理风险的文化、能力和实践。　　关于企业风险管理的定义变化最为彻底，直接抛弃了第一版的定义，将风险管理工作直接从　“ 一个流程或程序 ”　提升到“ 一种文化、能力和实践 ”，用以实现组织创造、保持和实现价值。另外，也从定义上撇清了风险管理和内部控制的模糊关系。　　2、一个真正的“ 管理框架 ”而不再是“ 控制框架 ”

虽然第一版框架就强调对利益相关方价值的创造，但是从内容上讲还是一个被放大了的“ 控制框架 ”，无法直接为价值创造服务，只能间接支持价值创造活动。新的框架从企业使命、愿景和核心价值出发，定位的宗旨为提升主体的价值和业绩，强调嵌入企业管理业务活动和核心价值链，从主要的要素和内容看也进行了翻天覆地的变化，从而使得一个崭新的“ 管理框架 ”诞生，这种视角是一种新型的企业管理视角，对企业管理界来说是一场理念的变革。如果说在原有“ 控制框架 ”下，会计师事务所可以在实施内部控制框架的基础上，协助企业加强风险管理工作，但新的“ 管理框架 ”更像是企业决策者或企业管理咨询顾问关心的范畴。近年来，基于风险导向的管理理念逐渐兴起，企业管理领域中常见的公司治理、企业文化、战略管理、卓越绩效、危机管理、高效沟通等都可以应用此套框架实现更好的标准化和科学化，因为基于风险的管理理念将成为主流并渗透到企业管理的各个方面。

3、更广泛的主体适用性　正式版发布日期之所以一推再推，COSO Hirth 主席向笔者解释了其中一个原因，虽然框架名为《企业风险管理》，但 COSO 希望这个框架可以适用于任何类型、任何规模的组织，包括盈利机构、非盈利机构、政府部门等。

所以 COSO 期望的主体适用性已经从企业面向了各类型的主

体，这一点也可以从正文部分的描述中看出，有些内容中故意回避了“ 企业 ”一词来显示了对不同主体本框架的包容性。理论上来讲，只要一个主体有明确的愿景、使命和核心价值观，设定了所要期望达到的目标，风险管理框架就具备了被实施的条件。

但是目前关于非盈利机构、政府部门等实施风险管理框架还是一个新的领域，我们也非常期待这些领域的最佳实践的出现。

笔者曾协助中国部分政府部门设计和实施部分风险的应对方案，借助此框架的颁布协助政府部门设计一套完善的风险管理体系也许是下一步可以探讨和尝试的领域。 4、关于风险管理的局限性 了解 COSO 1992 年、2004 年发布的内部控制框架和企业风险管理框架的人都应该清楚，两个框架均列示了企业内部控制和风险管理工作的局限性，而且这两个框架的局限性基本一致，这也在另外一个角度印证了 2004 年版的企业风险管理框架还是一个大内控的“ 控制框架 ” 。 新版本的框架中删除了对于风险管理局限性的章节，作为一套“ 管理体系 ”而非“ 控制体系 ” ，突破原来的局限性是不言自明的。 5、关于风险管理和内部控制的关系 在正式版新框架中，自然无法绕开关于风险管理和内部控制关系的解释，在第一册框架应用环境中，第一部分内容中就描述了风险管理和内部控制的关系： “ 内部控制主要聚焦在主体的运

营和对于相关法律法规的遵从性上。 ” “ 企业风险管理的相关概念并没有包含在内部控制中（例如，风险偏好、风险承受度、战略和目标设定等概念，这些都是内部控制体系实施的前提条件） ”。 为了避免重复，一些在内部控制中比较常见的概念部分，风险管理新框架并未重复叙述（例如，与财务报告目标相关的舞弊风险、与合规目标相关的控制活动、与运营目标相关的持续及独立评估） 。然而，一些在内部控制中概念在本框架中被进一步的研究和深化了（例如，企业风险管理中的治理和文化部分） 。 在 COSO 公布的《常见问题》解释上， COSO 表明两个体系并不是相互代替或取代，而是侧重点各不相同相互补充的作用，但同时也强调了内部控制作为一种经历时间考验的企业控制体系，是企业风险管理工作的一个基础和组成部分。 在历史上， COSO 在表述两个体系的关系时有时暧昧、有时清晰，这样算是现阶段给两个体系的关系做了个“ 了断 ” ，随着新框架在企业的实施，相信二者的关系和界限会越来越清晰。 6、关于是否强制实施 实施风险管理工作目的是为股东和利益相关方创造、保持和实现价值，这些并不能通过外部监管机构通过强制的方式来执行，所有需要监管机构强制要求的工作都是控制类而非价值创造类。所以各类主体的利益相关方需要明确实施风险管理工作并不是满足监管和合规要求，真正的目的是为了实现价值和达成业绩，支持主体使命、愿景和核心价值的实

现，这是为了满足更高层次的诉求。　　六、关于中文版出版

Hirth 主席向笔者介绍了和中国财政部在　　2013 年《内部控制框架》引进方面的合作，并表示前期与财政部已达成意向由中国财政部引进新版《企业风险管理框架》　　，并希望笔者可以在中文版引进的过程中与　　COSO 及中国财政部加强沟通，并给予必要的协助！笔者希望推动中文版尽早发布，与中国众多企业管理者、风险管理从业者和研究人员共飨！　　延伸阅读：深度解读《　COSO 新版企业风险管理框架（征求意见稿）》2016 年 6 月，美国反欺诈财务报告委员会（　　The Committee of Sponsoring Organizations ofthe Treadway Commission, COSO）发布了新版企业风险管理框架　“企业风险管理 -与战略和绩效协同”　（EnterpriseRisk Management-Aligning risk with strategy and performance　）征求意见稿，这是继 2004 年 COSO 正式公布企业风险管理框架（EnterpriseRisk Management Framework, ERM　）以来第一次对 ERM 框架进行修订和完善，　更确切的说是对　ERM 框架大刀阔斧的进行了重新构思和设计。　　新版 ERM 框架已经于 2016 年 9 月 30 日截止全球范围内收集反馈意见，并计划于 2017 年第一季度正式公布，　但实际上正式版迟迟推到了第三季度才公布，可见其内部经历了大量的讨论乃至争执，关于正式版框架解读稍候发布。　　一、新版 ERM 框架出台的背景

众所周知，在企业风险管理和内部控制理论研究领域，　　COSO

组织有着举足轻重的位置，从 1992 年出版企业内部控制整合框架（ InternalControl- Integrated Framework ）以来，作为在美上市公司内控体系建设的指导框架，不仅得到了美国证监会的认可，而且在全球范围内被众多国家相关企业和上市公司监管机构采用和推广， 如中国财政部 2008 年发布的《企业内部控制基本规范》即采用了 COSO 组织 1992 年发布的内部控制框架要素和内容。 2000 年以来，企业界在实施了十来年内部控制框架之后，发现即便建立了完善的内部控制体系，仍然会出现企业倒闭、破产、经营失败或预期不达标等风险损失案例， 所以 COSO 组织开始从更高的一个角度来思考企业的管理活动以及内部控制体系的局限性。内部控制体系确实对实现财务报告的可靠性和有效性提供了合理的保障（从实践经验看，内部控制体系的建立对经营和合规两个目标的支持力度并没有像财务目标那样得到很好的体现），但是企业需要从整合风险管理的角度为企业创造价值并合理保障公司战略目标的实现。 COSO 组织对 ERM 框架的初衷和定位是正确的，但在起草 ERM 框架时采用了在 COSO 内部控制框架的基础上进行升级和扩充的做法，这直接导致了两个理论框架虽然愿景和目标各不相同，但内容的重合度非常高，笔者回想过去这些年企业在实践这两个理论体系时出现的种种说法“ 内部控制就是风险管理 ” 、“ 风险管理就是内部控制 ” 、“ 风险管理是“ 大内控 ” ”等，在当时发

布起草 ERM 框架时就埋下了隐患。 图 1：内部控制框架和企业风险管理框架

2014 年， COSO 组织开始着手对 ERM 框架的升级换代，用其自身的阐述，原因在于过去十年间外部环境的复杂变化，利益相关方更加关心风险管理对企业价值的创造，尤其是在战略的制定和执行中风险管理价值的体现，以及增强风险管理和企业绩效之间的协同关系。 想必 COSO 组织也非常清楚过去十年间关于内部控制和风险管理之间关系的争论和对企业实际开展工作造成的影响，只好痛定思痛，着眼于未来了，这一点从新版的 ERM 框架中可以看出来。 COSO 组织对新版 ERM 框架进行了颠覆性的变化， 起码从表面上来看，没有一点从前的影子了，看来是有意和内控及 2004 版风险管理划清界限，结束这十年来的两者的纠葛和纷争。 图 2：COSO 新版企业风险管理框架

很多从事和熟悉风险管理工作的人，对 ERM 新框架一开始的感觉都是陌生和不适应，笔者最开始将征求意见稿发送给国内权威专家参考时，部分专家也提出“ 这是对历史的一种背叛 ”、“ 新框架太荒唐 ” 等批判性的反馈意见，笔者了解这是人们对于熟悉环境的突然变化抵触心理，待各位专家平复心情仔细研读后，还是非常肯定新框架做出的勇敢变化及对风险管理工作的准确定位。 二、新版 ERM 框架和旧框架的区别与联系 1、新框架采用了国际文件惯用的要素加原则的

结构（ Components and Principals）新版框架使用了构成元素原则的结构，包括 5 个构成元素，细分为 23 条原则， 2013 年 COSO 组织更新了企业内部控制框架的部分内容， 在文章的整体结构上就是采用的这种结构，新的结构加强了新框架的可读性、可用性和一致性。 2、修订了风险的定义旧版框架中对风险的定义为：风险是一个事项将会发生并给目标实现带来负面影响的可能性。新版框架对风险的定义为：事项发生并影响战略和商业目标实现的可能性。

可以看到，旧定义只强调了负面影响，而新定义的主要改动是兼顾了正面和负面的影响，这和国际风险管理标准 ISO 31000 及中国风险管理标准 GB-T24353 是一致的， 这种认识中国早在 2006 年国务院国资委发布的《中央企业全面风险管理指引》文件中就有体现。 3、简化和重新定义了 ERM 同时我们还可以比较 ERM 的定义。旧版框架对 ERM 的定义为：ERM 是一个过程， 它由一个主体的董事会、 管理层和其他人员实施，应用于战略制定并贯穿于企业之中，旨在识别可能会影响主体的潜在事项，管理风险以使其在该主体的风险容量之内。并为主体目标的实现提供合理保证。而新版框架对 ERM 的定义为：组织在创造、保持和实现价值的过程中，结合战略制定和执行，赖以进行管理风险的文化、能力和实践。 可以看到，新版框架简化了对 ERM 的定义以方便阅读和记忆。新定义方便所有读者的理解，而不只是风险管

理从业者，新定义包括文化和能力而不只是过程，更加强调风险与价值的相结合，突出价值创造而不只是防止损失，这样也避免了和内部控制定义的界限不清。　　4、强调风险与价值的关系新版框架中，　ERM 被视为战略制定的重要组成和识别机遇、创造和保留价值的必要部分。新版框架中　　ERM 不再是主体的一个额外的或是单独的活动，而是融入主体的战略和运营当中的有机部分。　　5、真正定位了风险管理与战略的协同作用新版框架注意到了自旧版框架发布以来，组织在实践 ERM 过程中遇到的一些问题，包括对风险管理工作的定位，风险管理工作的范围和目标等，新版框架定义了风险管理工作的高度，包括：战略和业务目标与使命、愿景和价值观不匹配的可能性；选定的战略所隐含的意义；执行战略过程中的风险。　　6、重新定义了风险偏好和风险容量旧版框架中，风险容量（　Risk Tolerance）只是颗粒化的、更细节的风险偏好（ Risk Appetite ）。新版本中，风险偏好保留了原来的定义，即主体在追求战略和业务目标的过程中愿意承受的风险量，而将风险容量重新确定为可接受的绩效变动区间（Accepted Variation in Performance ），新的定义更加明确和可度量，有助于组织在给定绩效目标下计算可以承受的风险边界。　三、新版　ERM 框架主要内容解读新版　　ERM 框架的五要素和　23 个原则

图 3：新版框架五要素和　　23 条原则

风险治理和文化风险治理和文化组成了 ERM 所有其他部分的基础。风险治理定下主体的基本基调，加强 ERM 的重要性并确立 ERM 的监管责任的分配； 文化则是主体的价值观、行为准则和对风险的理解。

1. 实现董事会对风险的监督： 董事会对主体的风险监督负有首要责任。首先要确认董事会和管理层对风险治理的责任分配。一般来说，董事会成员具有丰富的行业经验和技能，且独立于管理层。这使得他们能提供风险治理的整体战略和独立视角，并将风险管理的日常责任交给管理层或者特定的委员会，如风险管理委员会。 2. 建立治理和运作模式：在明确的责任分配下，组织应该建立完整的运营模式和汇报体系。影响组织建立何种运营模式的因素有很多，例如企业的战略目标，规模、行业、区域分布、财务税务等方面的法律法规等等。管理层结合企业的使命、愿景和核心价值来计划、组织并执行企业战略。一般来说，管理层通过授权给特定委员会的形式来掌握、管理与战略相关的风险。对于大型组织来说，这样的委员会可能不止一个，这就需要不同的委员会之间明确权责的分配并共享对风险的理解。明确权责十分重要，这能激发人们在授权范围内的能动性。而随着组织的发展，运营模式和授权 -报告体系也需要做出相应调整。 3. 定义期望的组织行为：董事会和管理层通过定义其期望的行为来将组织核心价值和对风险的态度具体化。建立一个所有员

工都接受的企业文化对于企业抓住机遇、规避风险来说至关重要。表现在下图所示的风险光谱上，风险激进的组织更倾向于接受追求战略和业务目标时所需承担的不同类型和数量的风险。图　4：风险光谱　4. 展现对诚实和道德的承诺：组织制定基调，建立员工行为准则并对偏离准则的行为做出回应。即使组织明确展示了对诚实和道德的承诺，还是难免发生违背企业的价值观的行为。这种行为可能是好人犯了错误，好人一时意志软弱，或者坏人蓄意造成破坏。因此需要对行为进行详尽的评估并制定细节的应对措施。关键是将个体的行为和组织文化结合起来，这需要管理层在日常工作中不断解读、强调和践行企业文化。　　5.加强问责：组织确保各个层级的个体在风险管理方面的职责明确，并确保其自身在提供准则和指导方面的职责明确。管理层向董事会负责，员工向管理层负责。个体是否负责受到奖励机制的很大影响，董事会和管理层应该在组织的各个层级建立奖励机制，这种建立可能是薪酬方面的，也可以是非物质的，比如授予更重要的工作。　6. 吸引、发展并留住优秀的个体：致力于根据战略和业务目标构筑人力资本。组织需要建立在各个层级评价工作能力的机制。董事会评价管理层的能力，管理层评价各个业务单元或者职能部门的能力。管理层通过在不同层面建立人力资源管理体系来吸引、培训、指导人才，评价和留住人才。　风险、战略和目标设定　　ERM 通过制定战略和业务目

标的过程与主体的战略计划融合在一起。通过对商业环境的理解，组织可以得到对内在和外在因素的看法以及它们对风险的影响。组织在战略制定中确定其风险偏好，而业务目标使得战略得以实践并形成主体日常的运营。 7. 考虑风险和业务环境：组织考虑业务环境对风险图谱的潜在影响。组织要理解业务环境，考虑内部和外部的环境和不同的利益相关者。外部环境包括政治、经济、社会、科技、法律和环境等方面，内部环境包括资本、人力、流程和技术等方面。 8. 定义风险偏好：组织在创造、保存和实现价值的过程中定义风险偏好。负责确定风险偏好的董事会和管理层必须完全了解不同风险偏好所代表的取舍和利害关系。对于一些组织来说，“ 高风险偏好 ”或“ 低风险偏好 ”已经足够区分，对已另外一些组织来说，风险偏好必须是可以量化的。风险偏好可以有“ 目标 ”、“ 范围 ”、“ 上限 ”、“ 下限 ”等不同的表达和设定方式。 9. 评估可供选择的战略： 组织评估可替代的战略和对风险状况的影响。组织必须明确战略的重要意义和不同战略选择所隐含的意义，将战略和风险偏好结合在一起考虑并依据不同情况和阶段调整战略。 10. 建立业务目标的同时考虑风险：组织建立不同层次的业务目标以制定和支持战略的同时考虑风险。业务目标可以使财务表现、客户满意度、卓越运营、合规、效率提升或者领先行业的创新等等。组织必须理解不同的业务目标所隐含的意义并确定不同的绩效

度量方式和目标。 11. 定义可接受的绩效浮动区间： 可接受的绩效浮动也可以理解为风险容忍度。衡量绩效的完成度可以是定量的也可以是定性的。前者如资本回报率等，后者如品牌知名度、媒体评价等。 执行中的风险组织识别并评估可能影响其实现战略和业务目标的风险，结合企业的风险偏好，对风险按照其严重程度排分优先次序，组织选择风险应对的方法并对绩效进行监控以做出调整。这样，企业对追求战略和业务目标时所面临的风险量建立起一个组合的观念。

12. 识别执行中的风险： 组织识别执行过程中影响业务目标实现的风险。风险识别的方法包括专题研讨会、访谈、流程分析、关键风险指标和数据追踪等。风险和机遇并存，识别风险的过程也是识别机遇的过程。 13. 评估风险的严重程度：风险评估的重要工具是风险热力图，热力图从风险发生的可能性和影响程度两方面对风险进行评级。风险评价要从固有风险、目标剩余风险和实际剩余风险三个层级进行。图5：风险热力图 14. 区分风险的优先次序：组织结合风险偏好，选定对风险排分优先等级的标准，然后对所有识别的风险进行排分。 15. 识别和选择风险响应： 风险响应有不同的方式，包括承受风险、回避风险、追逐风险、降低风险、分担风险等。管理层根据业务环境、性价比、法律法规、风险优先级、风险严重程度和风险偏好来选择和实施风险响应措施。一旦选择风险响应措施，就需要有效的控制活动来确保

响应措施的实施。这些控制活动在《内部控制—整合框架》中已经介绍。 16. 评估执行中的风险： 组织需要对绩效进行监测，如果绩效的浮动区间超出了可以接受的范围，则可能需要：重新考虑业务目标或战略；调整目标绩效，重新进行风险评估；重新进行风险优先级的排序；重新制定风险应对措施；重新确立风险偏好。 17. 建立风险的组合观：管理层需要从组织整体角度考虑风险，将组织风险作为一个整体去和实现绩效目标所需要承受的风险进行对比，而不是将其视为一个个单独的、分散的风险。 风险信息、沟通和报告沟通是在主体中不断迭代地取得并分享信息的过程。管理层利用从内部和外部取得的有效信息来支持企业风险管理工作，组织利用信息系统来捕捉、处理和管理数据和信息。通过利用应用于所有组成部分的信息，组织就风险、文化和绩效做出报告。 18. 使用相关信息： 组织利用支持企业风险管理的信息，首先考虑有哪些可用的信息来源，然后衡量取得这些信息的成本，最终确定需要哪些消息来源。外部的消息来源包括：公开指数、政府发布的地缘政治报告和研究、市场调查服务、客户满意度问卷、社交媒体和博客、运用报告及第三方发布的报告、产业报告和同业公司的财务报告。内部的消息来源包括：董事会和管理层会议、财务报表和投资回报分析、道德和行为相关的培训、交易和尽职调查的成果、工时报告、库存报告及检举热线的报告。这些信息需要满足：

容易取得、准确、真实、恰当、可靠、及时。　　19.　利用信息系统：信息系统可以是正式的或者是非正式的。组织应该应用分类学来管理　ERM 相关的信息，基于组织的规模大小、复杂程度将风险进行细分。管理层要依据内外部环境及时地维护信息系统并做出调整。　　20.　沟通风险信息：　沟通的对象既包括内部的员工，也包括董事会、股东及其他外部的利益相关者。沟通方法可以是电子信息、外部　　/第三方材料、非正式/口头、公共活动、培训和研讨会、内部文件。　　21.　对风险、文化和绩效进行报告：组织在各个层级对风险、文化和绩效做出报告。首先组织要确定这些报告的使用者和他们的职责。报告的形式和种类很多，包括：风险的整体判断、风险图谱、根本原因分析、敏感度分析、对新兴及发生变化的风险的分析、　KPI（关键业绩指标）　、趋势分析、　对意外事故、违规和损失的披露以及对　　ERM 计划和倡议的追踪。管理层需要确定报告的频率并对其质量负责。　　监控 ERM 效果通过监控 ERM 的效果，组织可以判断　ERM 的各组成部分的长期运作是否良好并获知有哪些实质性的变化。　　22.　对重大变化进行监控：组织识别和评估可能对战略和业务目标的达成造成实质性影响的内部和外部变化。造成这些实质性影响的变化可能来自内部的原因，例如快速成长、新技术或者管理层及其他人事变动；可能来自外部环境，例如法规和经济环境的变化；还可能来自组织文化方面，例如并购和重组带来的

文化冲击。 23. 对 ERM 进行监控：组织应监控 ERM 的效果并随时准备对其进行效率上和实用性上的改善。做出这些完善的机遇可能存在于以下任何领域：新技术、历史短板、组织方式转变、风险偏好、风险分类、沟通、同业对比、变化的速率。组织同样要明确未来理想中的 ERM 状态，如此才能做出持续改进。

四、重点内容—风险绩效曲线介绍

新版框架中数十次出现了一个新提出的曲线—风险绩效曲线，提出了将风险与绩效相结合并给出了图形化的解释。单个的风险和绩效并不总是一一相关的，但是整体的风险与绩效是相关的。为了提供相关指导，新版框架对风险和绩效的关系提供了图形化的表达和示例。为了完成对风险轮廓的描述，组织需要理解下面内容：战略和业务目标、绩效目标和可接受的浮动范围、风险承受能力和风险偏好、风险对达成战略和业务目标的影响程度。 如下图中所示，横坐标代表绩效，纵坐标代表组织所承受的风险。图中的蓝色曲线代表风险 -绩效曲线，即风险总体上随着绩效的升高而升高。红色水平线条表示组织确定的风险容限，而紫色垂直线条表示组织的绩效目标。可以看到， c 点表示目标绩效下组织所承受的风险， c 点到 a 点的距离则代表实际风险与风险容限的差距，距离越短，表示企业的风险偏好越激进。而 b 点代表达到 100% 风险容限时，组织所能达成的最大绩效，

但这也意味着组织承担的风险总量已经处于饱和状态。　　图 6：风险绩效曲线可以看出，风险绩效曲线是新版框架的创新，它成功地将风险、风险偏好、绩效、目标绩效、绩效偏差等概念的关系用图形的方式展现出来，简单形象，方便理解。

此示意图是风险 -绩效曲线的最基本的一张图，　在新版框架的附录中还有更详尽的解释。但是，我们需要注意，风险绩效曲线试图将风险和绩效进行量化对比，在实际操作中有一定的难度。目标绩效虽然容易设置　（通过收入、 收益率、 利润、市场占有率等确定），但是风险如何加总量化是一个复杂的问题。除此之外，示意图中风险与绩效的关系是一条平滑的曲线，但是实际情况是，风险和绩效的关系不会如此单纯，所以如果没有数据积累和大量分析，精确绘制这条实际的蓝色曲线是非常困难的。笔者曾经带领团队试图从一个项目风险评估中绘制风险绩效曲线，　但碰到的障碍很多，　希望 COSO 在正式发布 ERM 框架时，可以给出更具操作性的指导。　　五、几点探讨及观点

1、更好的区分风险管理和内部控制的边界本文背景介绍中已经对风险管理和内部控制的情况作了简单介绍，在企业风险管理体系和内部控制体系建设方面，中国企业积累的经验在全球范围内独树一帜，源于过去十几年中国企业走过的坎坷之路。 2006 年，国务院国资委发布《中央企业全面风险管理指引》，开启了中国企业尤其是中央和地方国有企业建设

全面风险管理体系的浪潮，在国务院国资委的推动下，绝大多数中央企业几年内建立起了全面风险管理体系。2008 年，财政部发布《企业内部控制基本规范》，要求大中型企业尤其是上市公司建立健全企业内部控制体系，2013 年，这些要求又在中央企业推广和落实。对于部分企业来说，无论是企业风险管理还是内部控制都属于新生事物，这两个体系从两个国家部委的角度一前一后进行要求和推广，很多企业感到迷惑，不知道如何处理这两个体系以及这两个体系和企业管理之间的关系，造成了一定的管理混乱和资源重复投入，这些问题从最开始理论框架的设计上确实没有划分清晰的界限。对于风险管理和内部控制的关系，2013 年 COSO 发布的内部控制框架更新版文件附录中提出，企业风险管理是企业治理中的组成部分，企业内部控制是企业风险管理中的组成部分，从中国理论和实践经验看，大部分专家还是比较认可这种关系界定。图 7：风险管理和内部控制关系图此次 ERM 新框架中，对于风险管理和内部控制的关系也做了进一步的阐述，新框架中有意规避了旧框架中对于控制活动的描述，把控制活动的内容留给了内部控制体系，而突出了风险的治理和文化的内容，以及强调和战略及绩效的关系，算是给两个体系“分家”做了个“了断”，关于两者的关系比较及经验总结限于篇幅，此处不再展开。期待 COSO 公布正式版之后，实践界可以尽快研究如何应用，尽快形成企业风险管理

体系建设的行业最佳实践。

2、推动风险管理更好的和企业管理的融合真正的风险管理工作是要支持管理决策的，而不仅仅是建立内部控制制度和流程，虽然 COSO 新版的 ERM 框架已经开始回到“正轨”，国际上某些一流的锋线管理咨询公司多年前为客户提供的风险管理方法论就是为企业的战略和管理决策提供支持，将风险管理工作融入管理决策的各个流程环节中，我们一直认为这是风险管理的真正价值所在。

3、关于新框架正式版和中文版发布笔者联系了 COSO 委员会的主席 RobertHirth 先生，表达了翻译 ERM 新框架的中文版的愿望， Hirth 先生表示中国财政部前期已经在接触， 如果最后没有成行，会和我们联系中文版翻译出版事宜，预计中文版会比英文版稍晚发布。 上述观点是笔者基于对新框架征求意见版并结合工作经验所形成的，供大家参考，如有纰漏和不完善之处，请大家批评指正！

本文来源于风险管理世界（ ID:ermworld ）微信公众号，作者：孙友文