谁对风险负责

毕颖
全球考试开发部总监

The Institute of Internal Auditors | Global

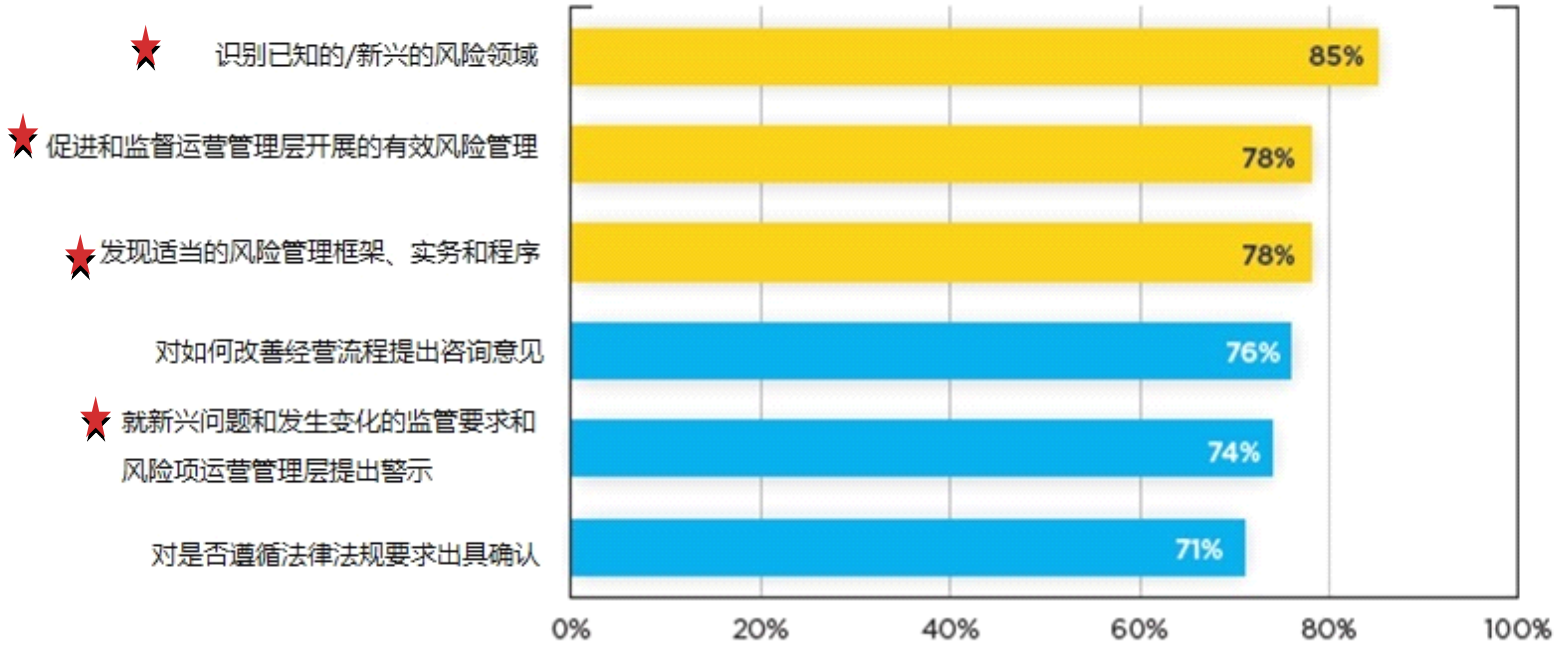
内容简介

1. 风险管理的全球性趋势
2. 风险管理框架
   - COSO ERM (建议稿)
   - ISO 31000
3. 内部审计在风险管理中的位置
4. 风险确认图谱
5. 应当采取的措施

1. 风险管理的全球性趋势

风险管理的全球性趋势

利益相关者认为内部审计在确认审计业务之外应当承担的职责：



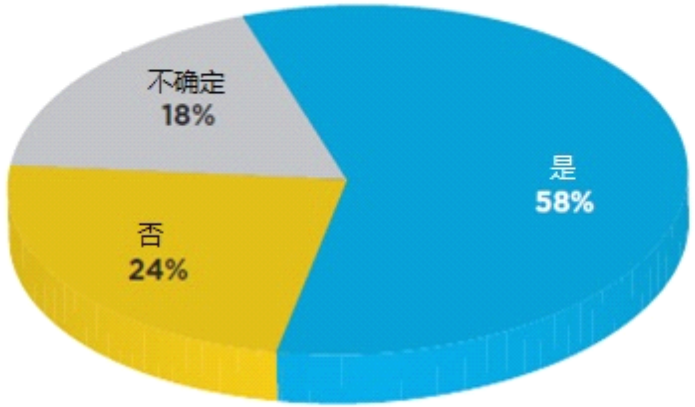
注：数据来源于问题10和问题13：除了确认之外，以下哪些领域也应当是内部审计的工作范围？（请选择所有适用的项目）仅限北美地区利益相关者作答。*n*=433.

数据来源：IIA知识共同体研究 (CBOK 2015)

风险管理的全球性趋势

- 关注战略风险，同时也关注运营、财务与合规风险
- 识别已知的/新兴的风险领域
- 促进/监督风险管理
- 向董事会和执行管理层通报关键风险

内部审计在面对战略风险时扮演的角色



注：数据来源Q16：你是否认为内部审计在评估和评价组织战略风险方面应当发挥更积极的作用？（例如：全球扩张计划、新产品、新分销渠道等）仅限北美地区利益相关者作答。*n*=468。

2. 风险管理框架

风险的定义

- ***风险 – 某个事件发生并对实现目标造成影响的可能性。风险主要从影响和发生概率两个维度进行衡量。***

IIA

- ***风险 – 某个事件发生并对实现目标造成负面影响的可能性。***

COSO – ERM 2004

- ***风险 – 不确定性对目标造成的影响。***

ISO 31000

ISO 31000风险管理标准

管理风险的
11项原则

强制要求
和义务

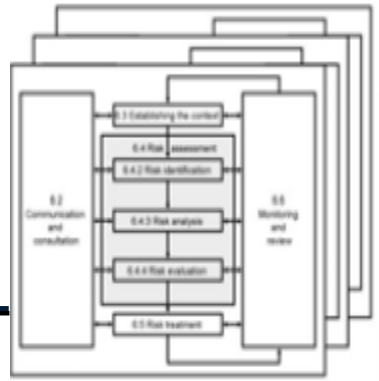
设计风险
管理框架

持续完
善框架

开展风
险管理

监控和修
订框架

管理风险的框架



管理风险的程序

高层的基调

整个企业层面的、综合性的方法

ISO 31000风险管理标准

管理风险的原则

1.风险管理创造和保护价值。

2.风险管理是组织进程中不可分割的组成部分。

3.风险管理是决策的一部分。

4.风险管理明确地将不确定性表达出来。

5.风险管理应系统化、结构化、及时化。

6.风险管理依赖于信息的有效程度。

7.风险管理应适应组织。

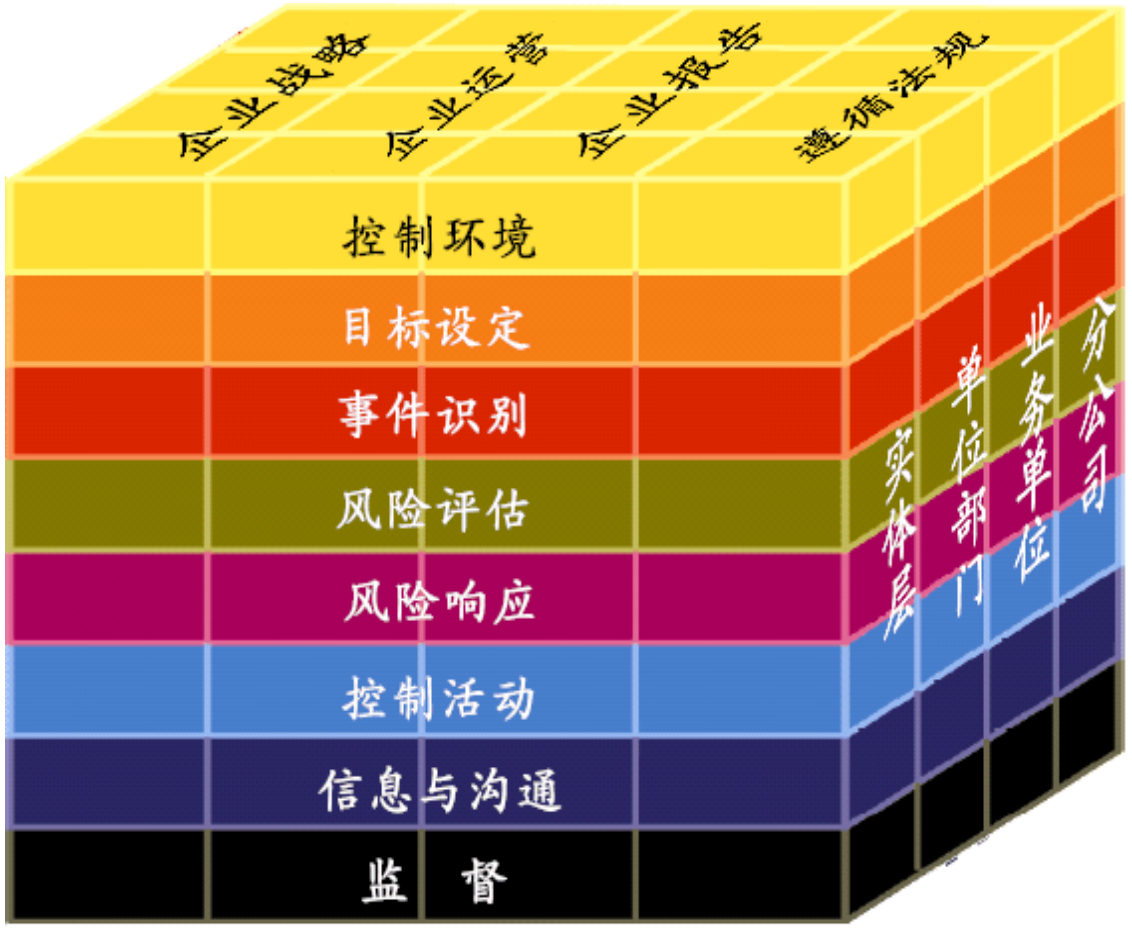
8.风险管理应考虑人力和文化因素。

9.风险管理应该是透明的、包容的。

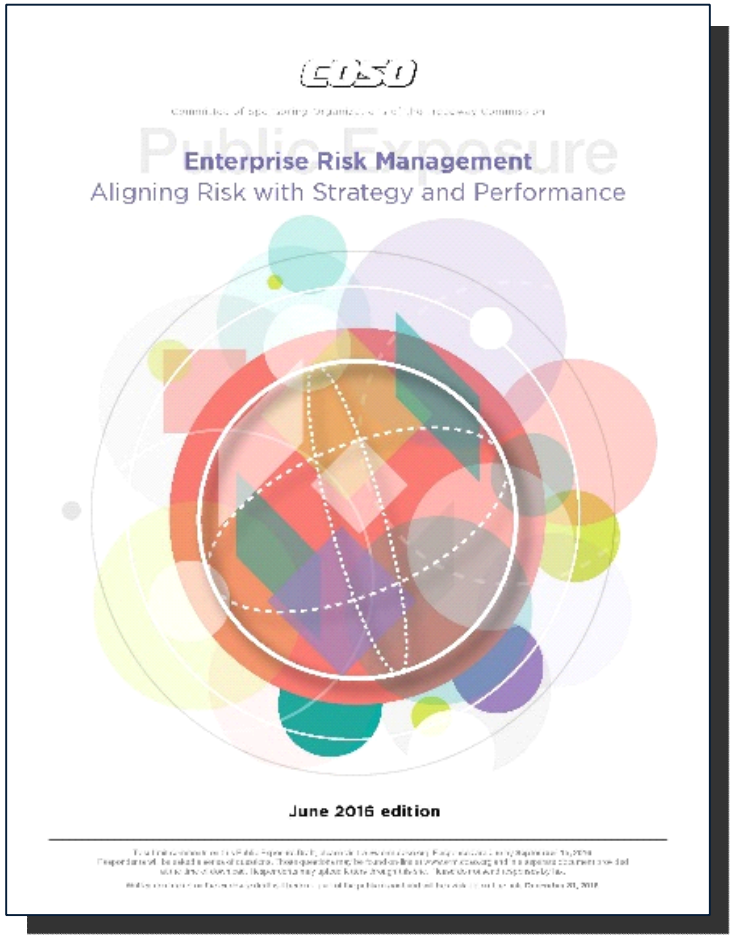
10.风险管理应该是动态的、反复的以及适应变化的。

11.风险管理促进组织不断强化和提升。

2004年的COSO – ERM框架



新的COSO – ERM框架 (征求意见稿)

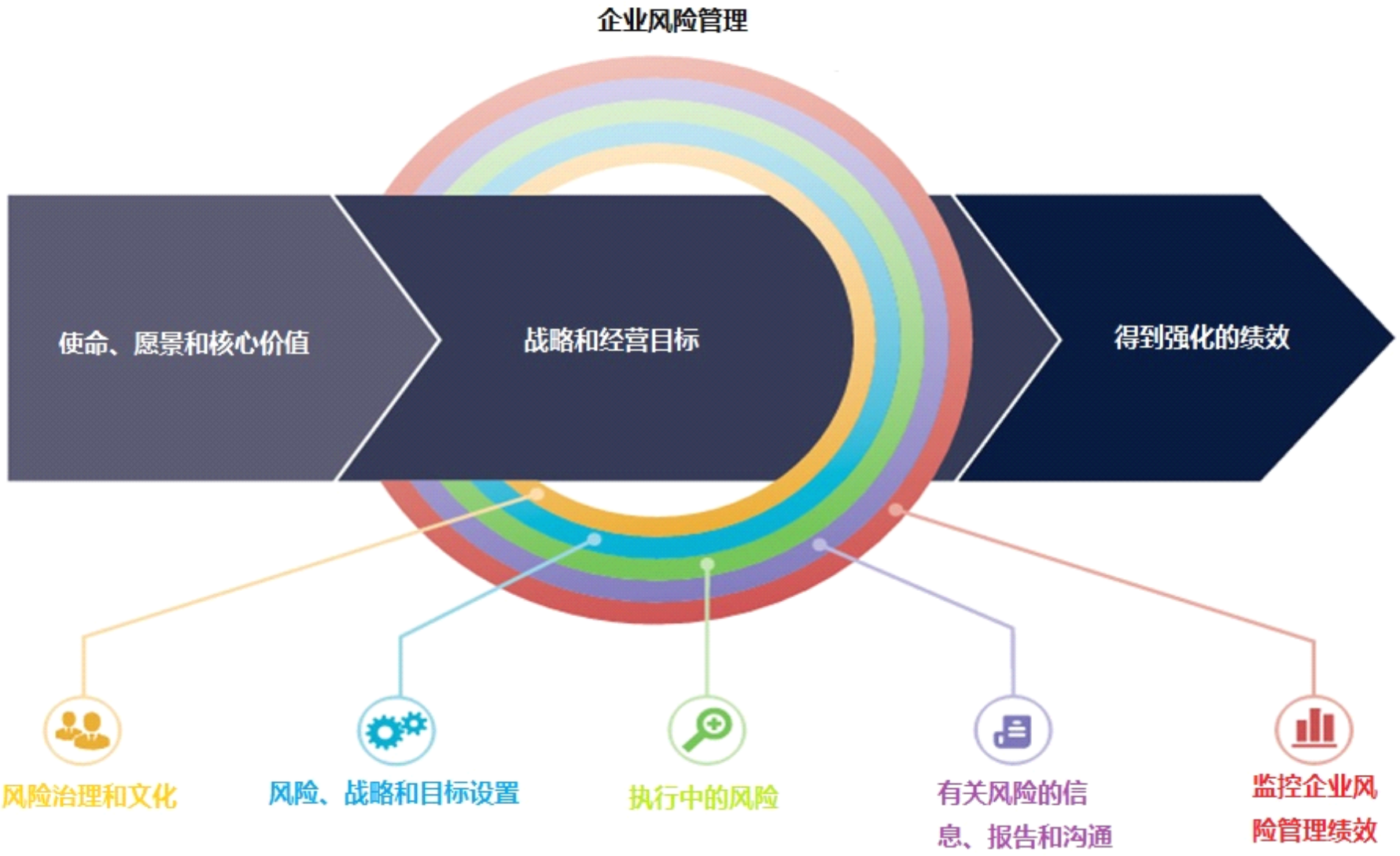


ERM –

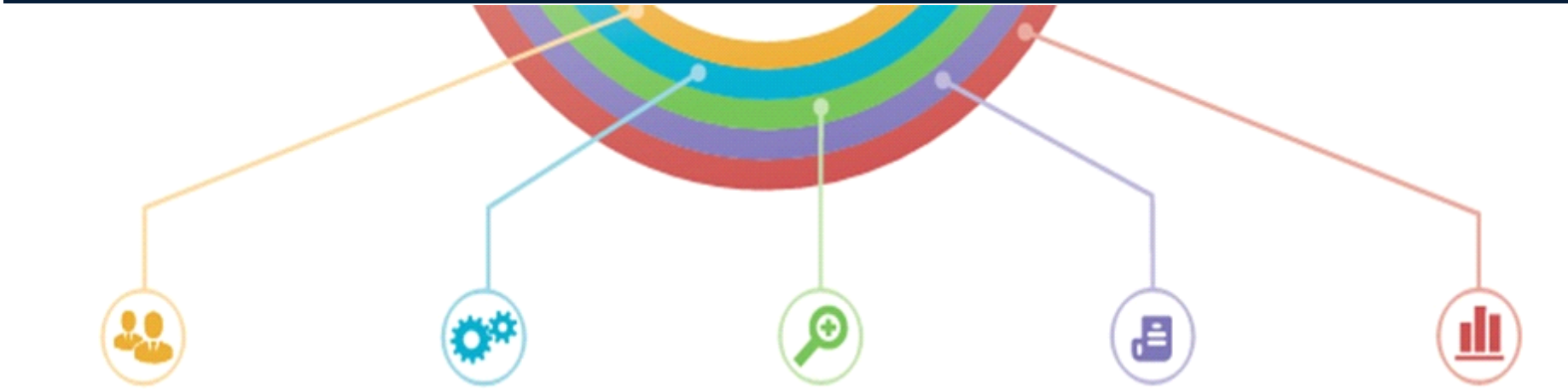
将风险与战略和绩效联系起来

新的COSO – ERM 框架(征求意见稿)

包含战略、目标和绩效的企业风险管理



新的COSO – ERM框架 (征求意见稿)
更新要素，接纳原则



风险治理和文化

1. 执行董事会对风险的监控
2. 建立治理和运营模型
3. 定义组织希望看到的行为
4. 展现追求诚信和职业道德的决心
5. 强化问责
6. 吸引、培养、留住人才

风险、战略和目标设置

7. 考虑风险和经营环境
8. 定义风险偏好
9. 评估替代战略
10. 在确立经营目标的同时考虑风险
11. 定义执行中可接受的偏差

执行中的风险

12. 发现执行中的风险
13. 评估风险的严重程度
14. 对风险进行排序
15. 识别和选择应对风险的方法
16. 评估执行中的风险
17. 建立组合评估的机制

有关风险的信息、报告和沟通

18. 使用具有相关性的信息
19. 利用信息系统
20. 就有关风险的信息进行沟通
21. 为风险、文化和绩效出具报告

监控企业风险管理绩效

22. 监控重大变化
23. 监控企业风险管理

新的COSO – ERM框架 (征求意见稿)

2004

- **风险** – 某个事件发生并对实现目标造成负面影响的可能性。
- **ERM** - 企业风险管理是一个过程，受企业董事会、管理层和其他员工的影响，在战略和整个公司得以应用，旨在发现可能对在组织造成影响的事件，依照风险偏好对风险进行管理，为实现组织目标提供合理确认。

2016征求意见稿

- **风险** – 某个事件发生并对战略实施和实现经营目标造成影响的可能性。
- **ERM –** 是指与战略和知性整合在一起的文化、能力和实践，组织依赖这些要素对创造、保护和实现价值过程中遇到的风险进行管理。

新的COSO – ERM框架 (征求意见稿)

主要变化：

- 强调了价值
- 与决策联系在一次
- 关注整合
- 检查了文化扮演的角色
- 更加深入地对战略进行了探讨
- 强化了与绩效的联系

3. 内部审计在风险管理中的位置

内部审计在风险管理中的位置

内部审计在风险管理中的位置

第一道防线

- 运营/业务条线的管理者对风险负责和进行管理。
  他们的职责包括：
  –识别与他们的目标和战略有关的风险
  –决定是否需要以及如何应对这些风险
  –设计适当的内部控制来对风险进行管理
  –执行内部控制
  –保持日常工作中内部控制的有效性

内部审计在风险管理中的位置

第二道防线

- 风险管理和合规职能

  ERM专家、合规人员、内部控制专家、质量控制、环境保护专员、舞弊调查员

  职责：

  –推动组织在风险管理方面的胜任能力不断提升

  –建立通用的风险管理术语和框架

  –就新的监管要求和新兴问题对运营管理人员提出警示

  –监控运营管理人员的风险管理程序

  –统合风险管理的结果并向CEO和董事会报告

  –在有需要的情况下提出建议措施

内部审计在风险管理中的位置

第三道防线

- **内部审计人员**

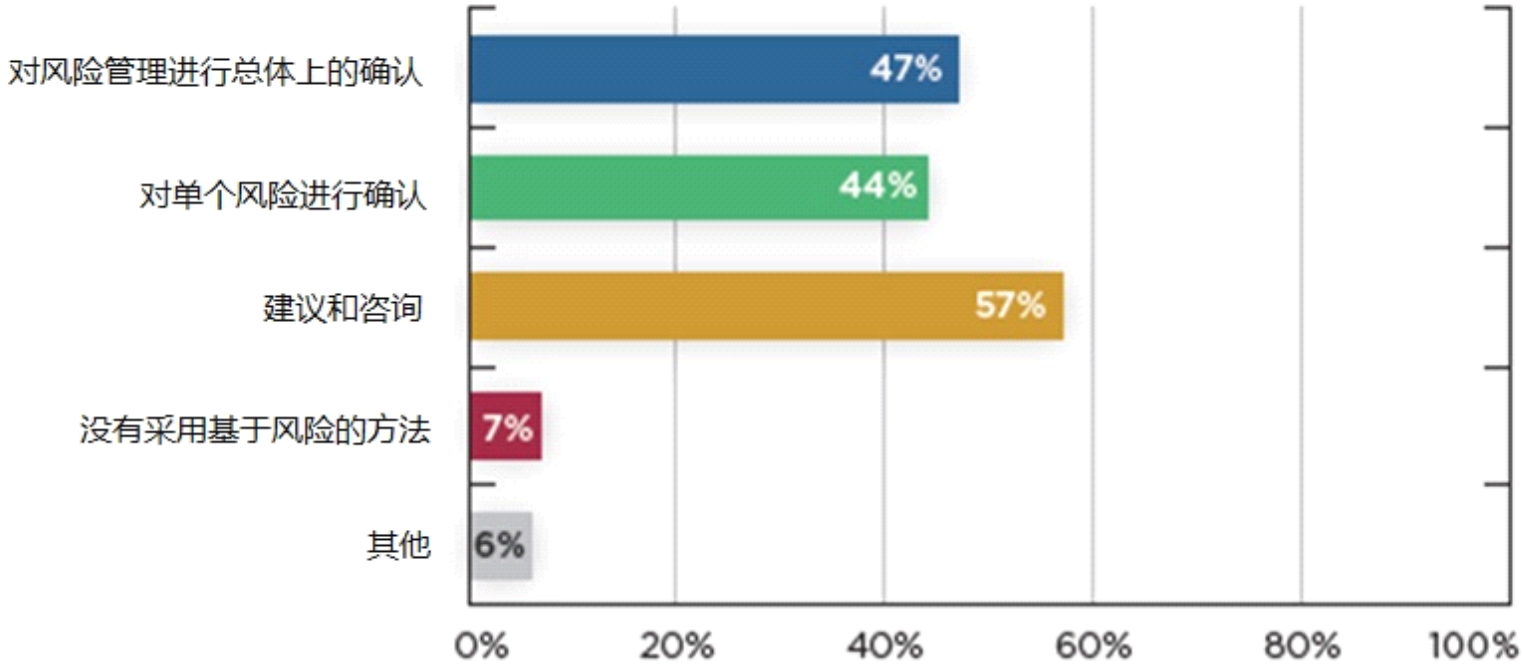
  职责：

  – 就风险管理的有效性为董事会和高级管理层提供独立确认

  – 为改善组织的风险管理和控制程序提出建议

内部审计在风险管理中的位置

内部审计在风险管理中的职责

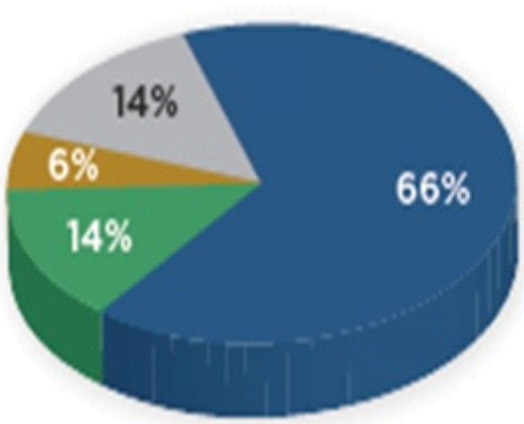


注：数据来源于Q60：您所在的组织中内部审计担负哪些与风险有关的职责？（请选择所有适用的项目。）

n=11,935

内部审计在风险管理中的位置

内部审计和*ERM*之间的关系



66% 内部审计和ERM是相互独立的，但两者开展协作，分享信息

14% 内部审计和ERM是相互独立的，同时两者也不会互动

6% 目前由内部审计负责ERM，但这部分职责即将被移交

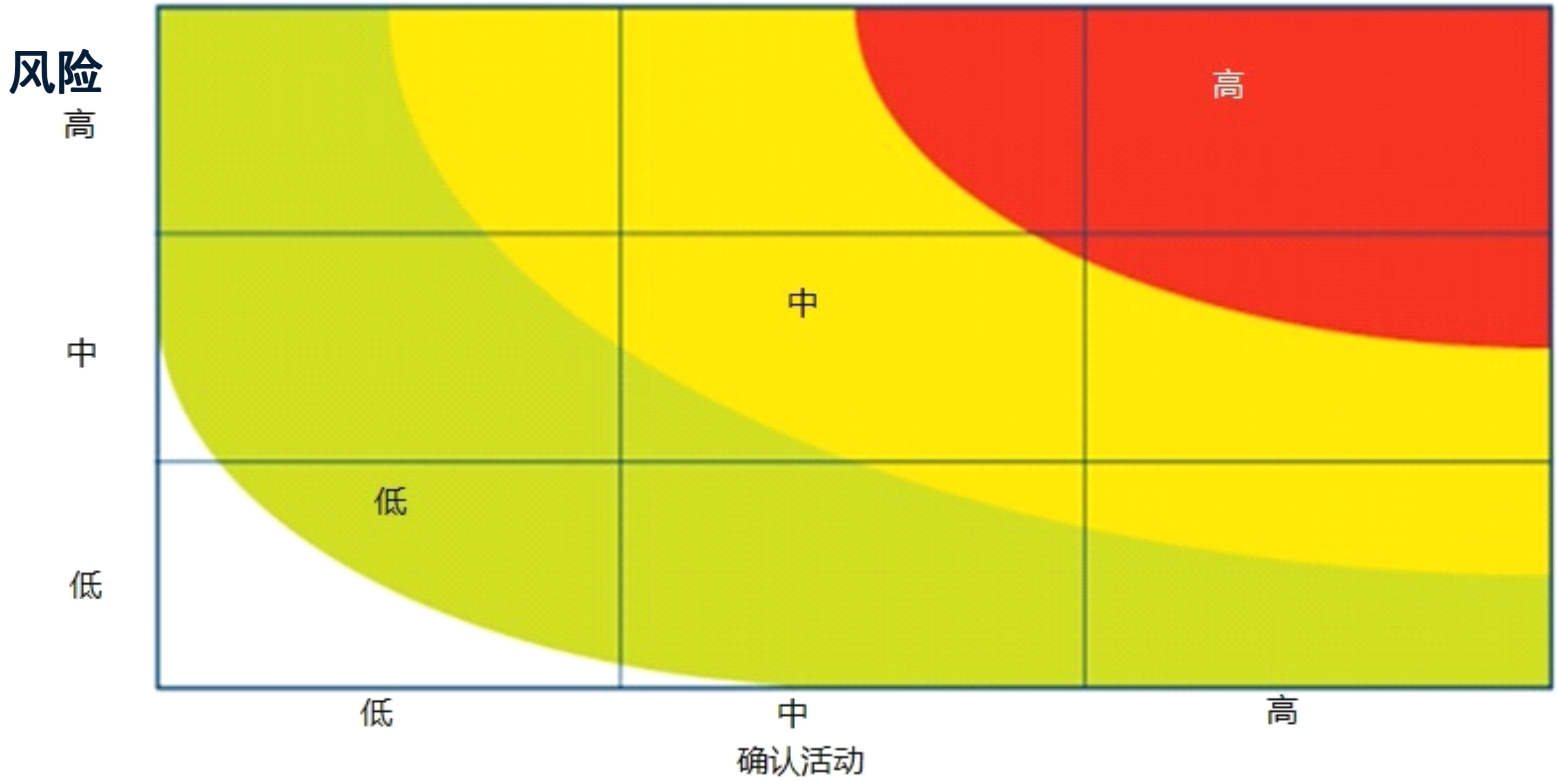
注：数据来源于Q59：您所在的组织中内部审计和企业风险管理（ERM）的关系是怎样的？

n=9,437

4. 风险确认图谱

风险和确认

风险越高，所需的确认层级也就越高。



确认的层级

什么是确认图谱

- 确认图谱是组织对关键风险的确认情况的完整反映。
- IIA发布的实务公告2050-2：确认图谱 – 为确认情况绘制图谱的实践：
  - 包括了根据组织的关键风险描绘确认工作的覆盖范围。
  - 使得组织能够发现和处理风险管理程序中存在的差距，让利益相关者了解到风险已经得到了管理。
  - 反映了整个组织的情况，以便理解各个职能在风险和确认方面的职责以及问责的对象。

确认图谱 – 范例A

	关键风险	固有风险	角色和职责			剩余风险
			第一道防线	第二道防线	第三道防线	
战略	风险1					
	风险2					
	风险3					
运营	风险4					
	风险5					
	风险6					
财务	风险7					
	风险8					
	风险9					
合规	风险10					
	风险11					

确认图谱的好处

- 组织可以全面地监控关键风险。
- 帮助董事会理解和评估组织对于关键风险的确认程序。
- 确保风险和确认程序全面完整，既不存在重复，也没有缺漏。
- 发现审计覆盖有待加强的领域。

5. 应当采取的措施

应当采取的措施

- 你在风险管理方面所做的所有工作，都应当与组织的目标、战略、绩效和文化联系起来。
- 与管理层和其他提供确认服务的内部职能加强协作，确保能够明确在三道防线中的分工。
- 探索将内部审计的确认服务与其他内部职能的确认整合到一起的方式，从而能够出具具有综合性、整体性的确认（更有效果，也更有效率）。
- 继续提升审计计划中关注风险管理的业务比例。

谢谢！

国际内部审计师协会

Lily Bi, CIA, QIAL, CRMA, CISA
Managing Director, Global Exam Development

Lily.Bi@theiia.org